Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY | NATIONAL CYBER THREAT ASSESSMENT 2018

CYBERCRIME

Cybercriminals take advantage of vulnerabilities in software, hardware and human behaviour online. Their goals include stealing personal and commercial information through fraud, and extortion. Cybercriminals targeting Canadians operate around the world, often beyond the reach of Canadian law enforcement agencies.

> ***“Cybercrime is the most common cyber threat that Canadians and Canadian organizations are likely to encounter.”***

Cyber fraud and extortion attempts directed at Canadians are becoming more sophisticated. Cybercriminals use both cyber tools and social engineering. Cybercriminals may defraud Canadians by posing as legitimate organizations, such as government agencies, banks or familiar service providers to entice Canadians to click on malicious links or attachments in order to download malware onto their devices.

Canadians’ exposure to cyber threats has increased due to the prevalence of internet-connected devices, such as televisions, home appliances, digital assistants and home control systems, which often prioritize convenience over security. Security flaws in these devices can be exploited to disrupt the functionality of the device or to use it as a platform to launch further malicious activity.

WHAT IS THE GOVERNMENT OF CANADA DOING?

Through the National Cyber Security Strategy, the Government of Canada is supporting the creation of the RCMP’s National Cybercrime Coordination Unit, which will act as a coordination hub for cyber crime investigations in Canada and work with partners internationally; provide digital investigative advice to Canadian law enforcement; and establish a national reporting mechanism for Canadian citizens and businesses to report cybercrime incidents.

In addition, the Canadian Anti-Fraud Centre operated by the RCMP, the Ontario Provincial Police and the Competition Bureau are Canada’s trusted sources for reporting and mitigating mass marketing fraud.

The Canadian Centre for Cyber Security has published extensive advice and guidance that can help Canadians stay secure online and reduce their likelihood of being successfully targeted by cybercriminals.

TOP TIPS: WHAT YOU CAN DO

- Use different user ID / password combinations for different accounts. Make the passwords more complicated by combining letters, numbers, special characters and change them 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 to prevent potential attacks on older software.
- Download applications from trusted sources to help make your mobile device less vulnerable to viruses and hackers.
- Make sure your social networking profiles are set to private. Check your security settings and be careful what information you post online.
- For more go to cyber.gc.ca

WHERE TO REPORT CYBERCRIME:

- If your bank accounts or credit cards are affected by cybercrime inform your bank and credit card providers.
- If any of your federally issued identification was affected, such as a passport or social insurance number, inform Service Canada.
- Contact Canada’s main credit reporting agencies to have a fraud alert added to your credit report.
- File a police report and keep note of the report number for reference.