Have You Been a Victim of Cybercrime?

November 2021 | ITSAP.00.037

The Canadian Centre for Cyber Security (Cyber Centre) and the Royal Canadian Mounted Police (RCMP) co-authored this publication to provide awareness on the identification, reporting, and mitigation of cybercrimes.

WHAT IS CYBERCRIME?

Cybercrime includes crimes in which technology is the primary target (e.g. malware or ransomware) or crimes that use technology as an instrument to commit crimes (e.g. money laundering or fraud).

SHOULD I REPORT IT?

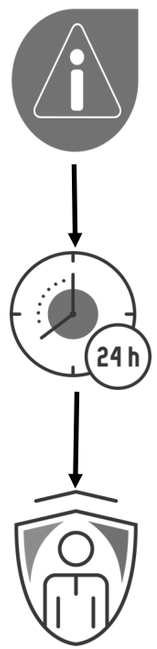
Yes! Whether you are the victim, are reporting for the victim, a business or a witness, we strongly encourage businesses and individuals to report cybercrime to the appropriate law enforcement authorities. You have invaluable information that could make a difference to more than one investigation. For the best outcome, it's important you report the incident within 24 hours of discovering it.

WHERE DO I REPORT A CYBERCRIME?

You should report a cybercrime to your local police department. For geographical areas where the RCMP is the police of jurisdiction, report cybercrimes to the local detachment. File a police report and keep note of the report number for your reference. In addition to reporting to your local law enforcement authorities, you should:

- Report cybercrimes to the Cyber Centre's online portal to get support and advice on how to protect your organization from being targeted repeatedly.
- Report cybercrimes and fraud to the Canadian Anti-Fraud Centre through their Fraud Reporting System. Or by telephone at 1-888-495-8501. The CAFC uses reports to maintain a repository of information to assist law enforcement.
- Inform your businesses, bank, and credit card providers to ensure that your accounts or credit cards have not been affected or targeted.
- Contact Canada's main credit reporting agencies to have a fraud alert added to your credit report.
    - Trans Union Canada (1-866-525-0262, Québec 1-877-713-3393) or
    - Equifax Canada (1-866-779-6440).
- Inform Service Canada if any of your federally-issued identification, such as a passport or a social insurance number, have been affected.

Depending on the nature of the incident, your case may fall under federal authority. In this case, the Royal Canadian Mounted Police (RCMP) may investigate the incident



TYPES OF CYBERCRIMES

RANSOMWARE: A type of malware that denies a user's access to files or systems until a sum of money is paid.

PHISHING: Email or text messages that appear to be from a legitimate source, but contain infected attachments or malicious links. If recipients open the attachments or click on links contained in phishing messages, they may download malware or be directed to malicious websites.

SPAM: Unsolicited messages, generally sent by email, to many recipients to advertise or to achieve malicious intentions.

FRAUD: The act of wrongful or criminal deception intended to result in financial or personal gain.

PROTECT YOURSELF

Follow the best practices below to help enhance your organization's online safety.

- Use different user IDs and password combinations for different accounts. Increase the complexity by combining letters, numbers, and special characters, or use passphrases. Change your passwords and passphrases on a regular basis.
- Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates.
- Research applications before downloading to check for possible scams. Only download from trusted sources to avoid phony or malicious applications.
- Review the privacy and security settings for your social media accounts. Be careful what type of information you post online.
- Establish an incident response plan to enhance your ability to recover from an incident quickly with minimal impact to your organization.

Government of Canada | Gouvernement du Canada

Canada

WHAT CAN I EXPECT?

The investigation process can seem overwhelming to victims. Knowing what to expect if you fall victim to a cybercrime can make the process much easier. The following section provides insight into the investigative process after you

INITIAL STEPS

- Identify potential evidence, preserve it, and ensure nothing is lost or damaged.
- Isolate your network from the Internet and activate your incident response plan.
- Take note of who was present in your organization before, during, and after the incident.
- Appoint a point of contact for law enforcement officers to speak to directly and gather information about the incident.

INVESTIGATIVE PROCESS

- Document the report number provided to you by law enforcement.
- Anticipate law enforcement may need access to your equipment to analyze the technological components of the cyber incident. The police will work with you to collect evidence while minimizing the impacts to your business and recovery efforts.
- Provide logs, employee statements, emails, and other similar items as potential evidence.
- Produce a list of key contacts within your organization for law enforcement.

RECOVERY

- Communicate the incident to staff, business associates, clients, and partners.
- Review your cyber security policies and ensure your staff receive training.
- Consider purchasing anti-malware and anti-virus software for your network and devices.
- Enhance your data security with protective measures (e.g. firewalls, virtual private networks, encryption).
- Prepare your organization for the possibility of testifying in court

DATA BREACHES

Cybercrime often targets the personal and proprietary data you collect, use, and store. It can be stolen and sold or used for malicious intent by threat actors. In Canada, the *Privacy Act* governs the Government of Canada. Private sector organizations are governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and are required to do the following in the event of a data breach:

- Report any data breach involving personal information that poses a risk of significant harm to individuals to the Privacy Commissioner of Canada.
- Notify individuals affected by the breach.
- Retain records related to the breach.

For more information regarding data breaches visit the Privacy Commissioner's website.

"Cybercrime is the most common cyber threat that Canadians and Canadian organizations are likely to encounter."

WHERE CAN I LEARN MORE?

For more information about cybercrimes and the investigative process, visit the RCMP's National Cybercrime Coordination Unit or Cyber Safety websites. Visit the Cyber Centre website to learn more about cyber security topics and find our entire collection of publications.

- Top Measures to Enhance Cyber Security for Small and Medium Organizations (ITSAP.10.035)
- Have You Been Hacked? (ITSAP.00.015)
- Ransomware: How to Prevent and Recover (ITSAP.00.099)
- Protect Your Organization From Malware (ITSAP.00.057)
- Spotting Malicious Email Messages (ITSAP.00.100)

Canada