A fraudster's toolbox

Fraudsters use different tactics combined with evolving technology and are always trying new ways to steal personal information and money from Canadians.

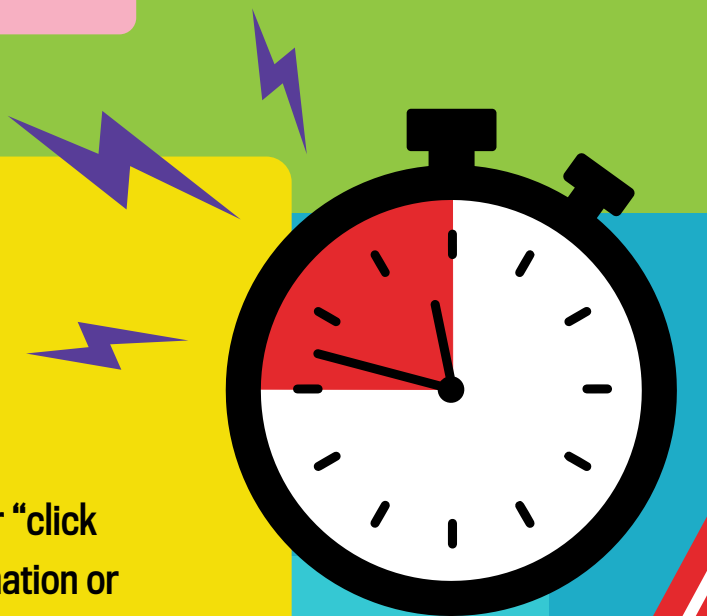
We're exposing some of the common tools in a fraudster's toolbox and offering tips to help you recognize these schemes and protect yourself from falling victim.

Spoofing

Fraudsters use spoofing, as a type of phishing scheme, to trick users into thinking they're communicating with a legitimate source. They change their caller-ID displayed on phones, send convincing information in messages and create emails impersonating someone you know to trick you into offering them personal information.

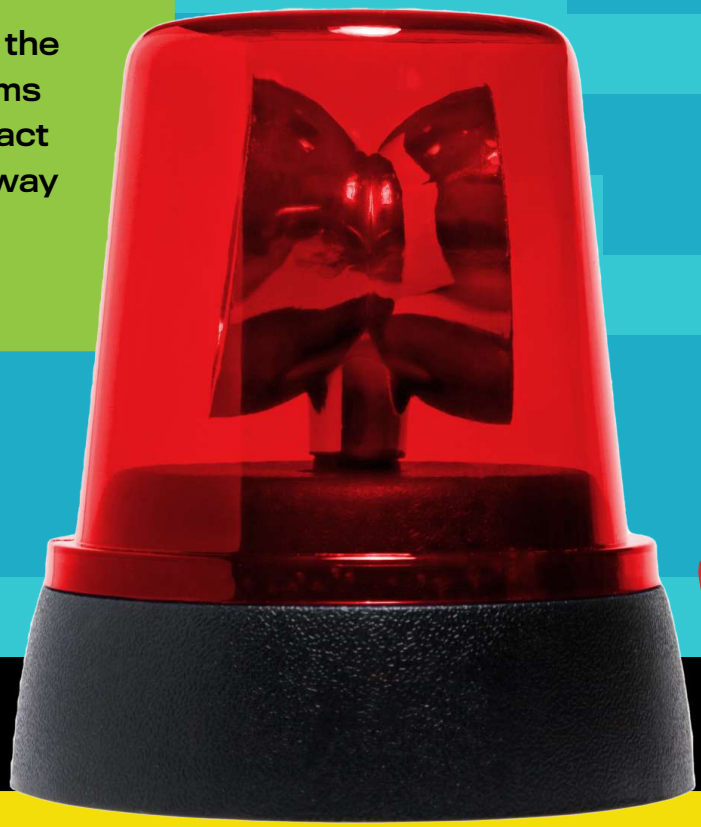
Tip: If a caller is asking for your personal information, hang up and call the official phone number of the legitimate source. For email and message spoofing, hover your mouse over the sender's email address and look closely for differences in the address.

Urgency



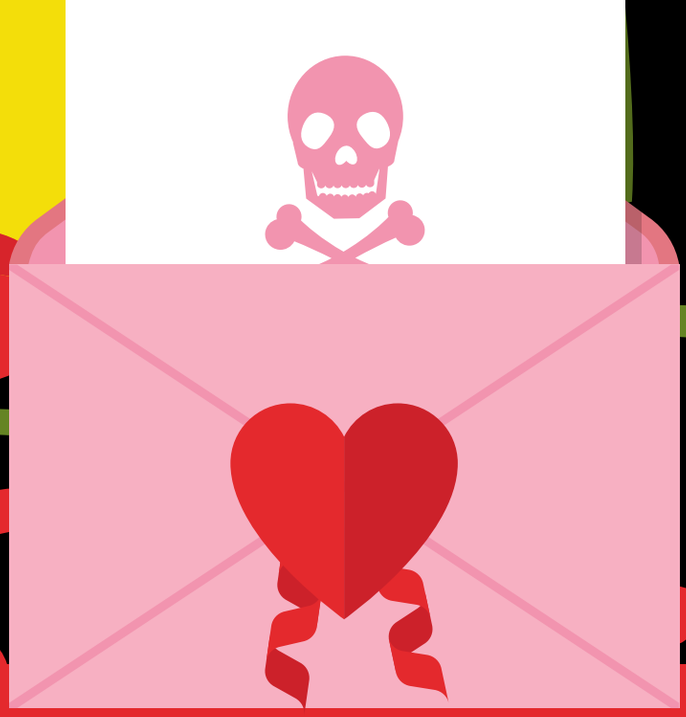
Fraudsters often use urgent language, like "act fast" or "click now", to trick you into sending money, personal information or clicking on malicious links before considering whether the request is suspicious.

Tip: Real emergencies don't happen over messages. Pause to think about whether the call or message seems suspicious and contact the source another way for confirmation.



Emotional manipulation

Fraudsters play on emotions to trick you into believing their story to send them personal information or money. They practice this by pretending to be a romantic interest, family member or charity, or by pretending to be involved in an emergency situation.



Tip: Be suspicious of anyone you meet online that claims their love or friendship to you, tells you a traumatic story or makes you feel uncomfortable. No matter how much time is invested in the online relationship, it is important to stay wary if they ever ask for personal information or money.

Threats

If you don't comply with their demands, a fraudster may threaten you or your family members with an arrest, physical or financial harm, or the release of sensitive information or pictures.

Tip: If you get a threatening call or message, hang up or delete it. If you feel you need to verify the legitimacy, contact the organization handling the supposed threat.

Pop-ups

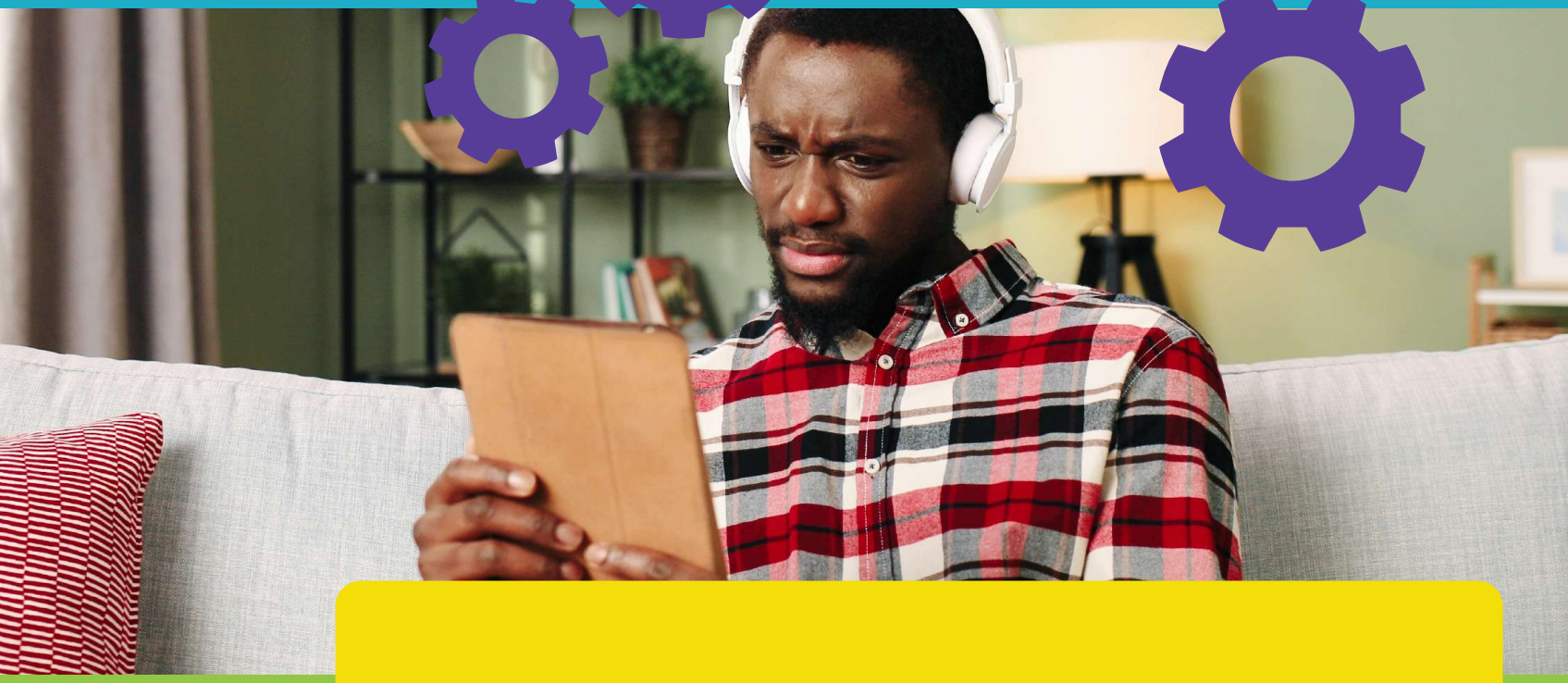
Fraudsters use pop-ups that appear on your device screen saying you've won a prize or that your device is infected, to trick you into clicking on a link or calling a phone number. These scams are trying to trick you into offering up personal information or installing malware on your devices.

Tip: Protect your device by installing anti-virus protection and pop-up ad blockers. Clear your cache and block cookies frequently and avoid using public wi-fi or unsecure networks. Never call a phone number or click on a link provided in a pop-up.

Search engine optimization

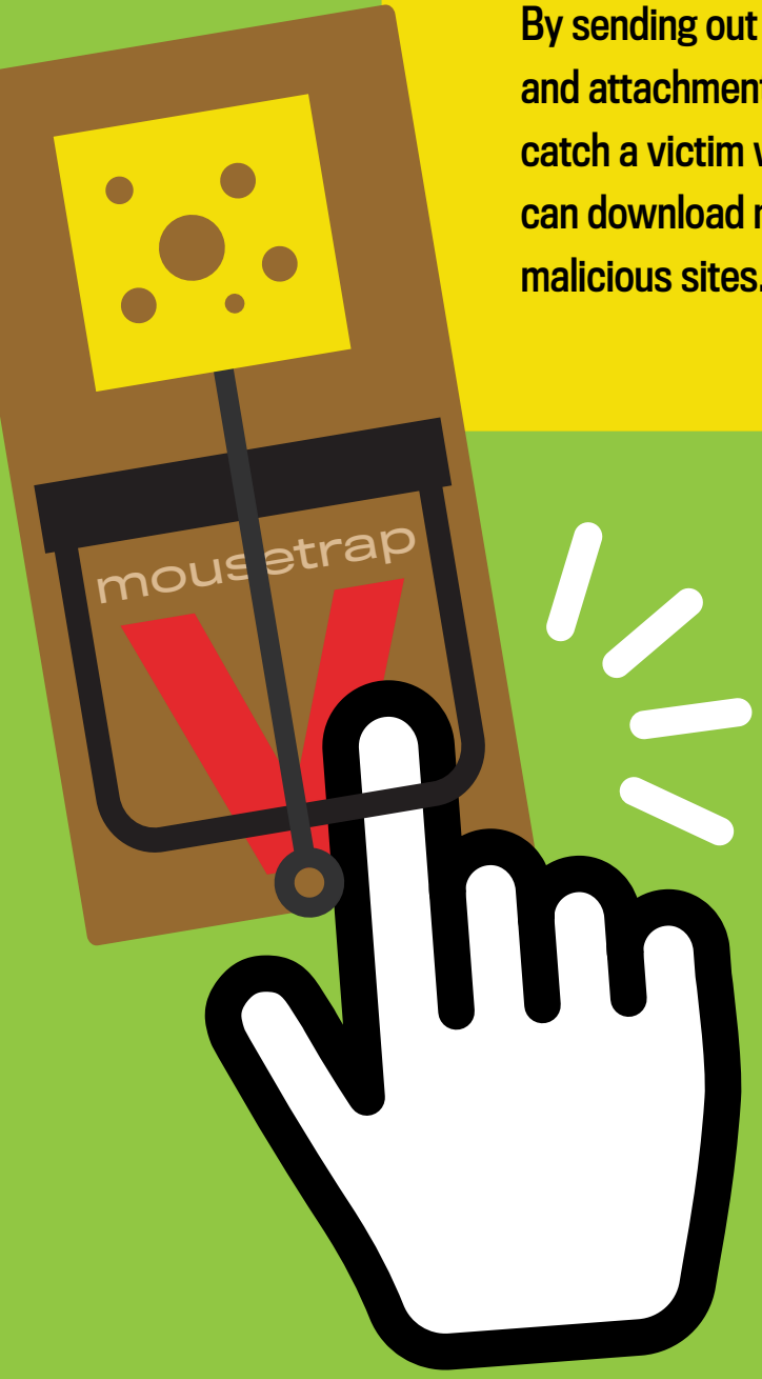
Fraudsters can optimize their websites to appear in the top results of an online search. Their malicious websites can appear as legitimate sources to trick you into offering personal information or downloading malware.

Tip: Don't assume the top results mean legitimacy or quality. Fraudsters will often create websites that look official but will change one letter or have a slightly different domain. Always verify the link and contact information.

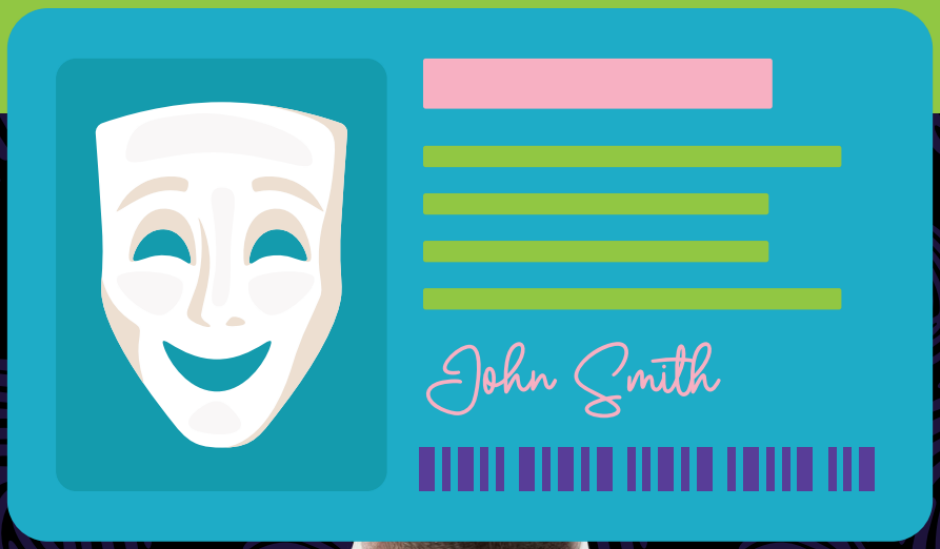


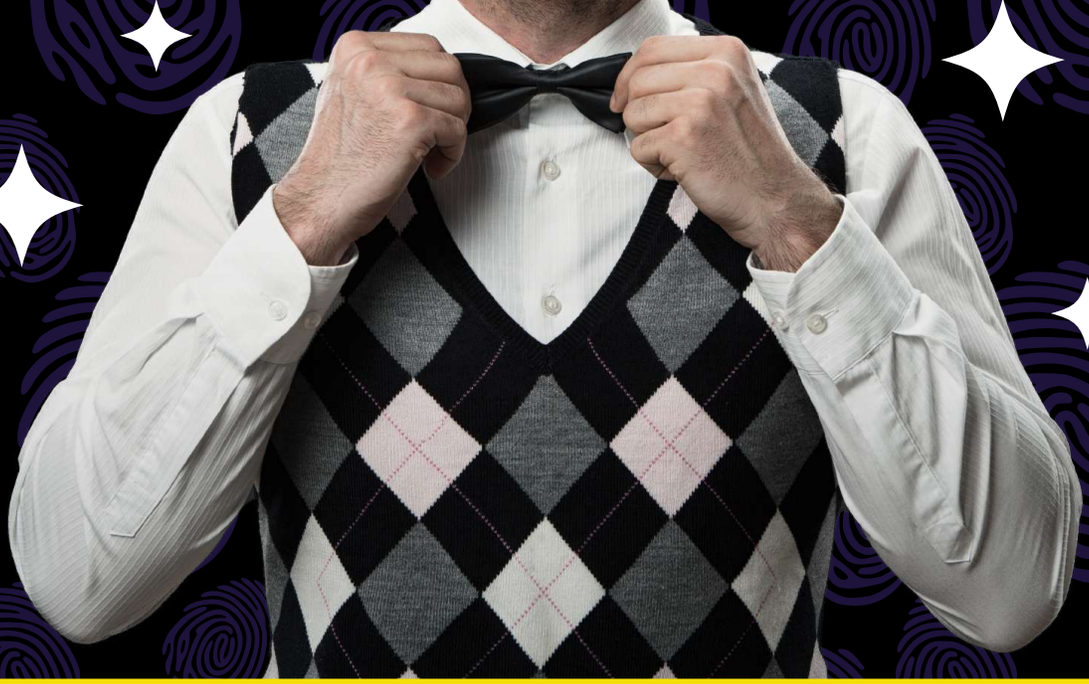
Links and attachments

By sending out mass phishing messages with malicious links and attachments, fraudsters can almost guarantee they will catch a victim who clicks on one. These links and attachments can download malware onto your devices or send you to malicious sites.



Tip: Don't click on a link sent to you in an email, text message or message on social networking sites. Navigate to the site through your own search engine and use the contact information from your search to contact the company to verify the legitimacy of the sender before downloading attachments.





Impersonation

Fraudsters research and learn about individuals and their connections to better impersonate them for more targeted scams, like spear phishing.

Tip: Don't trust that a message is from who the sender says they are, especially when it comes with a request to click a link or download a file. The impersonator might offer very convincing information to seem legitimate, but always verify the sender through another source.

Anyone who suspects they have been the victim of cybercrime or fraud should **report it** to their local police and to the Canadian Anti-Fraud Centre's online reporting system or by phone at **1-888-495-8501**. If not a victim, report it to the CAFC anyway.

Get more tips to protect yourself and your devices at

GETCYBERSAFE.CA

[redacted]

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

Catalogue number: XXXXX | ISBN: XXX-X-XXX-XXXXX-X