The Commercial Crime and Fraud Sections with the Regina Police Service, Saskatoon Police Service, Saskatchewan Financial Services Commission and the RCMP have joined forces to promote March as Fraud Awareness Month (www.sacp.ca/fraudawareness) to Saskatchewan residents and consumers.

Public education and awareness is key in preventing and reducing the number of victims of fraud. During the third week of Fraud Awareness Month, the fraudulent activity to be profiled is on-line banking identity theft.

On-line banking is SECURE. Personal information and more specifically, on-line banking information, can be compromised when individual users do not take steps to assist in protecting themselves.

A typical on-line banking compromise goes as follows:

You log into your on-line banking one morning and notice a money transfer to a payment card for $2,800.00. You know nothing about this transaction so you report it to your financial institution (FI). The FI starts an internal investigation and tell you that the money was transferred to the payment card and taken out in cash. You insist you did not authorize this transaction. The FI tells you to call the police. The police start an investigation and speak to security personnel at the FI. They are able to provide the IP address which accessed your account. Subsequent investigation reveals the Internet Service Provider (ISP) is located in eastern Canada. The investigator finds out the user is located in another country.

You turn your computer over to the police for analysis. This analysis reveals your computer is infected with a trojan/virus. This trojan is known as a "bot". This type of trojan is actually a key stroke logger. This means that every key you hit on your key board is being recorded. The hackers download the information and looks for your 16 digit debit card number/user name. After that they know is your password and answers to security questions. This allows them to access your on-line banking.

People often wonder, "How did I download this (bot) on my computer?" It may have been as simple as accessing a non-secure website. If the address bar does not indicate https: or show a lock, it is not secure and some trojans have been uploaded this way. Some people have allowed remote access to their computer when they have received a call from someone offering to “fix” their computer. Others have clicked on links in e-mails or responded to pop up advertisements or e-mails asking for on-line banking information. Typically, these look like legitimate banking e-mails or sites. But, remember the bank will NEVER ask for your banking information by e-mail. Also, if you do not bank with that FI DO NOT supply the information for the FI you bank with.

What can you do to avoid this terrible situation? A few simple steps can protect you:

First, use, update and run all the following individual software on a regular basis: malware, adaware, spyware protection and anti-virus software. These will protect you against Trojans, worms, spyware, adware and viruses and are available free on downloads.cnet.com. You will never be 100% protected, but installing these types of software will give you about 98% protection. Start with a full system scan and then at the very least, run a quick scan on a monthly basis.

Second, follow the guidelines set out by your financial institution. Some allow you to enter your 16 digit debit card number into your on-line banking and then check a box to remember this number. Use this feature! Once they ask your security questions there is a box you can check so they will not ask you your security questions when you use a certain computer. This is meant for a computer you would normally use to access your on-line banking, such as a home computer. Use this feature! This is not for a public access computer such as a library, hotel, etc.. Taking a few minutes to follow some of the security feature set up by your FI may save you some heart ache in the future.

Saskatchewan
Financial Services
Commission

If you are reading this article and have not done any of the above mentioned do not run to your computer and access your on-line banking unless you have all the software mentioned and used them. Instead install all the software, run a scan with each and removed the trojans/virus. Then access your on-line banking and follow your FI's instructions.

Remember your financial institution will never request personal information in an e-mail or over the phone. If you are suspicious of an e-mail contact your financial institution. If you are suspicious of a phone call, hang up and call your financial institution at a number you are certain is safe. Don't be so trustworthy of people soliciting information from you. You never know how it will be used.

PROTECT YOURSELF! DON'T BECOME A VICTIM!

Fraud Awareness is part of a national crime prevention campaign to increase Canadians' awareness of and knowledge about different types of fraud in order to help citizens to not become fraud victims. RCMP Saskatchewan's "F" Division Commercial Crime Section has offices in Regina and Saskatoon. Their role is to reduce the impact of economic crime on Canadians by maintaining the integrity of our economy through public education, crime prevention, and enforcement.

To better educate yourself with this scam and others, please visit www.rcmp-grc.gc.ca/scams or www.antifraudcentre.ca

- 30 -

For further information please contact

Cpl. Trevor ELLIS
"F" Div Commercial Crime – Regina Office
(306) 780-3959