Digital Security Guidelines for a Safer Way Forward

WELLINGTON-ALTUS

Just as we buy home insurance for that once-in-a-lifetime hailstorm and insure our vehicles in case of an accident, protecting your financial future in today's digital age calls for heightened awareness and a proactive approach to online safety. Many of us have seen friends or family members connect to Wi-Fi at an airport, coffee shop or hotel to check an account balance, post on social media or do some online shopping. It's a familiar habit, and one we've likely done ourselves, often without realizing our devices can potentially interface with a multitude of unsecure public networks as we move through the day.

With the growing number of login requirements across the websites and apps we use, reusing the same password can feel like a convenient shortcut. However, cybersecurity experts and financial institutions consistently warn that these practices, along with accessing or transmitting sensitive information over unsecured networks, can leave you vulnerable to fraud or identity theft. A single compromised session could potentially jeopardize everything you've worked hard to build and protect over a lifetime.

This article offers practical tips and guidance to help you safeguard your online activity, protect your financial well-being, and ensure you remain secure in an increasingly digital world.

"The best laid plans of mice and men often go awry."
- Robert Burns, 1785

Safeguarding Your Accounts

A strong password is one of the simplest and most effective ways to protect your online presence. Each one should be unique, memorable, relatively lengthy and made up of a mix of letters, numbers and special characters. Reusing passwords, especially for financial platforms, increases your risk if any single, seemingly unrelated account is compromised. Financial account credentials should never be reused for non-banking services. Consider updating your key passwords every few months for added security.

To further reduce risk, consider using a fraud-protection-focused credit card (ideally, with a lower limit) specifically designated for online purchases. This helps contain potential losses if the card information is ever compromised and keeps your primary accounts better protected while shopping or transacting online. Where possible, also consider using a password-manager application. Reputable password managers can securely store your credentials, help to automatically populate login details and facilitate safe password sharing with designated family members or your key advisors.

Multi-factor authentication (MFA) is another important line of defense. By requiring a one-time code delivered via text message, email or biometric confirmation (i.e., face-id or fingerprint), MFA ensures that possession of a password alone is insufficient for account access. Financial institutions, email providers and social networks commonly support MFA settings. Enabling these features typically requires only a brief configuration step in the user's security profile and goes a long way in securing your online presence.

[1] Conquest Planning user statistics.

Keeping Your Devices Safe

Your computer, tablet and phone all serve as gateways to your personal information, which makes keeping them up to date especially important. Most devices offer automatic updates that fix known security issues; ensure this feature is enabled on all your devices. Additionally, installing antivirus software (often available through your internet provider at no extra cost) can provide an added layer of protection against potential online threats.

You should also be cautious when using public Wi-Fi. That free network at your local café might be convenient, but it's not always secure. Avoid accessing sensitive accounts or making online purchases unless you're connected through your mobile data or a virtual private network (VPN), which adds encryption and shields your activity.

It also helps to check your device settings and turn off the feature that automatically searches for available networks. Many phones and tablets are set to connect to public Wi-Fi without notifying the user. This means you could unknowingly join an unsecured network just by walking into a busy space like an airport, hotel or shopping mall. Disabling this option gives you more control over which networks you use and helps maintain better control over your digital footprint throughout the day.

"Small habits also go a long way: disable Bluetooth when you're not using it, uninstall apps you no longer need and enable 'Find My Device' so you're prepared if your device is lost or misplaced."

Recognizing Scams and Protecting Privacy

Today, many scams come in the form of emails, text messages and phone calls. They appear official but are designed to steal your information. If a message asks for your password or payment details, pause and verify its source before responding. Look for signs like generic greetings, unusual URLs and pressure to act quickly. If anything feels off, reach out to the company directly using their official publicly available contact information.

Fraudsters often piece together online profiles using public information; think carefully about what you share. Details like your birthday, travel plans or home address may seem innocent but can be used to target you. Review the privacy settings on your social media accounts and limit who can view or tag you in posts.

When shopping online or entering personal details, glance at the company's privacy policy. If it's unclear, don't hesitate to contact their support team or privacy officer to ensure your information is handled responsibly.

Did You Know? In 2023, Canadians reported more than 201,000 police-recorded fraud incidents—nearly double the rate of a decade earlier.[1]

[1]Statistics Canada: "How much is fraud affecting Canadians and Canadian businesses?" (March 13, 2025)

Safe Transactions and What to Do If Something Goes Wrong

Before entering personal or banking information online, double-check that the site is secure. Look for a padlock symbol near the website address and confirm that the URL starts with “https” (that final ‘s’ stands for secure).

If your bank offers auto-deposit options, consider taking advantage of them to reduce the chance of interception during money transfers. Checking your bank and credit card statements on a regular basis can also help catch fraudulent activity early. If you spot anything unusual, notify your provider or financial institution immediately.

Sometimes, even with the best precautions, things happen. If you suspect your account has been compromised, change your passwords, sign out of all devices and alert your bank or service provider(s). You may also want to file a report with law enforcement or Canada’s fraud-reporting agencies. Don’t hesitate to speak with a friend, family member or your Wellington-Altus advisor; someone who you trust and who can help you navigate what to do next.

Final Thoughts

Digital security might not be top of mind every day but developing a few smart habits can make a big difference. Taking these simple steps to protect your information can provide peace of mind and help ensure that everything you’ve worked hard for stays safe in today’s increasingly connected world.

Additional Resources:

Get Cyber Safe

The Little Black Book of Scams 2nd edition

Seniors Guidebook to Safety and Security | Royal Canadian Mounted Police

www.wellington-altus.ca