CANADIAN ANTI-FRAUD CENTRE BULLETIN

20 Years of Fraud – Evolution of the Types of Fraud 2024-03-04

FRAUD: RECOGNIZE, REJECT, REPORT

This year marks the 20th anniversary of Fraud Prevention Month. The theme of this year's campaign is **"20 years of fighting fraud: From then to now**. With this theme, we'll be exploring how certain frauds have evolved with the rise of the digital age, drawing insightful comparisons between the past and present.

In this bulletin, the CAFC would like to highlight how some of the most commons fraud types have evolved over the last 20 years of Fraud Prevention Month.

Investment

Then: Twenty years ago, investment fraud took the form of traditional frauds such as Ponzi schemes and other fake investment opportunities promoted through boiler room operations, where high-pressure sales tactics were used to promote the fraudulent and worthless investments. Jewel or "gemstone" fraud was also a common variation of reported investment fraud.

Now: Investment fraud has evolved with the emergence of cryptocurrency. In 2023, the CAFC estimates that over 50% of the $309M in reported investment fraud loss is tied to crypto investment frauds. Fraudsters post ads on social media and lure investors through fake profiles on social media, dating websites and email.

While in-person Ponzi and pyramid schemes are still being reported, suspects are now using a variety of instant messaging applications and social media platforms to recruit investors.

Emergency

Then: Emergency frauds typically involved someone contacting a potential victim, often by phone or email, and pretending to be a relative or friend in urgent need of financial assistance due to a supposed emergency situation like being stranded in a foreign country, having a medical emergency, or facing legal trouble. The suspect would then request a payment through a money service business like Western Union or Money Gram to avoid consequences.

Now: Although emergency scams are similar to what was reported 20 years ago, specific scenarios like the ''grandparent scam'' where fraudsters show up in person to pick-up cash or request an etransfer have become prevalent in the last number of years. There are also recent reports showing fraudsters requesting cryptocurrency as a form of payment. Specific scenarios may have evolved over time, but the underlying principles of exploiting emotions and urgency remain consistent not only in emergency frauds, but in many types of fraud.

Job

Then: Job frauds often involved fraudulent job postings in newspapers, online job boards, or other media. These postings would promise high-paying jobs with minimal effort or experience required. Common variations included the Mystery Shoppers scams where victims would be sent counterfeit cheques to deposit and use the funds to test the services of Western Union or Money Gram. The other variation involved victims being asked to pay an upfront fee for training materials, access to job listings, or other services.

Now: Reporting in recent years indicates that job frauds are primarily cyber-enabled. Consumers are offered a job that features them as financial receiver/agent for the suspect company. Victims are told to accept payments into their personal bank account, keep a portion, and forward the remaining amount to third parties. Victims are eventually informed that the original payment was fraudulent and any debts accrued are the responsibility of the victim. Fraudsters will attempt to process many payments in a short amount of time before the victim's financial institution recognizes the fraud.

Using the names of real companies in Canada, fraudsters are offering victims freelance job opportunities to "boost" products, apps or videos using software created by the fraudsters. After the victim installs the software and creates an account, they receive "orders" or "tasks" they have to complete. Victims might receive a small payment or commission in order to convince them that the job is legitimate. Victims can earn higher commissions or "move up a level" by boosting more products or videos but need to pay fees to gain access to the additional work. Victims deposit their funds into crypto accounts or wallets. Victims may also be asked to recruit other victims in order to increase their earnings. Similar to crypto investment scams, victims will see funds in their crypto account, but will not have the ability to withdraw the funds they have deposited and earned.

Service

Then: Looking back at service scams 20 years ago, fraudsters used the telephone, mail-based fraud and door-to-door as their methods of solicitation. These scams relied on deceptive tactics to convince victims to pay for services that were either not performed or were of poor quality.

Now: Although fraudsters continue to use the solicitation methods mentioned above, service frauds have evolved to include social media platforms, email solicitation, fraudulent ads and search engine optimization.

Some of the most current common variations of the service scam include:

- Tech support scam
- Fraudulent phone call claiming to be a cellphone or internet service provider
- Timeshare resales fraud
- Fraudulent immigration or visa website
- Air duct cleaning and home maintenance or equipment

Phishing

Then: In 2005, Phishing was a relatively new tactic used by cybercriminals. It typically involved sending deceptive emails that appeared to be from legitimate sources, such as banks, financial institutions, or trusted companies which asked the victim to click on a link and provide personal information.

Now: Over time, phishing attacks have become more sophisticated. The evolution of technology has given fraudsters the opportunity to automate phishing messages which has increased the number of targets in recent years. Fraudsters now use more convincing email templates, and even text messages often impersonating service providers, government agencies or financial institutions. Phishing emails and text messages may also contain malicious links or attachments designed to infect the recipient's device with malware. In addition, phishing has proven to be a threat to businesses as it is one of the main contributors to ransomware and spear phishing attacks.

Warning signs - How to protect yourself

- Be careful when sending cryptocurrency; once the transaction is completed, it is unlikely to be reversed.
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project
- Verify if the investment companies are registered with your Provincial Securities Regulator or the National Registration Search Tool (www.aretheyregistered.ca).
- If you receive a suspicious phone call claiming to be from a family member in an emergency situation, hang up the phone and contact them directly on the number you have in your contact list.
- If the caller claims to be a law enforcement official and asked you to pay a fine or bail, hang up and call your police directly.
- If you receive funds for any reason from an unknown individual or company and you are asked to forward it elsewhere - DON'T! You could be breaking laws when you are acting as a money mule.
- If you are asked to "boost" apps, videos or merchandise, you will more than likely be providing fake reviews to fraudulent products.
- Use reputable service providers located in your area.
- Never click on a link or attachment from an unsolicited message.
- Learn more tips and tricks for protecting yourself.

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