

Data Breach Prevention and the Canadian Consumer

RESEARCH REPORT

Report produced by Option consommateurs
and presented to Innovation, Science and Economic Development Canada's
Office of Consumer Affairs

2021

Option consommateurs received funding under Innovation, Science and Economic Development Canada's Contributions Program for Non-Profit Consumer and Voluntary Organizations. The opinions expressed in this report are not necessarily those of Innovation, Science and Economic Development Canada or the Government of Canada.

Reproduction of this report, in whole or in part, is permitted provided that the source is acknowledged. Reproduction or any reference to its content for advertising or commercial purposes, however, is strictly prohibited.

Author: Alexandre Plourde

Legal Deposit
National Library of Québec
National Library of Canada
ISBN 978-2-89716-068-5

Option consommateurs
50 rue Sainte-Catherine Ouest, bureau 440
Montréal, Québec)
H2X 3V4
Telephone: 514 598-7288
Fax: 514 598-8511

Email: info@option-consommateurs.org
Website: www.option-consommateurs.org

Contents

Contents	iii
Option consommateurs	v
Acknowledgments	vi
Summary	vii
Introduction	8
Research objectives and methodology	8
1. Security breaches and their prevention	10
1.1. A multifaceted notion	10
1.2. The perils of the digital environment	11
1.3. An epidemic of security breaches	13
1.4. Consequences for consumers	16
1.5. Preventing security breaches	18
1.5.1. What companies can do	19
1.5.2. What consumers can do	21
2. A look at business practices	24
2.1. A huge digital footprint	25
2.2. The companies' security measures	27
2.2.1. A few snippets of information	27
2.2.2. A marketing argument	28
2.3. Unequal sharing of responsibilities	29
2.3.1. The consumer's obligations	29
2.3.2. Exemptions for the company	31
2.4. Helping and informing consumers	32
2.4.1. Optional parameters	32
2.4.2. Cybersecurity advice	34
3. From the consumer's perspective	36
3.1. Consumers are concerned	37
3.2. An unsuspected scale	39
3.3. Knowledge gaps	40
3.3.1. Information asymmetry	41
3.3.2. Reach out to the most vulnerable	42
3.4. Consumers sometimes reckless	44
3.4.1. Precautions taken	44
3.4.2. Protecting login credentials	45
3.5. Following a security breach	47
4. Legal aspects of security breaches	51
4.1. Information protected by law	51
4.2. The information security obligation	52
4.2.1. The level of obligation	52
4.2.2. An insufficiently preventive obligation	53
4.2.3. Whose fault is it?	56
4.3. Some additional obligations	58
4.3.1. The accountability principle	58
4.3.2. Limitation of collection and duration of storage	58
4.3.3. Transparency... and its limits	59
4.4. The consequences of a security breach	60

4.4.1. Notify and mitigate	61
4.4.2. Lack of deterrence	62
4.5. A look at abroad... and at the future	63
4.5.1. United States	63
4.5.2. European Union	65
4.5.3. Towards reform in Canada	66
Conclusion and recommendations.....	69
Appendix 1 – Survey report	73
Appendix 2 – Discussion guide (French version)	91
Appendix 3 – Discussion guide (English version)	101

Option consommateurs

MISSION

Option consommateurs is a non-profit association whose mission is to promote and defend the rights and interests of consumers and to ensure that they are respected.

HISTORY

Option consommateurs has been in existence since 1983, when it arose from the Associations coopératives d'économie familiale movement, more specifically, the Montreal ACEF. In 1999, it joined forces with the Association des consommateurs du Québec (ACQ), which had already pursued a similar mission for over 50 years.

PRINCIPAL ACTIVITIES

Option consommateurs helps consumers experiencing difficulties, by offering them budget consultation and information sessions on budgeting, debt, consumer law and the protection of privacy.

Each year we produce research reports on important consumer issues. We also work with policy makers and the media to denounce unacceptable situations. When necessary, we institute class action suits against merchants.

MEMBERSHIP

In its quest to bring about change, Option consommateurs is active on many fronts: conducting research, organizing class action suits, and applying pressure on companies and government authorities. You can help us do more for you by becoming a member of Option consommateurs www.option-consommateurs.org.

Acknowledgments

This research was conducted and the report written by Alexandre Plourde, lawyer and analyst at Option consommateurs.

The author wishes to thank all the employees, interns and volunteers at Option consommateurs who in one way or another collaborated in this research. He would particularly like to thank Léa Carresse, a law student at McGill University, as well as Simone Cullen, Étienne Jean and Edward Muzaleno, law students at Université de Montréal.

A significant portion of this research is based on interviews with experts in the field of cybersecurity and privacy protection. The author is grateful to all these experts for generously agreeing to grant him an interview.

The author thanks everyone who contributed to the review of this report. He would like to thank Bruno Marien, a sociologist and lecturer in the Faculty of Political Science and Law at Université du Québec à Montréal, for his methodological support. He also thanks Jean-Pierre Beaud, a professor at the same faculty, who evaluated the report. Finally, the author would like to thank Marie-Thérèse Duval for the revision of the text, as well as Roy Cartlidge, a lecturer in McGill University's Translation Studies program, for this translation.

Summary

In recent years, data breaches have been on the rise in Canadian companies. The risk of security leaks is heightened in the digital environment, exposing consumers to identity theft and other harmful consequences. Many cybersecurity experts are critical of the lack of effective preventive counter-measures in Canada, for businesses and consumers alike.

The online companies most popular with Canadian consumers generally give the public little information about the exact security measures they employ. A few occasionally provide more details, and even include cybersecurity as a marketing ploy to entice consumers to use their services. These companies' user agreements may stipulate a number of obligations that consumers must respect concerning the security of their accounts. On the other hand, these same contracts may contain clauses designed to absolve the companies of their responsibility with regard to data security.

The survey and focus groups we conducted with Canadian Internet users found that consumers consider security breaches to be a matter for concern. However, these consumers are poorly informed about the cybersecurity practices of companies, are unaware of many of their contractual obligations toward them, yet rely primarily on those same companies to keep their data safe. Furthermore, our study suggests that the need for cybersecurity information is more pronounced among groups that are generally considered the most vulnerable. Finally, we found that consumers' online behaviour is sometimes reckless, particularly when it comes to managing their login credentials.

Canada's privacy laws require businesses that store consumers' digital data to adopt adequate security measures to protect it from breaches and comply with other obligations to further ensure its protection. However, partly because it does not impose major financial penalties for security breaches, Canadian law is not sufficiently prescriptive or dissuasive to promote effective prevention. Certain draft legislation, based in part on European standards, could point the way to some interesting solutions for Canada in this regard.

In conclusion, Option consommateurs recommends strengthening companies' legal obligations with regard to prevention, substantially increasing the financial penalties that can be imposed on those that violate the law, and ensuring that the organizations responsible for enforcing data protection laws have sufficient funding and powers to enable them to carry out their mission fully. Considering the limited ability of consumers to evaluate online companies' security measures on their own, Option consommateurs recommends that the public authorities conduct proactive audits of such companies to ensure that consumers who use their services are adequately protected.

Introduction

The 1982 movie *Tron* features a computer scientist who attempts to penetrate the security defences of a corporation in the thrall of a corrupt leader. In dematerialized form, he infiltrates the company's computer network and succeeds in defeating malicious programs and obtaining data that proves that the CEO is a usurper. Justice is done, the rogue leader is deposed, and the credits roll.

It goes without saying that this is a Hollywood ending. In the real world, however, security breaches usually have far less optimistic outcomes. Rather than an exploit by a crusading vigilante, security breaches are most often the work of criminals who seize consumer data for malicious purposes. And, unlike in the *Tron* scenario, consumers do not end up winners when the credits roll; their data will flow unabated for years to come, constantly exposing them to the risk of identity theft.

Research objectives and methodology

This research focuses on consumer data security breaches in the online environment. In recent years, countless data breaches have occurred in Canadian companies. The question now becomes: how can we better prevent these leaks? In pursuit of possible answers, we devised a methodology comprising several components.

First, we drew up a portrait of the security breach phenomenon and the prevention issues it raises, both for businesses and for consumers (section 1). We were particularly interested in the scale of the phenomenon and the most common types of data breaches involved, as well as the initiatives in place to encourage consumers and businesses to adopt preventive measures.

We then analyzed the terms of use, privacy policies and other documentary material published by the companies most popular with Canadian Internet users (section 2). This step centered particularly on documenting consumers' contractual obligations towards these companies, the information the companies provide about their security measures, and the tools available to consumers to protect their data.

In addition, we conducted a Canada-wide survey and focus groups with Canadian Internet users (section 3). The aim of these initiatives was to better identify the experiences, knowledge and perceptions of consumers with regard to security breaches, protective behaviour they could adopt and their contractual obligations towards companies.

Finally, we studied the legal framework applicable to the protection of consumer data, both in Canada and abroad (section 4). Combined with the other results of our research, this analysis permitted us to identify possible solutions for better preventing security breaches.

To aid us in our analysis, we also requested interviews with cybersecurity experts and company representatives.¹ We interviewed Benjamin C. M. Fung, a professor in McGill University's School of Information Studies; Benoît Dupont, Scientific Director of the Smart Cybersecurity Network (SERENE-RISC), and professor of Criminology at Université de Montréal; Sébastien Gambs, a professor in the computer science department at UQAM and holder of the Canada Research Chair in Privacy Preserving and Ethical Analysis of Big Data; Gopinath Jeyabalaratnam, senior policy analyst at the Canadian Federation of Independent Business; Florian Kerschbaum, a professor in the David R. Cheriton School of Computer Science at the University of Waterloo; Anne-Sophie Letellier, co-founder of Lab2038 and IT security specialist; Claudiu Popa, a risk management, personal information protection and data security strategy consultant; and Steve Waterhouse, cybersecurity expert.

1. We requested interviews with all the companies that were part of our selection for the purposes of analyzing contracts (see section 2) as well as business groups. All refused our interview requests or left them unanswered, with the exception of the Canadian Federation of Independent Business and the firm AWS (Amazon), which agreed to provide written responses to a few of our questions.

1. Security breaches and their prevention

1.1. A multifaceted notion

The expression “security breach”² most commonly refers to a situation in which an attacker steals confidential information held by an organization. The image that comes immediately to mind is that of an obscure hacker seated in front of his computer, who manages to remotely download a precious database using cunning computerized maneuvers. Or we imagine a double agent who infiltrates the premises of a large corporation to steal crucial documents.

However, the notion of security breach is not limited to simple data theft. A security breach is generally defined as the loss of, unauthorized access to, or unauthorized disclosure of personal information held by a business or other organization.³ In other words, a security breach includes not only situations in which the confidentiality of the data is compromised, but also those in which this data is modified or made inaccessible to authorized persons.⁴ This could be the case, for example, during a ransomware attack, in which a malicious program is used to encrypt data and make it unreadable until a sum of money is paid. In such a situation, users still retain their data, but are no longer able to access it because it has been altered by a third party.

In addition, a security breach is not always the result of an intentional act. Human error, computer failure, accidents or other twists of fate may result in data held by a company being exposed, corrupted or lost. For example, an employee could send an email containing sensitive information to the wrong recipient. Likewise, a glitch in the servers hosting the data could lead to their being corrupted or even destroyed.

Often, of course, security breaches are the result of intentional, malicious acts. In the online environment, such misdeeds can be perpetrated by numerous actors. While the most common threat is posed by cybercriminals motivated by monetary gain, foreign states, hacktivists, or even the internal staff of an organization may also be at the root of security breaches, and their

2. Several terms can be used to designate a data security breach, including “security breach,” “data breach,” or “data leak.” These terms will be used interchangeably in this report.

3. John Lawford and Janet Lo, *Data Breaches: Worth Noticing?*, PIAC, 2011, pp. 20-24; Éloïse Gratton and Frédéric Neron, “Bris de sécurité informationnelle: étapes à suivre et gestion des risques” in Barreau du Québec - Service de la formation continue, *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé*, Yvon Blais, 2014, p. 117. This definition is also inspired by the legal framework respecting the security of personal information, which provides that a company must take measures “against loss or theft as well as against consultation, communication, copying, unauthorized use or modification” (see section 4). Note that a security breach can not only involve personal information, but also a company’s “confidential” information, such as its trade secrets. However, in the context of this research focused on the protection of consumer privacy, we will limit the scope of our definition to personal information only.

4. This definition, which relies on the three pillars of information security (confidentiality, integrity and availability) to define the concept of “security breach,” is proposed, among others, by the “Article 29” group in the European Union. See: Article 29 Data Protection Working Party, *Guidelines on Personal Data Breach Notification under Regulation 2016/679*, 18 / EN WP250rev.01, 2018, pp. 7-9. “Confidentiality” means ownership of information that can only be disclosed to authorized persons. “Integrity” refers to information that has not undergone any alteration during its processing or transmission. By “availability,” we mean the possibility of consulting a document or obtaining the information contained therein. See: Nicolas W. Vermeys, *Responsabilité civile et sécurité informationnelle*, Yvon Blais, 2010, p. 24-31; Crypto.Québec, *On vous voit: comment déjouer les malveillants sur Internet*, Trécarré, 2018, pp. 19-22.

motives are every bit as varied.⁵ For example, a theft of data that affected millions of Yahoo email subscribers has been attributed to agents operating on behalf of the Russian government.⁶

Such malicious actors have a very large arsenal of techniques at their disposal, and these are constantly evolving.⁷ These techniques may first of all be aimed at exploiting vulnerabilities in the organization's software or computer systems. Some of the most common involve the use of malicious programs, such as ransomware or spyware.⁸ A wide variety of other such methods may also be employed, ranging from exploiting known vulnerabilities in outdated software, to form hijacking,⁹ to highly sophisticated attacks that exploit a zero-day vulnerability.¹⁰

Likewise, a security breach can be achieved with the help of psychological hacking techniques, which target human vulnerabilities rather than computer system flaws. These techniques may be designed to arouse an emotion, a sense of urgency, or even fear in their targets. The most widely known method is phishing, in which a scammer impersonates a trusted source in order to steal information from someone. Many other scamming techniques can be employed, such as typosquatting¹¹ or fake mobile apps.¹²

1.2. The perils of the digital environment

The Internet environment is not merely bombarded with threats from “outside”; it also possesses many inherent vulnerabilities, which themselves increase the risk of security breaches. There are several factors that can exacerbate such risks.

First, the risk factor is increased by the phenomenal volume of personal information circulating in computerized networks. Consumers have an enormous digital footprint. The companies that provide consumers with online services conserve data about them, such as their contact information, passwords, date of birth, or financial and medical information. Digital consumers also generate a stupefying quantity of data when they browse the Internet or when they use connected objects, whether this be their geolocation, their web history or information about their habits, their preferences or their purchases. This leads to a simple equation: the more information that is stored about consumers, the greater the risk of their being the target of a security breach.

5. Canadian Center for Cybersecurity, *National Cyber Threat Assessment 2020*, Communications Security Establishment, 2020, pp. 10, 24; IBM Security, *Cost of a Data Breach Report*, IBM, 2020, p. 38.

6. Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, *The New York Times*, October 3, 2017.

7. For an exhaustive review of these techniques, consult the Att&ck knowledge base of the MITER organization: <https://attack.mitre.org/versions/v7/techniques/enterprise/>

8. This software could have been installed on computers by a virus or a Trojan horse.

9. Form hijacking involves entering malicious code into a poorly secured web form in order to steal the information entered by Internet users.

10. A zero day vulnerability is a flaw in a computer system or software that has not been made public, or for which there is as yet no known fix.

11. Typosquatting is a technique that consists of creating web addresses whose spelling is close to a legitimate site, so as to deceive Internet users.

12. Canadian Center for Cybersecurity, *An Introduction to the Cyber Threat Environment*, Communications Security Establishment, 2020, pp. 6-12.

The ever-increasing level of connectivity in our daily environment is matched by an increased risk of security breaches. The constantly growing number of mobile phones and connected objects,¹³ combined with the interconnections between all these devices, multiply the number of points in the network where vulnerabilities can arise.¹⁴ Despite these risks, experts are appalled that such a complex ecosystem is being developed with so little consideration paid to cybersecurity. Many common connected devices, for example, have all kinds of glaring security gaps, such as backdoors¹⁵ or weak authentication processes.¹⁶

These flaws in the digital environment do not merely expose consumers to economic harm or invasion of privacy. They are also a threat to their physical integrity. System connectivity now permits attackers to target critical infrastructure, such as power plants or hospitals, thereby endangering public safety.¹⁷ In 2020, Health Canada issued a warning that health devices such as pacemakers and insulin pumps could be hacked and expose their users to physical harm.¹⁸

The development of digital technology not only increases risks, it also facilitates the work of criminals, who are finding it increasingly easy to carry out attacks.¹⁹ On the Internet, distance is no obstacle. It allows an individual to operate from any location in the world. The scale of attacks has also grown: attackers can now simultaneously target a multitude of systems that possess the same vulnerability, rather than being restricted to attacking them one at a time. The ease with which digital information can be reproduced also facilitates data theft on a massive scale: an entire database can be siphoned off with just a few clicks.

Digital technology also makes it possible to easily reproduce the same attack. Sophisticated cybercriminals can create software that will permit amateurs to reproduce the same technique, even if they themselves do not have the knowledge to program such software.²⁰ In the arms race between attackers and defenders, then, it is no longer the “average” villains we have to

13. By 2025, it is expected that more than 41 billion objects will be connected to the Internet. See: IDC *The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast*, June 18, 2019, <https://www.idc.com/getdoc.jsp?containerId=prUS45213219>. A survey also indicates that 83% of households have at least one connected device: ALLOT *Connected Home Cybersecurity: The Consumer's Perspective*, Telco Security Trends, 2018.

14. Doug Black et al., *Cyber Assault: It Should Keep You Up At Night*, Report of the Standing Senate Committee on Banking, Trade and Commerce, 2018, pp. 21-23; Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*, WW Norton & Company, 2018, pp. 26-28; Commissioner for the Protection of Privacy, *Privacy and Cybersecurity*, Canada, December 2014, p. 3.

15. A backdoor is a feature that allows secret access to software, usually for the manufacturer's purposes, without the knowledge of the consumer.

16. Valérie Montcalm, Alexandre Plourde, Élise Thériault, *Enfants sous écoute. La protection de la vie privée dans l'environnement des jouets intelligents*, Option consommateurs, 2018, pp. 14-16.

17. Canadian Center for Cybersecurity, *National Cyber Threat Assessment 2020*, Communications Security Establishment, 2020, p. 10; Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*, WW Norton & Company, 2018, pp. 89-96.

18. Health Canada, *Cybersecurity vulnerabilities associated with some medical devices with Bluetooth Low Energy chips*, March 11, 2020, <https://canadiensensante.gc.ca/recall-alert-rappel-avis/hc-sc/2020/72555a-eng.php>

19. Bruce Schneier *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*, WW Norton & Company, 2018, pp. 32-33.

20. By way of illustration, the Mirai malware could be used by various amateurs to carry out distributed denial-of-service attacks: [https://en.wikipedia.org/wiki/Mirai_\(malware\)](https://en.wikipedia.org/wiki/Mirai_(malware))

worry about, but the more sophisticated ones—because they can strike from anywhere, and their attacks can then be reproduced by amateurs.²¹

Finally, the future holds many other dangers. In the opinion of many experts interviewed for this research, attacks such as ransomware will continue to increase over the next few years. As the technology develops, we may see the emergence of new forms of hacking that utilize artificial intelligence to fool consumers, through, for example, the use of deep fake techniques.²² In the longer term, the arrival of quantum computing could render current encryption methods obsolete, permitting them to be cracked with alarming ease.

1.3. An epidemic of security breaches

It truly is an epidemic. According to the firm Risk Based Security, 7,098 security breaches were reported around the world in 2019, exposing more than 15 billion files to outsiders.²³ According to Norton, in 16 countries around the world, over one billion adults say they have been victims of cybercrime.²⁴

This country is no exception. In recent years, there has been a staggering number of data breaches in companies operating in Canada.²⁵ Our media search turned up nearly a hundred over a period of ten years.²⁶ Large companies such as TransUnion, Equifax or Yahoo are targeted just as often as small companies.²⁷ The number of people affected by these data breaches can vary widely; some cases involved only a few thousand victims,²⁸ while others involved millions.

21. Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*, WW Norton & Company, 2018, pp. 30-32.

22. Nick Statt, *Thieves are now using AI deepfakes to trick companies into sending them money*, The Verge, September 5, 2019, <https://www.theverge.com/2019/9/5/20851248/deepfakes-ai-fake-audio-phone-calls-thieves-trick-companies-stealing-money>

23. Riskbased Security, *2019 Year End Report: Data Breach Quickview*, 2020.

24. Norton Life Lock, *Cyber Safety Insights Report Global Results*, report prepared by The Harris Poll, 2019, p. 6.

25. It should also be noted that many companies report having been the target of cyberattacks, even though not all these attacks were successful. According to a survey conducted by CIRA, 40% of companies say they have been the target of a computer attack in the past 12 months; among the largest companies, it is as high as 66%. According to Statistics Canada, 21% of Canadian businesses say they experienced a cybersecurity incident that affected their operations in 2017. See: Statistics Canada, *Impact of cybercrime on Canadian businesses, 2017*, *The Daily*, October 15, 2018; CIRA, *2019 Cybersecurity Report*, 2019: <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>

26. To carry out this media review, we researched articles for the period from August 1, 2010 to August 1, 2020 in *La Presse*, *Le Devoir*, the *Globe and Mail* and the *Toronto Star*, as well as on Radio-Canada and CBC. This research enabled us to identify 94 references to security breaches in companies. Although our analysis focused on security breaches occurring in businesses, we also noted that a considerable number of security breaches occur in the public sector and in the health sector, in particular.

27. For example, there are reports that small dental or law firms may have been victims of ransomware: Thomas Daigle, “Definite Uptick: Global wave of ransomware attacks hitting Canadian organizations,” CBC News, October 14, 2019; Sean Kavanagh, “Ransomware attacks lock 2 Manitoba law firms out of computer systems,” CBC News, April 14, 2020.

28. This was the case, for example, with the security breaches at TransUnion (37,000 people), the Ontario Cannabis Store (4,500 people), the National Bank (4,000 people) and the magazine *L’actualité* (3,000 people). The Office of the Privacy Commissioner also mentions instances in which only one person was affected. See: Office of the Privacy Commissioner of Canada, *A full year of mandatory data breach reporting: What we’ve learned and what businesses*

Most Significant Security Breaches in Canada Since 2010²⁹

Business	Number of victims	Year
LifeLabs	15 million	2019
Desjardins	9.7 million	2019
Yahoo	8 million	2013
Capital One	6 million	2019
NCIX	3.9 million	2018
Sony Entertainment	3.5 million	2011
Ashley Madison	2.2 million	2015
Bell Canada	1.9 million	2017
Nissan Canada Finance	1.1 million	2017
Canoe.ca	1 million	2017

2019 was a particularly significant year for security breaches. More than 9.7 million clients of the Québec credit union Desjardins saw their contact info, social insurance numbers and other financial data appropriated by an employee who had access to them.³⁰ Another financial institution, Capital One, suffered a security breach that affected 6 million Canadians, when an unauthorized third party accessed the company's cloud servers.³¹ Finally, the firm LifeLabs was hit by a cyber attack that compromised the medical data of 15 million Canadians.³²

Although our media review gives an idea of the scale of the phenomenon in Canada, the data breaches that make the headlines are clearly only a small fraction of all the security breaches that occur in the country. The Office of the Privacy Commissioner of Canada (OPC) announced that it received no less than 680 security incident reports for the period from November 1, 2018 to October 31, 2019 alone.³³ The organization states that these security breaches affected more than 28 million Canadians.

Once again, the number quoted by the OPC undoubtedly falls short of the real number. It will be recalled that until recently, most Canadian companies were not subject to a disclosure obligation in the event of a breach of confidentiality of personal information—which suggests

need to know, OPC Blogger, October 31, 2019. The number of people potentially affected by security breaches in other situations has not been publicly disclosed.

29. From: Canadian Center for Cybersecurity, *National Cyber Threat Assessment 2020*, Communications Security Establishment, 2020, p. 17.

30. OPC, *Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019*, PIPEDA Report of Findings #2020-005.

31. Radio-Canada, *Capital One: des données personnelles de 6 millions de Canadiens ont été volées*, July 29, 2019, <https://ici.radio-canada.ca/nouvelle/1241200/capital-one-vol-donnees-personnelles-etats-unis-canada-pirate-informatique>

32. Radio-Canada, *LifeLabs: 15 millions de clients touchés par une cyberattaque*, December 17, 2019, <https://ici.radio-canada.ca/nouvelle/1438127/lifelabs-15-millions-clients-informations-cyberattaque>. Note that a joint decision of the Federal Privacy Commissioners and British Columbia has been rendered on this case but, as of this writing, Lifelabs opposes its publication: <https://www.oipc.bc.ca/news-releases/3449>

33. OPC, *A full year of mandatory data breach reporting: What we've learned and what businesses need to know*, OPC Blogger, October 31, 2019, <https://www.priv.gc.ca/en/blog/20191031/>

that a considerable number of security breaches may have occurred in previous years that were simply not reported.³⁴ What is more, many companies don't know that they have been experiencing data breaches, meaning that the real numbers are potentially even greater.

Moreover, not all of these security breaches are of the same type. According to OPC statistics, 58% of privacy breaches are the result of unauthorized access: this includes cases in which employees gain unauthorized access to information as well as cases in which psychological hacking methods, such as phishing, are employed. Twenty-two percent of cases were caused by accidental disclosure, such as sending an email with confidential information to the wrong recipient.³⁵ In 12% of cases, the security breach was the result of lost storage devices or paper documents and, in 8% of cases, of the theft of equipment, such as a computer containing personal data.³⁶

Extract from a phishing email

Hi Customer,

Sorry for the interruption, but we are having trouble authorising your VISAMASTERCARD.

Please visit the account payment page to enter your payment information again or to use a different payment method.

Visit Page Payment

We're here to help if you need it. Visit the Help Center for more info or contact us.

—The Netflix Team

According to the OPC, a quarter of security breaches in Canada are the result of phishing techniques or other social engineering methods. A common tactic for scammers is to send emails claiming to be from a trusted business in order to trick the recipient into downloading attachments or disclosing their personal information.

Finally, the severity of the damage varies. Some security breaches involve only a person's contact details, or even just an email address, so the risk to which the targeted consumer is exposed remains moderate. Other security breaches may involve a client's entire file, and even include all the information that a company has about them. In some instances, such as the

34. The OPC reports a six-fold increase in the number of reports since disclosure became mandatory by law. According to a CIRA survey, only 58% of companies with a security breach reported it to a government authority. See: CIRA, *Cybersecurity Survey, 2019*, <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>

35 Ibid.

36 Ibid.

Desjardins case, financial data or even social insurance numbers may have been stolen. In other cases, very sensitive data such as medical data or passwords can be compromised,

In short, while the phenomenon of security breaches remains imperfectly documented, there can be no doubt that it is a major issue in Canada. In fact, in light of the statistics cited above, it can realistically be argued that almost every Canadian has been affected by a security breach in an organization, in one way or another.

1.4. Consequences for consumers

At the beginning of 2019, computer security experts discovered that a hacked database containing over 700 million email addresses and over 21 million passwords was circulating on the dark web.³⁷ Dubbed “Collection #1,” this database is in fact only one of many compilations of data stolen during various security breaches.³⁸

Such a discovery illustrates how long the repercussions of a security breach can endure over time. Once obtained, the consumer’s data can not only be used directly by the individuals who stole it, but can also be resold over underground networks. Any number of shady characters could use this information to open a credit account in the victim’s name, file a fraudulent government benefit claim, extort money, design phishing emails, or take control of someone’s online accounts.³⁹ On top of this is the fact that a security breach can also damage a victim’s reputation through the publication of personal data, occasioning endless stress and anxiety.

Consumers who have been victims of a security breach may see the specter of identity theft or other mischief hovering over them for years on end.⁴⁰ Unfortunately, they have few resources to mitigate these risks. While users can change certain types of identifiers, such as their access codes or passwords, to prevent access to their online accounts, other information such as their name, location, date of birth, social insurance number or biometric data cannot be changed, and once compromised, it will be able to circulate in underworld networks indefinitely.

Unfortunately, Canada is lagging behind in implementing initiatives to offset these challenges. According to several experts interviewed for this research, the use of digital identification methods⁴¹ would allow consumers to avoid sharing sensitive information with businesses to

37. Troy Hunt, *The 773 Million Record "Collection #1" Data Breach*, January 17, 2019, <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/>

38. A list of such databases can be found on the haveibeenpwned site: <https://haveibeenpwned.com/>

39. Canadian Center for Cybersecurity, *National Cyber Threat Assessment 2020*, Communications Security Establishment, 2020, p. 24.

40. According to statistics on fraud in Canada, these risks are very real. In 2018, Canadian police forces recorded more than 129,400 cases of fraud and identity theft, an increase of 12% over 2017. In fact, the rate of fraud in Canada has been rising steadily for ten years. See: Greg Moreau, *Police-reported crime statistics in Canada, 2018*, Statistics Canada, July 22, 2019, pp. 14-15.

41. The concept of “digital identity” can be defined as a body of personal information recorded in digital format that uniquely identifies a person. Unlike identity cards currently issued in Canada, a digital identity can be completely dematerialized and authenticated via the Internet. See: Julia Clark et al., *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, World Bank, 2016, p. 11.

identify themselves, thus limiting the impact of security breaches.⁴² However, Canada is slow to digitize its national identification systems. In addition, no “credit freeze” mechanism is made available by credit agencies in Canada⁴³ which would allow consumers to better control access to their credit report by third parties, thereby limiting the ability of fraudsters to subscribe to credit accounts in their name.⁴⁴

Without such protections, consumers who are victims of a data breach must turn to surveillance strategies in order to at least have the opportunity to react quickly in the event of fraud. It is therefore recommended that victims of security breaches consult their credit report regularly, to check if any fraudulent accounts have been created, and to mark these with a fraud alert. Consumers can also check if their email is circulating in illicit databases by carrying out a search on the site *haveibeenpwned.com*, a citizens’ initiative that collects databases disseminated in underground networks.

The companies themselves may offer some support to customers who fall victim of a security breach. Many of these companies, either voluntarily or as a result of legal obligations, already notify their clients when they have been the target of a security breach. This notification is often accompanied by the offer of a subscription to a credit bureau, which may include a service for monitoring fraudulent entries in their credit file and even insurance in the event of identity theft.

**Excerpt from a letter from the Desjardins cooperative advising clients
of the 2019 security breach**

Subject: Your personal information

Dear [name of member]

Desjardins has conducted an internal review and analysis, and found that an ill-intentioned employee had access to the personal information of our members and clients who have or had a *caisse* (banking) account, credit card or point-of-sale financing (in-store Accord D financing and auto and leisure vehicle loans). No credit cards or other payment methods, like Interac or debit cards, have been compromised.

Our review shows that the affected data may include some of your personal information. We want to assure you that you won't suffer a financial loss if any unauthorized transactions are made in your Desjardins accounts as a result of this situation. Additional security measures were put in place as soon as the situation was detected. Our top priority is to ensure the protection of our members' and clients' personal and financial data.

Please read the enclosed information very carefully. It explains how we're here to help protect you.

42. Interac, *Identité numérique: libérer tout le potentiel de l'économie numérique au Canada*, Interac Association and Acxsys Corporation, September 2017.

43. A “credit freeze” (or “security freeze”) is a mechanism that allows a consumer to block access to their credit report to businesses, unless they specifically give permission to access it. In practice, this service is offered by the credit agency that holds the credit report, whom the consumer will contact to authorize access to their credit report. This mechanism therefore adds an additional layer of security by making it more difficult for third parties to obtain credit in the consumer's name.

44. Note that Québec's *Credit Assessment Agents Act* will establish such a mechanism, but only in that province. See: *Bill 53, Credit Assessment Agents Act*, SQ 2020, c 21, s. 9. In Ontario, the law has also been amended to include security freeze provisions, but these have not been implemented. See: *Consumer Reporting Act*, RSO 1990, c C.33, s. 12.5 (10) [not in force].

Of course, consumers aren't the only ones paying the price for security breaches. For businesses, a data breach can involve significant costs, including loss of customers, damage to reputation, the expenditure required to correct the situation and provide assistance to victims, or ransom payments to recover data.⁴⁵ According to a report by IBM, security breaches cost Canadian companies an average of \$6.34 million.⁴⁶ Security breaches may also necessitate investigations by the competent authorities, or even legal proceedings (section 4.4).

That said, some authors question the actual financial impact on a business in the wake of a security breach. Although damage to reputation is often cited as a loss, surveys indicate that the majority of consumers continue to do business with a company that has suffered a security breach.⁴⁷ Other authors also point out that a company's stock market devaluation following a data breach is insignificant, especially since its losses may be covered by its insurance policies.⁴⁸ This suggests that in the end, the biggest losers in a security breach are the consumers who have their data stolen.

1.5. Preventing security breaches

Faced with the scale of data leaks, several experts deplore the lack of preventive measures against cybercrime in Canada. The importance of acting proactively, by implementing measures to prevent the occurrence of data leaks, was a recurrent theme among the stakeholders interviewed for this research. But what exactly can be done to better prevent security breaches?

Part of the answer undoubtedly lies in action by governments. In this regard, it is worth noting that several public sector initiatives have been developed in the area of cybersecurity in recent years. In 2018, the federal government implemented a national cybersecurity strategy.⁴⁹ We also saw the creation of the Canadian Center for Cyber Security and the National Cybercrime Coordination Unit, a branch of the RCMP.

Governments, however, are not the only entities who bear responsibility for preventing security breaches. Businesses, like consumers, also have a significant role to play.

45. IBM Security, *Cost of a Data Breach Report*, IBM, 2020, p. 7, 21-22; Statistics Canada, *Impact of cybercrime on Canadian businesses, 2017*, *The Daily*, October 15, 2018.

46. IBM Security, *Cost of a Data Breach Report*, IBM, 2020, p. 67.

47. Jeff Kosseff, "Defining Cybersecurity Law," (2018) 103 Iowa L. Rev. 985, p. 1015. A CIRA survey also indicates that only 13% of companies report that a cyber attack could have damaged their reputation. CIRA, *Cybersecurity Survey, 2019*, <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>

48. Claudiu Popa, *The Canadian Cyberfraud Handbook: A Professional Reference: How to Keep Up with the Evolution of Deceptive Practices and Reduce the Erosion of Online Trust*, Thomson Reuters, 2017, p. 139-141; Elena Kvochko and Rajiv Pant, "Why Data Breaches Don't Hurt Stock Prices," *Harvard Business Review*, March 31, 2015.

49. Public Safety Canada, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*, Canada, 2018. The Canadian strategy has also been implemented in a cybersecurity action plan: *National Cyber Security Action Plan (2019-2024)*, Canada, 2019. Provincial governments have also adopted initiatives along these lines, in particular, Québec: Secrétariat du Conseil du trésor, *Politique gouvernementale de cybersécurité*, Québec, 2020.

1.5.1. What companies can do

Businesses bear a considerable share of the responsibility for preventing security breaches. After all, since they are the ones who collect and store consumer data, they are the ones that create the risk of its being compromised. Consequently, they need to implement security measures designed to curtail these risks. But exactly what measures should a business take? What level of protection is sufficient?

To answer these questions, a business will need to conduct a risk analysis. Roughly summarized, this type of analysis involves identifying the information to be protected, determining the vulnerabilities and threats they are prone to, and then quantifying the likelihood that those risks will materialize and cause damage.⁵⁰ At the end of this exercise, the company will be able to select the relevant countermeasures needed to respond to the identified risks, while attempting to achieve a judicious balance between the seriousness of the threats and the cost of the countermeasures. The company's goal, therefore, is not to prevent any possible breach of security, but rather to deploy reasonable measures that take all the risks into account.

As can be imagined, the measures to be deployed will vary from one organization to the next, depending on the context and the specific type of risk identified in each. A "mechanical" approach to information security, in which countermeasures are applied without taking the context into account, is therefore inadvisable.⁵¹ Ensuring appropriate information security is a process that continues throughout the entire lifecycle of the data, which constantly requires evaluating, monitoring, testing one's countermeasures, and training personnel.

There are a number of models and standards for implementing security measures within an organization, which, with a few variations, generally follow the same risk analysis steps.⁵² One of the most common generalist models is the NIST 800-30 standard of the National Institute of Standards and Technology,⁵³ or the ISO/IEC 2700 family of standards of the International Standardization Organization.⁵⁴ In addition to these widely used omnibus standards are others

50. To assess the likelihood of a threat impacting the business, either a quantitative or a qualitative risk analysis can be performed. The aim of a quantitative analysis is to assign numerical values to the elements of the risk analysis, using formulas to calculate possible "losses." In qualitative analysis, different scenarios are evaluated according to a scale of criticality. For more details on the risk analysis process, see: Nicolas W. Vermeys, *Responsabilité civile et sécurité informationnelle*, Yvon Blais, 2010, pp. 33-67; Carol A. Siegel and Mark Sweeney, *Cyber Strategy: Risk-Driven Security and Resiliency*, 1st edition, Taylor & Francis Group, 2020, pp. 95-119.

51. Scott J. Shackelford et al., "Bottoms Up: A Comparison of 'Voluntary' Cybersecurity Frameworks," (2016) 16 *UC DAVIS Bus. LJ* 217, p. 256; OPC, *Privacy and Cyber Security*, Canada, December 2014, p. 3.

52. According to the firm PwC, there are more than a thousand cybersecurity standards around the world, in one form or another. See: PwC, *UK Cyber Security Standards*, Department for Business Innovation & Skills, 2013, p. 4.

53. It should also be noted that Canada has the ITSG-33 standard, which is the Canadian equivalent of NIST 800-53. See: <https://cyber.gc.ca/en/path-enterprise-security>

54. Other generalist standards and models exist, in particular: the ISACA Risk IT Framework, the Project Management Body of Knowledge (PMBOK Guide) of the Project Management Institute, the OWASP Risk Rating Methodology of the Open Web Application Security Project, the COSO ERM Framework of the Committee of Sponsoring Organizations of the Treadway Commission and the FAIR Institute's Factor Analysis of Information Risk. For a more detailed analysis of these models, see: Carol A. Siegel and Mark Sweeney, *Cyber Strategy: Risk-Driven Security and Resiliency*, 1st edition, Taylor & Francis Group, 2020, pp. 98-113.

aimed at specific industries, such as payment services.⁵⁵ Likewise, some government agencies may offer guides and tools designed to help businesses develop better data protection practices.⁵⁶

Moreover, companies can turn to the private sector to support them in their data protection efforts, by calling on specialized firms that offer various cybersecurity services. A company's information security practices can also be subject to certification, which involves a third party certifying a company's compliance with a standard.⁵⁷ Finally, companies can take out insurance to cover situations when they fall victims to a security breach.

That said, while businesses have access to a vast array of tools and services to protect consumer data, many experts criticize their lack of preparedness and investment in cybersecurity.⁵⁸ These shortcomings are particularly glaring in the smallest companies, where the lack of resources can hinder the development of appropriate measures.⁵⁹ Also, the scarcity of cybersecurity professionals makes it difficult for companies to recruit staff; this problem is so worrying that the Standing Senate Committee on Banking, Trade and Commerce in 2018 proposed the creation of national cybersecurity training programs to make up for the shortage of expertise in this area.⁶⁰

We also need to point out the ignorance, even negligence, displayed by certain companies.⁶¹ One survey states that despite numerous personal data leaks in 2019, almost half of Canadian businesses have failed to enhance the security of their computer systems.⁶² Another survey indicates that only 41% of companies provide mandatory cybersecurity training to their employees and that 43% are unaware of the existence of rules on mandatory notification of

55. Often cited in this sector are the PCI DSS standard of the Payment Card Industry Security Standards Council, or the SWIFT Customer Security Control Framework (CSCF), of the Society for Worldwide Interbank Financial Telecommunication, which oversees international payments.

56. The Canadian Center for Cyber Security, for example, publishes many informational pages and guides for businesses; accordingly, small and medium-sized businesses do have access to some basic cybersecurity controls. See: <https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>

57. For example, Innovation, Science and Economic Development Canada created CyberSecure Canada, a cybersecurity certification program designed for small and medium-sized businesses: <https://www.ic.gc.ca/eic/site/137.nsf/eng/home>. Although not mandatory, ISO standards can also be subject to certification.

58. OPC, *Privacy and Cyber Security*, Canada, December 2014, p. 6.

59. Claudiu Popa, *The Canadian Cyberfraud Handbook: A Professional Reference: How to Keep Up with the Evolution of Deceptive Practices and Reduce the Erosion of Online Trust*, Thomson Reuters, 2017, p. 93-94; Gopinath J.E. Jeyabalaratnam and François Vincent, *Bill 64: An important reform that should not be rushed*, CFIB, September 2020. In a CIRA survey, 43% of companies that responded claimed they had not employed a cybersecurity specialist, citing lack of resources. See CIRA, *Cybersecurity Survey, 2019*, <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>

60. Doug Black et al., *Cyber Assault: It Should Keep You Up At Night*, Report of the Standing Senate Committee on Banking, Trade and Commerce, 2018, pp. 15-16.

61. OPC, *Privacy and Cyber Security*, Canada, December 2014, p. 9.

62. Novipro and Léger Marketing, *IT portrait of Canadian medium and Large-sized companies*, vol. 4, 2020.

security breaches.⁶³ Moreover, even in cases in which companies have actually implemented security standards, these standards are often scantily respected.⁶⁴

Finally, several experts also deplore the fact that the legal and economic context provides insufficient incentives for the development of preventive measures within companies. Since Canadian laws do not impose high fines, the cost of failing to comply with security obligations may appear less onerous to some companies than the investment required to comply (see section 4.4). Far from fostering prevention, such behaviour encourages the adoption of merely “corrective” practices, whereby flaws are remedied only after systems are deployed, thereby increasing the risk⁶⁵.

1.5.2. What consumers can do

Of course, consumers also have a role to play in preventing data breaches. Like businesses, they can be the target of malware, phishing, or other types of scams.⁶⁶ Likewise, careless or reckless behaviour on the part of the user can negate the best protection measures deployed by a company. To protect their personal information, their privacy and their money, consumers can therefore not rely blindly on companies. Just as companies implement countermeasures aimed at reducing risk, they also need to adopt good protective practices.

In order to raise awareness among consumers and inform them of the basic precautions to adopt, several Canadian organizations, both public and private, have developed initiatives to educate consumers about cybersecurity. There is a substantial amount of information online that is issued by government agencies,⁶⁷ non-profit organizations⁶⁸ or private companies.⁶⁹ Wider campaigns have also been organized to raise public awareness, such as Cyber Security Awareness Month.⁷⁰ Some initiatives target specific audiences, most often children, using game

CIRA, *Cybersecurity Survey, 2019*, <https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey>

64. A Verizon report shows that only 27.9% of companies in the payments sector manage to fully comply with the PCI DSS standard. See: Verizon, *2020 Payment Security Report*, 2020; David Serabian, *Consumer Protection and Cybersecurity: The Consumer Education Gap*, Brookings Mountain West Publications, 2015, pp. 3-4.

65. Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*, WW Norton & Company, 2018, pp. 34-35.

66. The Canadian Anti-Fraud Center publishes a comprehensive list of the most common scams: <https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-eng.htm>. See also: Claudiu Popa, *The Canadian Cyberfraud Handbook: A Professional Reference: How to Keep Up with the Evolution of Deceptive Practices and Reduce the Erosion of Online Trust*, Thomson Reuters, 2017, pp. 34-36, 179 and following.

67. At the federal level, these include the Canadian Center for Cyber Security, the Canadian Anti-Fraud Center and the Office of the Privacy Commissioner. Provincial organizations may also publish cybersecurity advice.

68. Among these non-profit organizations, are SERENE-RISC, Option consommateurs, MediaSmarts, CybersafeBC, CryptoQuébec, Cybernb, Citizen Lab, and Knowledge Flow Cybersafety Foundation.

69. We will say more about advice provided by the private sector in section 2.4.

70. Cyber Security Month is an international campaign that takes place in October aimed at educating the public about cybersecurity. In the same vein, Fraud Prevention Month also touches on certain aspects of cybersecurity: <https://www.ic.gc.ca/eic/site/cb-bc.nsf/eng/03662.html>

platforms,⁷¹ or by training teachers to impart relevant information to children.⁷² A few Canadian organizations have also developed tools that offer more in-depth support to consumers. For instance, the Citizen Lab publishes the Security Planner, which allows Internet users to make choices adapted to their situation by providing customized cybersecurity advice.⁷³

On the whole, the advice given to the public through these various tools is relatively similar, although they may emphasize one theme rather than another depending on the circumstances.⁷⁴ Essentially, consumers are advised to adopt technical measures such as securing their home Wi-Fi network or choosing strong passwords, as well as acquiring certain behaviours and reflexes, such as refraining from clicking on hyperlinks in emails or avoiding sharing too much information on social media.⁷⁵

That said, although there is an abundance of information on cybersecurity on the Internet, we still see that many consumers engage in risky behaviour. For example, studies indicate that Internet users do not follow basic protection procedures when managing their login credentials. According to NordPass, as many as 2.5 million people use the extremely weak password “123456”⁷⁶. Other studies indicate that many Internet users share their passwords with relatives, which again contributes to an increased level of risk.⁷⁷

These serious gaps in digital literacy can be explained, in part, by the fact that public information strategies are not adapted to every clientele or context.⁷⁸ The need for education and awareness is probably more pressing among certain more vulnerable groups, such as the elderly, who would be more effectively reached through more traditional media or by resorting to in-person training workshops rather than online information.⁷⁹ In short, information

71. For example, the MediaSmarts organization and Carleton University have developed an online game for 11 to 13 year olds to raise awareness about protecting online privacy: <https://mediasmarts.ca/digital-media-literacy/educational-games/day-life-jos>. Google created the game *Interland* to educate children about information sharing: https://beinternetawesome.withgoogle.com/en_us/interland. Option consommateurs has also posted stories for children online to help them be more aware of cybersecurity issues: <https://option-consommateurs.org/contes>

72. See in particular: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/resources-for-teachers/>

73. <https://citizenlab.ca/category/research/tools-resources/security-planner/>. In the United States, the Electronic Frontier Foundation offers “Surveillance Self-Defense”: <https://ssd.eff.org/>

74. For a list of common advice given to consumers, see Claudiu Popa, *The Canadian Cyberfraud Handbook: A Professional Reference: How to Keep Up with the Evolution of Deceptive Practices and Reduce the Erosion of Online Trust*, Thomson Reuters, 2017, pp. 114-116.

75. By way of illustration, the SERENE-RISC website includes a wide range of standard advice given to consumers, such as updating and configuring the privacy settings of their online accounts. See: <https://www.serene-risc.ca/en/cybersecurity-tips>

76. <https://nordpass.com/most-common-passwords-list/>

77. Kenneth Olmstead and Aaron Smith, *Americans and Cybersecurity*, PEW Research Center, 2017, pp. 4-5. See also section 3.4.

78. Elissa M. Redmiles, Amelia R. Malone and Michelle Mazurek, “I Think They’re Trying to Tell Me Something: Advice Sources and Selection for Digital Security,” 2016 IEEE Symposium on Security and Privacy 272, 2016; Emilee Rader and Rick Wash, “Identifying patterns in informal sources of security information,” (2015) 1-1 *Journal of Cybersecurity* 121; Claudiu Popa, *The Canadian Cyberfraud Handbook: A Professional Reference : How to Keep Up with the Evolution of Deceptive Practices and Reduce the Erosion of Online Trust*, Thomson Reuters, 2017, pp. 28-29.

79. James Nicholson, Lynne Coventry and Pam Briggs, “If It’s Important It Will Be a Headline: Cybersecurity Information Seeking in Older Adults,” CHI Conference on Human Factors in Computing Systems Proceedings, 2019.

strategies on cybersecurity would benefit from being more carefully adapted to specific audiences.

2. A look at business practices

In this research, we wanted to more effectively document the information available to assist consumers in making cybersecurity choices as well as the protection methods the companies offer them to help them protect their data.

To do this, we analyzed the contractual terms and security statements of 25 companies that offer goods or services online in Canada. Our selection was concentrated on the companies most popular with Canadian consumers. In making our selection, we looked at the most common online activities of Canadian Internet users and identified five main categories of online services⁸⁰:

- social media platforms;
- messaging and email services;
- online merchants;
- streaming content providers;
- financial institutions.

For each of these categories, we selected the 5 companies most popular with Canadian consumers.⁸¹ These are the 25 companies we analyzed:

80. Our classification is based on the main activities Canadians perform online, as identified by CIRA:

<https://cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019>

81 For the “social media” category, we based our ranking on data provided by CIRA:

<https://canadiansinternet.com/2019-report-social-media-use-canada/>. For the “messaging and email services” category, we selected the three most frequently cited email services (<https://www.statista.com/statistics/547520/e-mail-provider-ranking-consumer-usa/>) as well as the two most popular messaging services (<https://www.statista.com/statistics/882273/canada-leading-messaging-apps/>). For the “online merchant” category, we used the Statista ranking: <https://www.statista.com/statistics/871090/canada-top-online-stores-canada-ecommercedb/>. We have removed the Apple company from this ranking, however, in order to avoid duplicating the “Streaming content providers” category. For the latter category, we based our ranking on data provided by CIRA: <https://cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019>. Finally, for the “financial institutions” category, we used the Statista ranking: <https://www.statista.com/statistics/434554/leading-banks-in-canada-assets/>. It should be noted that our selection of financial institutions also includes a company that is not one of the five largest companies in this category, namely the Desjardins cooperative; it was included due to the scale of the security breach it suffered in 2019.

Company	Category
Facebook	Social media
Instagram	
LinkedIn	
Twitter	
Snapchat	
Google	Messaging and email
Yahoo	
Microsoft Outlook (Hotmail)	
Skype	
WhatsApp	
Amazon	Merchants
Walmart	
Costco	
Hudson's Bay	
Best Buy	
Netflix	Streaming content
Prime Video	
Spotify	
Crave TV	
Apple Music	
Royal Bank of Canada	Financial institutions
TD Bank	
Scotiabank	
Bank of Montreal	
Desjardins	

We analyzed each company's user agreement, its confidentiality policy and the information published on its website.⁸² In cases where the companies selected had the same owner, we considered them to be distinct from the consumer's point of view, although some of them sometimes had similar or interrelated policies.⁸³

2.1. A huge digital footprint

The companies we analyzed collect an impressive amount of data about their online users.

The mind-boggling quantity of data collected by social media and big tech firms such as Google, Microsoft and Facebook is already well documented in the literature.⁸⁴ It should come as no surprise to learn that these companies, whose business model is based on the exploitation of

82. Some companies may publish many nested legal documents; in such cases, we analyzed all the documents pertinent to the relationship between the company and the internet consumer. With the financial institutions, in particular, we analyzed the contracts for the use of their online banking interfaces as well as the confidentiality policies applicable to these online services.

83. This is the case with Facebook, Instagram, WhatsApp (which are owned by Facebook); and LinkedIn, Hotmail, Skype (owned by Microsoft).

84. See: Alexandre Plourde, *How Free is "Free?": Setting limits on the collection of personal information for online behavioural advertising*, Option consommateurs, 2015, p. 18-22.

personal information for commercial purposes, collect a great deal of data on their users, including their contact information, date of birth, information about their preferences or their personal lives, their browsing history, their interactions with publications, the times when they connect, the third-party sites they visit or even their geolocation.

Online merchants and streaming content providers may also collect a wide range of data. Not only do these companies retain their customers' contact details and payment card information, but they also closely study their activities on their platform. The Apple Music service, for example, explains this as follows:

"When you use iCloud Music Library, Apple logs information such as the tracks you play, stop or skip, the devices you use, and the time and duration of playback."⁸⁵

Financial institutions are no exception. Naturally, in order to provide their services, they need to conserve sensitive financial data about consumers. In addition, their policies indicate that Internet users who visit their website may be subject to having their online activities monitored, and the data collected used for carrying out targeted advertising.⁸⁶

In short, the spectrum of information collected by online companies is vast: names, contact information, email addresses, birth dates, financial information, information about habits and preferences, data about online activities, correspondence, images and other publications—even biometric information.⁸⁷ Needless to say, this data, if compromised, could expose significant amounts of private information about consumers, which could prove very useful to criminals.

The digital footprint of consumers with these companies is not only very large; it also has an indefinite lifespan. Many companies say that they keep most of the data they hold "until it is no longer necessary to provide the services"⁸⁸ or until the account is deleted.⁸⁹ In short, with some exceptions,⁹⁰ the company could keep the data it holds indefinitely, for as long as the consumer's account remains undeleted.

85. <https://www.apple.com/legal/internet-services/itunes/ca/terms.html>

86. For example, the Bank of Montreal explains that it collects "information about your use of websites such as browsing behaviour on BMO websites and links, the places you click on, data from forms and downloads, and more. Data collected using Internet tools (e.g., cookies, web beacons, tagging) to better understand your interests and needs in order to better serve you." See: <https://www.bmo.com/main/about-bmo/privacy-security/our-privacy-code/canada/>

87. For example, Apple's policies address the collection of clients' biometric identifiers, such as facial identification or fingerprints as part of its services.

88. <https://www.facebook.com/privacy/explanation>

89 We found examples of such clauses at Facebook, Instagram, LinkedIn, Twitter, Snapchat, Hudson's Bay, Best Buy, Google, Yahoo, Microsoft, Skype, WhatsApp, Spotify, Royal Bank, Scotiabank and Bank of Montreal.

90. Particular exceptions are WhatsApp and Snapchat, which say they delete messages that pass through their servers. Google and Microsoft also claim to delete, after a certain delay, data such as keywords entered in a search engine.

2.2. The companies' security measures

How is all this data protected? In general, companies provide the public with little precise information about the security measures they employ (section 2.2.1). The few who occasionally give details about such measures most often do so as a marketing ploy to encourage consumers to use their services (section 2.2.2).

2.2.1. A few snippets of information

In their privacy policies, the majority of companies make general statements to the effect that they protect the privacy of consumer's data or that they utilize security measures commensurate with the risks entailed in processing it.⁹¹ By way of illustration, Netflix states:

We use reasonable administrative, logical, physical and managerial measures to safeguard your personal information against loss, theft and unauthorized access, use and modification. These measures are designed to provide a level of security appropriate to the risks of processing your personal information.⁹²

However, many companies are rather tight-lipped about the details of the exact measures they take to protect data. Some give a smattering of technical details, citing for instance the use of the HTTPS protocol or encryption methods. Others add that they have implemented administrative measures to ensure that only authorized persons have access to confidential information. Google, for example, explains it this way:

We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.⁹³

Online merchants also specify that they take care to protect consumer payment card data.⁹⁴ Amazon tells customers:

We reveal only the last four digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.⁹⁵

Many companies say they monitor their systems continuously in order to identify and respond to security flaws. The vast majority stipulate that the data they collect on their users may be

91. We found such mentions in particular at: LinkedIn, Google, Yahoo, Microsoft Outlook (Hotmail), Skype, WhatsApp, Amazon, Walmart, Costco, Hudson's Bay, Best Buy, Netflix, Prime Video, Spotify, Crave TV, Apple Music, Royal Bank of Canada, TD Bank, Scotiabank, Bank of Montreal, Desjardins.

92. <https://help.netflix.com/legal/privacy>

93. <https://policies.google.com/privacy>

94. This is notably the case with: Amazon, Walmart and Best Buy.

95. https://www.amazon.ca/-/fr/gp/help/customer/display.html?language=en_CA&nodeId=202056900

used to prevent fraud or to detect any other unauthorized use of the person's account.⁹⁶ Apple, for example, says it analyzes consumer activity data to establish a "confidence index" that permits it to assess the risk of fraud:

To help identify and prevent fraud, information about how you use your device, including the approximate number of phone calls or emails you send and receive, will be used to compute a device trust score when you attempt a purchase. The submissions are designed so Apple cannot learn the real values on your device. The scores are stored for a fixed time on our servers.⁹⁷

The information companies publish about their security measures is not only very fragmented, it is also poorly emphasized. Most often, it is found buried inside documents that are difficult to access. This suggests that most companies do little to make information security a primary argument in convincing consumers to opt for their services.

2.2.2. A marketing argument

While the majority of companies do not publicize their security measures very much, there are a few exceptions that sing the praises of the security measures they employ. These companies, in their representations, use data security and privacy protection as marketing arguments to gain the trust of consumers.

One notable case is Apple. This company details its security measures extensively and lauds the security of its products. Among the security methods it cites are end-to-end encryption, the use of random identifiers, restriction of transmitted data, and even artificial intelligence.⁹⁸ The company also posts a lengthy document entitled "Apple Platform Security," which describes its security practices in detail.⁹⁹

Similarly, the WhatsApp messaging service immediately introduces itself as a secure option for consumers. On its home page, the company calls attention to its use of encryption methods:

When end-to-end encrypted, your messages and calls are secured so only you and the person you're communicating with can read or listen to them, and nobody in between, not even WhatsApp.¹⁰⁰

Finally, financial institutions are also set apart by the fact that their websites generally contain more material about their practices and security measures. It is common for financial institutions to promote the security of their services, as in the case of Desjardins, which

96. We have found such clauses in particular at: Facebook, Instagram, LinkedIn, Twitter, Snapchat, Costco, Google, Yahoo, Microsoft, Skype, WhatsApp, Netflix, Spotify, Apple, Royal Bank, TD Bank, Scotiabank and Bank of Montreal. Some companies, including Facebook, also say they can exchange information for this purpose with "third party partners."

97. <https://support.apple.com/en-au/HT210584>

98. <https://www.apple.com/ca/privacy/features/>

99. <https://support.apple.com/en-ca/guide/security/welcome/web>

100. <https://www.whatsapp.com/security/>

announces “Identity Protection” for its clients.¹⁰¹ Considering the risks associated with online financial transactions, one can understand why these companies need to reassure their customers.

That said, the fact remains that, regardless of what information the company discloses about its security measures, consumers have neither the knowledge, the time, nor the resources to verify by themselves a company’s level of security and the veracity of its claims. Even if a company does publicize its security measures, users will still be at a loss to determine whether it is meeting its commitments and whether the security measures it employs are adequate. In such a context of information asymmetry, consumers who need to use the services of online businesses ultimately have little choice but to trust them.

2.3. Unequal sharing of responsibilities

Companies’ user agreements may stipulate a number of obligations that consumers must comply with regarding the security of their account (section 2.3.1). These same contracts, however, may also contain numerous clauses devised to exonerate the company from its responsibilities in security matters (section 2.3.2).

2.3.1. The consumer’s obligations

Companies generally state in their user contracts that the consumer has a significant share of responsibility for the security of their data.

Almost every contract we analyzed includes the general obligation for consumers to protect access to their account.¹⁰² Amazon, by way of illustration, states this in these terms:

You are responsible for maintaining the confidentiality of your account and password and for restricting access to your account, and you agree to accept responsibility for all activities that occur under your account or password.¹⁰³

More specifically, several companies forbid the user to share their password with others or reuse it elsewhere for other online services, and even require the choice of a strong password, “that is unique to you and not easily guessed by others¹⁰⁴.” Google, for instance, places responsibility for the password onto the consumer in these terms:

101. <https://www.desjardins.com/ca/security/desjardins-identity-protection/index.jsp>

102. We found such mentions in particular at: Facebook, LinkedIn, Twitter, Snapchat, Google, Yahoo, Microsoft Outlook (Hotmail), Skype, WhatsApp, Amazon, Walmart, Costco, Best Buy, Netflix, Prime Video, Spotify, Crave TV, Apple Music, Royal Bank of Canada, TD Bank, Scotiabank, Bank of Montreal, Desjardins.

103. https://www.amazon.ca/-/fr/gp/help/customer/display.html?language=en_CA&nodeId=201909000

104. <https://www.crave.ca/en/terms-and-conditions-84360459>

To protect your Google Account, keep your password confidential. You are responsible for the activity that happens on or through your Google Account. Try not to reuse your Google Account password on third-party applications.¹⁰⁵

A few companies occasionally stipulate various other obligations for consumers, such as logging out after using their platform, not leaving a public computer without closing a session, or not leaving their devices unattended. Netflix issues these caveats:

Where possible, users of public or shared devices should log out at the completion of each visit. If you sell or return a computer or Netflix ready device, you should log out and deactivate the device before doing so. If you do not maintain the security of your password or device, or fail to log out or deactivate your device, subsequent users may be able to access your account, including your personal information.¹⁰⁶

Best Buy goes further, warning consumers that they should not let a computer out of their sight when they are connected to their site:

once you have logged-on to the Website using the Codes, you will not leave the computer terminal used to access the Website unless and until you have terminated the session and logged-off the Website.¹⁰⁷

Finally, several companies also impose a condition on consumers to notify them as quickly as possible that their account has been compromised or when they suspect that its security might be compromised.¹⁰⁸ Walmart includes this statement in its Terms of Use:

You agree to notify Walmart Canada immediately in the event that the confidentiality of your account or password is compromised. Walmart Canada has the right to take any actions that it deems reasonable in such event provided that it shall have no liability for any acts or omissions in this regard.¹⁰⁹

Financial institutions are conspicuous for stipulating a host of contractual obligations for consumers related to information security. In addition to obligations similar to those of other companies, their contracts sometimes add very specific requirements concerning the behaviour that consumers need to adopt. For example, Scotiabank, among other things, requires its customers to comply by “using your own private wireless data connection, and avoiding use of public Wi-Fi services,” by “enabling the locking feature on your Digital Access Device” by “deleting, or having your wireless carrier delete, any Card credentials on your Mobile Device and/or SIM card prior to any voluntary transfer or disposal of your Mobile Device.”¹¹⁰

105. <https://policies.google.com/terms/archive/20171025?hl=en-CA>

106. <https://help.netflix.com/legal/privacy>

107. <https://www.bestbuy.ca/en-ca/help/policies-and-terms-and-conditions/conditions-of-use>

108. We found such clauses particularly at: Walmart, Costco, Best Buy, Crave, Spotify, WhatsApp, Apple, as well as in all financial institutions.

109. <https://www.walmart.ca/en/help/legal#TermsofUse>

110. <https://apps.scotiabank.com/digitalchannels/en/termsconditions-en-current.html>


Finally, it should be noted that every type of company forbids Internet users to make malicious use of their platforms or to test their vulnerabilities. However, some companies also say they have responsible disclosure programs, which give the public an opportunity to report security flaws and help companies beef up their security measures.¹¹¹

In sum, consumers who use the online services of the companies we have analyzed may have a multitude of obligations imposed upon them. Although the companies draw scant attention to these obligations, they could invoke them to accuse consumers of having violated them if their data is ever compromised. For example, many consumers use the same passwords on more than one service (see section 3.4.2), even though this violates the contractual terms of several of the companies.

2.3.2. Exemptions for the company

While companies impose security obligations on their users, many at the same time attempt to evade their responsibility toward them. In the contracts of almost every company we analyzed, we found various clauses that tend to limit their liability in the event of a breach of security.¹¹²

For example, financial institutions establish as a principle, in their representations and their contracts, that they will be responsible for losses in the event of unauthorized transactions. However, this commitment is conditional on consumers meeting their multiple security-related obligations as outlined previously.



You're protected.

In the unlikely event you experience a TD account loss resulting from a transaction through a TD online or mobile service, that you did not authorize, you will receive 100% reimbursement of those account losses provided you have met your security responsibilities.

Several financial institutions offer a “guarantee” of consumer protection against fraud. For example, on its website, TD Bank proclaims that consumers are “protected” against loss—on condition, however, that they have not breached any of their many contractual obligations.¹¹³

Of course, there is no such thing as absolute security. Several companies recognize that their systems cannot prevent every security breach and say so in their contracts. The Bay, for example, states:

111. See in particular: Desjardins, Apple, TD.

112 We found such clauses in particular at: Facebook, LinkedIn, Twitter, Snapchat, Google, Yahoo, Microsoft Outlook (Hotmail), Skype, WhatsApp, Amazon, Walmart, Costco, Hudson’s Bay, Best Buy, Prime Video, Spotify, Crave TV, Apple Music, Royal Bank of Canada, TD Bank, Scotiabank, Bank of Montreal, and Desjardins.

113. Such “guarantees” are offered by TD Bank, Scotiabank and Bank of Montreal.

While we make reasonable efforts to ensure that your information is secure on our system, no data transmission over the Internet can be guaranteed to be 100% secure. As a result, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk.¹¹⁴

Several contracts include non-liability clauses explicitly referring to situations in which a “loss of data” could occur.¹¹⁵ One might not be far wrong in believing that in the event of a security breach, the company could invoke such a clause in an attempt to avoid compensating consumers or to evade prosecution in civil court. Apple, for example, is very clear on this point:

APPLE DOES NOT REPRESENT OR GUARANTEE THAT THE SERVICES WILL BE FREE FROM LOSS, CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, OR OTHER SECURITY INTRUSION, AND YOU HEREBY RELEASE APPLE FROM ANY LIABILITY RELATING THERETO. YOU SHALL BE RESPONSIBLE FOR BACKING UP YOUR OWN SYSTEM, INCLUDING ANY CONTENT ACQUIRED OR RENTED THROUGH THE SERVICES.¹¹⁶

Most companies, however, recognize that such disclaimers will only apply to the extent permitted by law,¹¹⁷ which suggests that they might recognize the primacy of Canadian consumer protection laws over their contractual content (see section 4.2.3). Whatever the case, such stipulations cast doubt on the likelihood of companies being held liable in the event of a data breach.

2.4. Helping and informing consumers

Several of the companies we analyzed not only offer their users features designed to enhance the security of their accounts but also provide advice on cybersecurity. Companies that monetize consumer personal data on a large scale, such as Facebook and Google, as well as financial institutions, usually offer more in this regard. Conversely, we found hardly any such resources among players whose customers have a smaller digital footprint, such as Walmart, Costco, The Bay, Best Buy, Prime Video or Crave.

2.4.1. Optional parameters

Businesses may offer consumers various features to enhance the security of their online accounts.

The most common of these features is two-factor authentication, a method of securing online accounts that requires users, when they log on, to enter a code sent to their mobile phone in

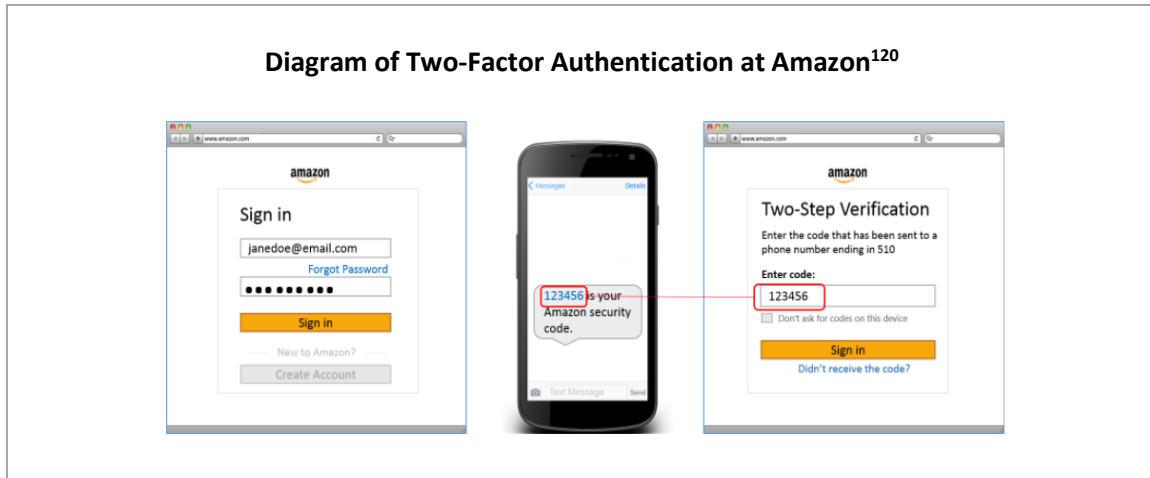
114. <https://www.thebay.com/TermsConditions.html>

115. We found such clauses in particular at: Facebook, Twitter, LinkedIn, Snapchat, Google, Walmart, Best Buy, Costco, Crave.

116. <https://www.apple.com/legal/internet-services/itunes/us/terms.html>

117. We found such clauses in particular at: Facebook, LinkedIn, Twitter, Google, Snapchat, Microsoft, Yahoo, Amazon, Walmart, Best Buy, Costco, Crave.

addition to their password.¹¹⁸ By default, no company enables this feature; likewise, it is generally not well publicized. Two-factor authentication is not always set up the same way in every company; some allow it to be used not only with a phone number or an email, but also with a mobile authentication app.¹¹⁹



In addition to two-factor authentication, companies may also offer various features to ensure more secure access to accounts. For example, Facebook offers a one-time password option, for situations when a user is concerned that their real password will be intercepted—such as when they are using a public network.¹²¹ Apple and certain financial institutions offer consumers a biometric solution for securing access to their accounts, that uses either fingerprint or facial recognition.

Some companies also include automatic alert or account monitoring functions. For example, Facebook issues an alert that notifies users when a connection is made by an unknown device, so that they can react if necessary.¹²² Companies also feature options that permit users to consult the list of devices connected to their account and disconnect from them remotely, or monitor all recent activity on their account.

To assist consumers in protecting their devices, some financial institutions offer free downloads of anti-virus or anti-malware software. For example, the Bank of Montreal offers its customers the malware protection software, Trusteer, as well as OnGuard, which monitors whether sensitive information is being posted on the Web.¹²³

In the event of an account being compromised, companies provide various methods for re-establishing access. Several companies offer the possibility of registering an e-mail address or a

118. We have found this functionality in particular at: Facebook, Instagram, LinkedIn, Twitter, Snapchat, Amazon, Google, Yahoo, Microsoft, WhatsApp, Apple, Royal Bank, TD Bank, Bank of Montreal, Desjardins.

119. Snapchat, for example, offers this: <https://support.snapchat.com/en-US/a/enable-login-verification>

120. <https://www.amazon.ca/hz/mycd/digital-console/privacysettings/>

121. This option is not available when the user has enabled two-factor authentication.

122. We have found features of this type especially on Google and Twitter. All financial institutions also offer alert functions to notify consumers of transactions posted to their accounts.

123. See: <https://www.bmo.com/main/personal/ways-to-bank/security-centre/how-to-protect-yourself/>

“back-up” telephone number, which can be used to gain access to the account; they may also issue a recovery code that the consumer can use should their account be compromised. Facebook also allows users to designate trusted contacts to help them reconnect in the event of a problem.¹²⁴

Finally, to help users navigate through these various features and privacy settings, some companies provide interfaces that allow users to configure them all *en bloc*.¹²⁵ For example, Facebook offers “security verification,” which permits users to define several privacy settings on the same platform in one procedure. This simple and effective type of formula suggests an interesting avenue for making life easier for consumers and ensuring that they configure their settings properly.

2.4.2. Cybersecurity advice

The majority of companies publish security tips and advice on their websites for their users.¹²⁶ In most cases, the company does not prominently display hyperlinks to this information on its website. At Amazon, for example, one has to browse through the tree structure of the website’s help pages to find it.¹²⁷

The information offered by companies generally covers one or more of the following broad topics:

- **Advice for securing your account,**¹²⁸ which may include tips for protecting and choosing your password, a reminder to log off after using the service, or information about the security settings offered by the company, such as two-factor authentication.
- **Advice for protecting your computer system,**¹²⁹ especially by installing an antivirus software, by avoiding connecting to public Wi-Fi networks for banking transactions or by regularly updating your software.
- **Warnings against the most common malware and scams,**¹³⁰ especially against phishing. Financial institutions generally provide the most information on this subject, in particular by reminding consumers not to respond to messages requesting access to account information.

124. See: <https://www.facebook.com/help/119897751441086>

125. In particular, Facebook, Google and Desjardins.

126. Many even have a section on user security. Yahoo, for example, has a very detailed “safety center”: <https://safety.yahoo.com/index.htm>

127 See: https://www.amazon.ca/gp/help/customer/display.html/ref=hp_bc_nav?ie=UTF8&nodeId=GRFTMVHP4HXMESSP

128. We found this type of advice in particular at: Facebook, Google, Snapchat, Netflix, Spotify, Apple, Yahoo, Microsoft, Desjardins, RBC Bank, TD Bank, Scotiabank.

129. See in particular: Facebook, LinkedIn, Amazon, Netflix, Desjardins, RBC Bank, TD Bank, Scotiabank.

130. See in particular: Facebook, LinkedIn, Snapchat, Microsoft, Google, Apple, Amazon, Spotify, Netflix, Costco, Desjardins, RBC Bank, TD Bank, Scotiabank.

- **Instructions and advice in the event of inability to log on to the account or when you believe you have been hacked.** Some sites may also address the issue of fraud or identity theft and how to respond to it, or, in the case of financial institutions, lost or stolen bank cards.
- **Finally, some companies are particularly interested in security threats posed by other users on their platform.**¹³¹ Instagram, for example, has a section that outlines ways to protect yourself from malicious users.¹³²

Overall, these tips and tricks are just common sense and remain relatively similar from company to company. However, the issue of protecting consumer access credentials carries extra pitfalls. Indeed, in addition to asking consumers to choose strong, unique passwords, several companies recommend that they change their passwords on a regular basis.¹³³ For example, Amazon puts it this way:

To protect your password, it's important to change it periodically and not share it, because anyone who knows your password can access your account. We recommend that you change your password every 30 to 60 days.¹³⁴

This all means that every consumer, in order to comply with all these requirements, should not only have a host of complex passwords for each company with which they have an account, but should also change them constantly. Given the very large number of online accounts the average Internet user is likely to have, it is understandable that requiring full compliance with such recommendations is unrealistic and conducive to consumer errors and omissions.

To alleviate these difficulties, a few companies recommend the use of a password manager.¹³⁵ However, recommendations in this regard may differ from one company to another. For example, the Royal Bank invites its customers to use such software¹³⁶; in contrast, Scotiabank urges its customers to avoid “using software that records your passwords and remembers them the next time you access the website from the same computer. This type of software could give anyone who uses your computer access to your accounts.”¹³⁷

131. We found such mentions at: Facebook, Instagram, Twitter, Snapchat, WhatsApp.

132. <https://about.instagram.com/community/safety>

133. We found such mentions at: LinkedIn, Amazon, Yahoo, Netflix, Microsoft, Skype, Spotify, Apple Desjardins, TD Bank.

134

https://www.amazon.ca/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=GRFTMVHP4HXMESSP

135 See: Amazon, Netflix, RBC Bank.

136 <https://www.rbc.com/cyber-security/how-to-protect-yourself-online/index.html>

137 <https://www.scotiabank.com/ca/en/about/contact-us/security/security-tools-and-tips/computer-security.html>

3. From the consumer's perspective

In this research, we wanted to better identify the experiences, knowledge and perceptions of consumers with regard to security breaches, what protective behaviour to adopt and their contractual obligations towards companies. To achieve this, we conducted two complementary procedures: a survey and focus groups.

The survey was carried out with 2,000 Canadian Internet users aged 18 and over who spoke English or French.¹³⁸ It was conducted over the Internet from May 19 to 28, 2020, with the assistance of the firm BIP. Respondents were selected so as to be representative of the entire Canadian population in terms of gender, age, region, mother tongue and level of education. Most survey respondents (71%) said they spend more than 10 hours a week on the Internet, while 13% said they spend more than 40 hours a week. Among the most common activities were messaging or email services and banking transactions¹³⁹:

Messaging or email services	88%
Banking transactions	80%
Social media	76%
Shopping	74%
Streaming content	47%

To complete this survey, we conducted 7 focus groups via videoconference with 38 Canadian Internet users.¹⁴⁰ Two of the groups were made up of participants from Québec, two others of participants from Ontario, two others of participants in the Maritimes, and one final group of participants from Alberta and British Columbia.¹⁴¹ The groups were composed of men and women between the ages of 18 and 70 with varying levels of education. They included workers, retirees, students and people looking for work.

We present below a concomitant analysis of these two methodological approaches, emphasizing the salient points of the results obtained.

138. The report of the firm BIP can be found in Appendix 1.

139. Not surprisingly, age, occupation and income have an influence on the most popular type of activity. People between the ages of 18 and 54 are more likely to use internet banking, shop online and use social media. Conversely, people aged 55 and over are more likely to use it for email and messaging services. On the other hand, people who are employed and those with the highest incomes do proportionately more banking, shopping and transactions online.

140. The discussion guide for these groups can be found in Appendix 2 (French) and Appendix 3 (English). The firm BIP had the mandate of recruiting the participants and holding the focus groups. These took place on October 13, 2020 (in French) and October 14, 15 and 19, 2020 (in English). Due to health restrictions enforced to counter the COVID-19 pandemic, it was not possible to meet these groups in person.

141. In each region where there were two groups, one was made up of individuals 45 and over and the other of individuals under 45.

3.1. Consumers are concerned

According to our survey, two-thirds of Canadians (66%) are afraid that a company they do business with online could be the target of a security breach within the next two years.¹⁴² These findings echo those of other polls showing that Canadians are concerned about the safety of their personal information on the Internet.¹⁴³

In the focus groups, consumers showed that their level of concern varies depending on the type of company involved. The data most important to the participants is their banking information. Some are particularly worried about using their bank's mobile app, and fear that of transactions made via this interface are not as safe as those made over a computer with a secure link.

Despite these concerns, the ease of doing business online wins out for many consumers. Most are aware that Internet banking carries some risk, but they seem willing to accept it. In addition, some argue that transactions through other channels, such as an ATM, are probably no more secure since all the personal and banking data is still stored in one place:

Obviously, I'm concerned, just like everyone else. On the other hand, I don't believe that doing online transactions exposes me more. Whether I have AccèsD or not, Desjardins knows how much money I have in my account and on what day the transactions are made. This information is not public, but is in the cloud in an abstract kind of a place. (Québec, ages 18-44)

Respondents in the focus groups also expressed concern about the way their personal data is stored and used by social media. The information available on these platforms—which includes personal photos and those of their children, personal information such as vacation periods, places near home or their birthdays—is considered to be sensitive information that is very attractive to criminals:

I'm quite concerned about what everyone pushes on social media. If anybody wants to get all your information, they have your birthday, your address, if you're travelling, where you work. That scares me because it's such personal information. If you had surgery, people post it, they post their kids' names, their age, the school they go to. There's so much personal information there that if someone wants to do ID theft, all the information is there. I find that really scary. I used to post occasionally, if I was leaving on a trip I'd tell it and there's this big advertisement that my house was going to be empty because I'm gone. Now I don't give out that personal information anymore for all to see. (Ontario, ages 45-70)

142. This result echoes the survey conducted by Norton, in which 64% of respondents said they believe they will be the target of cybercrime in the next few years: Norton LifeLock, *Cyber Safety Insights Report Global Results*, 2019, p. 21-22.

143. According to CIRA, 87% of Canadians are concerned that organizations that hold their data could be subject to a cyber attack; similarly, 78% of Canadians have concerns about the cybersecurity of connected objects. See: CIRA, *Canadians Deserve a Better Internet*, 2019, <https://www.cira.ca/resources/state-internet/report/canadians-deserve-a-better-internet>. According to Norton, 72% of Canadians are more alarmed than ever about the protection of their privacy. See: NortonLifeLock, *Cyber Safety Insights Report Global Results*, 2019, p. 16.

In contrast, the respondents showed little concern over the security of their data with online merchants, streaming content sites or email services. Many were of the opinion that the information they give out during an online purchase, namely their postal address, their credit card number and the type of purchase made, is of little value and is not very sensitive:

If I order something on the Internet, what do they steal? My name, my address and my postal code, the amount of my purchase. I don't usually gave them anything else. I still use the credit card, they have my number, but nothing bad has happened so far. The information they have on me is still quite limited. (Québec, ages 18-44)

In addition, our survey indicates that two-thirds of respondents say they trust companies (66%) or government agencies (63%) to protect their data. This level of confidence is mainly manifested among older people and those with higher incomes.



In focus groups, the participants again showed differing levels of confidence depending on the type of business in question. Despite their concerns about their financial data, they claim to trust financial institutions. Most consumers believe that banks are among the safest businesses and that it is in their best interest to protect the security of their customers' data, for their own sake. One remark often heard was: "If banks are not safe, what organizations are?"

Contrary to what was said about banks, the level of trust in social networks is low: similarly, confidence in streaming sites and online merchants remains mixed. Several consumers complained that many of these companies use their data for advertising purposes. Although most respondents understand that they have to agree to give access to their personal data in exchange for the "free" service provided by social media, they find such business models irritating:

What bothers me is that my activity is continually monitored. The reason it's free is because they're selling us, the users. We give them all this data for free in exchange for this platform and everything we find positive about a social network. But it bothers me when they tell me that I shop for such and such at such and such a time, and that I'm a 41-year-old girl. It's all this gathering of information, even if it's anonymous; it bothers me that they're in my private space, monitoring me. (Québec, ages 18-44)

In this context, several participants told us they either avoid social networks in general, avoid certain social networks such as Facebook, or are cautious about the information and photos they post. Nevertheless, many respondents have the impression that the “toothpaste is out of the tube” and that, intentionally or otherwise, they leave digital footprints all over the Web:

In reality, we have no control over what information people want to collect. Whatever we do on the Net, we leave traces everywhere. How do you go back and correct things? It’s almost impossible. No matter what policies we adopt, we remain at the mercy of people who can use data that we’ve voluntarily left lying around everywhere. (Québec, ages 45-70)

We detected a feeling of resignation among several participants. For these people, it is just a fact of modern life that we have to deal with certain companies and provide them with personal information (e.g., giving a social insurance number in order to receive a salary or open a bank account). Several participants suggested that in order to do business with certain companies, no one has any choice but to accept their policies in this regard.

3.2. An unsuspected scale

As we have seen, the number of consumers affected by security breaches in Canada is significant (see section 1.3). However, the results of our survey suggest that many people are simply unaware that they have been the victims of a security breach.

Given the huge amount of media attention focussed on the data breach at the Desjardins cooperative, we first looked at the percentage of Canadians who say they were targeted in that incident. One in six Canadians, or 16% of respondents (or one in three Quebecers, 31%), say they were a victim of the security breach at Desjardins.

Almost a third (31%) of respondents said that a business other than Desjardins, whose Internet services they use, has already had a security breach.¹⁴⁴ This proportion appears to be well below the number of security breach victims in Canada, which the OPC estimates at 28 million in 2018 alone. This suggests that a significant proportion of the Canadian population simply does not know whether they have been a victim of a data breach.

Excluding Desjardins, the companies most often mentioned by people claiming to have been the target of a security breach are as follows:

Capital One	16%
Yahoo	10%
LifeLabs	8%
Facebook (including Messenger)	7%

144. Other polls point to similar results, even though the questions are worded differently. According to CIRA, 32% of Canadians say they have been the victim of a successful cyberattack and 15% say they don’t know: <https://cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019>

Equifax	6%
BMO	6%
Marriott Hotels	5%
Don't know / Don't remember	9%

Our results reveal statistically significant differences in age, education and income. People aged 18 to 54 are more likely to say that a business whose online services they use have been the target of a security breach. The same is true for people with a university education (41%), for employed people (37%) and for people with an income of over \$100,000 (38%).

Finally, the results of our survey show that only 37% of respondents believe that their data was compromised as a result of the security breach at the company, and a third (34%) do not know if this was the case. Similarly, while one in six Canadians (14%) say they have been a victim of identity theft, only half (48%) believe that this identity theft was the result of a security breach that occurred in a company whose online services they use.¹⁴⁵ These results seem to indicate that consumers have little or no information about what happened to their data following the security breach.

The participants in the focus groups nevertheless admit that it is possible that they may have been victims of security breaches without their knowledge. By way of illustration, several people affected by the security breach at Desjardins mentioned that they were not notified until several months after the data theft, and that they might never have known if it had not been for the media coverage. In fact, if companies do not notify their customers about a security breach, how will they know it has happened?

Believing that these are situations beyond their control, most participants said they try to adopt safe behaviours and hope that the worst does not happen: “I believe I’ve done what I functionally know how to do to be safe, and beyond that there’s no point of worrying about it” (Maritimes, ages 45-70). It seems certain that the respondents here also seem resigned to the fact that they will very likely have to suffer a data breach one day, no matter what they do to protect themselves: “I’m pretty sure it will happen, but I don’t lose any sleep over it” (Québec, ages 45-70).

3.3. Knowledge gaps

The results of our study indicate that consumers know very little about companies’ cybersecurity practices, are unaware of many of their contractual obligations toward these companies, and rely heavily on them to ensure the security of their data. In addition, our study indicates that the need for information about cybersecurity appears to be greatest among groups generally considered to be the most vulnerable.

145. This proportion is higher than that found in other studies. According to Public Safety Canada, 5% of Canadians say they have been victims of identity theft. See: Public Safety Canada, *Cyber Security Internet User Survey*, Canada, 2018, pp. 53-54.

3.3.1. Information asymmetry

A majority of survey respondents (54%) said they do not find out about a company's cybersecurity practices before using its online services. Similarly, half (49%) said they do not read the cybersecurity advice given by these companies. We also noted that only 14% of respondents say they "always" read and 42% "sometimes" read the user agreements and confidentiality policies before subscribing to a service.

Participants In the focus groups scarcely knew what to answer when asked what security measures the companies have in place to ensure their data is protected. Generally speaking, the protection systems and other internal security measures are not well known.

Consumers assume that measures probably vary from company to company. Some hazarded a guess that companies could block employees' access to a customer's entire file (e.g., prevent anyone from seeing a social insurance number), protect their servers with firewalls, or even encrypt recorded data.

They do the encryption of our data, when it reaches them and what they send back to us. It scrambles our information. And they have firewalls and things like that, they're all relying on them to have a secure network that will hopefully not be penetrated. That is the only things I can think of. (Alberta/British Columbia, ages 18-70)

Several participants also cited user account settings, suspicious login alerts, the requirement to use a strong password, two-factor authentication, the use of security questions, or the use of the HTTPS protocol.

In addition, the vast majority of focus group participants confirmed that they do not read or only very partially read the companies' privacy policies.¹⁴⁶ They criticized these documents for being too abstract, for taking too long to read and for being expressed in difficult-to-understand legal jargon. Many said they feel that these policies are there mainly to protect the company (rather than its customers) and that they cannot prove that what they state is true:

I think most of the serious sites post a legal statement and the company's policies. I don't know a soul who has read these texts, because they're endless and there are pages and pages of them. All you have to do is go to the bottom of the declaration and check the box that says you've read it. I guess I do like everyone else: I check the box and move on. (Québec, ages 45–70)

Another participant added:

Look at their terms of service and then see if you can understand it. It details as much as they're going to tell us. And even if they tell us, how would we know that we understand it, how would we know that it's authentic, how would we know it's credible? The knowledge threshold required to be able to vet that, I hope they're doing it right. I don't know if the average person can understand it; no different than an insurance policy. Do

¹⁴⁶. Nonetheless, a few focus group respondents said they read a company's policies when the transaction involves a large amount of money or when the contract extends over a long period.

you actually know what you're insured for or do you find out when you need it?
(Maritimes, ages 45-70)

Even though they do not read the privacy policies that they are asked to agree to when opening an account, several respondents believe that they do contain a description of their cybersecurity practices. This led many to say that companies should be legally obliged to issue clear policies that can be read quickly and are easy to understand.

In short, our study shows that consumers do not know what the practices of companies are when it comes to data security, and are therefore not in a position to formulate a judgment as to the level of protection they could expect if they chose to do business with one of them. Despite not knowing what the actual practices of a company were, the participants said they chose to allow it to take care of their data because they trusted its reputation or believed that the site was secure:

I assume that companies like Facebook, Microsoft, and Yahoo have hundreds and thousands of people monitoring. Recently on Facebook, I got a message saying "there was an attempt at this location that somebody tried to log into your account." They always tell me to reset my password right away. I feel they are looking at it. (Ontario, ages 18-44)

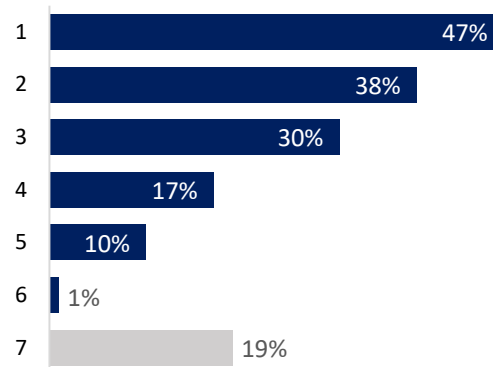
Some consumers feel that smaller companies are probably less secure: "With the smaller ones, you have your doubts a little, but the larger ones, you feel they must have a huge cybersecurity department protecting them. But overall, I need a product and I require it so it's a catch-22, I do it and hope for the best" (Alberta/British Columbia, ages 18-70). However, many saw Desjardins as an example of a large, reputable company that supposedly had several security measures already in place, but nevertheless suffered a massive data theft by one of its employees.

3.3.2. Reach out to the most vulnerable

Our study indicates that cybersecurity information needs are greater among groups generally considered to be the most vulnerable, such as seniors or low-income people. Accordingly, any cybersecurity awareness strategy should take the special situations of such consumers into account.

Almost half of respondents said they get information from the media and Internet about what to do to protect themselves from online threats:

Where do you go to find information about how to protect yourself against online threats?



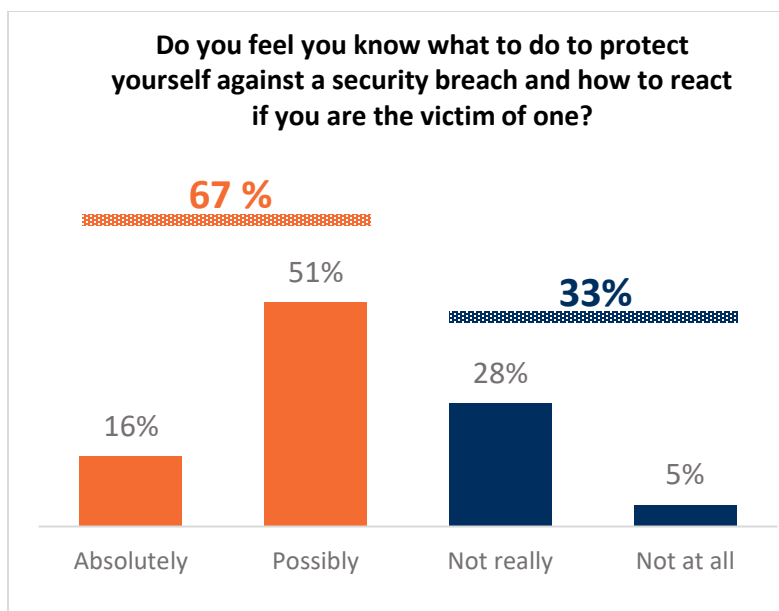
However, even though the Internet is the most common source of information for respondents, our results show statistically significant differences in terms of age, education and language. People aged 65 and over, as well as those with the lowest level of education, are least likely to obtain information from the media and the Internet. On the other hand, people whose mother tongue is English are more likely to seek information from companies.

These results are consistent with the findings in the literature, which indicate that when it comes to cybersecurity, the information strategies deployed must be adapted to target audiences. Studies show that seniors, who are more vulnerable to phishing attacks and other online scams, would prefer to receive in-person training to learn about computers and cybersecurity¹⁴⁷. Likewise, rather than turning to experts for information on cybersecurity, people with less education rely on members of their community, especially friends or family.¹⁴⁸

We should also mention that about two-thirds of our survey respondents (67%) said they feel they know how to protect themselves against security breaches and how to react if they fall victim.

147. Daniela Oliverira et al., *Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing*, CHI Conference on Human Factors in Computing Systems (CHI 2017), 2017; James Nicholson, Lynne Coventry and Pam Briggs, "If It's Important It Will Be A Headline": *Cybersecurity Information Seeking in Older Adults*, CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), 2019.

148. Ibid.



Here again, we note that people aged 65 and over, as well as those with the lowest incomes, are most likely to answer this question in the negative. In short, our results suggest that the groups generally considered to be the most vulnerable obtain information from channels other than the media and the Internet; correspondingly, they feel they are less able to cope with security breaches.

3.4. Consumers sometimes reckless

Our study revealed that consumers sometimes behave recklessly when it comes to taking precautions to protect themselves from online threats and managing their login credentials.

3.4.1. Precautions taken

In our survey, we asked respondents about the precautions they take to protect themselves from online threats. The behaviours most often mentioned are:

Do not download attachments in emails from strangers	71%
Protect your personal Wi-Fi network with a password	66%
Don't accept people you don't know as friends on social media	64%
Use antivirus software	62%
Make online transactions over secure networks	60%
Limit the information you share on social media	57%
Regularly update your software	52%
Delete cookies on your browser	49%
Use a virtual private network (VPN)	18%

Subscribe to a fraud monitoring system (e.g., Equifax)	17%
Use an encrypted messaging service	16%
Other	1%

We remarked some statistically significant differences among the youngest respondents. In fact, people aged 18 to 44 are the least likely, proportionally, to say they follow all these precautions. Interestingly, however, it is these same consumers who most often claim that they find out about the cybersecurity practices of the companies they do business with.

In the focus groups, we asked participants to self-assess their level of caution when using online services. The majority of respondents considered themselves to be “very” or “somewhat” safe online, even though they also felt they could do better. For example, the vast majority of focus group participants were able to identify behaviours that they considered appropriate to protecting their data, such as avoiding re-using their password on different sites, clicking on suspicious links or even disclosing too much personal information on social media. However, several admitted that they do not always apply these precautions.

That said, several participants also believe that it is impossible to protect one’s self completely from fraudsters since, in their opinion, the simple fact of being on social networks or doing business online exposes you to fraud or identity theft:

When you agree to go online, to shop, to have accounts and social networks, you are giving up something that you no have control longer over. You have to accept that you are putting yourself in danger. Even though I’m careful, I still use these platforms. Once I give out the information, it’s no longer mine, it belongs to the owners of the platforms and perhaps to the malicious individuals who will try to get hold of it (Québec, ages 18-44).

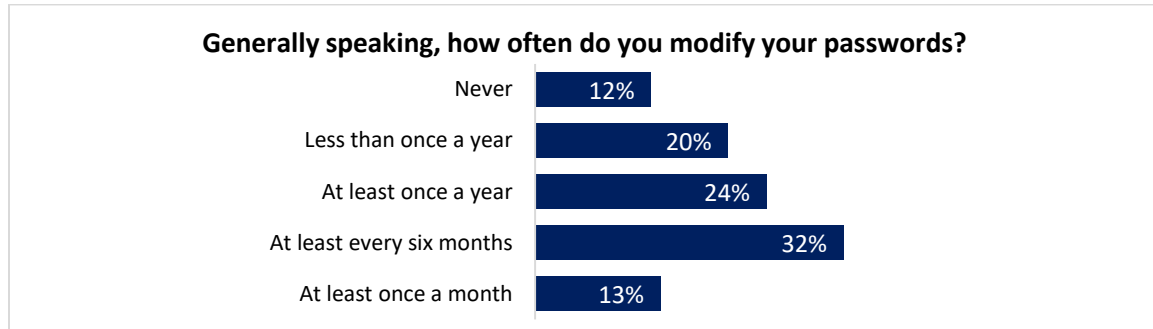
In short, while the majority of consumers are able to name several practices they could adopt to better protect their data, there is a certain nonchalance among consumers, who do not all seem to adopt such practices.

3.4.2. Protecting login credentials

Several of the questions in our survey focused on consumer practices with regard to protecting the login credentials they use to connect to their accounts. Right away, 77% of respondents said they use two-factor authentication when the company offers this option.¹⁴⁹ Similarly, 23% said they use a password manager and 40% said they use a biometric identifier, such as a fingerprint or facial recognition, to sign into their accounts.

149. By comparison, a Public Safety survey in 2018 reported that only 36% of Canadians used this method of protection. This discrepancy can be explained by the fact that our question asked if consumers activate it “when companies offer this option”; we suspect that respondents underestimate the number of sites offering this functionality, because it is often not well publicized (see section 2.4.1). See: Public Safety Canada, *Canadian Internet Use Survey*, 2018, p. 46.

We have noted certain behaviour among consumers that may be considered reckless or at least, contrary to the contractual obligations of certain companies regarding the management of their passwords. For example, 20% of Canadians admit to sharing a password with other people. More than half of Canadians say they use the same password on multiple accounts (58%) or store their passwords in written form (55%). Finally, nearly a third (31%) of Canadians say they change their passwords less than once a year, if ever.



This means that a considerable proportion of consumers do not follow all the advice that companies give them with regard to choosing and managing their passwords, particularly as regards the prohibition on sharing them, reusing them, or changing them frequently (see section 2). Note that for all these behaviours considered to be reckless, the youngest groups are proportionally over-represented.

The focus groups gave us a better understanding of consumers' objections to using certain methods of protecting their online accounts. Many said they were suspicious of password managers and doubted that these would protect them any better, because criminals only need to find one password to then gain access to all of them:

I don't use password managers because I think they can be hijacked or pirated just the same. I try to use pretty much the same passwords all the time, but with variations: upper case, lower case, replacing letters with numbers, and vice versa. I'm counting on my memory for now; when I'm older, we'll see (Québec, ages 45-70).

Another consumer adds:

I actually have a concern on the reliability of such programs. I have the same fear: what happens if I write down my passwords, it's the same thing. Somebody has access to the passwords (Ontario, ages 18-44).

The focus group participants also had mixed feelings about the use of two-factor authentication.¹⁵⁰ This procedure is considered useful for accounts containing sensitive or important information, such as bank accounts, investment sites or payment applications. Some

150. Note that even after having the definition read to them, some respondents seemed to confuse two-factor authentication with access notifications from another device.

participants find that this type of protection adds a level of security that reassures them and gives them a good impression of the company:

It's like a safety check. I quite like it because hopefully, no one else is going to be sitting there with my phone. It gives me that sense of security. You feel you're dealing with an organization that takes security seriously. They're considering me as the end-user and they're protecting me, as well as them (Alberta/British Columbia, ages 18-70).

However, many consumers do not like this type of protection because it makes the login process cumbersome and is considered unnecessary for some accounts, such as social networks, e-commerce, or online games. Some respondents are also annoyed that it is up to them to protect their data, as they believe that this responsibility should be borne by the companies:

I get a little fed up of waiting for the code sometimes. It used to be easier. I know it's safer, but I'm not entirely convinced it's going to be of any use. I don't know if the effort is being put in the right place. Why should I worry about protecting something that should be up to the company to be protecting? Whose responsibility is it? (Québec, ages 45-70)

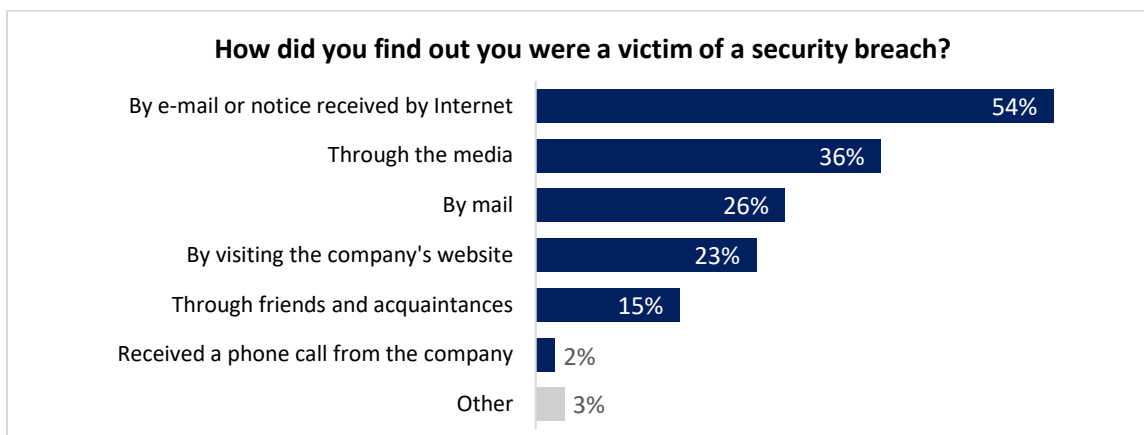
The focus groups also helped confirm the sometimes reckless practices of consumers when it comes to managing their passwords. Few participants said they regularly change their passwords; those who said they did explained it was only for the passwords they consider more important, such as their bank accounts. In addition, although most respondents said they do not share their passwords, a few admitted doing so with their spouses.

In addition, a large number of respondents write down their passwords in a notebook they keep at home or in an electronic document they save on their computer. Several also indicated that they save their passwords in a mobile word processing application, a behaviour that they recognize as being insecure. A few of these respondents explained that they do not always enter the password in full, but use, for example, a letter that reminds them of the first word in the password; they say they can be confident that their passwords will be protected even if someone accesses their document.

Participants who say they do not write down their passwords tend to have difficulty remembering them. To help them remember, they always use the same two or three passwords, with some variations. Many admit to choosing a password with a symbol-number-letter combination only when the sites oblige them to do so. Others said that they never log out of their accounts, so they don't have to re-enter their passwords—and when they get disconnected in spite of themselves, they click on “forgot password” and create a new one.

3.5. Following a security breach

Finally, our study looked at what happens to consumers after a security breach. In our survey, approximately 7 in 10 victims of a security breach in a company were contacted by the company, whether through an email, a letter or a phone call. About a third say they learned about it through the media.



Of those who said they had been victims of a security breach, 65% said they were satisfied with the way the company handled the situation. On the other hand, 35% said they stopped doing business with a company after learning that it had suffered a security breach.¹⁵¹

The participants in the focus groups said that their decision about whether or not to stop doing business with a company depended on the extent of the breach:

It depends on how severe the breach was. If it wasn't, I would just change my password and probably my security questions too. If it was very severe and there was a chance of them getting into my banking or my credit card then I would close the whole account, although they may have already gotten it (Maritimes, ages 18-44).

Respondents to the focus groups also said they expected transparency from companies targeted by a security breach. They believe that the company should make a public announcement explaining that a breach has occurred, and ideally, should apologize. It should also communicate directly with each of the clients affected, to advise them of the situation:

They have to do both because sometimes because let's say 1,000 customers may be a victim of a security breach and calling 1,000 customers will take time, maybe the quickest way to inform all the clients would be to publicly accept the fact that their security has been breached. So, all the customers, not only victims, can take measures, like checking if there is any unusual account activity. In the meantime, the company can call all the affected customers and inform them about the incident (Ontario, ages 18-44).

Such transparency increases customers' confidence in the company, thus demonstrating that it assumes responsibility. Some respondents wonder whether companies are legally obliged to disclose a security breach, but feel that they should be and that the announcement should be made as soon as possible after the breach:

151. This result is higher than that obtained in a CIRA poll, in which only 19% of Canadians said they would continue to do business with an organization that has suffered a security breach. See: https://www.cira.ca/sites/default/files/2019-06/canadians-deserve-better-internet_EN.pdf

I think it does more damage not to reach out. If you find out it happened and they didn't let you know, right away you lose trust, you want to pull out all your business from that company, versus if they reached out, you would be forgiving (Maritimes, ages 18-44).

Other participants said they want to know what the company will do to rectify the situation in the future to ensure that it is safe from security breaches. And if any customers should incur a monetary loss as a result of the breach, the respondents expect the company to reimburse all costs attributable to it. They do not believe that customers should pay in such situations.

Our survey also looked at the precautions consumers took when they learned there was a security breach in a business. The most common approach taken by participants was to change their passwords for their online accounts (64%). The other most common precautions are checking one's credit report, turning on two-factor authentication, and finding information on how to protect one's self.



In the focus groups, we again asked consumers what people should do when they learn that they have been the victim of a security breach. As in our survey, most respondents said that they should first change their password:

I think I would change my password, that would be my first thing. Then I would check. If it was Amazon I would also remove my credit card information that was already in, when you place an order you don't have to put in your credit card every time. I would check my bank accounts and make sure that no one went on a shopping spree on me. Besides that, there's not really much you can do (Ontario, ages 45-70).

Other behaviours to adopt following a security breach were suggested, such as subscribing to a credit agency's monitoring service, examining transactions on your bank accounts and credit cards, checking your credit report regularly, deleting the credit card registered in the company's file (if applicable) or cancelling your credit card and obtaining a new one:

Checking our credit report is something to do regularly to spot as quickly as possible if our data has been misused, even if we change financial institutions (Québec, ages 45-70).

Our survey also indicates that, in one out of ten cases, people say that they simply did not take any action after learning that they had been the victim of a security breach. Among the people most likely not to have taken any steps, we find Québec residents (17%), people with less education (18%), unemployed people (18%) and people having neither French nor English as their first language (18%).

Finally, we asked the participants of the focus groups what their recourse is in the event of a breach of security in a company they do business with. Most of them say they don't feel they have much recourse, except perhaps in the event of a credit card fraud. As far as they know, the steps to obtain compensation have to be undertaken by the victims, a process that some respondents find tedious.

4. Legal aspects of security breaches

According to Canadian privacy laws, companies that store consumers' personal data are obliged to adopt adequate security measures to protect them from security breaches (section 4.2). In addition, they must comply with obligations provided for in those laws that also touch on the context of data protection (section 4.3). However, Canadian law is not sufficiently prescriptive or dissuasive to promote effective prevention. Certain draft legislation, based in part on European standards, could point the way to some interesting solutions for Canada in this regard (section 4.5).

4.1. Information protected by law

In Canada, businesses that collect, use or disclose personal information for commercial purposes must comply with the information security obligations found in the *Personal Information Protection and Electronic Documents Act* (PIPEDA—hereinafter “The Federal Law”) or in other equivalent provincial laws.¹⁵²

The notion of “personal information” in these laws encompasses any information which, on its own or in combination with others, identifies an individual.¹⁵³ This definition has received a broad interpretation as a result of case law. It includes common identifiers such as the person's name, date of birth, address, or even their financial, medical or biometric information. It may also include various digital data collected by online businesses that, although not directly related to a person's name, could be used to identify them, such as the unique identifier of a mobile device,¹⁵⁴ an IP address,¹⁵⁵ geolocation,¹⁵⁶ the information contained in cookies¹⁵⁷ or a person's browsing history.¹⁵⁸

This means that the myriad of data collected by the companies in our study may, in general, be characterized as personal information within the meaning of the law (see section 2.1). As a

152. Under section 26(2) (b) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), SC 2000, c 5, the federal government may, by order, designate a provincial statute as being substantially similar to the Federal Law. Three provinces, Québec, Alberta and British Columbia, adopted laws which were subsequently designated as essentially similar: *An Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c. P-39.1 (hereinafter “Québec Act”); the *Personal Information Protection Act*, SA 2003, c. P-6.5 (hereinafter “Alberta Act”); the *Personal Information Protection Act*, SBC 2003, c. 63 (hereinafter “British Columbia Act”). See: *Organizations in the Province of Quebec Exemption Order*, SOR / 2003-374; *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219; *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220.

153. See in particular: *Gordon v. Canada (Minister of Health)*, 2008 FC 258; OPC, *Interpretation Bulletin: Personal Information*, October 2013.

154. OPC, *Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising*, PIPEDA Report of Findings #2013-017 20, 2013.

155. OPC, *Assistant Commissioner recommends that Bell Canada inform customers about Deep Packet Inspection*, PIPEDA Report of Findings #2009-010, September 2009.

156. OPC, *Use of Personal Information Collected by Global Positioning Tracking System*, PIPEDA Case Summary #2006-351.

157. OPC, *Customer complains about airline's use of 'cookies' on its Website*, PIPEDA Case Summary #2003-162.

158. OPC, *Use of sensitive health information for targeting of Google ads raises privacy concerns*, PIPEDA Case Summary #2014-001, January 14, 2014.

result, these companies will be subject to Canadian privacy laws — and will therefore be required to comply with their obligations with respect to data security.¹⁵⁹

4.2. The information security obligation

Under Canadian privacy laws, businesses have an obligation to take adequate measures to prevent data breaches. This obligation to ensure information security, which is expressed in a flexible way, could however be improved by the addition of more precise requirements aimed at urging companies to deploy more preventive measures.

4.2.1. The level of obligation

Canadian laws state that a company has an obligation to set in place security measures to protect the personal information it holds. According to the Federal Law, the company must thus protect the personal data it holds “against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.”¹⁶⁰

While the law is clear that companies must protect consumer data, it imposes no specific methods for achieving this, nor does it specify a precise level that this protection must attain. Rather, it states that the nature and degree of protective measures to be adopted will vary according to “the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage.”¹⁶¹ In short, the more “sensitive” the information processed by the company, the more rigorous its security measures must be.

However, evaluating the “sensitivity” of information, particularly in the digital environment, remains a perilous exercise. While the Federal Law explains that information relating to an individual’s health or personal finances will generally be considered sensitive, it adds that, depending on the context, any information may be sensitive.¹⁶² Case law has judged a variety of financial information to be sensitive, in particular, social insurance numbers¹⁶³ or information from a person’s credit report.¹⁶⁴ Likewise, many other types of information could be considered

159. In addition to privacy laws, there are other laws that may provide similar security obligations for businesses. For Québec, see in particular: *Act to establish a legal framework for information technology*, CQLR c C-1.1, ss. 19 and 26. Certain fields of activity subject to specific supervision, such as the banking sector, may also provide standards in this regard. See for example: Office of the Superintendent of Financial Institutions, *Outsourcing of Business Activities, Functions and Processes*, Guideline B-10, March 2009.

160. Federal Law, principle 4.7.1. Provincial laws also include obligations that are just as broadly stated: *Québec Act*, s. 10; *Alberta Act*, s. 33-35; *British Columbia Act*, ss. 33-35.

161. Federal Law, principle 4.7.

162. Federal Law, principle 4.3.4.

163. *Levy v. Nissan Canada inc.*, 2019 QCCS 3957, para. 72.

164. OPC, *Consent provided to open joint credit account not sufficient to authorize subsequent credit checks of account holders* PIPEDA Report of Findings 2015-009, February 17, 2015, para. 44. Each case is a specific case, however: for example, in certain contexts, financial information will not be considered to be sensitive; this was the case in the Trang affair, which teaches that personal information relating to a mortgage could be disclosed without

sensitive, including information relating to a person's family or love life, sex life, opinions, private communications, location or even advertising profiles.¹⁶⁵ Information about children¹⁶⁶ was also characterized as sensitive, even as "extremely delicate."¹⁶⁷ In addition, the combination of several pieces of information which, taken in isolation, are not necessarily sensitive, could lead to the creation of sensitive profiles on a person.¹⁶⁸

Closely linked to the concept of sensitivity, risk of harm is also relevant in determining the level of security measures to be adopted. According to the OPC, the company must take into account "the potential risk of harm to individuals from unauthorized access, disclosure, copying, use or modification of the information."¹⁶⁹ In this assessment, the company "should not focus solely on the risk of financial loss to individuals due to fraud or identity theft, but also on their physical and social well-being at stake, including potential impacts on relationships and reputational risks, embarrassment or humiliation."¹⁷⁰

To some degree, the security obligation provided for in the law echoes the risk analysis process undertaken by companies, in that it adopts a contextual and proportional approach to risks (see section 1.5.1). Thus, in order to determine the intensity and nature of the security measures to be implemented within the meaning of the law, a company will clearly have to identify the personal information to be protected, then assess the vulnerabilities of its systems and the threats they are prone to in order to adopt the appropriate countermeasures.¹⁷¹

4.2.2. An insufficiently preventive obligation

The law therefore proposes a holistic, flexible vision of information security that does not require the implementation of specific protection measures.¹⁷² While this approach has the advantage of being adaptive and technologically neutral, it has the disadvantage of being imprecise as to the exact security measures to deploy.

the express consent of the person concerned, because it was not sensitive. See: *Royal Bank of Canada v. Trang*, 2016 SCC 50.

165. See: Éloïse Gratton, "Publicité ciblée et défis en matière de protection de renseignements personnels", in Pierre-Claude Lafond and Vincent Gautrais (eds.), *Le consommateur numérique : une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016, pp. 203-206; *Profiles on PositiveSingles.com dating website turn up on other affiliated dating websites*, PIPEDA Report of Findings #2013-003, July 11, 2013.

166. OPC, *Connected toy manufacturer improves safeguards to adequately protect children's information*, PIPEDA Report of Findings #2018-001, January 8, 2018, para. 32.

167 OPC, *Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection*, PIPEDA Report of Findings #2011-008.

168. For example, in a case involving Bell, the OPC considered that the combination of several types of information, including web history and demographic data, increased their sensitivity. See: OPC, *Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program*, PIPEDA Report of Findings 2015-001, April 7, 2015, para. 66-76. See also: *R. v. Spencer*, 2014 SCC 43.

169. OPC, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, PIPEDA Report of Findings #2016-005, August 22, 2016, para. 44.

170. Ibid.

171. Nicolas W. Vermeys, *Responsabilité civile et sécurité informationnelle*, Yvon Blais, 2010, p. 73.

172. OPC and OIPCA, *TJX Companies Inc./Winners Merchant International L.P.*, Report of an Investigation into the Security, Collection and Retention of Personal Information.

At most, the Federal Law states that companies must resort to organizational, physical and technological protection measures, and gives examples of these.¹⁷³ Case law, however, particularly the conclusions of the , has allowed more light to be shed on these requirements.¹⁷⁴

From the administrative standpoint, the OPC stresses the importance of adopting internal policies and processes on the protection of personal information; these could extend, for example, to the keeping of files and the authorizations for accessing them, as well as to customer authentication processes. These policies must be documented, and therefore written down, in order to ensure they are applied uniformly.¹⁷⁵ Naturally, they must be diligently respected by the companies, which will need to provide their employees with training in their regard.¹⁷⁶ Finally, the company must periodically review its policies to ensure that they remain up to date.¹⁷⁷

Physical safeguards include the use of physical devices that restrict access to personal information, such as placing locks on doors and filing cabinets. For example, no business should leave confidential documents lying around in an office for anyone to see,¹⁷⁸ should properly destroy photocopies of identity documents rather than recycling them¹⁷⁹ and should ensure that the letters it sends are properly sealed to avoid exposing the recipient's personal information.¹⁸⁰

Technological safeguards include devices designed to mitigate computer threats. In its conclusions, the OPC cites several technological measures a business could employ, including data encryption,¹⁸¹ the use of two-factor authentication modes,¹⁸² segmenting the components

173. Federal Law, principle 4.7.3. This provision gives as examples of organizational measures: "security clearances and limiting access," of material measures: "locked filing cabinets and restricted access to offices" and of technological measures: "the use of passwords and encryption." Provincial laws equivalent to the Federal Law do not include such examples, and are expressed in general terms.

174. For a detailed outline, see: OPC, *Interpretation Bulletin: Safeguards*, June 2015.

175. OPC, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, PIPEDA Report of Findings #2016-005, August 22, 2016.

176. Éloïse Gratton and Frédérick Néron, "Bris de sécurité informationnelle : étapes à suivre et gestion des risques", in Barreau du Québec - Service de la Formation continue, *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé*, Yvon Blais, 2014, pp. 144-145; OPC, *Phone message left at client's workplace disclosed personal information without consent*, PIPEDA Report of Findings #2012-009.

177. OPC, *Individual's personal information fraudulently used by sales representative to issue him a new credit card*, PIPEDA Report of Findings #2015-008, July 7, 2015.

178. OPC, *Fax from debt collector contained debtor's personal information*, PIPEDA Case Summary #2005-317.

179. OPC, *Airline accused of collecting too much information for U.S. authorities*, PIPEDA Case Summary #2003-128.

180. OPC, *Individual alleged bank sent personal information in unsealed envelopes*, PIPEDA Case Summary #2003-197.

181. OPC, *Investigation into the Personal Information Handling Practices of WhatsApp Inc.*, PIPEDA Report of Findings #2013-001, January 15, 2013; OPC, *Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection*, PIPEDA Report of Findings #2011-008, para. 34.

182. OPC, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, PIPEDA Report of Findings #2016-005 #2016-005, August 22, 2016, para. 72-73.

of the internal network,¹⁸³ logging employee activity on computer systems¹⁸⁴ or implementing monitoring systems to detect unusual user behaviour.¹⁸⁵

Given the wide variety of measures that might be implemented and the difficulty of determining which ones to use, companies may find it useful to refer to industry standards and third-party certification (see section 1.5.1). For the OPC, the use of such certification may indeed constitute one acceptable means of complying with the law, provided certain conditions are met:

it would generally be reasonable, for the purpose of assessing a third party's compliance with PIPEDA's safeguards requirements, for an organization to rely on an up-to-date security certification conducted under the following conditions: (i) by an appropriate party, (ii) against an appropriate security standard, and (iii) in the absence of contradictory indicators of security concerns.¹⁸⁶

Consequently, while industry standards may be useful in guiding companies as to the correct practices to adopt, it should not be concluded from the fact that a company has announced that it has adopted a standard that it is in full compliance with the law. A standard may be appropriate, but poorly implemented, or the standard chosen may be too low to ensure compliance with the law.¹⁸⁷ This means that although the use of an industry standard can be a good approach for a company to adopt, it is not an absolute guarantee of compliance.¹⁸⁸

That said, although companies are subject to the legal obligation to provide data security, the ways that this obligation is implemented can at least be improved. As evidenced by the high number of security breaches in Canada resulting from deficiencies in the companies' data management practices, many companies would appear to be shirking their legal obligations.

Faced with such shortcomings, it appears desirable that more details regarding preventive measures be incorporated into the law, in order to ensure more rigorous compliance by the private sector. One such measure could be the obligation to conduct a privacy impact assessment that would explicitly oblige the company to ensure that its practices are truly respectful of privacy (see section 4.5.3). Similarly, incorporating the principles of data protection by design and data protection by default into Canadian law could also encourage a more proactive deployment of security measures (see section 4.5.2).

183. OPC, *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information*, PIPEDA Report of Findings #2019-001, April 9, 2019, para. 25, 34.

184. OPC, *Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection*, PIPEDA Report of Findings #2011-008, para. 34.

185. OPC, *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information*, PIPEDA Report of Findings #2019-001, April 9, 2019, para. 25-26.

186. OPC, *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information*, PIPEDA Report of Findings #2019-001, April 9, 2019, para. 90-94.

187. For example, the OPC concluded that Equifax had inadequately implemented the PCI-DSS and ISO 27001 standards in its processes. See: *Ibid.*, para. 90-94.

188 See: Nicolas W. Vermeys, *Responsabilité civile et sécurité informationnelle*, Yvon Blais, 2010, pp. 119-138.

4.2.3. Whose fault is it?

Even if it deploys appropriate safeguards, no company can guarantee absolute data security. All systems are fallible and can be broken into, provided enough effort is put into it. As a result, it would be unrealistic to impose a legal obligation on companies to unfailingly prevent any and every security breach.

In law, the obligation of information security is therefore an obligation of means. Companies are asked to adopt all reasonable security measures appropriate to the context, not to prevent any data whatever from being compromised.¹⁸⁹ The OPC also espouses such an interpretation, conceding that “security safeguards are not guarantees, but they play an important preventative role in protecting privacy.”¹⁹⁰

In short, although a large share of the responsibility rests on a company in the event of a security breach, certain circumstances may allow it to be exempted from its liability. These limits of the security obligation have often been raised in connection with the human factor, whether it be an employee of a company or a consumer who is affected by a data breach. Indeed, even if a company deploys adequate security measures, trains its staff and provides information to consumers about their obligations, it may happen that some employees or customers fail to respect these instructions, whether by choice or otherwise.

First, many security breaches are the result of human error. For example, case law reports the case of an employee who entered personal information in the wrong field of a computerized form, which had the consequence of this information being revealed at a later point.¹⁹¹ In another case, a bank employee failed to follow the usual procedures to verify someone’s identity.¹⁹² In these cases, the OPC did not consider that the company had failed in its obligations, since it had nevertheless taken adequate protective measures—and the breach was the result of a simple error.¹⁹³

Many failures, however, are the result not of an error, but rather of a malicious action by an employee. An example of this would be an employee who steals a customer’s personal information in order to have a credit card issued in their name¹⁹⁴ or who accesses a consumer’s file out of curiosity.¹⁹⁵ The company’s responsibility with regard to the commission of such

189. However, the intensity of this obligation remains high for companies. According to Professor Vermeys, this is an “enhanced” obligation of means, in which there is an inverse burden of proof towards the debtor of the obligation. This means that, once the consumer can demonstrate that he has been the victim of a security breach, the company will have to demonstrate that it took all reasonable protective measures to avoid it. See: Nicolas W. Vermeys, *Responsabilité civile et sécurité informationnelle*, Yvon Blais, 2010, p. 73., p. 111-118.

190. OPC, *Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection*, PIPEDA Report of Findings #2011-008.

191. OPC, *Bank offers \$20 gift certificate as compensation for privacy violation*, PIPEDA Case Summary #2002-003.

192. OPC, *Wife accuses bank of telling husband about her credit card*, PIPEDA Case Summary #2002-108; OPC, *Woman accuses bank of telling her mother about her bank account*, PIPEDA Case Summary #2002-100.

193. OPC, *Woman accuses bank of telling her mother about her bank account*, PIPEDA Case Summary #2002-100.

194. OPC, *Individual’s personal information fraudulently used by sales representative to issue him a new credit card*, PIPEDA Report of Findings #2015-008, July 7, 2015. Admittedly, using a computer to commit a crime or even to steal data may be considered criminal acts. See in particular: Criminal Code, RSC 1985, c. C-46, s. 342.1 (1) and 430 (1.1).

195. OPC, *Bank implements significant measures to address unauthorized access of client information for non-business purposes by bank employee*, PIPEDA Report of Findings #2015-011, July 20, 2015.

offenses by an employee is still a subject of debate in case law, with Canadian courts sometimes maintaining that the company was not responsible for a criminal act committed by an employee while they were at work.¹⁹⁶

Given the state of the law, we must therefore conclude that the company will not be immediately responsible for an act by an imprudent employee. For it to be held accountable, one would need to assess whether the security measures that were deployed were reasonable, given the context, in order to reduce this risk of error or intrusion on the part of personnel. This assessment could take into account the amount of awareness training given to employees and the presence of technological measures and monitoring systems.¹⁹⁷

In addition, consumers also bear some responsibility for cybersecurity, and in particular must protect access to their personal information by following the usual instructions in this regard. In one of its conclusions, the OPC refused to hold a company responsible for a data breach, because the user had neglected to follow the company's advice on matters of security—guidelines that were nevertheless easy to understand.¹⁹⁸

Such a determination has worrying implications for consumer protection. Our analysis shows that many contracts are teeming with clauses that impose a range of obligations on consumers related to the security of their accounts (section 2.3), thus raising the concern that companies could invoke non-compliance with one or another of these requirements in order to blame the consumer in the event of a security breach. This is all the more worrying given that, as we have seen previously, consumers are often unaware of the extent of their security obligations (section 3.3.1).

Admittedly, certain Canadian consumer protection laws prohibit merchants from excluding their liability in a consumer contract, so clauses exonerating them from liability in the event of a security breach may have no legal force.¹⁹⁹ However, this does not preclude requiring the consumer to bear their share of responsibility if they have committed a wrongful act that led to their personal information being compromised. This situation at least argues for the obligations that companies wish to impose on consumers being reasonable and clearly explained, and that efforts continue to inform and educate the public about cybersecurity.

196. In Québec civil law, article 1463 of the *Civil Code of Québec* states that the principal is liable to reparation for injury caused by the fault of his agents in the performance of their duties. However, according to certain case law, an employee who commits a criminal act at work for his own benefit is not acting in the performance of his duties. See in particular: *Havre des Femmes inc. v. Dubé*, 1998 CanLII 13167 (QC CA); *Desjardins General Insurance v. Patry*, 2010 QCCQ 11527. In common law, responsibility for the fault of the principal is attributed to a company if the act is sufficiently linked to conduct authorized by the employer. Here again, case law remains undecided on the issue of security breaches. See in particular: *Ari v. Insurance Corporation of British Columbia*, 2015 BCCA 468; *Evans v. Bank of Nova Scotia*, 2014 ONSC 2135; *Hynes v. Western Regional Integrated Health Authority*, 2014 NLTD (G) 137.

197. OPC, *Bank implements significant measures to address unauthorized access of client information for non-business purposes by bank employee*, PIPEDA Report of Findings #2015-011, July 20, 2015.

198. OPC, *Web-centred company's safeguards and handling of access request and privacy complaint questioned*, PIPEDA Case Summary #2005-315.

199. In Québec: *Consumer Protection Act*, RSQ, c P-40, s. 10.

4.3. Some additional obligations

In addition to the obligations specifically related to information security, other provisions of the law may also be invoked when determining whether a company has adequately protected personal data. This shows that, ultimately, security of information depends on compliance with all the obligations respecting the protection of personal information.

4.3.1. The accountability principle

The Federal Law states that a business is responsible for the personal information in its possession. It must designate, from among its personnel, one person whose role is to ensure compliance with the law and the implementation of policies aimed at protecting personal information.²⁰⁰ In short, the “accountability principle” plays a transversal role in the law and makes it possible to highlight a company’s obligations with regard data protection. Poor data protection or deficiencies in a response to a security incident may also constitute a breach of the principle of accountability.

This principle is particularly relevant in the context in which personal information collected by a company is entrusted to a third party. Indeed, the Federal Law states that “an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing.”²⁰¹ In such a case, the company must “provide a comparable level of protection while the information is being processed by a third party.”²⁰² By way of illustration, the OPC concluded that Equifax Canada had violated the accountability principle by failing to obtain a written agreement from its American branch before disclosing personal information to it, as well as for failing to implement control mechanisms to monitor their application.²⁰³

4.3.2. Limitation of collection and duration of storage

Collecting more personal information than necessary or keeping it too long increases information security risks. The more information a database contains about consumers, the greater the potential harm they will be exposed to in the event of a security breach. The legal provisions that set limits on the personal information a company can collect or keep are therefore of considerable interest in cybersecurity, because the risks are mitigated if they are applied.

First of all, the law provides that a company can only collect the personal information it needs for its purposes.²⁰⁴ Also, it cannot require a consumer to provide information that is

200. Federal Law, principle 4.1. According to the OPC, this principle “is implicit in the laws of Alberta, British Columbia and Québec.” See: OPC, *Getting Accountability Right with a Privacy Management Program*, April 2012.

201. Federal Law, principle 4.1.3.

202. Ibid.

203. OPC, *Investigation into Equifax Inc. and Equifax Canada Co.’s compliance with PIPEDA in light of the 2017 breach of personal information*, PIPEDA Report of Findings #2019-001, April 9, 2019, para. 72-74.

204. Federal Law, principle 4.4; Alberta Act, s. 11; British Columbia Act, s. 11; Québec Act, s. 5.

inessential to obtaining a good or service.²⁰⁵ As an illustration, the OPC lamented in one conclusion that a chain of stores kept the driver's license numbers of customers who returned items back to the store.²⁰⁶ This sensitive information, which it did not need to collect to prevent fraud, was unfortunately compromised during a security breach in the company's computer systems.

Next, the law provides that a company may keep personal information only for the time necessary to achieve the purposes for which it was collected.²⁰⁷ When an organization no longer needs personal information for these purposes, it must erase it or render it anonymous.²⁰⁸ Under the Federal Law, it must also implement procedures to regulate the destruction of personal information.²⁰⁹ As an example of a breach of this obligation, we cite the investigation into the security breach that occurred at Desjardins in 2019, in which the OPC declared that the company did not have a clear data deletion policy and that for decades, it retained information about millions of people who were no longer its clients.²¹⁰

4.3.3. Transparency... and its limits

Under Canadian law, businesses must be transparent about the practices they employ to manage personal information and must obtain informed consent from consumers to collect, use or disclose it.²¹¹ In particular, this means that companies must be transparent about their security measures and their information storing practices.²¹² The company must also be transparent in the aftermath of a security breach, in particular by adequately informing consumers who want to find out whether their personal information has been compromised.²¹³

205. Federal Law, principle 4.3.3; Alberta Act, s. 7 (2); British Columbia Act, s. 7 (2); Québec Act, s. 9.

206. OPC and IPC, *TJX Companies Inc./Winners Merchant International L.P.*, Report of an Investigation into the Security, Collection and Retention of Personal Information, September 25, 2007.

207. Federal Law, principle 4.5; Alberta Act, s. 35; British Columbia Act, s. 35. In Québec, however, the law states that the use of the information contained in a file is only permitted once the object of the file has been achieved, with the consent of the person concerned, subject to the time limits prescribed by the law or by a retention schedule established by government regulation. However, no such a timetable has been adopted. See: Québec Act, s. 12.

208. Ibid.

209. Federal Law, principle 4.5.2.

210. OPC, *Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019*, PIPEDA Report of Findings #2020-005, para. 87-97; OPC, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, PIPEDA Report of Findings #2016-005, August 22, 2016, para. 116; OPC, *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information*, PIPEDA Report of Findings #2019-001, April 9, 2019, para. 51.

211. Federal Law, principles 4.3 and 4.8. The obligation to inform the person and to obtain their consent is included in the equivalent provincial laws, with some variations in formulation. See in particular: Alberta Act, s. 7-10; British Columbia Act, s. 6-9; Québec Act, s. 8, 12-14.

212 OPC, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, PIPEDA Report of Findings 2016-005, August 22, 2016, para. 192.

213. OPC, *After a significant Adobe data breach, customer questions company's security safeguards and the response it provided about impacts on his personal information*, PIPEDA Report of Findings #2014-015, September 3, 2014, para. 38-39.

When it comes to data security, such transparency obligations sometimes pose a problem. Indeed, it is hardly prudent for a company to reveal in great detail the methods it employs to protect personal information. It is understandable that preserving the secrecy of information that is “sensitive from a commercial point of view”²¹⁴ will be part of any reasonable cybersecurity strategy. According to the OPC, it is thus “logical that a bank would not want to publicize the specific steps it takes to prevent fraud because to do so would give criminals information about how to circumvent the bank's safeguards.”²¹⁵ Our analysis of company policies also shows the parsimony with which they generally approach the subject (see section 2.2).

This context of information asymmetry between businesses and consumers illustrates the limitations of an approach to public protection based exclusively on transparency. On the one hand, companies have an interest in limiting how much information they disclose about their security measures, in order to ensure their effectiveness. On the other hand, consumers do not generally possess the technical knowledge and resources to assess the value of these measures. Obviously, mechanisms other than mere information are therefore necessary to protect the public and help them make an informed choice, such as proactive action by public authorities to verify companies' compliance with the law.

Of course, not only must a company be transparent, its claims must also be truthful. A company that falsely announces that it has certain security measures could contravene various Canadian consumer protection laws that prohibit misleading representations.²¹⁶ One problematic situation to this effect arose in the Ashley Madison case, when the OPC discovered that the company displayed a bogus security certification icon in addition to failing to notify consumers, when they subscribed to their service, that it would cost them nearly \$20 to delete their profile.²¹⁷

4.4. The consequences of a security breach

Not only must companies comply with legal obligations to prevent security breaches, they are also required to implement measures when they fall victim to them (4.4.1). However, although they impose several obligations in terms of information security, Canadian laws are insufficiently dissuasive towards offending companies (4.4.2).

214. *Ibid.*, s. 36.

215. OPC, *Bank not required to publicize detailed privacy policies and procedures*, PIPEDA Case Summary #2003-183.

216. This is provided for in various federal or provincial laws containing consumer protection provisions, including: the *Competition Act*, RSC (1985), c. C-34, art. 52 and 74.01; the *Consumer Protection Act*, RSQ, c. P-40.1, ss. 219 and 228; the *Consumer Protection Act* 2002, SO 2002, c. 30, Schedule A, s. 14.

217. OPC, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, PIPEDA Report of Findings #2016-005, August 22, 2016, para. 177-178.

4.4.1. Notify and mitigate

According to the Federal Law, companies have an obligation to report security breaches “as soon as possible”²¹⁸ to the OPC “if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.”²¹⁹ They must also notify the victim in these same circumstances.²²⁰ Finally, the company must keep a record of breaches to its security safeguard measures.²²¹

Significant harm, within the meaning of the Federal Law, includes in particular “bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.”²²² In determining whether there is a real risk of significant harm, a company will need to consider the sensitivity of the personal information involved and “the probability that the personal information has been, is being or will be misused.”²²³ Such a broad definition will ensure that many security breaches could be considered to present a risk of significant harm.

At the provincial level, only Alberta has a general security breach disclosure regime, which is somewhat different from the federal regime.²²⁴ However, even though Québec and British Columbia do not currently have express security breach notification provisions in their respective laws, companies operating in these jurisdictions can be considered to have certain obligations in the aftermath of a security breach.

In fact, the general standards of civil liability could entail that any company must ensure that it carries out mitigation measures when it discovers that it has been the subject of a security breach, irrespective of which province it is in.²²⁵ These measures may include the preliminary assessment and containment of the breach, an internal fact-finding investigation, and a strategy to notify and assist the parties affected, such as issuing subscriptions to credit agencies.²²⁶

218. Ibid., s. 10.1 (2) and (6).

219. Federal Law, s. 10.1-10.3; Breaches of Security Safeguards, SOR/2018-64.

220. Ibid., s. 10.1 (3).

221. Ibid., s. 10.3.

222. Ibid., s. 10.1 (7).

223. Ibid., s. 10.1 (8).

224. Alberta Act, s. 34.1. This regime differs somewhat from the federal regime in that it does not define what constitutes a risk of “significant harm.” Likewise, the Alberta disclosure obligation is only applicable to the provincial commissioner, who can decide whether or not it is appropriate to notify consumers. See: Jean-François De Rico, Caroline Deschênes and Marie-Pier Desmeules, “Cyber-risques : la gestion d’un incident de sécurité,” in Barreau du Québec, *Développements récents en enquêtes internes et réglementaires*, vol 457, Yvon Blais, 2019, p. 52. In addition, standards that apply in certain activity sectors may also impose a mandatory disclosure regime on companies, particularly under provincial laws on the protection of personal information in matters of health or in the financial sector. See, for example: Autorité des Marchés Financiers, *Ligne directrice sur les saines pratiques commerciales*, June 2013; IIROC, *IIROC Notice 19-0194 – Rules Notice – Notice of Approval/Implementation – Dealer Member Rules [IIROC Rules] – Amendments Respecting Mandatory Reporting of Cybersecurity Incidents*, November 14, 2019.

225. Jean-François De Rico, Caroline Deschênes and Marie-Pier Desmeules, “Cyber-risques : la gestion d’un incident de sécurité,” in Barreau du Québec, *Développements récents en enquêtes internes et réglementaires*, vol. 457, Yvon Blais, 2019, pp. 54-55.

226. For an exhaustive presentation of the various steps in the management of a security breach, see: Éloïse Gratton and Frédéric Neron, “Bris de sécurité informationnelle: étapes à suivre et gestion des risques,” in Barreau du Québec - Service de la formation continue, *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur*

Failure to implement such measures could result in legal consequences for the company, which could be accused of negligence or be sued for damages.

4.4.2. Lack of deterrence

The issue of the legal framework applicable to companies in cases of security breaches leads inexorably to that of recourse for consumers, and more broadly to the mechanisms for enforcing the law in businesses by the authorities.

The public bodies responsible for enforcing privacy laws are endowed with relatively modest powers and resources and appear ill-equipped to fulfill their mission in the context of the digital economy. At the end of an investigation into a company's practices, the OPC can only issue non-binding recommendations and cannot impose any financial penalties.²²⁷ Even in cases in which the OPC found alarming breaches of the law, the company did not suffer any sanction and sometimes even refused to implement the Commissioner's recommendations. The only option available to the OPC is to go to the Federal Court, which can issue a binding decision.²²⁸

In addition, consumers may seek civil remedies when a company that has had a security breach fails to meet its obligation to protect personal information.²²⁹ Often, the announcement of a security breach has led to the filing of class action proceedings. However, the usefulness of such legal proceedings in deterring negligent businesses, or even in enabling consumers to obtain substantial compensation, remains to be demonstrated.

The difficulty here is that the damages claimed in these cases are intended to compensate for the damages suffered by consumers. However, given that the financial losses and the costs of consumer protection are absorbed by the company that suffered the security breach, it is difficult to identify one identical damage suffered by the entire group of consumers bringing the action.

In Québec civil law, simple annoyances, such as stress or anxiety suffered as a result of being the victim of a data breach, have not been considered a compensable injury by the courts.²³⁰ The same type of difficulty arises in the common law provinces, where moral damages in a class

privé, Yvon Blais, 2014. Guides have also been produced by public authorities: Treasury Board of Canada Secretariat, *Strengthening privacy breach prevention and management*; Commission d'Accès à l'Information, *Aide-mémoire à l'intention des organismes et des entreprises : Quoi faire en cas de perte ou de vol de renseignements personnels?* November 2020; OPC, *Preventing and responding to a privacy breach*, September 2018.

227. Federal Law, s. 13. Note that provincial commissioners have the power to make orders, unlike the OPC. See: Alberta Act, s. 52; British Columbia Act, s. 52; Québec Act, s. 83.

228. Federal Law, ss. 14-16.

229. In Québec, these remedies may be carried out by way of civil liability. See: *Civil Code of Québec*, art. 1457. In the common law provinces, several torts may be invoked as the basis for these remedies. Certain provincial laws can also create such torts. See: *Privacy Act*, RSM 1987, c. P125 (Manitoba); *Privacy Act*, RSS 1978, c. P-24 (Saskatchewan); *Privacy Act*, RSNL, 1990, c. P-22 (Newfoundland and Labrador).

230. See in particular: *Lamoureux v. Investment Industry Regulatory Organization of Canada (IIROC)*, 2021 QCCS 1093; *Li v. Equifax inc.* 2019 QCCS 4340; *Bourbonnière v. Yahoo! Inc.*, 2019 QCCS 2624; *Sofio v. Investment Industry Regulatory Organization of Canada (IIROC)*, 2015 QCCA 1820; *Mazzonna v. DaimlerChrysler Financial Services Canada Inc./DaimlerChrysler Financial Services Inc.* 2012 QCCS 958.

action resulting from a security breach have not yet been awarded on the merits.²³¹ Finally, it should be added that significant obstacles also arise for the possibility of granting punitive damages, which might require demonstrating an unlawful, intentional fault on the part of the company.²³² In short, a company that offers free assistance measures to victims of a security breach, such as registering them for the services of a credit agency, could avoid other financial claims before the courts.

In short, making an offending company pay for a breach in data security, both through criminal and civil mechanisms, appears to be an approach beset with pitfalls. In the absence of serious financial penalties that could result from a security breach, the Canadian regime remains a relatively weak deterrent – and an unscrupulous company could calculate that the cost of not complying with the law is less than the cost of the resources it would need to deploy to ensure adequate protection of personal information. To restore the balance, Canadian laws must be reformed to ensure that dissuasive financial penalties are imposed on companies that break the law.

4.5. A look at abroad... and at the future

In the United States, the obligation to ensure information security differs little from that in Canada, except that it is fragmented in various sectoral and state laws (section 4.5.1). The European Union offers some more inspiring solutions for Canada, in particular by imposing more severe preventive obligations and higher penalties for non-compliant companies (section 4.5.2). A number of recently tabled bills, which incorporate some of the European standards, could provide solutions of interest to Canada (section 4.5.3).

4.5.1. United States

In the United States, the applicable legal framework for the protection of personal information is fragmented, both at the federal and state levels and in the various industrial sectors.

At the federal level, the Federal Trade Commission (FTC) has been active in personal information security. The FTC's activity in this area is based primarily on a general provision of the *Federal Trade Commission Act*, which prohibits false or deceptive business practices.²³³ This provision states that a practice may be considered illegal if it is likely to cause substantial injury to consumer which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

231. Molly Reynolds and Shalom Cumbo-Steinmetz, *Data breach class actions — Two fundamental problems with liability*, Torys LLP, June 25, 2020.

232. In Québec, a person can claim punitive damages for infringement of their right to privacy, provided that this infringement is unlawful and intentional. However, this criterion is not automatically fulfilled simply because the company was negligent. See: *Charter of Human Rights and Freedoms*, CQLR c C-12, ss. 5 and 49; *Levy c. Nissan Canada inc.*, 2019 QCCS 3957, para. 109-120.

233. 15 USC § 45 (2012); Woodrow Hartzog and Daniel J. Solove, "The Scope and Potential of FTC Data Protection," (2015) 83 *Geo. Wash. L. Rev.* 2230.

Based on this provision, the FTC has instigated several court cases against companies that did not have adequate security measures or made false representations in this regard. Examples of breaches alleged by the FTC include failing to use encryption for medical records, lack of oversight in handling sensitive information, or lack of data security training for employees.²³⁴

In addition to the standards established by the FTC, some federal sectoral and state laws could be applicable to cybersecurity. The *Gramm-Leach-Bliley Act* and its corresponding regulations, for example, require financial institutions to implement written procedures to ensure the security and confidentiality of their customers' data.²³⁵ The *Health Insurance Portability and Accountability Act* also sets forth security obligations for organizations operating in the health sector.²³⁶ At the state level, several US jurisdictions have passed laws imposing security obligations on businesses; as in Canada, most of these laws impose a general obligation to deploy reasonable security measures with regard to personal information, without further detailing this obligation.²³⁷

The state jurisdiction that has received the most attention in recent years is undoubtedly California, which in 2018 passed the *California Consumer Privacy Act*, a general law on the protection of personal information.²³⁸ This law provides a number of rights for consumers, including the right to delete personal information and the right to refuse the sale of personal information.²³⁹ With respect to the security of personal information, the California law states that any consumer whose unencrypted information has been subject to theft or unauthorized access may institute legal proceedings if this breach results from negligence by the company with regard to data protection.²⁴⁰

Several American laws, at both the state and federal level, also provide disclosure obligations in the event of a security breach.²⁴¹ Although the vast majority of US states have adopted such laws, the obligations they contain, as well as their applicable time limits or their form, may vary from state to state. Finally, as elsewhere in the world, American companies that experience a security breach may face class action suits based on common law claims or on state laws. However, as in Canada, a major impediment to these civil remedies resides in assessing the harm suffered by consumers.²⁴²

In short, when it comes to information security for businesses, the American framework scarcely provides any more interesting solutions than those already available in Canada. In fact, in many cases this legal framework is revealed to be even more fragmented and narrower in scope.

234. Jeff Kosseff, "Defining Cybersecurity Law," (2018) 103 *Iowa L. Rev.* 985, pp. 1011-1012.

235. *Gramm-Leach-Bliley Act of 1999*, 15 USC § 6801 (2012).

236. *Health Insurance Portability and Accountability Act of 1996*, 42 USC § 1320d2 (d) (2) (2012).

237. Jeff Kosseff, "Defining Cybersecurity Law," (2018) 103 *Iowa L. Rev.* 985, pp. 1012-1013. According to the author, some states, notably Nevada and Massachusetts, impose more detailed obligations regarding the measures to be adopted.

238. *California Consumer Protection Act*, 2018 Cal. Legis. Serv. Ch. 55 (AB 375) (West) (hereinafter "CCPA").

239. <https://oag.ca.gov/privacy/ccpa>

240. CCPA, art. 1798.150.

241. Jeff Kosseff, "Defining Cybersecurity Law," (2018) 103 *Iowa L. Rev.* 985, pp. 1022-1023.

242. *Ibid.*, p. 1016.

4.5.2. European Union

Within the European Union, the essential *General Data Protection Regulation* (GDPR) defines the standards directly related to information security—including certain innovations that could provide some inspiration for Canada.

As in Canada, the European regime requires companies to protect the personal data they collect employing a level of security that varies depending on the context. The regulation states, for example, that a company must develop adequate measures, “taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.”²⁴³ In evaluating the measures to be taken, the risks inherent in processing the data must therefore be taken into account.

The GDPR, like the Federal Law, also offers suggestions on measures that could be used to protect data. It does not define any specific obligation in this regard, but explains that such measures may include:

- a) the pseudonymization and encryption of personal data;
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.²⁴⁴

In order to determine the appropriate level of security, the GDPR states that a company must take into account “in particular [...] the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.”²⁴⁵ In short, the general European framework does not differ significantly from Canadian law, because it also adopts a contextual approach to the information security obligation, which echoes the risk analysis process.

Likewise, the GDPR specifies notification obligations in the event of a security breach. A company must therefore notify the local competent authority, within a maximum of 72 hours, when the data leak is “likely to create a risk for the rights and freedoms of natural persons.”²⁴⁶ When the risk to consumers affected by the breach is high, the company must also notify them

243. GDPR, s. 32.

244. Ibid.

245. Ibid.

246. GDPR, s. 33; Jean-François De Rico, Caroline Deschênes, Marie-Pier Desmeules, “Cyber-risques : la gestion d’un incident de sécurité,” in Barreau du Québec, *Développements récents en enquêtes internes et réglementaires*, vol 457, Yvon Blais, 2019, pp. 53-54.

directly.²⁴⁷ However, the company may avoid this obligation in certain cases, in particular when the compromised data is encrypted (and therefore unreadable by unauthorized persons) or when the company has implemented measures subsequent the security breach, “[...] is no longer likely to materialize.”²⁴⁸

In addition, the GDPR includes certain innovations that could provide some inspiration for Canada. These include a provision that obliges companies to adopt, depending on the context, data protection measures by design, as well as a data protection obligation by default²⁴⁹. These general principles require companies to meet their security obligations as soon as they design a product, particularly by minimizing the collection of data. This will presumably entail the privacy settings of user accounts being configured by default to provide maximum privacy protection.

Another innovation of interest in the GDPR is the legal recognition of industry codes of conduct and third-party certification mechanisms, which may be subject to approval by the local supervisory authority.²⁵⁰ Given the general nature of the information security obligation, the development of codes and certification could serve as a guide to companies in adopting best prevention practices. Although certifying a company’s practices cannot exonerate it from liability in the event of a breach of the regulations, the GDPR states that the application of such a code of conduct is an element to be considered in demonstrating a company’s compliance with security obligations.²⁵¹

Finally, unlike the current situation in Canada, the GDPR provides significant financial penalties for corporate offenders. The regulation states that the penalties must be “effective, proportionate and dissuasive” and adaptable to contextual factors.²⁵² These penalties may be as high as up to 4% of an offending company’s annual turnover worldwide.

4.5.3. Towards reform in Canada

In 2020, two pieces of draft legislation were tabled in Canada aimed at modernizing laws on the protection of personal information in the digital age.²⁵³ Québec’s Bill 64 thoroughly reviews the *Act Respecting the Protection of Personal Information in the Private Sector*, which applies to businesses. On the federal side, Bill C-11 totally rewrites the Federal Law, which will be renamed the “*Consumer Privacy Protection Act*.” These two bills, which draw inspiration from European standards, include several provisions of interest for the domain of cybersecurity. Of course, at the time of this writing, we are not in a position to know whether these bills will be passed and, if so, what form they will take.

247. GDPR, s. 34.

248. Ibid.

249. GDPR, s. 25.

250. GDPR, ss. 40-42.

251. GDPR, s. 25 (3), 32 (3).

252. GDPR, s. 83.

253. *An Act to modernize legislative provisions as regards the protection of personal information*, Bill 64 (June 12, 2020), 1st sess., 42nd legis. (Qc) (hereinafter “Bill 64”); *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, Bill C-11 (November 17 2020), 2nd sess., 43rd legis. (Can) (hereinafter “Bill C-11”).

Québec's Bill 64 incorporates new preventive standards that may strengthen implementation of the companies' information security obligation. For example, the Bill states that a company will have to conduct a privacy impact assessment of any project "involving the collection, use, disclosure, retention or destruction of personal information."²⁵⁴ Such an assessment would consist of a process aimed at determining whether projects involving the use of personal information present any risks related to privacy protection, including data security.²⁵⁵

In addition, the Québec bill provides that a company that offers "a technological product or service must ensure that, by default, the parameters of this product or service provide the highest levels of confidentiality."²⁵⁶ This approach, which is evidently inspired by the principle of data protection by default enunciated in the GDPR, could again help ensure better security upstream, while letting consumers avoid having to configure each of their accounts to ensure optimal privacy protection.

In addition, Bill 64 brings Québec up to standard with the rest of Canada by including measures related to the mandatory disclosure of security breaches, similar to those found in the Federal Law.²⁵⁷ The bill also explicitly incorporates the principle of accountability into Québec law and requires companies to designate a person responsible for the protection of personal information.²⁵⁸ These are all aspects that could contribute to better protection against data breaches.

On the federal side, Bill C-11 provides for the enhancement of the powers of the OPC, which will now be able to issue binding orders against non-compliant companies.²⁵⁹ Similar to what is included in the GDPR, the OPC will also be able to approve industry codes of practice and certification programs;²⁶⁰ demonstrating compliance with such a certification program will allow a company to avoid financial penalties.²⁶¹

Finally, both bills provide for an increase in the penalties stipulated in the event of non-compliance, thus ensuring more effective deterrence. In Québec, the fines provided for in the law have been substantially revised upwards, and the Commission d'accès à l'information will be vested with the power to issue financial penalties of up to \$10 million or 2% of the offending company's annual turnover worldwide, whichever is greater.²⁶² The federal bill, however, is more timid, in that it only gives the OPC the power to make recommendations on financial

254. Bill 64, s. 95 (3.3).

255. COMMISSION D'ACCÈS À L'INFORMATION, *Évaluation des facteurs relatifs à la vie privée : Savoir détecter et atténuer les risques d'atteinte aux renseignements personnels*, 2018, https://www.cai.gouv.qc.ca/documents/CAI_FI_efvp.pdf

256. Bill 64, s. 100 (9.1).

257. Bill 64, s. 95 (3.5 to 3.8).

258. Bill 64, s. 95 (3.1).

259. Bill C-11, s. 2 (92).

260. Bill C-11, s. 2 (76-81).

261. Bill C-11, s. 2 (93 (3)).

262. Bill C-11, s. 2 (90.12).

penalties, which will instead have to be issued by a personal information and data protection tribunal.²⁶³

263. Bill C-11, s. 2 (93).

Conclusion and recommendations

One might think that *Tron* merely recounts an entertaining fiction, in which the magic of cinema creates an illusion of how easy it would be to break through a company's security defenses. But fiction, unfortunately, is catching up with reality. Twenty-first century computer systems are every bit as fallible and vulnerable as those in *Tron*. The threats to personal information are very real and expose consumers to all kinds of harm.

Our study shows that there is still much work to be done to develop reliable data protection practices. As the number of security breaches in Canada skyrockets and the risks of data leaks in the digital environment increase, many experts complain that companies are not taking the issue of data protection seriously enough. How did such a situation come about?

A first line of response lies in the Canadian legal framework. In fact, although the information security obligation provided for in the law has the advantage of being flexible and adaptive, it has the disadvantage of not providing the precise preventive measures that companies should be obliged to adopt upstream (section 4.2).

To ensure stronger compliance with this obligation on the part of businesses, Canadian laws should require prior privacy impact assessments. Such a process, whose aim is to determine whether projects that involve the use of personal information present risks with regard to privacy protection, could contribute to a more proactive deployment of adequate security measures. Also, Canadian laws should incorporate the principles of data protection by design and data protection by default, as is already done in Europe. For consumers, such obligations may ensure that the confidentiality settings of their accounts are configured by default so as to offer maximum protection of their privacy.

That said, all such efforts to improve the law will be of little use if companies can fail to comply with impunity. In recent years, moreover, there have been several decisions by Canadian privacy commissioners concluding that companies have violated the law, not only regarding their obligation to protect personal information but also regarding other legal obligations, such as respecting limits on the amount of data collected or on how long data may be retained. However, many of these companies did not receive the slightest sanction for their shocking breaches of the law and sometimes even refused to implement the OPC's recommendations.

Our research at this point confronts an oft-repeated observation in cybersecurity: compliance with the law can only be promoted by truly dissuasive measures. Here again, Canada could find inspiration in Europe, where the General Data Protection Regulation inflicts severe financial penalties on organizations that fail in their data protection duties. In tandem, Canadian law enforcement authorities must be granted the necessary powers and financial resources to fulfill their mission.

Of course, consumers also have a share of responsibility in cybersecurity matters. Our study points to some worrying findings in this regard (section 3). Many Canadian consumers do not inform themselves about the companies' security practices before using their services, and rely heavily on these companies to keep their data secure. Even though they are concerned about

security breaches, many engage in reckless behaviour, such as sharing their passwords with others.

However, one may wonder whether this digital literacy deficit among Canadians may not partly be explained by shortcomings in information and awareness strategies, which have difficulty reaching certain audiences. In fact, our study shows that the information needs in terms of cybersecurity are more pronounced among groups generally considered to be most vulnerable, in particular the elderly or those with a lower income.

In addition, due to the considerable information asymmetry that prevails between businesses and consumers with regard to cybersecurity, it seems unrealistic to place a disproportionate burden on consumers to ensure the security of their data. Few companies make explicit reference to their security measures, except in exceptional cases where they are used as a marketing ploy (section 2.2). Either way, even if companies did provide a wealth of technical details about their security measures, consumers have neither the knowledge, time, nor resources to appreciate them. In this context, mechanisms based on information alone appear clearly insufficient to ensure that the public is protected.

The situation becomes all the more problematic when we consider that the terms of use issued by Canadian online businesses not only impose numerous obligations onto consumers with regard to the security of their accounts, but also assign to these same consumers a large share of the risk entailed in security breaches. In short, consumers have little choice but to trust the companies they do business with; in doing so, they have to accept contractual stipulations that protect the interests of these companies and that impose obligations on them of which they are not always fully aware. In any event, the consumers' options are all the more limited when we consider that a number of web giants have a virtual monopoly over certain essential services in the digital society.

Faced with this imbalance between businesses and consumers, another recommendation is in order: the public authorities responsible for applying the law must play a more proactive role in verifying the quality of the security measures employed in the private sector in order to ensure that the online services commonly used by consumers are secure. Preventive checks on businesses, in addition to adding a factor of deterrence, would help identify security failures before leaks occurred.

In addition, while many companies give various tips and offer features to help users better secure their accounts, efforts still need to be made to make Internet users' lives easier in this regard. For example, while an average consumer may have dozens and dozens of online accounts, some businesses still require users to use unique, different passwords for each account and, in addition, to change them regularly. Clearly, getting more consumers to adhere to good cybersecurity practices will require clear, reasonable guidelines that take into account their overall situation. Similarly, businesses should offer consumers tools to make their privacy choices easier, for example by supplying an interface that would allow them to configure multiple settings at once.

Finally, let us remember that security breaches may have serious consequences for consumers that can last for years. The bills recently tabled in Ottawa and Québec City address a number of difficulties raised during our study. However, these initiatives alone will not succeed in

alleviating the risks for victims of security breaches. We must hope that Canada will be able to make up for lost time in the development of a national digital identity and that it will be able to establish a “credit freeze” mechanism applicable to credit agencies, that will more effectively prevent identity theft.

Recommendations to the federal and provincial governments:

- **Option consommateurs recommends that the laws on the protection of personal information be amended so that the public bodies responsible for their application have the power to impose severe financial penalties, issue binding orders and conduct proactive audits of the security measures employed by companies.**
- **Option consommateurs recommends conducting proactive audits of the security measures employed by online businesses, in order to ensure that consumers who use their services are adequately protected. These audits should also include a review of the contractual obligations imposed on consumers, to ensure that these are reasonable, lawful and clearly communicated.**
- **Option consommateurs recommends improving the funding of public bodies responsible for applying the laws respecting the protection of personal information so that they can fulfil their mission in the digital context.**
- **Option consommateurs recommends amending the laws respecting the protection of personal information to include the obligation for businesses to conduct privacy impact assessments prior to deploying new consumer services.**
- **Option consommateurs recommends amending the laws respecting the protection of personal information to include the principles of data protection by design and data protection by default.**
- **Option consommateurs recommends the development of a national digital identity, which would allow consumers to avoid transmitting certain sensitive information to businesses, while taking all the necessary precautions to ensure that this digital identity offers high guarantees of privacy protection.**
- **Option consommateurs recommends the development of a free, Canada-wide “security freeze” mechanism that would enable consumers to protect their credit reports against illicit requests following a security breach.**
- **Option consommateurs recommends incorporating within all provincial laws respecting the protection of personal information a notification obligation in the event of a security breach occurring in businesses.**
- **Option consommateurs recommends pursuing initiatives aimed at informing the public and raising awareness on cybersecurity, by developing segmented strategies adapted to different audiences, paying particular attention to the needs of the most vulnerable groups.**

Recommendations for companies:

- **Option consommateurs recommends that consumers be better informed about their contractual obligations in terms of information security, in particular as regards the management of their login credentials, and to ensure that these obligations are reasonable and lawful.**
- **Option consommateurs recommends offering consumers tools that facilitate their choices in terms of confidentiality, for example via interfaces that allow them to configure several parameters from a single source.**
- **Option consommateurs recommends that, following a security breach, consumers be provided, free of charge, with all the information and assistance they need to protect themselves from identity theft and other damage.**

Recommendation to consumers:

- **Option consommateurs recommends that consumers learn about best practices in cybersecurity and use the security settings offered by companies, such as two-factor authentication.**

Appendix 1 – Survey report



1

Table des matières		
03 CONTEXTE & MÉTHODOLOGIE	09 BRIS DE SÉCURITÉ DESJARDINS	20 COMPORTEMENTS DE PROTECTION
04 PROFIL DES RÉPONDANTS	13 BRIS DE SÉCURITÉ AUTRES ENTREPRISES	25 PRÉOCCUPATIONS
06 FAITS SAILLANTS	18 VOL D'IDENTITÉ	29 ANNEXE

2

2

Contexte et méthodologie



CONTEXTE ET OBJECTIFS

Bip Recherche a été mandaté par Option Consommateurs afin de réaliser une étude sur les expériences, comportements, connaissances et préoccupations des Canadiens à l'égard de la cybersécurité (bris de sécurité, vols d'identité, etc.).



MÉTHODE DE COLLECTE DES DONNÉES

Entrevues en ligne de 10 minutes, en français et anglais, effectuées du 19 au 28 mai 2020.
Un prétest du questionnaire de 50 cas a été réalisé les 15 et 16 mai 2020.



PROFIL DES RÉPONDANTS

Canadiens âgés de 18 ans ou plus, en mesure de s'exprimer en français ou en anglais.



ÉCHANTILLON

Total de **2 000 répondants**. Aux fins de comparaison, un échantillon probabiliste de cette taille aurait une marge d'erreur de $\pm 2,19\%$, et ce, 19 fois sur 20.











RÉSULTATS

À l'aide des données du recensement de 2016, les résultats ont été pondérés selon l'âge, le sexe, la langue maternelle, la région et le niveau de scolarité afin de refléter le portrait réel de la population générale adulte du Canada.

En raison de l'arrondissement de certaines données, le total peut ne pas correspondre à la somme des parties.

Profil sociodémographique des répondants

	Total (n=2 000)
 SEXE	
Homme	49%
Femme	51%
 ÂGE	
18 à 24 ans	13%
25 à 34 ans	15%
35 à 44 ans	16%
45 à 54 ans	18%
55 à 64 ans	18%
65 ans et plus	21%
 PROVINCE	
Colombie-Britannique	14%
Prairies	17%
Ontario	38%
Québec	23%
Maritimes	7%
 LANGUE MATERNELLE	
Français	22%
Anglais	56%
Autre	22%

	Total (n=2 000)
 SCOLARITÉ	
Primaire et secondaire	52%
Collégial	20%
Universitaire	28%
 OCCUPATION	
Travailleur	55%
Ne travaille pas	15%
Étudiant	4%
Retraité	25%
 PRÉSENCE D'ENFANTS	
Ménages sans enfants	73%
Ménages avec enfants	27%
 REVENU FAMILIAL	
Moins de 40 000\$	24%
Entre 40 000\$ et 59 999\$	15%
Entre 60 000\$ et 79 999\$	15%
Entre 80 000\$ et 99 999\$	14%
Entre 100 000\$ et 124 999\$	11%
125 000\$ et plus	12%

Le complément à 100% représente la non-réponse.

Profil virtuel des répondants

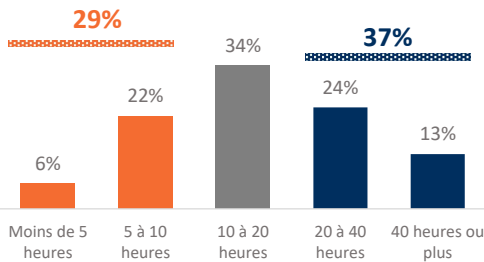
La plupart des Canadiens passent plus de 10 heures par semaine sur Internet, et le tiers plus de 20 heures. Sans surprise, la consommation d'Internet augmente avec la scolarité et le revenu, et décroît avec l'âge.

La majorité utilisent les courriels (*surtout les plus de 55 ans et les Québécois*), font des transactions bancaires (*surtout les 35-54 ans*), utilisent les médias sociaux (*surtout les moins de 45 ans, les femmes et les Québécois*) et magasinent (*surtout les moins de 45 ans et les Ontariens*).

ACTIVITÉS EN LIGNE

Utiliser des services de messagerie ou de courriel	88%
Faire des transactions bancaires	80%
Aller sur les médias sociaux	76%
Magasiner	74%
Visionner du contenu sur abonnement (streaming)	47%
Faire de la recherche (<i>mention spontanée</i>)	1%
Jouer à des jeux vidéos (<i>mention spontanée</i>)	1%
Lire les nouvelles / L'actualité / Sport (<i>mention spontanée</i>)	1%
Regarder du contenu vidéo gratuit en ligne (YouTube, etc.) (<i>mention spontanée</i>)	1%
Autres activités	3%

HEURES PAR SEMAINE SUR INTERNET



Q1. Parmi les activités suivantes, lesquelles faites-vous en ligne?

Q2. Excluant le temps passé pour le travail ou les études, combien d'heures passez-vous habituellement sur Internet par semaine?

Base: Tous les répondants (n=2 000)

BIP

5

5

FAITS SAILLANTS



6

6

Faits saillants

BRIS DE SÉCURITÉ CHEZ DESJARDINS

- ▶ Un Canadien sur six (16%), ou un Québécois sur trois (31%), ont été victimes du bris de sécurité de Desjardins l'an dernier.
- ▶ Les deux tiers (69%) sont satisfaits de la gestion de la crise par Desjardins (quoique seulement 23% se disent *très* satisfaits) et près de la moitié (44%) affirment avoir coupé leur lien d'affaires avec l'institution financière.
- ▶ Dans l'ordre, les démarches entreprises par les victimes de Desjardins suite au bris de sécurité sont d'abord consulter leur dossier de crédit et ensuite de changer le mot de passe, s'inscrire à un service de protection de la fraude et chercher de l'information sur la façon de se protéger.

BRIS DE SÉCURITÉ D'UNE AUTRE ENTREPRISE

- ▶ Près du tiers des Canadiens affirment avoir été victime d'un bris de sécurité d'une entreprise autre que Desjardins, dont principalement de Capital One.
- ▶ Les deux tiers des victimes de bris de sécurité d'une entreprise autre que Desjardins (65% se disent satisfaits de la manière dont la situation a été gérée (dont 29% se disent *très* satisfaits). C'est un niveau de satisfaction similaire à celui des victimes de Desjardins.
- ▶ Cependant, le tiers des victimes (35%) affirment avoir cessé de faire affaire avec l'entreprise après avoir appris être victimes du bris de sécurité. C'est un taux d'abandon un peu moins élevé que pour Desjardins.
- ▶ Dans l'ordre, les démarches entreprises par les victimes suite au bris de sécurité sont d'abord de changer leur mot de passe, et ensuite de consulter leur dossier de crédit, d'activer l'authentification à deux facteurs et de chercher de l'information sur la façon de se protéger.
- ▶ Tout comme chez les victimes de Desjardins, environ une personne sur 10 n'a fait aucune démarche.

Faits saillants

VOL D'IDENTITÉ

- ▶ Un Canadien sur six (14%) affirme avoir été victime d'un vol d'identité.
- ▶ La moitié de ces victimes (48%) croient que ce vol résulte d'un bris de sécurité survenu dans une entreprise dont ils utilisent les services en ligne.

COMPORTEMENTS DE PROTECTION ET PRÉOCCUPATIONS

- ▶ Le comportement de protection le plus fréquent est la modification par les utilisateurs de réseaux sociaux des paramètres de protection de la vie privée par défaut pour limiter les auditoires qui peuvent voir leurs publications (77%) ainsi que l'emploi de l'authentification à deux facteurs lorsqu'offert (77%).
- ▶ La moitié des Canadiens ont des comportements à risque comme utiliser le même mot de passe sur plusieurs comptes (58%) et conserver leurs mots de passe par écrit (55%). En effet, 20% des Canadiens partagent leur mot de passe avec d'autres, quoique 23% utilisent un logiciel gestionnaire de mots de passe et 40% un identifiant biométrique. Près du tiers (31%) des Canadiens changent leur mot de passe moins d'une fois par année ou même jamais, alors que près de la moitié (44%) les modifient aux six mois ou plus fréquemment.
- ▶ Au cumul, c'est le tiers des Canadiens (32%) qui lisent les politiques de confidentialité, les conseils de cybersécurité et se renseignent sur les pratiques de cybersécurité des entreprises avant d'utiliser ses services en ligne.
- ▶ Les deux tiers des Canadiens (66%) craignent qu'une entreprise avec qui ils transigent en ligne soit la cible d'un bris de sécurité. Cependant, la même proportion (67%) ont l'impression de savoir comment se protéger contre ses bris, disent avoir confiance envers les entreprises (66%) ou envers les autorités gouvernementales (63%) pour protéger leurs données hébergées chez les entreprises.



9

Victime du bris de sécurité de Desjardins

16% des Canadiens (31% des Québécois) ont été victimes du bris de sécurité survenu chez Desjardins l'été dernier.

Les victimes sont plus nombreuses parmi les hommes et les 18-44 ans.

On remarque aussi que les victimes de Desjardins sont plus nombreuses à être également victimes d'un bris de sécurité d'une autre entreprise ou encore à être la cible d'un vol d'identité.



Ne sait pas : 13%

RÉGIONS	OUI %
Maritimes	9%
Québec	31%
Ontario	12%
Ouest	10%

Q3. Avez-vous été victime du bris de sécurité survenu chez l'institution financière Desjardins au cours de l'été 2019?
Base: Tous les répondants (n=2 000)

BIP 10

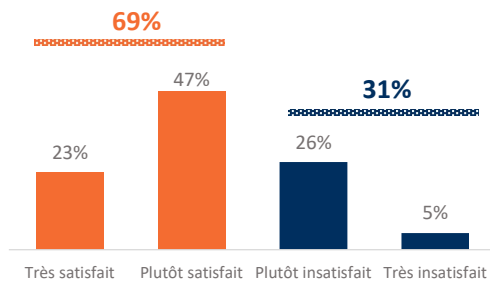
10

Satisfaction de la gestion de crise par Desjardins

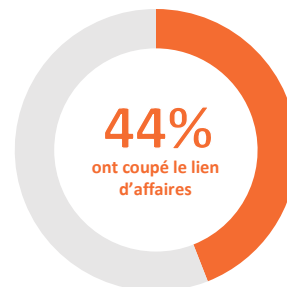
Les deux tiers des victimes du bris de Desjardins se disent satisfaits de la manière dont la situation a été gérée. Le niveau de satisfaction est plus élevé chez les résidents des provinces de l'Ouest, chez les plus éduqués, et parmi ceux qui ont confiance aux entreprises pour protéger leurs données.

Malgré ce niveau de satisfaction élevé, près de la moitié des victimes affirment avoir cessé de faire affaire avec Desjardins après avoir appris qu'ils étaient l'objet du bris de sécurité. C'est surtout le cas des 18-44 ans, des résidents des provinces de l'Ouest et des Ontariens, de ceux qui sont également la cible d'un vol d'identité et des gens qui ont moins confiance aux entreprises pour protéger leurs données.

SATISFACTION ENVERS GESTION DE LA CRISE



MIS FIN À LA RELATION D'AFFAIRES



Q8A. Quel est votre niveau de satisfaction quant à la manière dont Desjardins a géré la situation?
Q9A. Avez-vous cessé de faire affaire avec Desjardins après que vous ayez appris qu'elle a fait l'objet d'un bris de sécurité?
Base: Ceux ayant subi le bris de Desjardins (n=336)

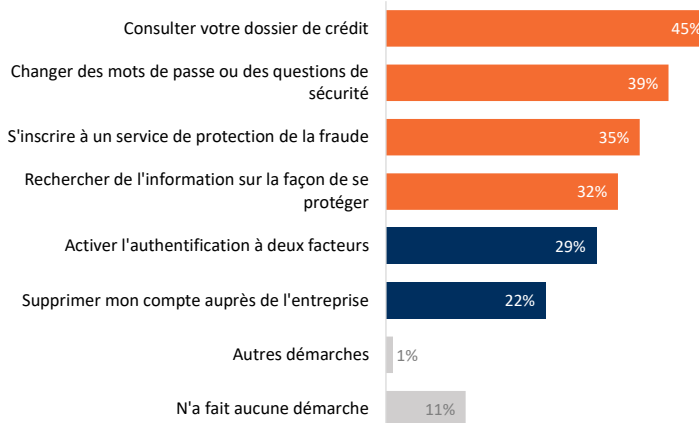
BIP 11

11

Démarches effectuées suite au bris

Près de la moitié des victimes ont consulté leur dossier de crédit suite au bris de sécurité chez Desjardins. Les autres démarches effectuées sont de changer le mot de passe, de s'inscrire à un service de protection de la fraude et de chercher de l'information sur la façon de se protéger.

Environ 1 victime sur 10 n'a fait aucune démarche. C'est surtout le cas des 55 ans et plus et des Canadiens qui se renseignent peu sur la cybersécurité.



Q10A. Parmi les démarches suivantes, lesquelles avez-vous faites après avoir entendu parler du bris de sécurité chez Desjardins?
Base: Ceux ayant subi le bris de Desjardins (n=336)

BIP 12

12



13

Victime d'un bris de sécurité d'autres entreprises

Près du tiers des Canadiens affirment avoir été victime d'un bris de sécurité d'une entreprise autre que Desjardins, dont principalement de Capital One. Les victimes de bris autre que Desjardins sont plus nombreux parmi les 18-44 ans et les Ontariens. Le tiers des victimes croient que leurs données ont été compromises lors de ce bris de sécurité.

VICTIME D'UN BRIS DE SÉCURITÉ

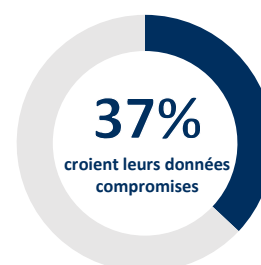


Ne sait pas : 32%

ENTREPRISES RESPONSABLES

Capital One	16%
Yahoo	10%
LifeLabs	8%
Facebook / Messenger	7%
Equifax	6%
BMO	6%
Marriott hôtel	5%
TD Canada Trust, Home Dépôt, Google, Simplii	<2% chacun
RBC, CIBC, Bell, Sony Playstation, Walmart, Apple, Koodo	<1% chacun
Autres	29%
Ne sait pas / Se souvient pas	9%

DONNÉES COMPROMISES



Ne sait pas : 34%

Q4. Outre Desjardins, à votre connaissance, une entreprise dont vous utilisez les services sur Internet a-t-elle déjà été la cible d'un bris de sécurité?

Base: Tous les répondants (n=2 000)

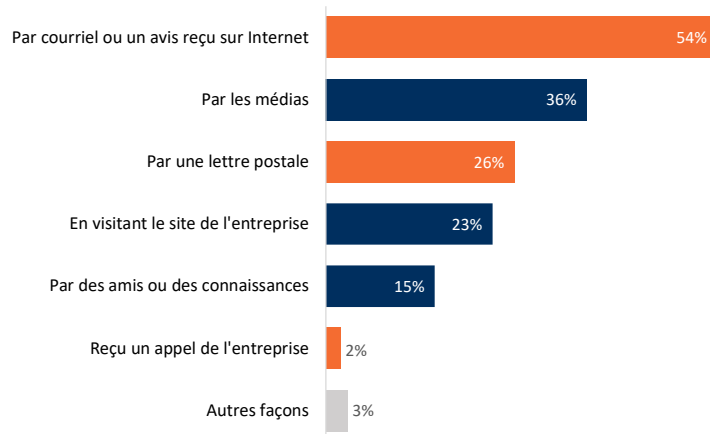
Q5. Quelle(s) entreprise(s) a fait l'objet d'un tel bris? / Q6. Croyez-vous que vos données ont été compromises lors de l'un de ces bris de sécurité?

Base: Ceux ayant subi un bris (n=681)

14

Communications du bris

Environ 7 victimes sur 10 ont été avisées être la cible d'un bris de sécurité par une communication de l'entreprise (courriel, lettre, appel). Le tiers des victimes l'ont appris par les médias.



Q7. Comment avez-vous appris que vous étiez victime d'un bris de sécurité?
Base: Ceux ayant subi le bris et dont les données ont été compromises (n=264)

BIP 15

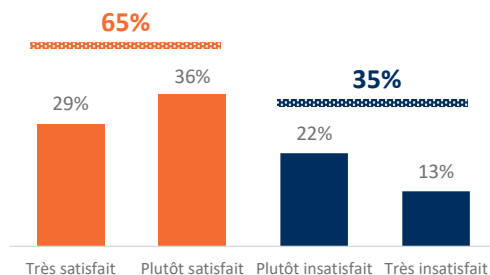
15

Satisfaction de la gestion de crise

Les deux tiers des victimes de bris de sécurité se disent satisfaits de la manière dont l'entreprise responsable a géré la situation. Le niveau de satisfaction est plus élevé parmi ceux qui ont confiance aux entreprises et aux autorités gouvernementales pour protéger leurs données.

Malgré tout, le tiers d'entre eux affirment avoir cessé de faire affaire avec cette entreprise après avoir appris être victime du bris de sécurité. C'est surtout le cas des 18-44 ans, des Ontariens et de ceux qui sont également la cible d'un vol d'identité et des gens qui ont moins confiance aux entreprises pour protéger leurs données.

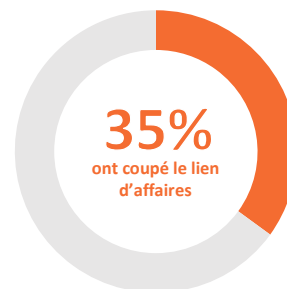
SATISFACTION ENVERS GESTION DE LA CRISE



Q88. Quel est votre niveau de satisfaction quant à la manière dont l'entreprise a géré la situation?
Base: Ceux ayant subi le bris et dont les données ont été compromises (n=264)

Q98. Avez-vous déjà cessé de faire affaire avec une entreprise en ligne après que vous ayez appris qu'elle a fait l'objet d'un bris de sécurité?
Base: Ceux ayant subi un bris (n=681)

MIS FIN À LA RELATION D'AFFAIRES



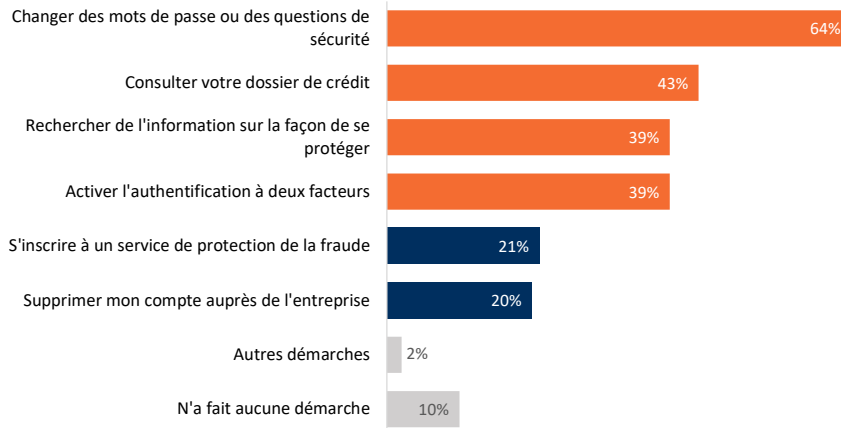
BIP 16

16

Démarches effectuées suite à un bris

Les deux tiers des victimes ont changé leur mot de passe après avoir entendu parler du bris. Les autres démarches effectuées sont de consulter leur dossier de crédit, d'activer l'authentification à deux facteurs et de chercher de l'information sur la façon de se protéger.

Environ 1 victime sur 10 n'a fait aucune démarche. C'est surtout le cas des 45-64 ans, des femmes, des Québécois, des gens moins scolarisés et des Canadiens qui se renseignent peu sur la cybersécurité.



Q10B. Parmi les démarches suivantes, lesquelles avez-vous déjà faites après avoir entendu parler d'un bris de sécurité?
Base: Ceux ayant subi un bris (n=681)

BIP 17

17



18

Victime d'un vol d'identité

Un Canadien sur six affirme avoir été victime d'un vol d'identité. Ils sont plus nombreux parmi les hommes, les 18-44 ans, les plus scolarisés et ceux qui ont davantage confiance aux autorités gouvernementales pour protéger leurs données, mais moins nombreux au Québec.

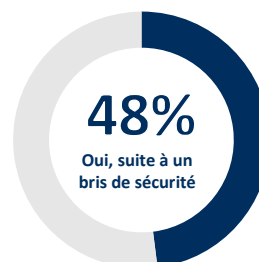
La moitié de ces victimes croient que ce vol résulte d'un bris de sécurité survenu dans une entreprise dont ils utilisent les services en ligne.

VICTIME D'UN VOL D'IDENTITÉ



Ne sait pas : 13%

VOL RÉSULTANT D'UN BRIS DE SÉCURITÉ



Ne sait pas : 23%

Q11. À votre connaissance, avez-vous déjà été victime d'un vol d'identité? Base: Tous les répondants (n=2 000)

Q12. Croyez-vous que ce vol d'identité résulte d'un bris de sécurité survenu dans une entreprise dont vous utilisiez les services en ligne? Base: Ceux ayant subi un vol d'identité (n=332)

BIP 19

19

Comportements de protection

20

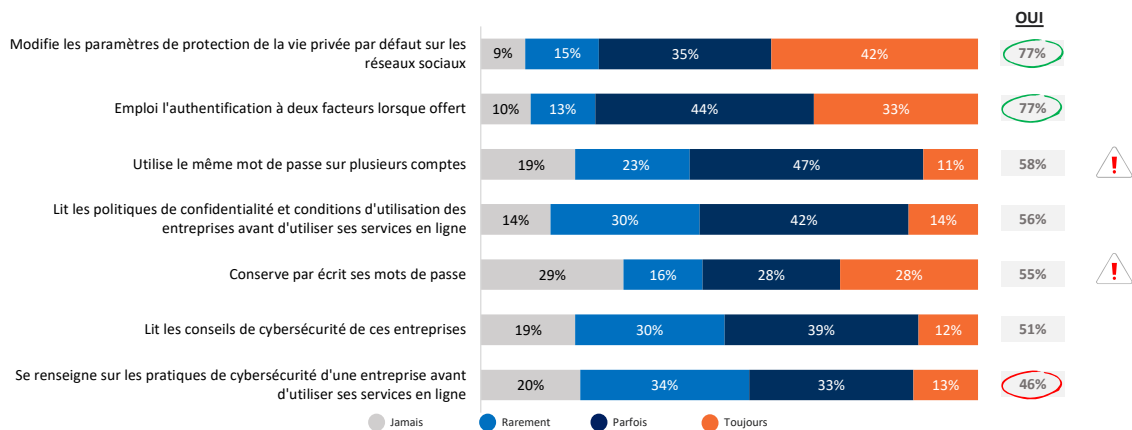
20

Comportements de protection

La majorité des utilisateurs canadiens de réseaux sociaux modifient les paramètres de protection de la vie privée par défaut pour limiter les auditoires qui peuvent voir ce qu'ils publient. Dans une même proportion, la majorité des Canadiens emploient l'authentification à deux facteurs lorsqu'offerte (surtout les 18-44 ans et les Ontariens).

Cependant, plus de la moitié des Canadiens utilisent le même mot de passe sur plusieurs comptes (surtout les 18-44 ans et les Ontariens) et conservent leurs mots de passe par écrit (surtout les 55 ans et plus, les Ontariens et les moins scolarisés).

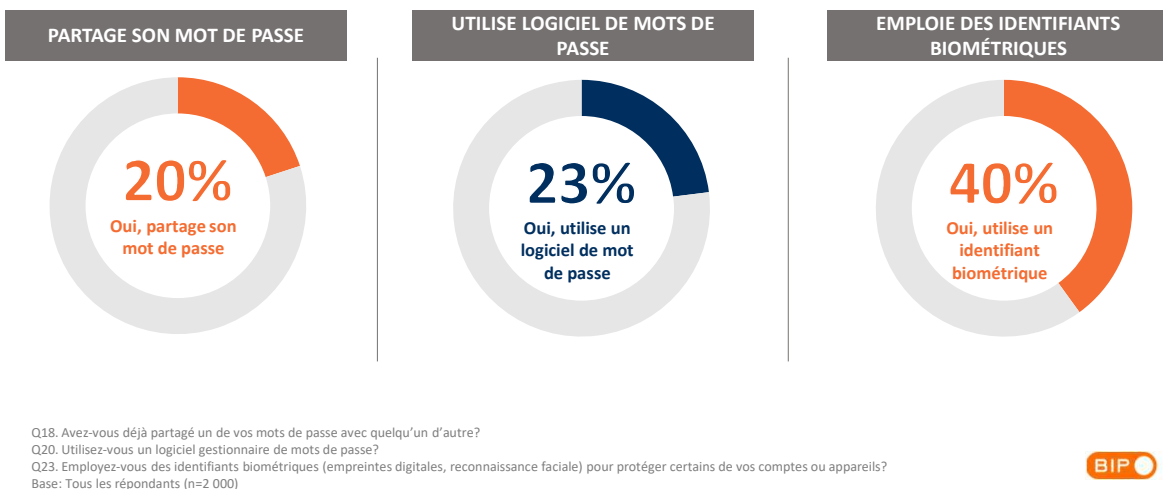
Au cumul, c'est le tiers des Canadiens qui lisent les politiques de confidentialité et les conseils de cybersécurité et se renseignent sur les pratiques de cybersécurité des entreprises avant d'utiliser ses services en ligne. C'est davantage le cas des 18-34 ans, des Québécois et de ceux qui passent moins de 10 heures par semaine sur Internet.



21

Mot de passe et identifiant

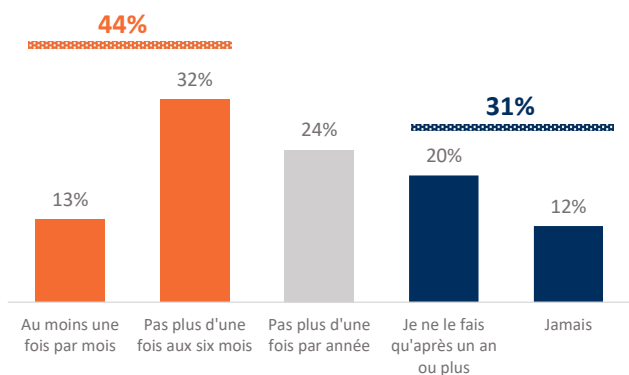
Un Canadien sur cinq partage son mot de passe avec d'autres, surtout les 18-34 ans. Près du quart utilise un logiciel gestionnaire de mots de passe (surtout les hommes, les 18-34 ans et les Ontariens) et 40% un identifiant biométrique (comme une empreinte digitale ou la reconnaissance faciale) (surtout les 18-34 ans, les universitaires et les résidents des provinces de l'Ouest).



22

Fréquence de modification du mot de passe

Près du tiers des Canadiens changent leur mot de passe moins d'une fois par année ou même jamais (*surtout les 18-34 ans et les personnes n'ayant jamais été victimes d'un bris de sécurité ou d'un vol d'identité*), alors que près de la moitié les modifient aux six mois ou plus fréquemment (*surtout les 35-54 ans, les Ontariens et ceux ayant déjà été victimes d'un bris de sécurité ou vol d'identité*).



Q22. En général, à quelle fréquence modifiez-vous vos mots de passe?
Base: Tous les répondants (n=2 000)

Précautions contre les menaces en ligne

Les précautions les plus fréquentes que prennent les Canadiens pour se protéger des menaces en ligne sont de ne pas télécharger des pièces jointes de courriels d'inconnus, protéger leur réseau WI-FI par un mot de passe, ne pas accepter les inconnus comme amis sur les réseaux sociaux, employer un antivirus et faire des transactions en ligne sur des réseaux sécurisés.

Ne pas télécharger de pièces jointes dans des courriels provenant d'inconnus	71%
Protéger son réseau WI-FI personnel par un mot de passe	66%
Ne pas accepter des gens que vous ne connaissez pas comme amis sur les réseaux sociaux	64%
Employer un logiciel antivirus	62%
Faire des transactions en ligne sur des réseaux sécurisés	60%
Limiter les renseignements partagés sur les réseaux sociaux	57%
Faire régulièrement les mises à jour de vos logiciels	52%
Supprimer les témoins sur mon fureteur (cookies)	49%
Utiliser un réseau privé virtuel (VPN)	18%
S'abonner à un système de surveillance de la fraude (exemple: Equifax)	17%
Utiliser un service de messagerie chiffrée	16%
Autres	1%

Q24. Parmi les précautions suivantes pour mieux se protéger des menaces en ligne, lesquelles avez-vous adopté?
Base: Tous les répondants (n=2 000)

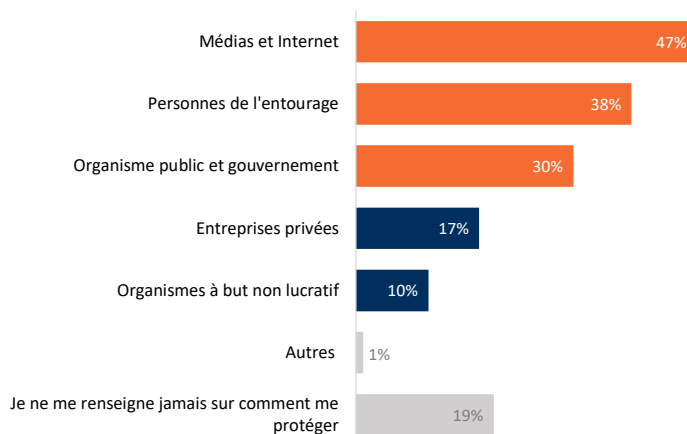
Préoccupations

25

25

Sources de renseignement

Les Canadiens se renseignent sur la protection contre les menaces en ligne d'abord par les médias et ensuite par les personnes de leur entourage. Le tiers se fie aux organismes publics et aux gouvernements. C'est près d'un Canadien sur cinq qui affirme ne jamais s'informer sur comment se protéger.



Q25. Où vous renseignez-vous pour savoir quoi faire pour vous protéger des menaces en ligne?
Base: Tous les répondants (n=2 000)

BIP 26

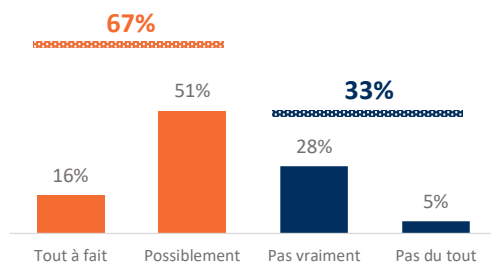
26

Confiance en eux et craintes envers entreprises

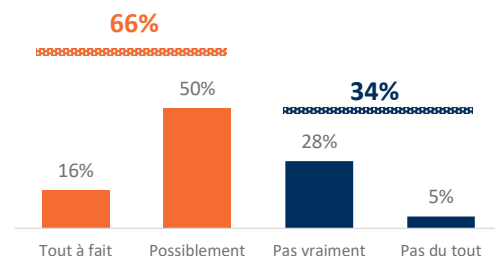
Les deux tiers des Canadiens ont l'impression de savoir comment se protéger contre les bris de sécurité et quoi faire s'ils en sont victimes (surtout les hommes, les 18-44 ans et les universitaires).

Toutefois, la même proportion craint qu'une entreprise avec qui ils transigent en ligne soit la cible d'un bris de sécurité au cours des deux prochaines années (surtout les hommes, les 35-54 ans, les universitaires et ceux qui passent plus de 10 heures par semaine sur le web).

CONFIANCE EN LEUR HABILITÉ À SE PROTÉGER ET À RÉAGIR



CRAINTE QUE LES ENTREPRISES SOIENT LA CIBLE D'UN BRIS



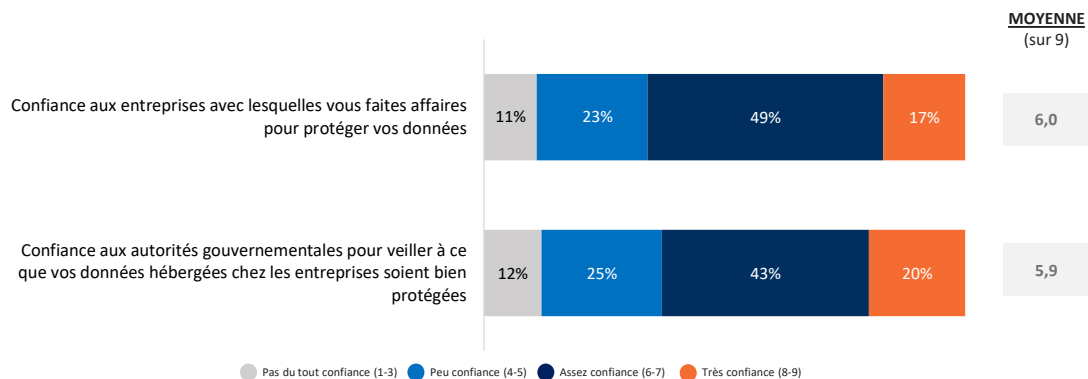
Q26. Avez-vous le sentiment de savoir quoi faire pour vous protéger contre les bris de sécurité et comment y réagir si vous en êtes victime?
Q27. Craignez-vous qu'une entreprise en ligne dont vous utilisez les services soit la cible d'un bris de sécurité dans les deux prochaines années?
Base: Tous les répondants (n=2 000)

BIP 27

27

Confiance aux entreprises et aux autorités

Les deux tiers des Canadiens disent avoir confiance envers les entreprises (66%) ou envers les autorités gouvernementales (63%) pour protéger leurs données hébergées chez les entreprises. Les plus confiants sont plus nombreux parmi les gens plus âgés (55 ans ou plus) et parmi ceux qui se renseignent davantage en lisant les politiques de confidentialité, les conseils de cybersécurité et les pratiques de cybersécurité des entreprises avant d'utiliser leurs services en ligne.



Q28. Sur une échelle de 1 à 9, où 1 signifie « Pas du tout » et 9 signifie « Tout à fait », à quel point faites-vous confiance aux entreprises avec lesquelles vous faites affaires pour protéger vos données?
Q29. Sur une échelle de 1 à 9, où 1 signifie « Pas du tout » et 9 signifie « Tout à fait », à quel point faites-vous confiance aux autorités gouvernementales pour veiller à ce que vos données hébergées chez les entreprises soient bien protégées?
Base: Tous les répondants (n=2 000)

BIP 28

28

ANNEXE



29

Questionnaire (1/5)

OPTION CONSOMMATEURS
Étude Cybersécurité
Questionnaire (FINALE)

QUESTIONS SOCIO-DÉMOGRAPHIQUES

PROV. Quelle est votre province/territoire de résidence?

Colombie-Britannique	01
Alberta	02
Saskatchewan	03
Manitoba	04
Ontario	05
Québec	06
Nouveau-Brunswick	07
Nouvelle-Écosse	08
Île du Prince-Édouard	09
Terre-Neuve / Labrador	10
Territoires du Nord-Ouest	11
Yukon	12
Nunavut	13

CODE. Quel est votre code postal?

AGE. Quel âge avez-vous ?

Moins de 18 ans	1
Entre 18 et 24 ans	2
Entre 25 et 34 ans	3
Entre 35 et 44 ans	4
Entre 45 et 54 ans	5
Entre 55 et 64 ans	6
Entre 65 et 74 ans	7
75 ans et plus	8

SEXE. Êtes-vous de sexe :

Masculin	1
Féminin	2

Note : comme indiqué par Statistique Canada, les Canadiens transgenres, transsexuels et intersexuels doivent indiquer le sexe (masculin ou féminin) auquel ils s'identifient le plus.

1

LANGUE. Quelle est la langue que vous avez apprise en premier lieu à la maison dans votre enfance et que vous comprenez toujours ?

Français	1
Anglais	2
Autre	3
Français et anglais	4
Français et autres	5
Français et anglais et autres	6
Anglais et autres	7
Autre(s) et autre(s)	8

SCOL. Quel est le plus haut niveau de scolarité que vous ayez complété (diplôme obtenu)?

Primaire	1
Secondaire général ou professionnel	2
Collège général postsecondaire ou professionnel technique	3
Universitaire	4

PORTRAIT VIRTUEL DES RÉPONDANTS

Q1. Parmi les activités suivantes, lesquelles faites-vous en ligne?

[PLUSIEURS MENTIONS - ALÉATOIRE]

Aller sur les médias sociaux	01
Utiliser des services de messagerie ou de courriel	02
Magasiner	03
Visionner du contenu sur abonnement (streaming)	04
Faire des transactions bancaires	05
Autres activités (veuillez préciser : _____)	97

ANCER. OUVERTE.

Q2. Excluant le temps passé pour le travail ou les études, combien d'heures passez-vous habituellement sur Internet par semaine?

Moins de 5 heures par semaine	1
De 5 à moins de 10 heures par semaine	2
De 10 à moins de 20 heures par semaine	3
De 20 à moins de 40 heures par semaine	4
40 heures ou plus par semaine	5

2



30

30

Questionnaire (2/5)

EXPÉRIENCES

[PRÉSENTER SUR UNE PAGE DISTINCTE]

MESSI. Un **bris de sécurité** survient lorsque les données hébergées par une entreprise sont volées par une personne malintentionnée ou qu'elles sont compromises de toute autre manière.

Les **données** faisant l'objet d'un **bris de sécurité** peuvent inclure, notamment, votre nom, vos coordonnées, votre date de naissance, vos renseignements financiers ainsi que toute autre information sur vos activités en ligne.

Q3. Avez-vous été victime du bris de sécurité survenu chez l'institution financière Desjardins au cours de l'été 2019?

Oui 1
Non 2
Je ne sais pas/incertain(e) 9

[DEMANDEZ SI Q3-1 (A SUBI UN BRIS CHEZ DESJARDINS)]

Q3A. Quel est votre niveau de satisfaction quant à la manière dont Desjardins a géré la situation?

Très satisfait 1
Plutôt satisfait 2
Plutôt insatisfait 3
Très insatisfait 4

[DEMANDEZ SI Q3-1 (A SUBI UN BRIS CHEZ DESJARDINS)]

Q3A. Avez-vous cessé de faire affaire avec Desjardins après que vous ayez appris qu'elle a fait l'objet d'un bris de sécurité?

Oui 1
Non 2

[DEMANDEZ SI Q3-1 (A SUBI UN BRIS CHEZ DESJARDINS)]

Q3A. Parmi les démarches suivantes, lesquelles avez-vous faites après avoir entendu parler du bris de sécurité chez Desjardins?

[PLUSIEURS MENTIONS - ALÉATOIRE]

Consulter votre dossier de crédit 01
S'inscrire à un service de protection contre la fraude 02
Changer des mots de passe ou des questions de sécurité 03
Activer l'authentification à deux facteurs 04
Supprimer mon compte auprès de l'entreprise 05
Rechercher de l'information sur la façon de se protéger 06

Autres (veuillez préciser : _____) 97 **ANCHER, OUVERTE.**
Je n'ai fait aucune démarche 99 **ANCHER, EXCLUSIF.**

Q4. Outre Desjardins, à votre connaissance, une entreprise dont vous utilisez les services sur Internet a-t-elle déjà été la cible d'un bris de sécurité?

Oui 1
Non 2
Je ne sais pas/incertain(e) 9

[DEMANDEZ SI Q4-1 (A SUBI UN BRIS)]

Les prochaines questions portent sur ce(s) bris de sécurité vécu(s) dans ces entreprises autre que Desjardins.

Q5. Quelle(s) entreprise(s) a fait l'objet d'un tel bris?

Veuillez inscrire votre(s) réponse(s) : _____ 97 **OUVERTE**

[DEMANDEZ SI Q4-1 (A SUBI UN BRIS)]

Q6. Croyez-vous que vos données ont été compromises lors de l'un de ces bris de sécurité?

Oui 1
Non 2
Je ne sais pas 9

[DEMANDEZ SI Q4-1 (A SUBI UN BRIS) ET SI Q6-1 (DONNÉES COMPROMISES)]

Q7. Comment avez-vous appris que vous étiez victime d'un bris de sécurité?

NOTE : Si vous avez subi un bris de sécurité dans plus d'une entreprise (autre que Desjardins), veuillez cocher toutes les situations qui s'appliquent.

[PLUSIEURS MENTIONS - ALÉATOIRE]

Par un courriel ou un sms reçu sur Internet 01
Par une lettre postale 02
En visitant le site de l'entreprise 03
Par les médias 04
Par des amis ou des connaissances 05
Autres (veuillez préciser : _____) 97 **ANCHER, OUVERTE.**

Questionnaire (3/5)

[DEMANDEZ SI Q4-1 (A SUBI UN BRIS) ET SI Q6-1 (DONNÉES COMPROMISES)]

Q8A. Quel est votre niveau de satisfaction quant à la manière dont l'entreprise a géré la situation?

NOTE : Si vous avez subi un bris de sécurité dans plus d'une entreprise (autre que Desjardins), veuillez donner votre appréciation générale.

Très satisfait 1
Plutôt satisfait 2
Plutôt insatisfait 3
Très insatisfait 4

[DEMANDEZ SI Q4-1 (A SUBI UN BRIS)]

Q9A. Avez-vous déjà cessé de faire affaire avec une entreprise en ligne après que vous ayez appris qu'elle a fait l'objet d'un bris de sécurité?

Oui 1
Non 2

[DEMANDEZ SI Q4-1 (A SUBI UN BRIS)]

Q10A. Parmi les démarches suivantes, lesquelles avez-vous déjà faites après avoir entendu parler d'un bris de sécurité?

[PLUSIEURS MENTIONS - ALÉATOIRE]

Consulter votre dossier de crédit 01
S'inscrire à un service de protection contre la fraude 02
Changer des mots de passe ou des questions de sécurité 03
Activer l'authentification à deux facteurs 04
Supprimer mon compte auprès de l'entreprise 05
Rechercher de l'information sur la façon de se protéger 06

Autres (veuillez préciser : _____) 97 **ANCHER, OUVERTE.**
Je n'ai fait aucune démarche 99 **ANCHER, EXCLUSIF.**

Q11. Parlez maintenant de vol d'identité.

Un **vol d'identité** survient lorsqu'un fraudeur utilise les données qu'il a volées pour faire une fraude, par exemple pour se procurer une carte de crédit au nom d'une autre personne.

À votre connaissance, avez-vous déjà été victime d'un vol d'identité?

Oui 1
Non 2
Je ne sais pas 9

[DEMANDEZ SI Q11-1 (VICTIME VOL IDENTITÉ)]

Q12. Croyez-vous que ce vol d'identité résulte d'un bris de sécurité survenu dans une entreprise dont vous utilisez les services en ligne?

Oui 1
Non 2
Je ne sais pas/incertain(e) 9

COMPORTEMENTS

Q13. Est-ce que vous vous renseignez sur les pratiques en matière de cybersécurité d'une entreprise avant d'utiliser ses services en ligne?

Oui, toujours 1
Oui, parfois 2
Non, rarement 3
Non, jamais 4

Q14. Lisez-vous les politiques de confidentialité et les conditions d'utilisation des entreprises dont vous utilisez les services en ligne?

Oui, toujours 1
Oui, parfois 2
Non, rarement 3
Non, jamais 4

Q15. Lisez-vous les conseils en matière de cybersécurité de ces entreprises?

Oui, toujours 1
Oui, parfois 2
Non, rarement 3
Non, jamais 4

Q16. L'**authentification à deux facteurs** est une méthode de sécurisation de vos comptes en ligne qui demande que vous fournissiez, lors de votre connexion, un code qui vous est envoyé sur votre téléphone en plus de votre mot de passe.

Lorsque les entreprises offrent cette option, employez-vous l'authentification à deux facteurs?

Oui, toujours 1
Oui, parfois 2
Non, rarement 3
Non, jamais 4

Questionnaire (4/5)

Q17. Sur les médias sociaux, modifiez-vous les paramètres de protection de la vie privée par défaut pour limiter les auditeurs qui peuvent voir ce que vous publiez?

Oui, toujours 1
Oui, parfois 2
Non, rarement 3
Non, jamais 4
Ne s'applique pas 9

Q18. Avez-vous déjà partagé un de vos mots de passe avec quelqu'un d'autre?

Oui 1
Non 2

Q19. Conservez-vous par écrit, dans un cahier ou autre, vos mots de passe?

Oui, toujours 1
Oui, parfois 2
Non, rarement 3
Non, jamais 4

Q20. Utilisez-vous un logiciel gestionnaire de mots de passe?

Oui 1
Non 2

Q21. Utilisez-vous le même mot de passe sur plusieurs comptes?

Oui, toujours 1
Oui, parfois 2
Non, rarement 3
Non, jamais 4

Q22. En général, à quelle fréquence modifiez-vous vos mots de passe?

Au moins une fois par mois 1
Pas plus d'une fois aux six mois 2
Pas plus d'une fois par année 3
Je ne le fais qu'après un an ou plus 4
Jamais 5

Q23. Employez-vous des identifiants biométriques (empreintes digitales, reconnaissance faciale) pour protéger certains de vos comptes ou appareils?

Oui 1
Non 2

Q24. Parmi les précautions suivantes pour mieux se protéger des menaces en ligne, lesquelles avez-vous adoptées?

[PLUSIEURS MENTIONS - ALÉATOIRE]

Employer un logiciel antivirus 01
Supprimer les témoins sur son navigateur (cookies) 02
Utiliser un réseau privé virtuel (VPN) 03
Faire régulièrement les mises à jour de vos logiciels 04
Utiliser un service de messagerie chiffrée 05
Protéger son réseau Wi-Fi personnel par un mot de passe 06
Faire des transactions en ligne sur des réseaux sécurisés 07
S'abonner à un système de surveillance de la fraude (exemple : Equifax) 08
Ne pas télécharger de pièces jointes dans des courriels provenant d'inconnus 09
Limiter les renseignements partagés sur les réseaux sociaux 10
Ne pas accepter des gens que vous ne connaissez pas comme amis sur les réseaux sociaux 11
Autres (veuillez préciser : _____) 97

ANCHER, OUVERTE.

CONNAISSANCES/PRÉOCCUPATIONS

Q25. Où vous renseignez-vous pour savoir quoi faire pour vous protéger des menaces en ligne?

[PLUSIEURS MENTIONS - ALÉATOIRE]

Organisme public et gouvernement 01
Entreprises privées 02
Organismes à but non lucratif 03
Médias et Internet 04
Personnes de l'entourage 05
Autres (veuillez préciser : _____) 97
Je ne me renseigne jamais sur comment me protéger 99

ANCHER, OUVERTE.

ANCHER, EXCLUSIF.

Q26. Avez-vous le sentiment de savoir quoi faire pour vous protéger contre les bris de sécurité et comment s'écarter si vous en êtes victime?

Oui, tout à fait 1
Oui, probablement 2
Non, pas vraiment 3
Non, pas du tout 4

8

BIP 33

33

Questionnaire (5/5)

Q27. Craignez-vous qu'une entreprise en ligne dont vous utilisez les services soit la cible d'un bris de sécurité dans les deux prochaines années?

Oui, tout à fait 1
Oui, probablement 2
Non, pas vraiment 3
Non, pas du tout 4

Q28. Sur une échelle de 1 à 9, où 1 signifie « Pas du tout » et 9 signifie « Tout à fait », à quel point faites-vous confiance aux entreprises avec lesquelles vous faites affaires pour protéger vos données?

1 2 3 4 5 6 7 8 9
Pas du tout confiance Tout à fait confiance

Q29. Sur une échelle de 1 à 9, où 1 signifie « Pas du tout » et 9 signifie « Tout à fait », à quel point faites-vous confiance aux autorités gouvernementales pour veiller à ce que vos données hébergées chez les entreprises soient bien protégées?

1 2 3 4 5 6 7 8 9
Pas du tout confiance Tout à fait confiance

PROFIL SOCIODÉMOGRAPHIQUE

Pour terminer, quelques questions qui permettront de classer vos données.

FOYER. En vous indiquant, combien de personnes résident à votre adresse actuelle?

a) Nombre d'adultes (18 ans et plus) : _____ [BORNES 1 À 10]
b) Nombre d'enfants (moins de 18 ans) : _____ [BORNES 0 À 10]
[CALCULER FOYER = FOYERa + FOYERb]

[DEMANDEZ SI FOYERb=0 (A DES ENFANTS)]

ENFANT. Dans quel(s) groupe(s) d'âge se situe(nt) les enfants âgés de moins de 18 ans qui habitent avec vous?

Plusieurs réponses possibles. Une réponse par enfant.

[PLUSIEURS MENTIONS]

Moins de 2 ans 1
2 à 6 ans 2
7 à 11 ans 3
12 à 17 ans 4
Je préfère ne pas répondre 9 EXCLUSIF

9

EMPLOI. Quelle est votre situation d'emploi actuelle?
Si vous êtes en congé sabbatique, de maternité, de maladie ou d'accident de travail ou si vous avez vécu un changement de situation suite au Covid-19, veuillez indiquer votre statut habituel.

Employé à temps plein 1
Employé à temps partiel 2
À votre compte / travailleur autonome 3
Ne travaille pas actuellement, mais en recherche d'emploi 4
Ne travaille pas actuellement et ne recherche plus d'emploi / en incapacité de travail 5
Étudiant 6
Au foyer 7
Retraité 8
Je préfère ne pas répondre 9

REVENU. Parmi les catégories suivantes, laquelle reflète le mieux le REVENU total annuel avant impôt de tous les membres de votre foyer?

Moins de 20 000 \$ 1
De 20 000 \$ à 39 999 \$ 2
De 40 000 \$ à 59 999 \$ 3
De 60 000 \$ à 79 999 \$ 4
De 80 000 \$ à 99 999 \$ 5
De 100 000 \$ à 124 999 \$ 6
125 000 \$ ou plus 7
Je préfère ne pas répondre 9

10

BIP 34

34

Appendix 2 – Discussion guide (french version)

INTRODUCTION (5 min)

PRÉSENTATION

- Présentation de l'animatrice
- Rien à vendre
- Confidentialité
- Les informations recueillies ne serviront qu'aux fins de l'étude.

RÈGLES DE DISCUSSION

- Enregistrement
- Parler une personne à la fois, répartition du temps de parole
- Importance de la spontanéité et des opinions personnelles
- Pas de mauvaise réponse

OBJECTIF DE LA RENCONTRE

Ce soir, nous allons parler de **vos données personnelles sur Internet**.

Nous allons parler des **entreprises qui recueillent et conservent ces données**, comme des **institutions financières**, des **commerçants**, des **médias sociaux**, des services de **streaming** et autres.

Les « **données** » peuvent inclure **tous les renseignements que ces entreprises peuvent détenir sur vous** : votre **nom**, vos **coordonnées**, votre **date de naissance**, votre **numéro d'assurance sociale**, vos **informations financières**, vos **identifiants biométriques**, comme vos **empreintes digitales**. Cela englobe aussi des **données comme vos activités sur Internet**, votre **historique de navigation**, votre **géolocalisation**, vos **enregistrements vidéos**, vos **photos**, etc.

Cumul : 5 min

PRÉSENTATION DES PARTICIPANTS (5 min)

TOUR DE TABLE : Parlez-moi un peu de vous:

- votre ville/province de résidence
- votre occupation
- votre situation familiale : habite seul, enfants, etc.
- le nombre d'heures/semaine passées sur internet (excluant le travail ou les études)

Cumul : 10 min

BLOC 1 – ENTREPRISES (25 min)

Pour commencer, j'aimerais **connaître les types d'entreprises dont vous utilisez** les services en ligne (que ce soit d'un ordinateur bureau, portable, d'une tablette ou d'un cellulaire).

MAGASINAGE (5 minutes)

- Commençons d'abord par le magasinage en ligne. À quelle fréquence **magasinez-vous sur internet?**

(Sondage Q1 : Très souvent, À l'occasion, Rarement, Jamais)

- Quels **types de produits** achetez-vous en ligne?

Exemples au besoin :

- *Billets spectacle, cinéma, activités, voyage*
- *Produits technologiques (jeux vidéos, accessoires, tablette, téléphone, etc.)*
- *Produits d'occasion (Kijiji, etc.)*
- *Articles de mode : vêtements, accessoires, souliers*
- *Articles maison, cuisine*
- *Cours et formation en ligne*
- *Santé et bien-être*
- *Nourriture*
- *Musique*
- *Etc.*

- Sur quels **sites ou de quels magasins** achetez-vous en ligne?

SONDEZ :

- *Amazon*
- *Sites locaux vs canadiens vs américains vs européens*
- *Etc.*

- Êtes-vous **préoccupé par la sécurité de vos données** qui sont stockées par ces commerces?

- Si NON : Pourquoi non préoccupé?
- Si OUI : Qu'est-ce qui vous préoccupe? Quelles sont vos craintes?

- Est-ce qu'il y a des sites ou magasins où **vous n'achèteriez pas en ligne pour des raisons de sécurité des données?** Lesquels?

INSTITUTIONS FINANCIÈRES (5 minutes)

- Parlons maintenant des **transactions bancaires en ligne**. Parmi vous, **qui en fait?**

- Quels **types de transactions bancaires** faites-vous en ligne?

Exemples au besoin :

- *Vérifier solde du compte*
- *Faire des virements (entre comptes, entre personnes)*
- *Payer des factures*
- *Commander des chèques*
- *Acheter des placements (stocks, obligations, etc.)*
- *Etc.*

- Avec quelles **institutions financières** transigez-vous en ligne?

SONDEZ :

- *Desjardins*
- *Banques en ligne seulement (Tangerine)*
- *Etc.*

- Êtes-vous **préoccupé par la sécurité de vos données** qui sont stockées par ces institutions financières?

- Si NON : Pourquoi non préoccupé?
- Si OUI : Qu'est-ce qui vous préoccupe? Quelles sont vos craintes?

- Est-ce qu'il y a des institutions financières avec lesquelles **vous ne feriez pas affaire en ligne pour des raisons de sécurité des données**? Lesquelles?

SERVICES DE COURRIEL (5 minutes)

- Parlons maintenant des services de courriel en ligne. D'abord, **qui utilise le courriel** en dehors du travail?

- Quels services de **courriel** utilisez-vous?

SONDEZ :

- *Google Gmail*
- *Etc.*

- Êtes-vous **préoccupé par la sécurité de vos données** qui sont stockées par ces entreprises?

- Si NON : Pourquoi non préoccupé?
- Si OUI : Qu'est-ce qui vous préoccupe? Quelles sont vos craintes?

- Est-ce qu'il y a des services de courriel en ligne **que vous n'utiliserez pas pour des raisons de sécurité des données**? Lesquels?

SERVICES DE STREAMING (5 minutes)

- **Parlons maintenant de services de streaming** (films, émissions de télé, musique). **Qui utilise** ou est abonné à ce genre de service en ligne?
(Sondage Q2: Présentement, Dans le passé, Jamais)
- **À quels services de streaming** êtes-vous ou avez-vous déjà été abonné?
SONDEZ :
 - *Netflix*
 - *Spotify*
 - *Sites locaux comme Tou.tv, CTV, etc.*
 - *Etc.*
- Êtes-vous **préoccupé par la sécurité de vos données** qui sont stockées par ces entreprises?
 - Si NON : Pourquoi non préoccupé?
 - Si OUI : Qu'est-ce qui vous préoccupe? Quelles sont vos craintes?
- Est-ce qu'il y a des services de streaming auxquels **vous ne seriez jamais abonné pour des raisons de sécurité des données**? Lesquels?

MÉDIAS SOCIAUX (5 minutes)

- Maintenant, à quelle fréquence **utilisez-vous les médias sociaux**?
Par médias sociaux, on entend Facebook, Instagram, Twitter, YouTube, LinkedIn, Pinterest, Snapchat, WhatsApp, TikTok, etc.
(Sondage Q3: Plusieurs fois par jour, Une fois par jour, Quelques fois par semaine, Quelques fois par mois, Quelques fois par année, Jamais)
- Quels **réseaux sociaux** utilisez-vous le plus régulièrement?
Exemples au besoin :

- <i>Facebook</i>	- <i>Pinterest</i>
- <i>Instagram</i>	- <i>Snapchat</i>
- <i>Twitter</i>	- <i>WhatsApp</i>
- <i>YouTube</i>	- <i>TikTok</i>
- <i>LinkedIn</i>	- <i>Etc.</i>
- Êtes-vous **préoccupé par la sécurité de vos données** qui sont stockées par ces réseaux sociaux?

- Si NON : Pourquoi non préoccupé?
- Si OUI : Qu'est-ce qui vous préoccupe? Quelles sont vos craintes?
- Est-ce qu'il y a des réseaux sociaux que **vous n'utiliserez pas** pour des raisons de sécurité des données? Lesquels?

POUR TOUTES LES ACTIVITÉS EN LIGNE (5 minutes)

Les prochaines questions portent sur toutes les activités en ligne dont nous venons de parler : magasinage, institutions financières, courriel, streaming, médias sociaux.

- Selon vous, quelles sont les **mesures de sécurité** que ces entreprises emploient pour **protéger** vos données?
- Vous **renseignez-vous sur les pratiques en matière de cybersécurité** d'une entreprise avant de faire affaire avec elle ou d'ouvrir un compte chez elle?
(Sondage **Q4** : *Toujours, À l'occasion, Rarement, Jamais*)
 - Si NON : Pourquoi?
 - Si OUI : Comment le faites-vous?
Que recherchez-vous comme information?
Facile ou difficile à trouver?
- Que pensez-vous des **politiques de confidentialité ou des conditions d'utilisation** que les entreprises vous présentent et vous demandent d'accepter avant d'utiliser leurs services en ligne ou encore lors de l'ouverture d'un compte?
 - Est-ce que ces politiques **sont généralement rédigées ou présentées de façon à motiver** leur lecture, à donner envie de les lire? Pourquoi?
- À votre avis, est-il **utile ou nécessaire de lire ces politiques de confidentialité** ou conditions d'utilisation? Pourquoi?
- Selon vous, **est-ce que la majorité des gens lisent** ces politiques de confidentialité?
 - Si OUI : Au complet ou en partie?
 - Si NON : Pourquoi? Quels sont les raisons qui expliquent que les gens ne les lisent pas?
- Et vous personnellement, lisez-vous généralement **les politiques de confidentialité ou les conditions d'utilisation** de ces entreprises avant d'utiliser leurs services?
(Sondage **Q5** : *Au complet/toujours, En partie/à l'occasion, Ne lit pas/jamais*)
 - Si NON : Pourquoi?
 - Si OUI : Lesquels lisez-vous?

- Combien de temps prenez-vous pour les lire? Temps acceptable?
- Jugez-vous que la longueur en pages de ces politiques est adéquate?

Cumul : 35 min

BLOC 2 – COMPORTEMENTS (25 min)

Dans le prochain bloc, nous allons parler des comportements prudents ou sécuritaires pour protéger la sécurité de nos données en ligne.

- D’abord, avez-vous l’**impression de savoir quels sont les comportements sécuritaires** à adopter pour protéger vos données en ligne?
- Pouvez-vous **nommer des comportements prudents ou des façons de faire sécuritaires** pour protéger nos données en ligne? Que devrait-on faire idéalement? Qu’est-ce qui est recommandé?

Exemples au besoin :

- Effacer les cookies
 - Ne pas cliquer sur un lien reçu par courriel/texto provenant d’un inconnu
 - Ne pas utiliser le même mot de passe sur plusieurs sites/comptes
 - Ne pas utiliser un mot de passe facile à deviner
 - Ne pas partager nos mots de passe avec quelqu’un d’autre
 - Ne jamais modifier nos mots de passe
 - Mettre un mot de passe d’accès à notre téléphone/tablette/ordinateur
 - Ne pas accepter l’invitation d’étrangers sur nos réseaux sociaux
 - Utiliser un gestionnaire/trousseau de mot de passe
 - Utiliser des empreintes digitales ou reconnaissance faciale
 - Etc.
- Personnellement, considérez-vous que vous **avez des comportements prudents/sécuritaires sur Internet**, que vous vous protégez bien en ligne?
(Sondage Q6 : Très sécuritaires, Assez sécuritaires, Peu sécuritaires, Très peu sécuritaires, Je ne sais pas)
 - Si SÉCURITAIRES : Que faites-vous pour vous protéger en ligne? Avez-vous des exemples?
 - Si NON SÉCURITAIRES : Donnez-moi des exemples de vos comportements moins sécuritaires.

PROTECTION DES MOTS DE PASSE

- (SI NON DISCUTÉ AUPARAVANT) Que faites-vous **pour protéger vos mots de passe**?

SONDEZ :

- *Non-utilisation du même mot de passe pour plusieurs comptes*
- *Fréquence de modification des mots de passe*
- *Non-partage d'un mot de passe avec quelqu'un d'autre*
- *Utilisation d'un gestionnaire de mot de passe*

AUTHENTIFICATION À DEUX FACTEURS

- Qui d'entre vous a **déjà entendu parler de l'authentification à deux facteurs**? Qu'en savez-vous?

- LIRE AUX RÉPONDANTS :

L'authentification à deux facteurs est une méthode de sécurisation de vos comptes en ligne qui demande que vous fournissiez, lors de votre connexion, un code qui vous est envoyé sur votre téléphone en plus de votre mot de passe.

Qui d'entre vous utilise l'authentification à deux facteurs?

- Si OUI : Pour quelles raisons l'utiliser? Avez-vous l'impression que ça protège bien vos données?
- Si NON : Pourquoi ne pas l'utiliser?

SONDEZ :

- *Trop compliqué*
- *Trop long/ajoute une étape*
- *Pas si sécuritaire*
- *Etc.*

- **Sur quels sites** utilisez-vous l'authentification à deux facteurs?

SONDEZ :

- *Sites ou comptes bancaires*
- *Sites ou comptes avec information de carte de crédit*
- *Etc.*

- **Pourquoi l'utiliser** avec ces sites **et pas avec d'autres**? Pourquoi ne pas l'utiliser partout?

SONDEZ :

- *L'utilise sur les sites qui l'offrent*
- *Trop long*
- *Etc.*

RENSEIGNEMENT SUR LES FAÇONS DE SE PROTÉGER

- Est-ce que vous vous renseignez **pour savoir quoi faire afin de vous protéger** en ligne?
Et comment vous renseignez-vous?
 - Si OUI : Quelles sources utilisez-vous pour vous renseigner?
 - Si NON : Pourquoi ne pas vous renseigner?

Cumul : 60 min

*****L'animatrice prend connaissance des questions des observateurs.*****

BLOC 3 – BRIS DE SÉCURITÉ (20 min)

Le prochain bloc de questions porte sur les bris de sécurité.

Un bris de sécurité survient lorsque les données hébergées par une entreprise sont volées par une personne malintentionnée ou qu'elles sont compromises de toute autre manière.

Il ne faut pas confondre un bris de sécurité avec un vol d'identité. Un vol d'identité survient lorsqu'un fraudeur utilise des données qu'il a volées pour faire une fraude, par exemple pour se procurer une carte de crédit au nom d'une autre personne.

- À votre connaissance, avez-vous **déjà été victime d'un bris de sécurité** dans une entreprise dont vous utilisez les services en ligne?
(Sondage **Q7** : Oui, Non)

SI OUI :

- Pouvez-vous **expliquer ce qui est survenu**?
 - Quelle est l'entreprise?
 - Comment avez-vous su que vos données avaient été compromises?
 - (le cas échéant) Comment l'entreprise vous a-t-elle avisé du bris?
 - Savez-vous où sont allées vos données?
- **Qu'avez-vous fait**?
 - Cela s'est-il bien passé?
 - Êtes-vous satisfait de la gestion du bris de sécurité par l'entreprise?
- **Faites-vous toujours affaire** avec une entreprise en ligne qui a fait l'objet d'un bris de sécurité? Pourquoi?

- Quelles **conséquences** a eues ce bris de sécurité pour vous?

SONDEZ :

- *Perte de temps?*
- *Stress?*
- *Coûts?*

À TOUS :

- Quel est votre niveau de **crainte de vous être fait voler** vos données sans le savoir?
(Sondage **Q8** : *Grand, Modéré, Léger, Aucune crainte*)
- **Comment** pourriez-vous **le savoir**? Y a-t-il des moyens de le savoir?
- De ce que vous savez, **que doit-on faire après avoir appris qu'on a été victime** d'un bris de sécurité?
- Selon vous, **qu'est-ce qu'il faut faire pour prévenir** les bris de sécurité?

VOL D'IDENTITÉ

Une question maintenant sur le vol d'identité. Je vous rappelle qu'un vol d'identité survient lorsqu'un fraudeur utilise des données qu'il a volées pour faire une fraude, par exemple pour se procurer une carte de crédit au nom d'une autre personne.

- Avez-vous **déjà été victime d'un vol d'identité** (provenant d'internet ou ailleurs)?
(Sondage **Q9** : *Oui, Non*)

SI OUI :

- Pouvez-vous **raconter ce qui s'est passé**?
- Pensez-vous que ce vol d'identité **résulte d'un bris de sécurité** dans une entreprise? Pourquoi?

Cumul : 80 min

BLOC 4 – OBLIGATIONS LÉGALES ET PROSPECTIVES (20 min)

Le dernier bloc de questions porte sur les responsabilités.

- Selon vous, **quelles sont vos obligations légales ou contractuelles** quant à la protection de vos comptes en ligne ou de vos mots de passe?

- Avez-vous des responsabilités? Quelles sont-elles?
- Quels sont **vos recours** lorsqu'il y a un bris de sécurité dans une entreprise?
- **Qu'attendez-vous d'une entreprise** lorsqu'il y a un bris de sécurité? Comment devrait-elle gérer cela?
- Quelle est la **meilleure façon par laquelle une entreprise peut vous informer** d'un bris de sécurité?
- **Pensez-vous que les entreprises en font assez** pour vous informer des mesures de sécurité qu'elles mettent en place?
 - Si NON : Que peuvent-elles faire de plus? (Dans un contexte où vous ne lisez pas leurs politiques de confidentialité ou leurs conditions d'utilisation)
- Croyez-vous qu'il y aura **moins, autant ou plus** de bris de sécurité dans le futur?
(Sondage **Q10** : Moins, Autant, Plus)
Pourquoi?

Cumul : 100 min

CONCLUSION (5 min)

- Y a-t-il des points que nous n'avons pas traités, mais que vous trouvez important que nous sachions?
- Pour terminer, parmi tout ce qui a été discuté aujourd'hui, qu'est-ce que vous retenez le plus?

L'animatrice prend connaissance des questions des observateurs.

Merci!

Cumul : 105 min

Appendix 3 – Discussion guide (english version)

INTRODUCTION (5 min)

PRESENTATION

- Moderator presentation
- Nothing to sell
- Confidentiality
- The information gathered today are for the purposes of the study only.

RULES FOR THE DISCUSSION

- Recordings
- Speak one at a time, allocate turn to speak
- Importance of spontaneity and personnel opinions
- No wrong answers

OBJECTIVES OF THE MEETING

This evening we will talk about **your personal data on the internet**.

We are going to talk about **the companies that collect and store this data**, like **financial institutions, merchants, social media, streaming** services and others.

"Data" can include **any information these companies may hold about you**: your **name, contact details, date of birth, social insurance number, financial information, biometric identifiers**, such as your **fingerprints**. It also includes **data such as your Internet activities**, your **browsing history**, your **geolocation**, your **video recordings**, your **photos**, etc.

Cumulative: 5 min

PARTICIPANT PRESENTATION (5 min)

ROUND TABLE: Tell me a bit about yourself:

- your city/province of residence
- your occupation
- your family situation: live alone, kids, etc.
- the number of hours per week spent on the internet (excluding for work or study)

Cumulative: 10 min

SECTION 1 – BUSINESSES (25 min)

To begin with, I'd like to know the **types of businesses whose online services you use** (whether it is from a desktop, laptop, tablet, or cell phone).

SHOPPING (5 minutes)

- Let's start with online shopping. How **often do you shop on the internet?**
(Survey **Q1**: *Very often, On occasion, Rarely, Never*)
- What **types of products** do you buy online?
Examples if needed:
 - *Tickets for shows, movies, activities, travel*
 - *Technological products (video games, accessories, tablet, phone, etc.)*
 - *Used products (Kijiji, etc.)*
 - *Fashion items: clothes, accessories, shoes*
 - *Home, kitchen items*
 - *Online courses and training*
 - *Health and well-being*
 - *Food*
 - *Music*
 - *Etc.*
- What **sites or stores** do you shop online?
PROBE:
 - *Amazon*
 - *Local vs Canadian vs American vs European sites*
 - *Etc.*
- Are you **concerned about the security of your data** that are stored by these businesses?
 - If NO: Why not concerned?
 - If YES: What are you concerned about? What are your fears?
- Are there any sites or stores that **you would not shop from online for data security reasons?** Which ones?

FINANCIAL INSTITUTIONS (5 minutes)

- Now let's talk about **online banking**. Who among you **does it?**
- What **types of banking transactions** do you do online?

Examples if needed:

- *Check account balance*
 - *Make transfers (between accounts, between people)*
 - *Pay bills*
 - *Order cheques*
 - *Buy investments (stocks, bonds, etc.)*
 - *Etc.*
- Which **financial institutions** do you bank with online?
PROBE:
 - *Desjardins*
 - *Online (virtual) banks (Tangerine)*
 - *Etc.*
 - Are you **concerned about the security of your data** that are stored by these financial institutions?
 - If NO: Why not concerned?
 - If YES: What are you concerned about? What are your fears?
 - Are there any financial institutions that **you would not bank with online for data security reasons**? Which ones?

EMAIL SERVICES (5 minutes)

- Now let's talk about online email services. First, **who uses email**, other than for work?
- What **online email services** do you use?
PROBE:
 - *Google Gmail*
 - *Etc.*
- Are you **concerned about the security of your data** that are stored by these businesses?
 - If NO: Why not concerned?
 - If YES: What are you concerned about? What are your fears?
- Are there any email services that **you would not use for data security reasons**? Which ones?

STREAMING SERVICES (5 minutes)

- **Now let's talk about streaming services** (movies, TV shows, music). **Who uses** or subscribes to this kind of online service?
(Survey **Q2**: *Currently, In the past, Never*)
- **What streaming services** do you subscribe to, currently or in the past?
PROBE:
 - *Netflix*
 - *Spotify*
 - *Local services like Tou.tv, CTV, etc.*
 - *Etc.*
- Are you **concerned about the security of your data** that are stored by these businesses?
 - If NO: Why not concerned?
 - If YES: What are you concerned about? What are your fears?
- Are there any streaming services that **you would not subscribe to for data security reasons**? Which ones?

SOCIAL MEDIA (5 minutes)

- Now how often do you **go on social media**?
By social media we mean Facebook, Instagram, Twitter, YouTube, LinkedIn, Pinterest, Snapchat, Whatsapp, Tik Tok, YouTube, etc.
(Survey **Q3**: *Many times a day, once a day, A few times a week, A few times a month, A few times a year, Never*)
- What **social networks** do you go to most regularly?
Examples if needed:

- <i>Facebook</i>	- <i>Pinterest</i>
- <i>Instagram</i>	- <i>Snapchat</i>
- <i>Twitter</i>	- <i>Whatsapp</i>
- <i>YouTube</i>	- <i>Tik Tok</i>
- <i>LinkedIn</i>	- <i>Etc.</i>
- Are you **concerned about the security of your data** that are stored by these social networks?
 - If NO: Why not concerned?
 - If YES: What are you concerned about? What are your fears?
- Are there any social networks that **you would not use for data security reasons**? Which ones?

FOR ALL ONLINE ACTIVITIES (5 minutes)

The next questions are about all of the online activities we just discussed: shopping, financial institutions, email, streaming, social media.

- What **security measures** do you think these companies employ to protect your data?
- Do you **inform yourself about a company's cybersecurity practices** before doing business with them or opening an account with them?
(Survey **Q4** : *Always, On occasion, Rarely, Never*)
 - If NO: Why?
 - If YES: How do you do inform yourself?
What kind of information do you look for?
Easy or hard to find?
- What do you think of the **privacy policies or terms of use** that companies present and ask you to accept before using their online services or when opening an account?
 - Are these policies **generally written or presented in such a way as to motivate** people to read them, to make them want to read them? Why?
- In your opinion, **is it useful or necessary to read these privacy policies** or terms of use? Why?
- In your opinion, **do the majority of people read** these privacy policies?
 - If YES: In full or in part?
 - If NO: Why? What reasons could explain why people don't read them?
- You personally, do you read **the privacy policies or terms of service** of these companies before using their services?
(Survey **Q5**: *In full/always, In part/on occasion, Don't read/never*)
 - If NO: Why?
 - If YES: Which ones do you read
How long do you take to read them? Acceptable time?
 - Do you think the page length of these policies is adequate, is it the correct length?

Cumulative: 35 min

BLOC 2 – BEHAVIOURS (25 min)

In the next section, we are going to discuss cautious or safe behaviors to protect the security of our data online.

- To start, do you **feel you know what security behaviors you need to adopt** to protect your data online?
- Can you name some safe behaviors to protect our data online? What should we do ideally? What are the recommendations?

Examples if needed:

- Clear cookies
 - Do not click on a link received by email / text from a stranger
 - Do not reuse the same password on multiple sites / accounts
 - Do not use an easy to guess password
 - Do not share your passwords with anyone else
 - Never modifying our passwords
 - Set a log-on password to our phone / tablet / computer
 - Do not accept the invitation of strangers on our social networks
 - Use a password manager software
 - Use fingerprints or facial recognition
 - Etc.
- Personally, do you consider **yourself to be prudent / safe on the Internet**, that you protect yourself well online?
(Survey Q6: Very safe, Somewhat safe, Only a little, Not very, I don't know)
 - If SAFE: What are you doing to protect yourself online? Do you have any examples?
 - If NOT SAFE: Give me examples of your less safe behaviors?

PASSWORD PROTECTION

- (IF NOT DISCUSSED BEFOREHAND) What are you doing to **protect your passwords**?

PROBE:

- Not reusing the same password for multiple accounts
- Frequency of changing passwords
- Not sharing a password with someone else
- Using a password manager software

TWO-FACTOR AUTHENTICATION

- Who among you has **ever heard of two-factor authentication**? What do you know about it?

- READ TO RESPONDENTS:

The two-factor authentication is a method of securing your online accounts when you log in, that requires you provide a code, which was sent to your phone, in addition to your password.

Who of you uses two-factor authentication?

- If YES: What are the reasons for using it? Do you feel like it protects your data well?
- If NO: Why not use it?

PROBE:

- *Too complicated*
- *Too long / adds a step*
- *Not that safe*
- *Etc.*

- **What sites** do you use two-factor authentication at?

PROBE:

- *Banking or bank accounts*
- *Sites or accounts with credit card information*
- *Etc.*

- **Why use it** with these sites and **not with others**? Why not use it everywhere?

PROBE:

- *Uses it on sites that offer it*
- *Takes too long*
- *Etc.*

INFORMATION ON HOW TO PROTECT YOURSELF

- Are you informing yourself on **what to do to protect yourself online**? And how do you find information?
 - If YES: What sources do you use for information?
 - If NO: Why don't you inquire?

Cumulative: 60 min

*** The moderator takes note of the observers' questions. ***

SECTION 3 – SECURITY BREACH (20 min)

The next section pertains to security breaches.

A security breach occurs when the data, hosted by a company, is stolen by a malicious person or is compromised in any other way.

It is important not to confuse security breach and identity theft.

Identity theft occurs when a fraudster uses the data that was stolen for fraud, for example to obtain a credit card in the name of another person.

- To your knowledge, have you **ever been the victim of a security breach** from a company whose online services you use?
(Survey Q7: Yes, No)

IF YES:

- Can you **explain what happened**?
 - What is the company?
 - How did you know your data had been compromised?
 - (if applicable) How did the company notify you of the breach?
 - Do you know where your data has gone?
- **What did you do**?
 - How did it go?
 - Are you satisfied with the company's handling of the breach?
- Are you **still doing business** with an online business that has been the subject of a security breach? Why?
- What **consequences** did this breach of security have for you?
PROBE:
 - *Waste of time?*
 - *Stress?*
 - *Costs?*

TO ALL:

- How **worried are you that your data has been stolen** without knowing it?
(Survey Q8: Very, Moderately, Not very, Not at all)
- **How would you know** that? Are there ways to find out?

- From what you know, **what should you do after learning** about a security breach?
- What do you think **needs to be done to prevent** security breaches?

IDENTITY THEFT

A question on identity theft now. A reminder that **identity theft occurs when a fraudster uses the data that was stolen for fraud**, for example to obtain a credit card in the name of another person.

- Have you ever been a victim of identity theft (from the internet or elsewhere)?
(Survey Q9: Yes, No)

IF YES:

- Can you **tell us what happened**?
- Do you think this identity theft **was the result of a security breach** in a company?
Why?

Cumulative: 80 min

SECTION 4 – LEGAL AND FORWARD-LOOKING OBLIGATIONS (20 min)

The last section pertains to responsibility.

- In your opinion, **what are your legal or contractual obligations** regarding the protection of your online accounts or your passwords?
 - Do you have any responsibility? What are your responsibilities?
- What is **your recourse** when there is a security breach in a business?
- **What do you expect from a business** when there is a security breach? How should they handle it?
- What's the **best way a business can notify you** of a security breach?
- **Do you think companies are doing enough** to let you know what security measures they are putting in?

- If NO: What more can they do? (In a context where you do not read their privacy policies or terms of use)
- Do you think there will be fewer, as many, or more security breaches in the future?
(Survey **Q10**: *Fewer, As much, More*)
Why?

Cumulative: 100 min

CONCLUSION (5 min)

- Are there any points that we haven't covered that you think are important for us to know?
- To finish, of all the topics discussed tonight, what stands out the most?

The moderator collects the last questions from the observers.

Thank you!

Cumulative: 105 min