Cybersecurity essentials to better protect your money and your identity

The internet is an efficient way for you to stay connected with family and friends. On the flipside, like any public environment, you need to be aware and cautious. Just as locks on your doors can help you secure your home and belongings, there are steps you can take to safeguard your computer and personal information. Even the most tech-savvy among us can become the target of con artists. Recognizing the signs of online fraud is an important first line of defence – and, fortunately, there are a few simple tactics you can use to protect yourself.

Common internet scams

Phishing/spoofing is when someone tries to trick you, typically by email or text message, into revealing valuable personal information, like your Social Insurance Number (SIN). A typical scenario involves a scammer impersonating your bank in an email to get you to enter your personal or banking details into a fraudulent website to gain access to your money.

Forex and investment scams use false or fraudulent claims to solicit investments or loans. You might notice claims on social media (Facebook, Twitter), on websites or in your email promising outsized returns for trading in foreign currency and offshore investment "opportunities." These scams typically ask for help moving money out of a country, with the offer to share the proceeds.

Malware/scareware/ransomware is malicious software designed to damage or disable computer systems. In the case of ransomware, the cybercriminal will block your access to your computer until you pay a ransom, typically in virtual currency such as bitcoin (which will make their crime less traceable).

Cybersecurity best practices

Critical steps to protecting your digital life include:

- **Using passwords and a password manager.** A good password manager will generate and save strong passwords, then autofill them on the associated website or login screen as needed. No more memorizing or keeping unsafe paper records.

- **Using security software.** Install anti-virus software and anti-spyware on your devices from a reliable source and keep it updated. Steer clear of apparent security updates from pop-up ads or emails – they may be malware that could infect your computer. Using a firewall is another step you can take to fend off hackers who might try to crash your computer or delete or steal sensitive information.

- **Having the latest operating system.** Be sure your computer operating system reflects the most recent update, which can include patches to fix newly identified security holes.

iA
Investia
Financial Services Inc.

- **Being watchful with downloads.** Carelessly downloading attachments from your email can circumvent even the most vigilant anti-virus software. Never open email attachments from people you don't know and be wary of any unexpected attachments forwarded to you from those who you do know, but who may be unwittingly spreading malicious code because their accounts were hacked.

- **Turning off your computer.** Shutting down your computer severs an attacker's connection, be it spyware or a botnet, which is a string of connected computers that may be using your computer's resources to find other unwitting victims.

When online, embrace your inner skeptic

While there's no foolproof method for staying safe online, you can take meaningful steps to avoid and deter criminal encounters. A healthy dose of skepticism is useful here. Take what you see online with a grain of salt, question claims that seem too good to be true and keep important details about yourself private. All these actions can go a long way in ensuring you're as safe on your computer as you are in real life – or IRL, for the tech-savvy.

How we can help

Preserving your assets is key to any wealth management strategy. Securing your online presence and working with one of our skilled Advisors can help you position your portfolio for success and achieve greater financial well-being.

iA Investia
Financial Services Inc.

INVESTED IN YOU.