CREA
THE CANADIAN REAL ESTATE ASSOCIATION

REALTOR® Safety
Raising Cybersecurity Awareness Resource

By adopting safety practices like these and staying aware of the latest cyber scams and digital threats, REALTORS® can safeguard themselves and their businesses from cyberattacks.

Mobile Device Safety and Security

While mobile devices are valuable tools for real estate professionals their convenience does come with risks.

REALTORS® can practice mobile device safety by:

- Using strong passwords and enabling multifactor authentication, such as a fingerprint scan or a numerical pin.
- Using encryption to keep your client data secure.
- Disabling location settings when taking pictures.
- Using a unique password for each account.
- Using your smartphone's built-in safety features, such as Find My Device/iPhone and emergency calling.
- Checking privacy and application settings on your smartphone to ensure you are sharing information (location, photos, microphone, video, etc.) intentionally and sparingly.

Social Media Safety

REALTORS® can use social media to connect with clients, build relationships, and maximize their online visibility and growth potential. REALTORS® should always exercise caution when using these platforms, as privacy and security can easily be compromised.

REALTORS® can stay safe while using social media by:

- using strong, unique passwords and multifactor authentication;
- ensuring the information you share is accurate and from a trusted source;
- reviewing and adjusting privacy settings regularly;
- avoiding oversharing or posting content containing personal or sensitive information;
- turning off your location sharing before posting;
- refraining from showing homeowners' valuables in pictures;
- never clicking on links or downloading attachments from unknown sources;
- staying on top of common scams such as phishing and smishing; and
- being aware of social engineering tactics geared to trick you into sharing sensitive information.

Cybercrime: Scams and Frauds

Cybercrime is a global issue. Cyber-based scams and fraud are a significant threat and REALTORS®, buyers and sellers can be targeted.

Here are common examples of cybercrime:
Wire fraud: Criminals may try to deceive real estate professionals and their clients by providing false wire instructions and diverting funds into their own accounts.

Business email compromise (BEC): Criminals pose as trusted senders and try to convince the recipient to send money or share financial information.

Title fraud: This involves cybercriminals using fake identification documents to target a home with a mortgage that's paid off, then taking out a second mortgage on that home, by posing as the real homeowner.

Artificial intelligence (AI) scams: AI-fueled techniques are used to create fake personas or automate fraudulent activities, strengthening the sophistication of the scam.

Common Social Engineering Tactics

Social engineers use deception to manipulate victims into disclosing confidential information. It's a tactic often seen on social media disguised as fun and interactive posts, though it can also be used via email, direct message and text message.

Social engineers typically try to obtain private information by:

- **Phishing –** Where emails are structured to look like they're from trusted, legitimate sources pointing recipients to fake websites to input personal and financial information, exposing them to potential financial fraud and identity theft.
- **Vishing –** Where cybercriminals use fake phone numbers, voice altering software and other tactics to entice people to divulge their personal information over the phone.
- **Smishing –** Like phishing, smishers use text messages to convince individuals to share information by responding to a message or clicking a compromised link within the message.
- **Ransomware –** According to the Canadian Centre for Cyber Security (CCCS), ransomware is the most common cyber threat facing Canadians. Cybercriminals use malicious software to encrypt, delete or steal data before demanding a ransom to restore it.

REALTORS® can stay safe in virtual environments by:

- using secure communication channels, such as encrypted emails;
- staying up to date on cybersecurity risks and best practices;
- adopting multifactor authentication;
- conducting regular software updates;
- using secure, password-protected Wi-Fi networks; and
- regularly backing up essential data.

Artificial Intelligence (AI) Threats

Though the full power of AI has yet to be seen, it hasn't stopped cybercriminals from using it for malicious purposes. REALTORS® should try to stay aware of the dangers that can be associated with AI, and the types of scams to be on the alert for.

Fraudulent property listings: Using AI, cybercriminals can create fake property listings that may trick REALTORS®, buyers and sellers. Look for inconsistencies within the text (for example, spelling errors and bland, repetitive content) and verify the identity of the parties involved.

Misinformation: AI has the potential to generate fake reviews, testimonials, listings, emails, and other information that can mislead buyers and sellers and damage the reputation of real estate professionals.

Phishing scams: Emails generated by AI can appear genuine, prompting recipients to disclose personal or financial information.

Ransomware attacks: AI can be used to pinpoint vulnerabilities in a real estate company's network and launch a ransomware attack, which could result in the loss of sensitive client data.

Deepfake media: Deepfakes are AI-generated synthetic media that broadcast false events. Deepfake video can mimic REALTORS®, lenders, buyers and sellers, and can result in fraudulent transactions and monetary losses. Deepfake images of properties can result in misrepresentation and possible legal issues, and audio deepfakes, designed to imitate the voices of trusted sources, can be used by cybercriminals to convince targets to reveal sensitive personal and financial information over the phone.

With their ability to detect patterns and inconsistencies, AI technology and machine learning (ML) algorithms are starting to play a significant role in fraud detection. AI-based tools like fact-checking verifiers, deepfake detectors, and video authenticators can help REALTORS® avoid inaccurate information.

REALTORS® can use AI technology safely to:

- detect altered video and images;
- verify misleading content; and
- identify fraudulent listings.

Malware, Ransomware and Viruses

The first step in protecting yourself and your business is to understand the common types of potential cyber threats.

Malware is software designed to intentionally damage computer systems and can take many forms, including viruses, spyware, adware, and ransomware.

Ransomware is a type of malware that encrypts a user's files, threatening to publish or block access to sensitive data unless a ransom is paid.

Viruses are malware that duplicate themselves and spread to other computers or systems.

REALTORS® can mitigate cyber threats and risks by:

- keeping all software systems up to date and enabling automatic updates on your device(s);
- using strong passwords and multifactor authentication;
- backing up important data;
- staying up to date on cybersecurity best practices;
- using anti-virus software and firewalls; and
- having a response plan in place if a data breach occurs.

Password Hygiene

Password hygiene is an integral part of maintaining privacy and safety online.

Tips for good password hygiene include:

- Using a combination of upper- and lower-case letters, numbers, and special characters of up to 12 in length.
- Considering using a memorable phrase with letters substituted for numbers, or vice versa.
- Not using the same password for multiple accounts.
- Never sharing your passwords with anyone.

REALTOR®. Member of The Canadian Real Estate Association and more.