IDENTITY THEFT

The Commercial Crime and Fraud Sections with the Saskatoon Police Service, Regina Police Service, Saskatchewan Financial Services Commission, and the RCMP “F” Division have joined forces to promote March as Fraud Awareness Month to Saskatchewan residents and consumers.

During this fourth week of Fraud Awareness Month, the fraudulent activity to be profiled is identity theft.

Have you ever fell victim to unauthorized transactions on your bank account or credit card?

Have you had a collection agency contact you and had no clue what they were talking about?

If this has happened to you, you are not alone. You could have been a victim of Identity Theft. Identity related offences are on the rise and Canadians need to be aware of how to prevent it from happening. But in order to prevent it you must understand what “fraudsters” are looking for, how they use your identity and how to prevent them from getting your identity.

What are “fraudsters” looking for?

The fraudster is looking for **identity information**, which includes items like your name, date of birth, social insurance number and passport number. But it also includes debit card numbers, credit card numbers, passwords and written signatures. New Canadian legislation includes a person’s fingerprint, DNA profile, retina image and digital signature as identity information. This may seem strange to some but it indicates how technology can play a role in identity theft.

How can “fraudsters” get my identity?

- Break into your home or car to steal wallets and purses that contain your identification
- Steal or redirect your mail
- Go through your garbage
- Access personal information databases

These methods are risky for criminals because there is a chance of getting caught. Today, “fraudsters” can get your identity without being seen because they are online.

How do fraudster’s get my identity online?

- Phishing including Spear-Phishing
- Banking Trojans
- Social networking sites
- Job postings

People today do not realize how much personal identity information can be accessed online. Organized crime groups exploit the internet and spend time and money developing new methods to access Canadian’s personal computers. Organized crime groups send out “Phishing” e-mails or websites that appear to be

legitimate. The victim responds to the e-mail or enters personal information onto the “hoax” website thinking it’s their financial institution or another reputable company. Now the organized crime group has your personal information. They may use the information to apply for loans, then default on the payments, and leave you with bad credit. They may store the information for months and months, only to use it a year later. They may sell your information to another crime group for a profit.

“Spear-Phishing” works along the same line but instead of sending out e-mails in mass they will target specific people. They research small businesses and contact a person that is involved with the financial transactions for that business. They will contact this person posing to be someone in a position of authority like the “network administrator”. The e-mail is opened or it provides a link to an infected website. Once you open the attachment or go to the infected site malware is installed on your computer. This malware contains a keystroke logger which is a program that records your activity on your computer such as keystrokes, mouse clicks, opened and closed files and websites visited. With the information saved, the organized crime group will wait until the victim accesses the business’ accounts through online banking and are able to make numerous transactions and transfer out funds.

Because people have been warned against “Phishing” emails they are not as effective as they used to be so criminals have gone one step further. They have developed software to specifically focus on getting a person’s banking information. These banking Trojans infect your computer in similar ways to phishing. The difference is that they will lay dormant on your computer until you access your online banking website. It too is a keystroke logger and records your account number, credit card number, password, PIN, or security questions. This malware can run in the background while you are making financial transactions. Some can redirect the transactions directly into the fraudster’s account. Some can copy the webpage with a picture of your account balance; they make a transaction on your bank account and then replace it with the picture they took earlier. You are not aware of the different balance and it may take days before you notice the change. By that time the transaction has cleared and the funds cannot be frozen. Some Trojans are very simple and transfer small amounts that mimic your normal banking habits which will not be detected by the financial institution’s anti-fraud systems. Other banking Trojans are so complex that when the financial institution attempts to track the money transfer it will be traced back to the computer of their complaining customer.

Trojans are not new but they are continually evolving and have infiltrated social networking sites. Social networking users are usually mindful of what security options to use and what personal information to include. But how closely do they watch what they click on? Youtube.com videos, Facebook.com, blogs, Twitter.com status updates can all be ways that banking Trojans have infected computers. These are popular sites that are visited by millions not only with a computer but also Smartphones. With all of the latest Smartphone developments there are so many ways malicious software can upload to your phone. Plus you can get text messages that trick you into giving up personal information, known as “Smishing”. As you can see we have almost come full circle and it is up to us to educate ourselves to the new scams and techniques used by criminals.

Now that the criminals have our personal information and can access our bank accounts how do they pick up the money without getting caught? They again use the internet. They post job advertisements online asking if you want to work at home and become financial agents. Again these advertisements look legitimate and people believe they are working for real organizations. Yes they are real. That is real organized crime groups and this person is a “money mule”. The financial transactions that are done with the use of banking Trojans are being transferred into the “money mule’s” bank account. The “money mule” transfers the money into another account or uses a wire transfer service to move the money to the fraudster. In essence this is a money laundering service and the mule gets paid a small percentage.

How do we protect ourselves from online identity theft?

Protect your computer and Smartphone. Ensure to have up to date Antivirus, Anti Spyware, and Firewall protection. It is recommended to have the latest version of your web browser as it's the most secure. Contact your financial institution and ask what they recommend for appropriate protection programs. Make sure you access your online banking regularly to check for unauthorized transfers. Use complex or unique passwords and change them frequently. As tempting as it is, don't reuse passwords and don't store them on your computer. Do not open suspect attachments, or go to links provided in strange emails or spam. Be careful when you are providing personal information and ask who and why you are providing this information to.

If the unforeseen happens, REPORT IT. It is estimated that only 5% of people will report being a victim of fraud. Every victim will provide information to the police that can either lead to a criminal or can prevent someone incurring a loss. Please share this information with coworkers and loved ones to prevent others from becoming a victim of identity fraud.

For more information contact:

Constable Ferrah Yaeger
F Division Commercial Crime Section Regina Office
(306) 780-6005