The Rise of Cyber Crime Against Individuals

Cybercriminals target individuals. Learn how to build cyber protection in a digital world.

The Rise of Cyber Crime Against Families and Individuals

The COVID-19 pandemic has widened avenues of cyber attack on families and individuals. As many continue to work from home, banking, shopping, and bill paying has continued to move online. Social media connects us more than ever before, and Internet of Things (IoT) devices are linking everything from automobiles to our home appliances.

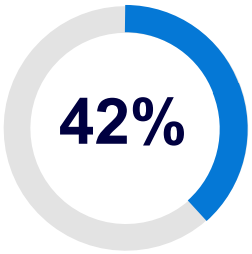
COVID-19 has accelerated digitization for many industries by as many as seven years.[1] According to the Canadian Anti-Fraud Centre, Canadians lost a total of CAD $100 million to online fraud in 2021, in part as a result of increased ability to steal identities.[2]

Because of the sheer volume of potential victims coupled with a relative lack of cyber security practices in the home, individuals can be prime targets. In addition, with the continued growth of remote work, individuals, families, and their guests are often all connecting to a single home network, leaving them more vulnerable than ever.

The potential cost to an individual is enormous. In addition to direct financial losses, individuals can face costs associated with lost time, enhancing security measures, stolen identities and fraudulent accounts, and other associated indirect costs.

Worse, many may think cybercrime only happens to other people — but as many as 42% of Canadians knowingly experienced a cyber security incident in 2020.[3] It's likely that this number is significantly higher today and continues to grow.

Learn how to build protection from the surge in cybercrime. HUB International helps breakdown the various risks, how to protect your digital footprint and what to do if you fall victim to cyber crime.



Of Canadians experienced a cyber security incident in 2020.

Most common forms:

PHISHING

MALWARE

36%
REPORTED LOST TIME, DATA, OR MONEY

SOURCE: *STATISTICS CANADA 2020*

[1] McKinsey & Company, "How COVID-19 has pushed companies over the technology tipping point—and transformed business forever," October 2, 2020. [2] MonsterCloud.com, "Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic," August 11, 2020.
[3] Statistics Canada, *"Canadians spend more money and time online during pandemic and over two-fifths report a cyber incident,"* October 14, 2020.

Cyberthreats: Old tactics, updated for our times

The top cybersecurity threats are familiar to most, but they've been updated for the times, including new aspects or threat vectors. Three of the most common cyberthreats include identity theft, reputational threats, and social engineering:

1. IDENTITY THEFT

In one of the oldest types of cybercrime, fraudsters will access your identity, either selling it immediately or using it later for a bigger payout. Identity theft is also one of the hardest breaches for a victim to uncover. And recovering from identity theft can take an individual on average six months and 100-200 hours of time.[5] Identity theft plays itself out in many ways:

- **Credit monitoring accounts opened with** consumer credit bureaus **in** victims' **names.** Thieves will scan your credit report for accounts or credit cards you're not using and have a new card sent to them.
- **Hacking into cell phones, computers or tablets.** When a device is connected to public WiFi, thieves can swipe personal information. They'll grab login IDs and passwords to financial institutions, email address and password, and any other personal data stored on the device.
- **Leverage breach data.** Thieves will obtain personal information — including Social Insurance Numbers, email addresses, passwords and more — from major data breaches, like the Cit0Day breach that leaked more than 23,000 databases containing more than 13 billion records.
- **Checking your mailbox.** Thieves will canvass neighborhoods and collect mail containing personal information they can sell or leverage to uncover more information about individuals and families.

CASE STUDY

An email hack leads to a major loss

An individual's personal email was hacked, and after watching interactions with her bank for 30 days, the hackers posed as her and asked to have several hundred thousand dollars wired to their account. The bank complied after asking the standard security questions, which the bad actors were able to answer. An additional request two weeks later led to the bank calling the account holder, uncovering the fraud. By then, she had lost thousands of dollars — then law enforcement got involved but the funds were never recouped.

More than 37 billion records were exposed globally in 2020, an increase of 141%.

SOURCE: New Research: No. of Records Exposed Increase of 141% in 2020 — *RiskBasedSecurity.com*

[5] AllState Identity Protection, "How long does it take to correct identity theft," 2020.

2. REPUTATIONAL THREATS

Hackers can and will extort individuals through compromising photos, private information, or known travel plans. In return for not releasing information that may prove damaging, cybercriminals will demand large financial ransoms.

3. SOCIAL ENGINEERING

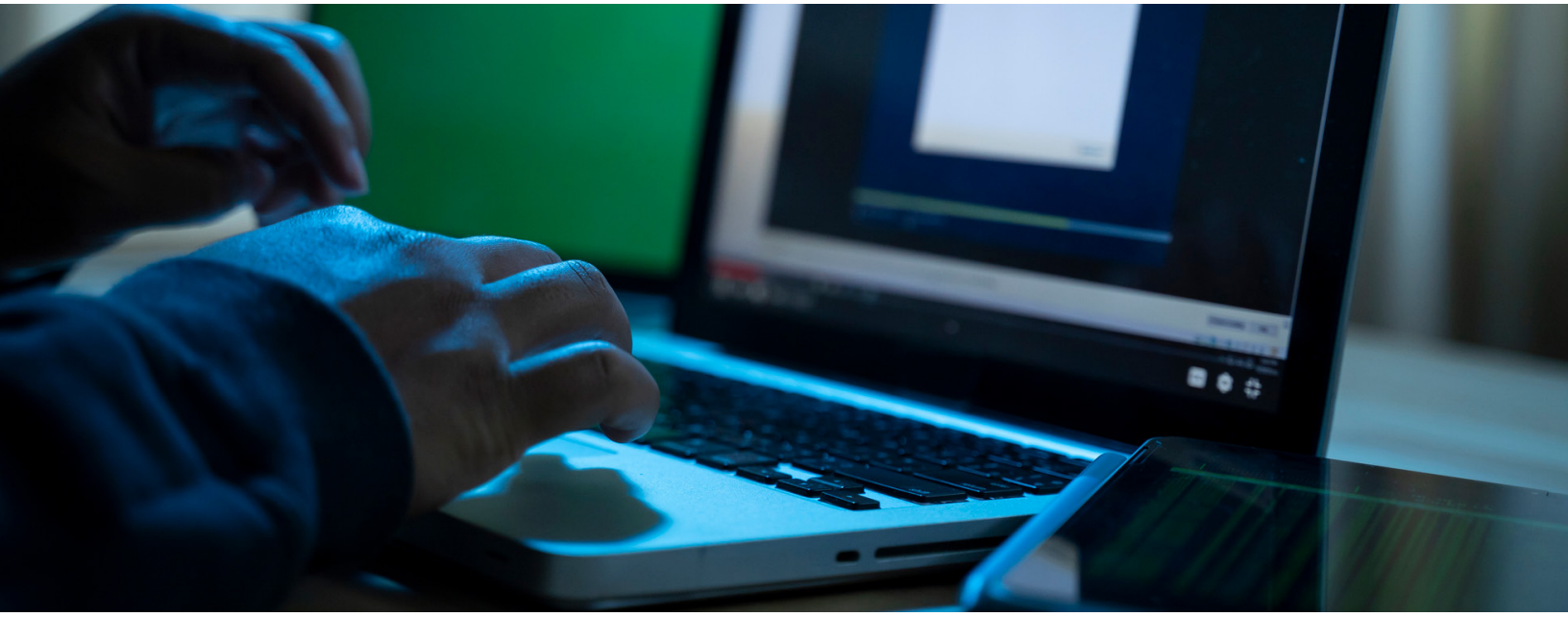
Manipulating someone into releasing money or information through an email or telephone scam is common and profitable. Social engineering usually at its core, requires human error for success, making it the most preventable form of cybercrime.

Although tactics involving mass spamming remain common, sophisticated hackers often target individual victims. A criminal may be in a victim's network for weeks or months and studied their habits and activities to wait for an ideal time to strike.

CASE STUDY

Innocent online photos become an extortion tool

The son of a successful professional uploaded pictures of himself at a party to his Facebook account. A hacker who had been following the teen downloaded and altered the pictures and uploaded them to a website, so he could attempt to extort the family.



How to Build Cyber Walls Around Your Assets

Like a medieval castle with a moat, drawbridge and knights, a multi-tiered approach to cyber security provides extra layers of protection. There are several steps you can take to build these layers and safeguard your assets.

DON'T SKIP THE BASICS. Simple tools and best practices are an important first layer of protection. For example, consider installing password managers like Dashlane or Password1 to create and organize strong, complex passwords for each individual account; use webcam covers to ensure privacy; and consider locking or freezing your credit. Also, be careful about the links you click on, and teach good cyber hygiene to your kids as well.

TWO-FACTOR AUTHENTICATION. Using two-factor authentication — a password and a passcode sent through a different medium — provides a double-locked gate for important information. Set up two-factor on all of your online financial accounts and social media accounts as soon as possible.

TIP: *Using your phone as the second-factor authentication works, but for an added layer use an app authenticator like Authy or software tokens for an even greater level of protection.*

USE DIFFERENT EMAILS FOR DIFFERENT THINGS. By using an email address for work, another for personal use and another for banking, it's easier to identify suspicious communications or compromised accounts. For instance, you'll be able to identify a phishing scam asking for banking information if that email address is not used for your financial accounts.

SEGMENT YOUR HOME NETWORK. While we may trust guests in our homes, it's best to have a separate network for them. An infected device or malicious program inadvertently downloaded on your home network can corrupt all devices using the network. Creating segments in your home network, such as a guest network and segments for other family members, personal matters, and work provides extra levels of protection.

CASE STUDY

Surprise during the mortgage closing

An individual was eagerly anticipating closing on a new home mortgage, only to find out that new fraudulent accounts had been opened in her name between the time she had been approved for the mortgage and the closing date. The identity theft and fraudulent activity took months to resolve.

[6] SecureLink, "80% of Hacking-Related Breaches Leverage Compromised Passwords," December 10, 2020.

STRENGTHEN YOUR WIFI SECURITY. An unlocked internet router gives intruders access to every single device connected to it. Hackers can easily search for default router logins, so change the default name and avoid using personal identifiers in your WiFi name. Anonymous names are more private and therefore more secure.

NEVER USE PUBLIC WIFI

Airport lounges, hotel lobbies and coffee shops are hot spots for hackers. It's best to use secure networks instead. Unlike most home and office wireless networks, the data flowing around a public hotspot is often not encrypted and can serve as a window into any device connected to it.

TIP: *Cybercriminals will often go into public areas of airports and malls to set their computer as an additional hotspot. Be aware of your phone's WiFi automatically connecting to them. Go to your WiFi settings and turn off "Auto-Join Hotspot."*

USE A VIRTUAL PRIVATE NETWORK (VPN)

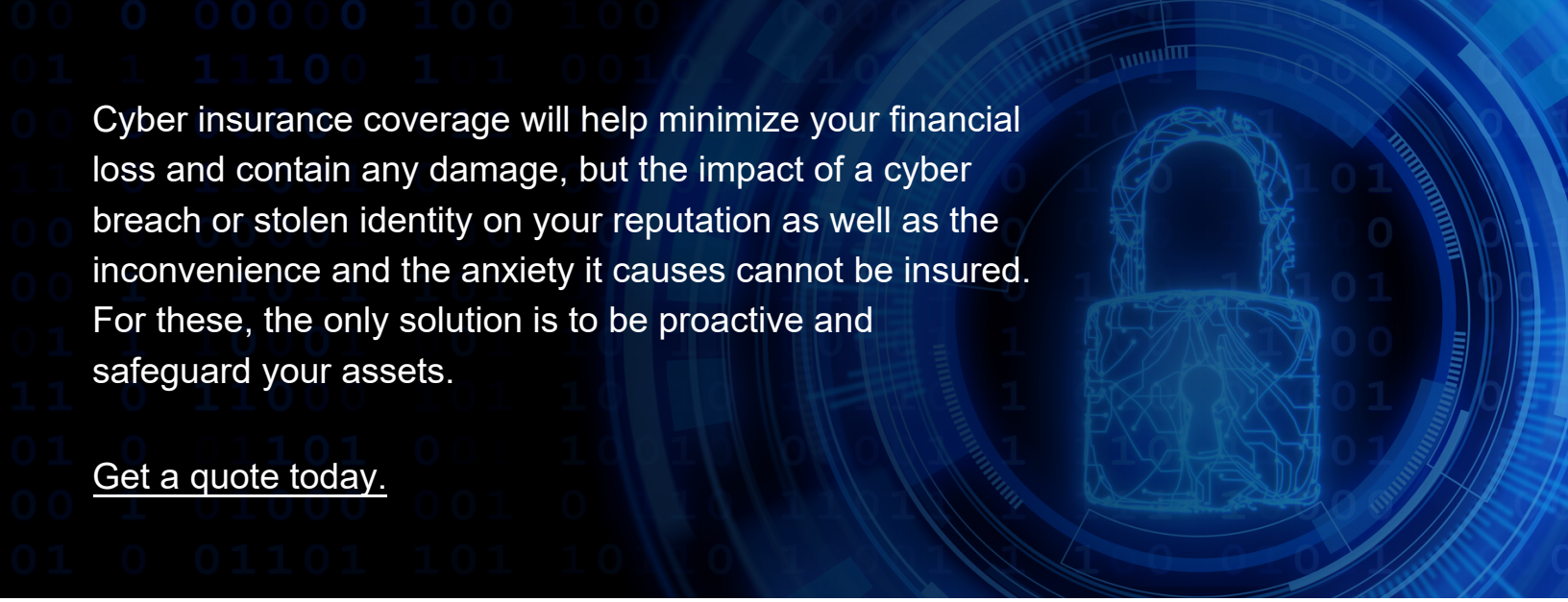
Airport lounges, hotel lobbies and coffee shops are hotspots for hackers, so use secure networks instead. Unlike most home and office wireless networks, the data flowing around a public wifi is often not encrypted and can serve as a window into any device connected to it.

GET INDIVIDUAL CYBER INSURANCE

Ask your employer about access to individual cyber insurance solutions that may be available to you through your employee benefit packages.

HAVE A RESPONSE PLAN

It's also essential to know who to call if you become a victim. If you have a personal cyber insurance policy, familiarize yourself with the support resources available to you as part of the policy. Be certain to store contact information and response hotline numbers in a place you can find them if your devices become unusable.



Cyber insurance coverage will help minimize your financial loss and contain any damage, but the impact of a cyber breach or stolen identity on your reputation as well as the inconvenience and the anxiety it causes cannot be insured. For these, the only solution is to be proactive and safeguard your assets.

Get a quote today.

What to do if you get hacked?

If you fall prey to a cybercrime, you should immediately act to contain the damage and move toward resolution. Here are three important steps in case you become a victim:

1. **Call the cyber response hotline attached to your** personal **cyber coverage.** The insurance representative will give you instructions to help stop continuing fraud and provide guidance for remediation.

2. **Contain the breach.** Take any breached device offline immediately. If you've built strong walls around your data (see "How to Build Cyber Walls Around Your Assets" on page 5), you should be able to locate and isolate the attack.

3. **Engage experts.** Your cyber insurance team will connect you to appropriate resources. The faster you can get expert eyes on the problem, the better chance of limiting the damage.

Safeguard your family and assets *now*

Most hackers or gangs aren't criminal masterminds. Engage the resources and tools at your disposal to safeguard you and your family from cybercrime.