Lucas Sarweh

Professor D. Mayo

COMP2057

31 March 2021

Types of Internet Fraud

Topic 1: Fake shopping websites and apps

To identify fraudulent websites be weary of: Poorly designed websites, websites without any contact information, policies on returns are difficult to locate, the back button is disabled by the website, you are asked for personal information when it is not necessary. For mobile apps: The name of the app is close to that of another major store, an app description or user feedback is non-existent, the app asks for many or questionable system permissions while installing, or the app has many pop-up ads that are designed for accidental clicking.

The way these criminals take advantage of people is to make their websites or apps look like genuine retailer websites. They come up with names that may sound like a real business. The goal is to trick people into inputting credit card or other personal information. When you download a malicious app the permissions it asks for may allow it to steal saved passwords and credit card information.

To prevent yourself from becoming a victim always shop with reputable retailers who have contact information easily accessible and get their app from their official website. Also look for websites beginning with https instead of http because the “s” means the website is secured. Try to avoid using public Wi-Fi when making purchases as you never know who could be searching for others information through the web. Do not respond to pop-ups on websites as they could be dangerous, and they are also annoying. Make sure your computer anti-virus is always up to date and always pay with a credit card as credit card companies usually have protection against fraud.

If you are a victim of a shopping scam you should report it to your local police department. Most importantly if you believe you have been scammed or your credit card details have been compromised, call the number on the back of your credit card immediately. Credit cards companies will do all they can to protect you from fraud.

Topic 2: Tax season scams

To identify tax season scams it is better to understand what the Canadian Revenue Agency will never do. Receiving urgent or threatening messages are red flags as well as emails or texts that require you to follow an external link to “verify” your information. This verifying is them trying to steal your information. Things that the CRA will never do are sending you an email with a link asking you to give personal information, sending you an email or text with a link to your refund, threaten you with the police force, require you to pay with less refundable or trackable payments such as interact e-transfer, bitcoin, or pre-paid cards, and use any kind of instant messenger to contact you such as Facebook, WhatsApp, or Messenger.

The way the scam works is by using pressure to make a less rational decision. This pressure could be threats of arrests or possibly if you are talking to a person, they could be rushing you. With this sense of urgency, you are now more prone to being hasty. They will try and trick you into paying for debt that does not exist or they will try to steal personal information. They could say things such as: “You owe use X amount of money in bitcoin,” or, “You have not filed your taxes correctly pay immediately or legal action will be taken,” or, “Click Here to claim your tax refund.”

To prevent this from happening always keep in mind the things that the CRA would never do. If someone does contact you in this manner, you could also log into your online CRA account and check there directly.

If you believe you have been scammed and gave away your financial information, contact your financial institution immediately and work with them to prevent further damage.

Topic 3: Ransomware

The ransomware scam works like a regular ransom, but instead of kidnapping people it kidnaps your computer and its files. These criminals lock out your computer to extort money from you.

To identify this scam, you will need to go to shady websites or email messages that when you click on pop-up ads or even anything sometimes it will try to download malicious programs to lock you out of your computer. The program will give the criminal access to your files so that they may encrypt them, which means that only people who know a key or can decrypt them can access those files. The criminal will then ask for payment to unencrypt the files, which they may not do anyway.

To prevent this type of scam is to not allow these malicious programs to be downloaded on your computer. To do this you can install the best anti-virus software’s while also keeping them up to date. Keep your operating system up to date. Keep backups of your files in a cloud not associated with your computer such as Microsoft One Drive. Do not mess with unknown emails and suspicious websites and add an ad blocker to your web browser.

If you are a victim of this fraud and are familiar with data recover you could ask anti-virus providers to help detect the malware and remove it. An IT specialist may be able to help you recover your files and back them up. You may want to change all online passwords especially if you had files that stored your passwords. Also, to help track down the criminals you should alert your local police department and the Canadian Anti-Fraud Centre.

Topic 4: Identity Theft

Identity theft is an attempt to steal other people’s private information like your birth date, social insurance number, and your name to impersonate you to commit financial frauds. This will allow the illegal activity they do to be traced back to the victim instead of themselves. Keep in mind that even a small amount of information may be enough to start posing as you.

Identity theft can be identified in many forms. A phone call or letter telling you that you have been denied or approved for things like credit cards that you did not sign up for. You suddenly stop receiving mail that you would have expected, or even if an account in your name has defaulted and are now being contacted by a collection’s agency, but you never opened that account. Pretty much any activity that only you could do but has been done regardless are red flags as that person is posing as you.

To prevent this from happening first you must be careful with what personal information you share online. On social media platforms check your privacy settings so you know what is being shared and do not share your birthday with unknown people. Choosing unique passwords for your most sensitive accounts is great because if one password is found criminals may try and use that password for different services as well. This is especially important for your main email, financial institutions, and government accounts. Where applicable allow multi factor authentication so that more than just a password is required to access an account. Finally, you should shred or destroy any and all-important documents you no longer need such as any financial documents, old credit cards, or physician notes. This prevents criminal dumpster divers to get your information.

If you become a victim of identity theft contact your bank immediately. They will take steps to try to help you as much as they are able by investigating, reversing transactions, or reissuing debit/credit cards. Also, you should contact your local police department as well as Canada’s credit reporting agencies, Equifax, and TransUnion, to obtain your credit report. If there are creditors you have never dealt with let them know you have been a victim of identity theft. You should also consider a fraud alert so that for any company that inquires about your credit, they must contact you before giving out the credit. Finally, it may be necessary to contact other organizations like the CRA in case your social insurance number has been stolen or any other important information.

Topic 5: SIM swapping scam

A SIM card is the small, removeable card inside a mobile device that identifies the user and gives access to the mobile provider’s network. Unfortunately, scammers can now contact your provider and swap SIM cards to gain access to your phone and steal information. You may notice that calling or texting may no longer work, and this may be the case.

This fraud first starts with some way of finding the victims information such as a phishing email so that they can impersonate you. Once they have enough information, they will contact your mobile provider and request a new SIM card in your name. Now that they have your SIM card, they can access all your phones services such as your bank account, email, pictures, phone calls, and text messages.

To protect yourself you can set up a PIN with your service provider to access your phone for any contact between the customer and the provider. It would be best to use a unique pin. Do not publish your phone on social media and limit personal information available about yourself. Avoids using the same passwords for all accounts as fraudsters may use one stolen password for other companies. Remember that your bank will never call or email you to disclose personal information.

If you are a victim then you should immediately contact your service provider to deactivate the fraudulent SIM card and possibly get a new phone number with new contacts. You may also want to contact your bank to secure your accounts that may have been compromised and notify your contacts that your number has been compromised to avoid any further malicious intent.