SaskTel News

March 2017 Issue 79

Fraud Awareness

Awareness is the key to protecting yourself from fraud.

Here are some steps to protect your personal information:

- Shred or burn all documents that include your name, address, Social Insurance Number, financial information, or other sensitive personal information.
- Do not recycle papers containing personal information.
- Information posted on social networking sites may be seen by just about anyone. Also be sure to read the privacy statement and policies and use privacy settings to limit who may view your information. Also, please be sure to read website privacy statements before submitting personal, financial or medical information.
- Be wise about Wi-Fi. Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, check and see if your information will be protected. When you are using an encrypted website, it protects the information you send to and from that site. If you use a secure wireless network like SaskTel Select Wi-Fi, all the information you send on that network is protected.
- Always delete personal information before discarding or selling a computer.
- Use overwrite software or destroy the hard drive because information can remain on that hard drive even after deleting files from folders.

Further information can be found on the website of the Federal Office of the Privacy Commissioner at www.priv.gc.ca/en/, the Office of the Saskatchewan Information and Privacy Commissioner at www.oipc.sk.ca, your banking website, and the Department of Health at www.saskatchewan.ca/residents/health/accessing-health-care-services/your-personal-health-information-and-privacy.

Another fraudulent practice that can affect both wireline and wireless customers is called “cramming”. Cramming as a fraudulent act is not new, is still happening, and can result in unauthorized charges appearing on customers’ monthly bills.

An example of how cramming works is as follows: A customer receives a call during which the caller hangs up. When the customer returns the call to the number on their Caller ID, they are connected to a “premium service”, such as a paid international adult entertainment service, a chat line, or other alleged call centre service usually located outside Canada.

When customers call the number back they are then charged for the unsolicited “premium service”. These charges are then added to a customer’s monthly SaskTel bill and detailed as third party charges. SaskTel does have processes in place to remove one-time only calls from the SaskTel bill, though the third party vendor may still attempt to collect the supposed charges through traditional means such as collection agencies.

Please be advised that these charges are not levied by SaskTel, but by the third party vendor. In many cases crammers may only put a small charge of a few dollars, so as not to arouse suspicion.

“Spoofing” has also been around for years and is becoming increasingly common. This is the use of technology to mask the true number or identity of a caller on your Caller ID. Calls can come from any area code including Saskatchewan. In these cases, the criminals are using familiar area codes or even business names to create a false sense of familiarity with their victims as they “phish” for sensitive personal or financial information.

Avoiding these types of calls can be problematic. Unfortunately, SaskTel cannot control the behaviours of incoming callers so customers need to be aware of these types of calls. If you do not recognize a telephone number on your Caller ID, ignore it. Legitimate callers will generally leave messages identifying themselves. Check your communications bills carefully and immediately inform your carrier if you spot any unauthorized charges.

A good guideline to follow to avoid falling victim to these practices: if you do not know the number and the caller did not leave a message, do not call the number back.

And remember, usually if it seems too good to be true, it likely is.

SaskTel News

Voice Mail Fraud

Voice mail has become an everyday communications tool for business and residential customers alike. Criminal minds have found that poorly protected voice mail boxes, primarily medium to large businesses, can be used to make long distance calls all over the world. This method of fraud uses the “through-dialing” feature that legitimately enables corporate employees to make long distance calls from outside of the business by calling into their office voice mail. This can run into the thousands of dollars of unauthorized long distance calls for which the company would remain responsible because the calls originated from their own phone lines.

Residential users are far less vulnerable to hacking attempts because few have access to the “through-dialing” feature. How it works: The hacker calls a business after hours and uses the automated voice mail service to search for inadequately protected mailboxes. The hacker is looking for mailboxes which have simple or “default” passwords. Though there are many different voice mail systems, the prompting patterns can be used by the hacker to determine which system is in place. The hacker then determines the “default” password for that system, and it is just a matter of time until they come across a mailbox that they can access.

Users need to keep in mind that the password for their voice mail is the primary security method to protect their mailbox from being hacked. The “default” password should be immediately changed. Passwords like “1111”, “1234”, “9999” or the last four digits of the telephone number should never be used. Also be aware that using real words related to numbers on the keypad is also unsafe.

Customer Privacy

SaskTel is an open and honest company and we want to emphasize that we comply with Saskatchewan’s privacy laws and take active steps to protect and safeguard our customers’ information. There is a team of people within SaskTel that have a mandate and directive to proactively manage privacy on a day to day basis.

All customer information requests that SaskTel responds to require, as a prerequisite, a legal basis for making such a request. Many requests we receive respond to court orders from law enforcement agencies, or government departments who are authorized by statute to request information to enforce laws like the Income Tax Act, and through assisting police services in life threatening emergencies or where there is an ongoing investigation concerning child exploitation.

Customer privacy is of utmost importance to SaskTel.

2016 SaskTel Scholarships

Each year SaskTel awards a large number of scholarships to Saskatchewan students studying in fields related directly to information and communications technology. SaskTel is pleased to congratulate all the worthy candidates selected to receive awards in 2016.

The recipients of the SaskTel Scholarship Program for 2016 are: Shane Buchanan, Emily Erhardt, Andrea Mah, Emilyn Marshal, Savannah Serbu, Tyler Wellman, and Hussein Yaqub; and the recipient of the 2016 Gord Kuhn Scholarship is Shelby Piechotta.

SaskTel also extends its congratulations to the recipients of SaskTel’s 2016 Métis Scholarships provided through a partnership between SaskTel and the Gabriel Dumont Institute (GDI). The successful candidates are: Justin Boyer, Bailey Doucette, Matthew Iverson, Amanda Johnson, Celena Kelly, Bryce Maffenbeier, Justine Montgomery, Gabriel Olver, Paul-Remi Poulin, Cynda Sayers, Cassidy Venne, and Danna Wagner.

In addition, SaskTel congratulates the recipients of SaskTel and the Saskatchewan Indian Institute of Technologies (SIIT) 2016 scholarships. They are: Sonja Eninew, Tony Kay, and Ariel Morin.

For more information on the availability, requirements and application deadline for scholarships, as well as information on the successful candidates, please visit www.sasktel.com/about-us/careers/.

SaskTel