CANADIAN ANTI-FRAUD CENTRE BULLETIN

What's in a fraudster's toolbox? vs. What's in yours?

FRAUD: RECOGNIZE, REJECT, REPORT

March 2, 2023

The theme of this year's Fraud Prevention Month is "Tricks of the trade: What's in a fraudster's toolbox?". We're exposing some of the top tricks and tactics fraudsters use to victimize Canadians. We're also helping you equip your own toolbox to protect yourself.

What's in a fraudster's toolbox?

Although fraudsters are always changing tactics and using advancements in technology to steal personal information and money, here are some of their common tools:

- **Spoofing:** This is used by fraudsters to mislead and convince you that you're communicating with people you know, or legitimate companies and organizations. Fraudsters can change the caller-ID that is displayed on your phone, the sender address in an email, and often mimic legitimate websites, etc.
- **Urgency:** Fraudster's use urgency to trick you into sending money, personal information or clicking on malicious links. By using urgency, they are trying to give you less time to consider whether the request is suspicious.
- **Emotional manipulation:** Fraudster's play on your emotions to trick you into believing their story and sending them money. They will do this in romance, emergency, grandparent and charity scams, etc.
- **Threats:** Threats are often used alongside urgency and emotional manipulation. A fraudster may threaten arrest, physical harm, financial harm, release of sensitive information or pictures, and make threats against family members if you don't send money. They may also scare you to remain silent about the transaction to further isolate you.
- **Pop-ups:** These are boxes that pop up on your computer or device screen. The pop-ups may say you've won a prize or that your computer is infected and then provide a toll-free phone number for you to call. In other cases, they want you to click on them so they can install malicious software or lead you to a fraudulent site.
- **Search engine optimization:** Did you know that fraudsters can optimize their websites to appear in the top results of an online search?

- **Links:** By sending out hundreds of thousands of messages with malicious links, fraudsters are guaranteed to catch a victim who clicks on one. Malicious links can look suspicious or legitimate. Don't click links in messages.
- **Impersonation:** Fraudsters impersonate anyone you can think of to trick you into sending money or information. In cases of business email compromise, fraudsters study emails and interactions between employees so they can better impersonate someone.

What's in your toolbox?

Be a detective with every message and call you get. Were you expecting this? Are you normally contacted in this way? Are there spelling mistakes? Are they pushing you to click a link? Fraudsters never stop trying to trick you so get ahead by approaching every message and call with suspicion and remembering the tips below.

- **Spoofing:** Hang up and call the official phone number of the company or agency in question. If the call is claiming to be someone you know, hang up and make the outgoing call to the number you have in your contact list.
    - **Email spoofing:** Hover your mouse over the sender's email address or hit reply. After clicking reply, a different email address will appear in many cases.
- **Urgency:** Time is on your side. You do not have to immediately send money, click a link or respond. Take five minutes to think about whether the call or message seems suspicious. Use this time to try out the tools in your toolbox.
- **Emotional manipulation:** Be suspicious of interactions online where someone you just met professes love or friendship to you, tells you a sob story or makes you feel unsafe. Don't feel isolated, reach out to your friends or family and talk about the encounter with them - see what they think. Check out the CAFC's A-Z index to browse different scams to see if your situation is on there.
- **Threats:** If you get a call that sounds suspicious, hang up! Hang up if you are being threatened, asked for money or personal information or if you're just unsure about the credibility of the call.

- **Pop-ups:** There are many ways to protect your device. Install anti-virus protection and pop-up blockers. Clear your cache and block cookies when you can. Don't use public wi-fi or unsecure networks. Never call a phone number provided in a pop-up.
- **Search engine optimization:** Don't assume the top results mean legitimacy or quality. Verify the link and contact information. Fraudsters will often create websites that look official, but will change one letter or have a different domain.
- **Links:** If you get a link sent to you in an email, text message or message on social networking sites, don't click it. You can navigate to the site through your own search engine or find the contact information in your search engine and contact the company directly to see if the message you got was legitimate.
- **Impersonation:** Never trust that a message is from who the sender says they are, especially when it comes with a request for sending something. Verify the person's identity by either searching for their information online, talking to them in person if you know them, or asking them questions only the real person would know.

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.