CYBERCRIME & SECURITY

HOW TO REPORT

& BETTER PROTECT YOURSELF

Cybercrime is generally defined as a criminal offence that targets a computer system or an electronic device, or where a computer system is used as a tool to commit the crime.

Cybercrime is increasing in frequency and complexity every year and is expected to cost the world over $6 trillion annually by 2021. One of the greatest challenges facing law enforcement is the lack of reporting. Like any other crime, a cybercrime needs to be reported to the proper authorities.

Cybercrimes go unreported for several reasons. Embarrassment, perceived stigma attached to a data breach and its impact on brand reputation, lack of information about reporting, or a victim's lack of confidence in the capacity of law enforcement to investigate a cybercrime.

The timely reporting of a cybercrime is important to ensure all potential digital evidence is properly preserved for a law enforcement investigation. With comprehensive reporting, law enforcement can construct a clear picture of cyber threats affecting communities and will be able to provide accurate information on the threats targeting the general public.

Law enforcement strongly recommends that all cybercrime incidents be reported as soon as the crime has been discovered. While collecting any potential digital evidence, law enforcement will take great care to protect the victim's privacy and reputation.

Who to Report To:

- Your local police

What to Report (info to have ready if possible):

- Date, time, and detailed account of the incident
- The impact to you and/or your organization (unable to pay employees, loss of client data, etc.)
- The systems and the data type affected
- Activity log files (e.g. security logs), any suspicious or malicious files, and any communications with the threat actors

When to Report (as soon as possible):

- The incident has directly impacted your life or the operations of your business
- The incident resulted in unauthorized access to sensitive data such as Personally Identifiable Information (PII), financial records, trade secrets, employee records, etc.
- You are being threatened or extorted

CYBER SECURITY AWARENESS MONTH

Ontario

CYBERCRIME & SECURITY
HOW TO REPORT
& BETTER PROTECT YOURSELF

In addition to reporting cybercrimes to your local police force, there are a number of other steps you can take to mitigate the effects of, or recover from, a cybercrime or cyber incident. If you have been a victim of a cyber incident and provided personal or financial information, please contact the following organizations as appropriate:

1. **Call your bank.** If your bank account or credit cards are involved, you'll want to report it, and cancel cards right away to avoid being liable for the losses.
2. **Call the police** and keep note of the report number for reference.
3. **Call Canada's main credit reporting agencies** and put a fraud alert on your credit report:
    1. Trans Union Canada (1-866-525-0262, Québec 1-877-713-3393)
    2. Equifax Canada (1-866-779-6440)
4. **Call Service Canada at 1-800-O-Canada** if any of your federally-issued ID was compromised (for example social insurance number or passport).
5. **Contact the Canada Revenue Agency.** If you believe your Canada Revenue Agency (CRA) user ID or password has been compromised or to disable online access to your information on the CRA login services, contact the CRA.
6. **Call your province/territory.** If you believe your driver's licence or health card was compromised, contact your provincial or territorial ministry responsible for transportation or the provincial or territorial government department responsible for health.
7. **Call the companies where your identity was used.** They will tell you what information they need, whether an investigation has been started and how you can recover the money that was stolen.
8. **Contact the Privacy Commissioner of Canada** for identity theft issues. The Personal Information Protection and Electronic Document Act - (PIPEDA) 1-800-282-1376 or www.priv.gc.ca for advice and assistance. (Note: Quebec, British Columbia, and Alberta have separate privacy laws that are similar to PIPEDA, so please contact your Provincial Commissioner.)
9. **Call the Canadian Anti-Fraud Centre (CAFC)** at 1-888-495-8501 or visit www.antifraudcentre.ca to report any incidents of fraud or cyber-related fraud.

Always take time to record the things you've done to report and recover from the incident. A few extra minutes could save you a lot of frustration down the road. And remember, many of these incidents can be prevented by implementing these five practical measures on all of your devices.

This article has been in collaboration between the Government of Ontario, OPP, Government of Canada, Get Cyber Safe, Public Safety Canada, City of Toronto and University of Toronto