MOKSHA
CANADA FOUNDATION

CYBER FRAUD AND SCAMS

What is Cyber Fraud?

- Cyber fraud is the crime committed via a computer with the intent to corrupt another individual's personal and financial information stored online. Cybercrime is a criminal activity that either targets or uses a computer, a computer network, or a device linked to an internet device such as a cell phone.
- Fraudsters can use the cyber world to gain access to victims' identities, online accounts, and bank accounts. Individuals and organizations need to be vigilant and protect their information from fraudsters.
- Cybercrime and fraudsters normally try to hack into victims' personal and financial information online via phishing, emails, and viruses. If you receive an email with an attached link that either asks you to present your bank information or to confirm your bank account information, do not provide that information.
- Even if the email or the phone call sounds legitimate and honest, you should call the institution back yourself and ask them if this email originated from them or not.

Think before you click. Refrain from clicking on a link that is sent to you, as well as, never giving out any personal information. Verify the sender. There's nothing wrong with going online, finding the legitimate number of that delivery company or that store, and giving them a call to verify that they are the ones who called.

Always confirm the origins or the source of any links sent to you by email or text.

Financial fraud

This fraud involves individuals giving out personal, confidential information to an unknown person on the phone or computer. Legitimate financial institutions will never ask you to divulge information in this manner.

- Remember banks do not cold call or email customers to verify financial information.
- Never give out any banking or financial information over the phone or the Internet - especially passwords or PINs (Personal Identification Numbers).
- Always ask for receipts.
- Do not open any emails or attachments from people or organizations you do not know.

- Ensure your computer has an updated virus-protection program.
- Internet users can check for email scams by going to Snopes or other search engines.
- Be cautious. You have the right to research an investment or buyer by requesting written information, seeking references, asking questions, weighing the answers, and taking the time to think over the offer.

Online Shopping

- Keep your apps on your computer updated. Most of the updates are related to security.
- Look for the padlock on a web browser. Also, look for the https:// in the address bar. This means the website is secure.
- Use separate emails and different passwords on every sight. Don't recycle your passwords.
- Use Credit card, not E-Transfer – If the transaction was fraudulent, with a credit card you can call the credit card company and try to get your money back. You're not able to do that with an e-transfer.
- There is a phone number on the back of the card so that you can contact the financial institution.
- Take notice of advertisements with information that is too good to be true. Scammers want you to click and divert you to fake sites or links that are trying to steal your information.

Gift Cards

Two methods are being used. Scammers copy and reprint a barcode of a gift card in their possession and stick it on a gift card that hasn't been purchased yet. That way, when you purchase a gift card and "activate it" you are activating the scammer's gift card. The second method is even simpler, the scammer will take pictures of gift card barcodes and once it's purchased and activated, they will use a self-checkout kiosk and simply pay for the item with an image of the barcode on their phone.

How do you protect yourself?

- Inspect the gift card to ensure that it was not tampered with. Check to see if a sticker has been placed on top of the original barcode.

- When purchasing a gift card, ensure that the information on the receipt (usually the type of gift card and the barcode that will be printed on it) match.
- If possible, check the balance of the gift card after purchasing it.

Advance Fee Fraud

- Use caution when transferring money through a third party.
- A newspaper ad or telephone call about "easy credit" or an "easy loan" is a red flag.
- If you are asked to pay a fee in advance of receiving the funds, it is a scam.
- Never send money in advance.
- It is illegal in Ontario to ask for an advance fee for a loan. If asked to do any of the above-mentioned, report it to the police and the Ministry of Consumer and Business Services.

Computer Security

- Turn on multifactor authentication apps that add a layer of security when logging on.
- Turn on accounts alerts that will notify you when there is a new log-on.
- Use strong passwords, and ideally a password manager to generate and store unique passwords.
- Back up your data to external hard drives or USBs. If you are locked out of your computer, you will still have access to important information.

When posting digital pictures:

- Scammers are always on the lookout for any information that can identify you.
- Don’t tag the location – people will know your location.
- Avoid putting your full name when posting.
- Look at what is in the background of the photo that can provide unwanted information – be cognizant of your surroundings.

Trending Scams

Romance Scams

Fraudsters operate online by targeting people who are vulnerable such as recently divorced, widowed, lonely, etc. The fraudster will create online romantic relationships and then fool the

victim into sending money. Be cautious when they ask for material things or money. Scammers will play on your feelings to extort money from you. Be careful when embarking on a new relationship and educate yourself on the techniques, scammers use.

Canada Revenue Agency (CRA) scam

- Fraudsters will call victims by telephone and identify themselves as police officers collecting overdue taxes owed to the CRA. Back taxes have been demanded in the form of cash, wire transfer, or iTunes gift card. The fraudster advises the victim that they have an overdue amount of taxes to pay and if they don't, they will be arrested.
- Police do not engage in tax collection of any type and do not arrest individuals about overdue taxes. Any call or email of this nature should be considered a scam. If you have concerns about the possibility of overdue taxes, this should be discussed and confirmed directly with the CRA.

Credit And Debit Card Fraud

If your identity is stolen or your credit history is compromised, it can take years to recover and affects your sense of security. Take the necessary steps to protect yourself:

- Immediately report lost or stolen credit cards.
- Check monthly statements carefully and report any discrepancies to the issuing credit card company.
- Never loan your credit cards to anyone and sign all credit cards when you receive them.
- Cancel credit cards you do not use and keep a list of the ones you use regularly.
- Promptly remove mail from your mailbox after delivery and do not leave pieces of mail lying around your residence or workplace.
- Shred bank statements and all paperwork you no longer need.
- Never give out your passwords or Personal Identification Number (PIN).

Telephone Fraud

- Everyone has received a call stating you've won a free cruise, the lottery, or received a request for a donation. Use extreme caution when answering these calls.
- Always verify that the charity/company is legitimate.
- Often what is initially free, can end up costing you thousands of dollars.

- Never give personal information over the telephone or the Internet.
- Ask the caller if you can call them back so you can research the information, they have given you. Don't be surprised if they hang up.

ATM Fraud

While using an ATM is a quick and convenient way to conduct financial transactions, you need to use caution to ensure your account is secure.

- Be aware of your surroundings when entering your PIN and do not disclose your PIN to anyone.
- Cover the keypad when you enter your PIN.
- Be mindful of people trying to distract you.
- Immediately report lost or stolen credit/debit cards.
- Check your account statements monthly and report any discrepancies.
- If you discover anything at a banking machine that looks suspicious (a card skimmer, for example), notify your bank immediately or contact the police for assistance.
- Anyone who does fall victim to any of these scams should contact your local police service and the Canadian Anti-Fraud Centre.

Additional Resources

- Canadian Anti-Fraud Centre: https://www.antifraudcentre-centreantifraude.ca/index-eng.htm
- Get Cyber Safe: https://www.getcybersafe.gc.ca/en
- Peel Regional Police Cyber Safety Tips and Resources: https://www.peelpolice.ca/en/safety-tips/cyber-crime-computer-and-internet-safety.aspx
- RCMP seniors guidebook for safety and security: https://www.peelpolice.ca/en/safety-tips/cyber-crime-computer-and-internet-safety.aspx

Get Cyber Safe

Get Cyber Safe is a national public awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online.

https://www.getcybersafe.gc.ca/en