itworldcanada.com

Understanding Canadian cybersecurity laws: 'Insert something clever here' — Canada's Anti-Spam Legislation (Article 5)

Melissa Lukings and Arash Habibi Lashkari

16-21 minutes

Introduction

As we continue to adapt to the changing demands to navigate the spread of COVID-19, an increasing number of workspaces and social interactions have had to rely much more heavily on email and other online forms of electronic forms of communication. Our increased reliance on electronic messages, particularly in the context of doing business, exposes individuals and organizations to the increased risk of receiving unsolicited commercial electronic messages, which we call "spam". Only a mere six years ago, Canada was home to seven of the world's top 100 spamming organizations. This changed in 2014, with the implementation of Canada's Anti-Spam Legislation.

We have previously outlined the provisions in the *Privacy Act* and the *Access to Information Act* which regulate federal government institutional access to, use of, and disclosure of personal

information. We have also examined the laws regulating private sector access to, use of, and disclosure of personal information, which apply to both federally-regulated and private sector commercial organizations, and were established in the *Personal Information Protection and Electronic Documents Act*. Finally, while governmental institutions, private companies, and organizations are bound by the *Privacy Act* and *PIPEDA*, individual malicious actors are not governed by the same set of laws. For malicious parties participating in cybercriminal activity, the *Criminal Code of Canada* provides the Canadian criminal justice system with the applicable laws and penalties.

In case you missed it

- Understanding Canadian cybersecurity laws: The foundations (Article 1)
- Understanding Canadian cybersecurity laws: Privacy and access to information, the Acts (Article 2)
- Understanding Canadian cybersecurity laws: Privacy protection in the modern marketplace — PIPEDA (Article 3)
- Understanding Canadian cybersecurity laws: Interpersonal privacy and cybercrime — Criminal Code of Canada (Article 4)

This article in the Understanding Canadian Cybersecurity Laws series will focus on Canada's Anti-Spam Legislation (CASL), which is the federal law dealing with spam and other electronic threats and establishes rules for the sending of commercial electronic messages (CEMs) and the installation of computer programs.

Defining 'SPAM'

"Spam", with respect to computer privacy, refers to unwanted or unsolicited commercial electronic messages received over the internet. A **"commercial electronic message"** (CEM) is any electronic message that encourages participation in a commercial activity, such as an email that contains a coupon or tells customers about a promotion or sale. That said, a message that includes hyperlinks to a website or contains business-related information does not make it a commercial electronic message.

Spam messages can be found on Internet forums, in text messages, blog comments, and social media. As an activity, **"spamming"** involves the use of computer messaging systems to send unwanted messages, often unsolicited advertising, to a large number of individual recipients for a prohibited purpose. Spamming is a serious security concern as it may be used as a means to deliver Trojan horses, viruses, worms, spyware, etc.

We can see spamming in the use of advertisement emails for stores, services, and other profitable enterprises, which, prior to 2014, were not required to be sent with the consent of the recipient. The implementation of Canada's Anti-Spam Legislation made this type of advertising scheme more regulated, with violations of these provisions being punishable by fine. If Person A is employed by, or acting on behalf of, a business or organization, then the corporate directors, officers, and agents of that business or organization can be liable for the actions of Person A. Under Canada's Anti-Spam Legislation, the penalties for violating the legislation can be as severe as $1 million for individuals and $10 million for businesses.

While regular spam is simply any unsolicited email, messaging which contains infected attachments, phishing messages, or

malicious URLs, is more specifically known as **"malspam"**. During the earlier stages COVID-19 pandemic, cybercriminals took advantage of the heightened global emotional response to disseminate malspam, under the pretence of providing COVID-19 information and updates, across the globe.

Spam in the cybersecurity landscape

One of the most well-known malspamming threats faced by cybersecurity experts involves the use of a weaponized Rich Text Format (RTF) document — which is a file format used by Microsoft products, including MS Word and MS Office — to exploit a remote code execution vulnerability within MS Office. This was then used to download and execute a Warzone remote access Trojan.

A **"remote code execution"** (RCE) refers to the ability of a cyberattacker to access and make changes to a computer owned by another, without authority, and regardless of where the computer is geographically located. A **"remote access Trojan"** (RAT) is a type of malware program that provides a back door for remote access and administrative control over the target computer. RATs are often downloaded invisibly through a user-requested program — like a game — or sent as an email attachment.

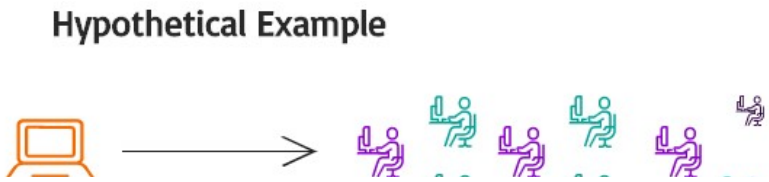
Imperva, a cybersecurity software and services company based in California, has provided data indicating that at the height of the cryptocurrency boom in December 2017, almost 90% of all remote code execution attacks were driven by cryptocurrency mining. They also reported that 88% of all remote code execution attacks in December 2017 involved having a request sent to an external source to try to download a cryptocurrency mining malware.

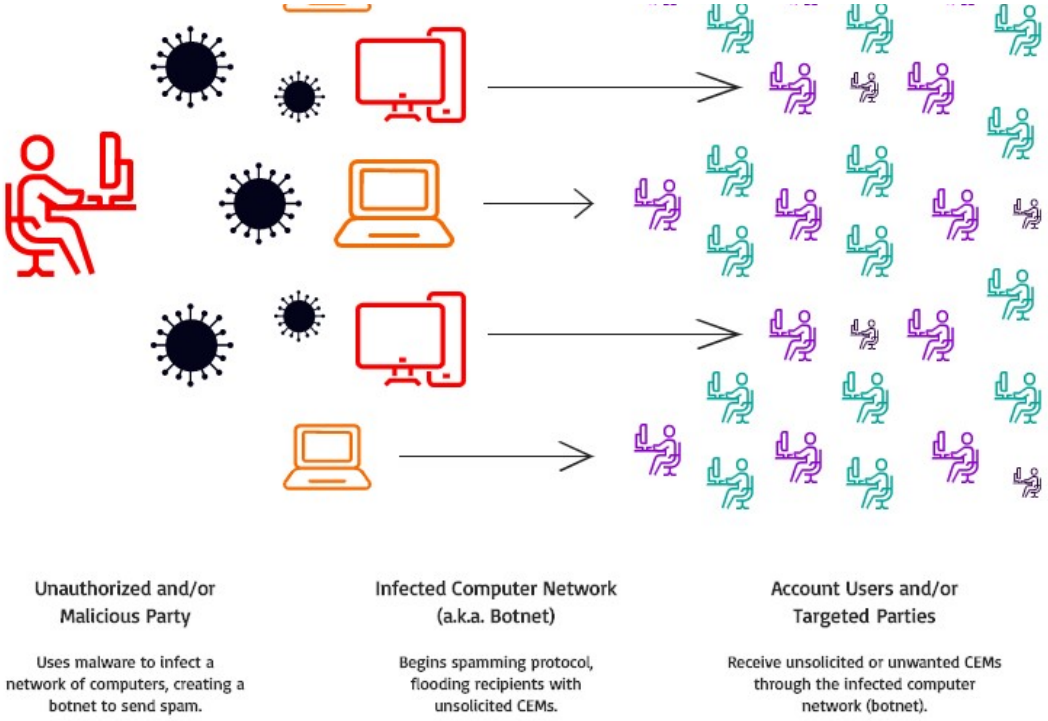
"These attacks try to exploit vulnerabilities in the web application source code, mainly remote code execution vulnerabilities, in order to download and run different crypto-mining malware on the infected server… [which] usually uses all CPU computing power, preventing the CPU from doing other tasks and effectively denies service to the application's users."

— Imperva

Spammers aim to reroute their outbound spam through an external computer, making it less detectable by Spamhaus, the world leader in supplying real-time highly accurate threat intelligence to the Internet's major networks. One of the most common techniques to achieve this is by using an inventory of compromised systems, called a "**botnet**", which can be remotely controlled by an external "**botmaster**". When the botmaster issues a command to the botnet to begin sending out malspam in a widespread attack, it is called "**spamming botnet attack**".

As an example of a **"spamming botnet attack"**, we can consider the below hypothetical case of Person A, an unauthorized or malicious party, who wishes to send out mass communications for the purpose of phishing. In this example, Person A uses malware to infect a network of computers, which creates a botnet. The botnet begins spamming account users or targeted parties, flooding them with unsolicited commercial electronic messages. In this case, the recipients of these unsolicited messages will then be the target of phishing by Person A and potentially exploited for illegal financial gain.





Canada's Anti-Spam Legislation (CASL)

Canada's Anti-Spam Legislation (CASL) aims to protect consumers and businesses from the misuse of digital technology, including spam and other nonconsensual activities. It applies to all electronic messages (like emails and text messages) that businesses and organizations send in connection with a **"commercial activity"** — that is, for the purpose of making a profit. The key feature of this legislation is the requirement that Canadian and global organizations that send commercial electronic messages within, from, or to Canada must receive consent from recipients prior to sending those messages.

It goes much further than regulating the bulk, unsolicited email communications, which we know as spam. Canada's Anti-Spam Legislation creates an "**express consent-based regime"** that applies to almost all electronic messages which are sent for any commercial purpose. Unlike the United States' CAN-SPAM Act,

which relies on opt-out consent or a functioning unsubscribe mechanism, CASL requires "**express opt-in consent**". As well, all requests for consent and almost all commercial electronic messages must meet the prescriptive requirements given for sender and contact person identity and withdrawal of consent. The same opt-in consent standard also applies to the installation of a computer program on a computer, smartphone or other computing devices. There are also prescriptive requirements for both the form and the content of certain user notices and acknowledgments.

To be caught under CASL, commercial electronic messages must be sent to an electronic address. Confirmations of successful unsubscribes, any courtesy SMS sent to roaming customers, and publication of blog posts on micro-blogging and social media sites are out of the scope of this legislation. As well as providing regulations for the use of commercial electronic messages, CASL regulations also include provisions relating to the use of address harvesting tools, the inclusion of misleading sender and subject matter information in an electronic message, and the alteration of transmission data in an electronic message.

The scope of CASL is not limited to activities in Canada. CASL applies to electronic messages where the computer system used to send or access the message is located in Canada. In the case of computer programs, CASL applies if the computer program is installed on a computing device in Canada or if the person who installs or causes the installation of the program is in Canada. This means that parties that are located outside of Canada, and that either send messages to computers located in Canada or install computer programs on devices in Canada, must also operate under the CASL prescriptive requirements.

You do not need to be a spammer, or be located in Canada, for CASL to regulate electronic communications within your business activities. Under CASL, everyday activities – such as simply sending an email message to a customer, operating a company website and making a new mobile application available for download – are all subject to the detailed prescriptive rules for operational practices.

Consent requirement

In order to send a commercial electronic message, businesses and organizations are required to get express consent from recipients—either orally or in writing. Consent given electronically is considered to be written consent. To prove consent, communication records should be made within a reasonable period of time from when the consent was obtained and should include information such as the electronic address, the date and the method that consent was received.

Organizations don't need express consent to send a CEM in the context of an existing business or non-business relationship, or if recipients conspicuously publish their electronic contact information or voluntarily disclose it without indicating they don't want to receive communications. **"Express consent"** means that a person has clearly agreed, either orally or in writing, to receive a CEM. Unless the recipient withdraws his or her consent, express consent is not time-limited. In order to comply with the rules regarding obtaining express consent, organizations should follow a number of steps before sending communications.

In particular, the communication should fulfill two requirements: (1)

it should ask for permission to send future electronic messages, and (2) it should show that the recipient can easily unsubscribe at any time, preferably with one click.

Business communications that are fully exempt from the CASL requirements are those in which **"implied consent"** already exists. This can include commercial electronic messages that are:

(1) sent between family and friends;

(2) sent within or between organizations with an existing business relationship;

(3) solicited or sent in response to complaints, inquiries, requests; or

(4) sent due to a legal obligation or to enforce a right;

Or where:

(5) goods or services were purchased between the sender and the recipient in the previous 2 years;

(6) the recipient has entered a written contract with the sender that expired within the previous two years;

(7) the recipient has accepted a business opportunity from the sender within the previous two years; or

(8) the recipient who has published or provided their electronic address without stating that they do not wish to receive messages, but this only applies if the message is relevant to their business or professional role.

There are also categories of implied consent within an already existing, non-business relationship. These might include a donation, a membership in a club, or a volunteer activity. For

example, if you received a business card from someone, it would likely be considered to be a form of implied consent to send them a commercial electronic message.

Under CASL, telecommunications service providers need consent to install certain computer programs, including programs that prevent unauthorized or suspicious legal activities or programs unrelated to system-wide upgrades or updates. Under CASL, TSPs are permitted to install computer programs without consent for two purposes only: to prevent illegal activities that pose an imminent risk to network security, or to update or upgrade devices across an entire network.

Exemptions to Canada’s Anti-Spam Legislation

Canada’s Anti-Spam Legislation does not apply to commercial electronic messages that are simply routed through Canada or to unsolicited telecommunications — including live voice and automated telemarketing calls, to telephone numbers — which are regulated under the Unsolicited Telecommunications Rules.

There are also five full exemptions to the CASL requirements. Those exemptions apply to:

(1) commercial electronic messages sent from instant messaging platforms where the required identification and unsubscribe mechanisms are clearly published on the user interface;

(2) limited-access, secure, confidential accounts;

(3) commercial electronic messages sent to listed foreign countries, where it is reasonable to believe that the message will

be opened in a listed foreign country that has similar rules as those in CASL;

(4) commercial electronic messages sent by registered charities for the primary purpose of fundraising; and

(5) commercial electronic messages sent by political parties seeking contributions.

There is a partial exemption provided for third-party referral messages. Under this partial exemption, businesses can send one single message to obtain consent for future messages. This means that the first commercial electronic message sent following a referral doesn’t require consent, as long as an existing business, personal or family relationship exists and the sender includes the full name of the individual who made the referral, the identity of the sender and an unsubscribe mechanism. Any commercial electronic message sent following the first referral must then comply with the form and content requirements specified in CASL, including the provision of an unsubscribe mechanism.

Non-compliance

The legislation has penalties for non-compliance with anti-spam provisions. Individuals, businesses and other organizations can file a complaint about receiving unsolicited emails to the Government of Canada’s Spam Reporting Centre. Legitimate complaints may then be referred to the Canadian Radio-television and Telecommunications Commission (CRTC) for investigation.

When the CASL requirements are not followed, corporate directors, officers, and agents can be held liable for corporations, and corporations are liable for the actions of their employees. For

corporations, fines can be up-to $100,000 for the first offence, and $250,000 for repeat offences. For individuals, fines can be $10,000 for a first offence and $25,000 for subsequent offences. Penalties for violating the legislation can be as severe as $1 million for individuals and $10 million for businesses.

Conclusion

Email and electronic messages have become a necessary staple in our day-to-day life; at home, at work, and within our communities. This has been compounded, recently, with the increased reliance on remote workspaces. With electronic communication becoming the prevalent form of communication, it follows that advertising and other commercial communication would also rely on electronic communication services to connect with customers. Canada's Anti-Spam Legislation provides the necessary provisions to reduce the occurrence and impact of unsolicited commercial electronic messages for anyone doing business in Canada.

In our next article, we will discuss interpersonal privacy breaches and cybersecurity violations within the context of the Canadian common law, specifically the tort of intrusion upon seclusion, and the criminal nonconsensual distribution of intimate images.

Would you recommend this article?

Thanks for taking the time to let us know what you think of this article!

We'd love to hear your opinion about this or any other story you read in our publication. **Click this link to send me a note →**

Jim Love, Chief Content Officer, IT World Canada

Related Download

Sponsor: **CanadianCIO**

Cybersecurity Conversations with your Board – A Survival Guide

A SURVIVAL GUIDE BY CLAUDIO SILVESTRI, VICE-PRESIDENT AND CIO, NAV CANADA

Download Now