Prevent and protect

How to guard against online financial fraud.

YOUR EMAIL ALERT PINGS AND YOU READ THIS: "As part of our efforts to protect your account, it has come to our attention that your online banking profile needs updating. Simply click on the link below…"

The message looks legit. It bears your bank's logo and other identifying information. But the last thing you should do is click on the link or key in any personal information.

This email is an example of "phishing," which is just one of many ways that online criminals aim to defraud individuals and businesses. Clicking the link could download a virus into your computer. Or it could lead you to a fraudulent website that obtains your personal information so that others can gain access to your financial accounts.

A global issue

Online financial fraud is a growing international criminal enterprise. Often it's committed by sophisticated organized crime networks, with proceeds funding such illegal activities as drugs and weapons trafficking, prostitution and money laundering.[1] Fraudsters often pose as legitimate organizations, family members in distress or peddlers of get-rich-quick schemes. They may ask for money directly, but just as often their goal is to steal your identity. Armed with personal data, scammers can open new bank accounts, transfer funds and apply for loans, credit cards, passports and government benefits – all under your name!

The Canadian Anti-Fraud Centre received 42,000 complaints in 2014, representing some 14,000 victims and reported losses of over $74 million.[2]

[1] www.cba.ca/en/media-room/50-backgrounders-on-banking-issues/662-protecting-canadians-from-fraud
[2] www.antifraudcentre-centreantifraude.ca/reports-rapports/2014/ann-ann-eng.htm#a2

One estimate pegs the global cost of cybercrime at more than US$400 billion annually.[3] The good news is you can take steps to protect yourself from cyber bad guys.

Keep your information safe

A few common-sense barriers can help you safeguard your personal information and avoid becoming a victim.

Protect your devices. Computers, smartphones and tablets contain sensitive information. So your first line of defence is to password-protect every device and never leave them unattended in public. Most mobile devices have the ability to enable encryption, which offers another layer of protection. Second line of defence: install the latest anti-virus, anti-malware and anti-spyware software, and keep operating systems up to date. New releases usually contain stronger security.

Be Wi-Fi wary. If it's not encrypted and password-protected, Wi-Fi can be the weakest link in your security chain. When setting up your home network, use WPA2 encryption (currently it offers the strongest level of protection), assign a complex password and change it annually. Limit your use of Wi-Fi in public places and avoid entering sensitive information – such as credit card numbers, user names and passwords – while on a public network.

Watch out for scams. Even if something on your screen looks legitimate, use caution before clicking links, downloading attachments or entering information. Reputable organizations will never ask you to confirm your credentials via email. If in doubt, don't call the number on your screen; instead, use the contact information listed on a statement or bill.

Shop smart. For maximum security when shopping online, visit reputable sites and ensure the site is secure (secure addresses start with "https" instead of "http"). If you see a broken key or open lock in your browser window, the site isn't secure. And always log off and close your browser once you're done.

Secure social networks. Enable appropriate privacy settings and avoid posting personal information, which can attract prying eyes. Once your information goes online, it's nearly impossible to remove.

MUSCLE UP YOUR PASSWORDS

- Avoid the obvious such as your name, names of family members and pets, or addresses and phone numbers
- Steer clear of common words or phrases
- Use a combination of upper and lower case letters, numbers and symbols
- Use a different password/user name combination for each account
- Don't write down or share passwords, and be sure to change them regularly

Educate others. People aged 65 and older make up the fastest-growing group of internet users in Canada, with approximately 70 per cent surveyed going online every day.[4] Children are also increasingly connected online, with 99 per cent surveyed having internet access outside of school.[5] Have regular discussions with family members about protecting their personal information.

Suspect you've been scammed?

The best thing to do is report it immediately:

- Contact your bank, financial institution or credit card company. They'll guide you through the process to help minimize or prevent any losses
- Call Equifax Canada at 1-800-465-7166 or TransUnion Canada at 1-877-525-3823 to issue a fraud alert
- Report the incident to your local police and to the Canadian Anti-Fraud Centre at 1-888-495-8501

Safe and sound

The internet has introduced enormous benefits to modern life, but those benefits are not without risks. As cybercriminals become ever more sophisticated, your best defence is to stay well informed. Read up, discuss the risks and implement best practices to help keep your information safe online. ■

Look for the next issue of Solutions, *where we'll examine credit card, mail and telephone fraud, and we'll take a peek at some new security technologies that can help keep information secure.*

[3] www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf [4] www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-fml/snrs-nln-en.aspx [5] globalnews.ca/news/1098160/canadas-youth-are-highly-connected-girls-face-different-rules-online-study/