CANADIAN ANTI-FRAUD CENTRE BULLETIN

Service Scams: What's in a fraudster's toolbox? 2023-03-21

FRAUD: RECOGNIZE, REJECT, REPORT

The Fraud Prevention Month campaign is held each March to inform and educate the public on the importance of protecting yourself from fraud. This year's theme is "**Tricks of the trade: What's in a fraudster's toolbox?**". Follow our social media and visit our website for fraud prevention information. Don't forget to use #FPM2023 on all fraud prevention posts!

Service scams

Service scam fraudsters will often claim that they are one of your existing service providers or claim to offer services at a much lower cost. These fraudsters are attempting to steal your money without providing a service or your personal information.

The following are the most common variations of service scams observed by the CAFC:

Cellphone or existing service provider scam:
Fraudsters call victims claiming to be from their cellphone service provider offering them a deal they "cannot pass on". The fraudsters proceed to ask for the victim's personal information including their Social Insurance Number (SIN) and Driver's License number in order to perform a "credit verification". In many cases, their personal information is used to commit identity fraud like ordering a cellphone using their identity.

Immigration services:
Online and social media ads are targeting victims looking to apply for a visa or immigrate to Canada. Fraudsters create fake websites offering immigration services or may even guarantee high paying jobs. The application will ask for personal information and a payment to process the application.

Tech support:
Fraudsters will call victims, appear in pop-ups which seem to freeze your computer, send you an email with a fake invoice or will appear in your online search results for 'reputable service providers' providing a phone number for victims to call. Once in contact with victims, fraudsters will request remote access to their computer. If remote access is gained, victims put themselves at risk for identity fraud. Fraudsters may also ask for a payment for their "services".

Home Services: Air duct cleaning, furnace repairs, general contractors and more!
Victims are approached on social media, telephone or come across a fraudulent ad online. Fraudsters will often ask for a prepayment and won't provide the service. If the company provides the service, they could be low quality, offer invalid warranties or the repairs can cause potential risks.

What's in a fraudster's toolbox?

- **Remote access:**
  - By granting remote access to your computer or device, the fraudsters can watch you type in your usernames and passwords or send themselves money.
- **"Great deals!"**
  - Fraudsters will offer low interest rates or services that are discounted or much better than competitor's rates.
  - They may claim they're new and don't have any reviews online yet so you can't search them up.
  - If it's too good to be true, it probably is.
  - If the services are completed at all, they are of low quality and can cause further damage.
- **Search engine optimization:**
  - Fraudsters frequently use search engine optimization for service scams. Make sure you are dealing with the official company by verifying the address, phone number and website address.

What's in your toolbox?

- **Local technicians:**
  - Never allow an individual to remotely access your computer. If you are experiencing problems with your operating system, bring it to a reputable local technician.
  - Research all companies and contractors offering services before hiring them.
- **Cellphone provider:**
  - Verify any incoming calls claiming to be from your service provider offering a deal. Let them know you will call them back; end the call and find your service provider's official phone number.
- **Caution:**
  - Never provide any personal or financial information over the telephone, unless you initiated the call.
  - If you receive a call from your service provider, advise them that you will call them back and end the call.

    - Be suspicious about unsolicited phone calls, emails or pop-ups stating your computer/device is infected with a virus, a threat has been detected or a subscription will be automatically renewed.
- **Research:**
    - Look up the legitimate phone number for the company and communicate with them directly by always making the outgoing call.
    - For information on immigration scams, visit : http://www.cic.gc.ca/english/helpcentre/answer.asp?qnum=1206&top=31

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.