

SaskTel News

November 2018

Issue 83

Internet Protection

The Internet is a valuable tool, but it's important to remember that using it can pose risks that we need to guard against. Sophisticated spyware or malware can be delivered via email or unintentionally installed by surfing a website. These rogue programs can steal personal or financial information and, in some cases, damage installed software, the operating system, or your computer's hardware.

Some of the most common attacks are carried out by spamming and phishing email; however, other exploits may leverage instant messaging services, mobile phones, and social networking websites.



Spam email are unsolicited bulk messages; they usually attempt to sell a product or service or promote a website. Phishing email pretend to be from a trustworthy source such as a bank, or other reputable company, and attempt to fraudulently obtain sensitive information such as usernames, passwords, credit card details or some other personally identifiable information.

Follow these tips to help protect your personal information:

- If you receive an email or instant message that appears suspicious, delete it and contact the sender to whom it appears to have originated from to check whether they are really trying to make contact with you.

- Be wary of email and instant messages from originators you don't recognize, especially if the message directs you to click a link or open an attachment. Attachments of all types have the potential to carry malware. Instead of clicking links in an email, navigate to reputable websites by typing the address into your browser's address bar, or use a search engine to locate the website and use the link in the search results provided.
- Be sure to use anti-virus and anti-malware/spyware programs and install operating system updates and critical security patches as soon as they are available.
- If you access the Internet using Wi-Fi, SaskTel strongly recommends that you configure your wireless network to utilize the stronger WPA2 security protocol. If your wireless network is currently configured to utilize WEP security protocol, please be aware that WEP is no longer considered secure and is easily compromised, and therefore increases the risk breach of your security and privacy. If you need assistance making the change to WPA2, instructions are provided on sasktel.com.

It is also important to use a strong and unique password for each website or service you access. Phishing campaigns and malware often target email account (or other) credentials. Using the same username and password with several of your web-based service accounts increases the likelihood of a serious breach as all services using those credentials become vulnerable.

Users should also consider using unique passphrases instead of passwords. Passphrases are much easier to remember and ultimately much stronger than passwords. Visit sasktel.com/strongpasswords for more information on creating strong passphrases.

Security is a priority at SaskTel. The Support section of our website provides information about new email threats and security issues as they arise. However, it's your cyber savvy that is the single most effective tool for protecting your security.

Keeping Your Connected Home Safe

Smart technology is everywhere. With smart TVs, locks, thermostats, and voice-activated digital assistants making their way into a growing number of homes, it's clear to see this is a trend that won't be slowing down any time soon.

But before you install the latest smart device in your home, it's important to know how you can prevent unauthorized use and access. Recent media coverage has highlighted the fact that hackers are more than willing to take advantage of security vulnerabilities in these systems to listen or watch your activities at home.



But there are steps you can take to protect yourself:

- Always make sure you are buying your device from a trusted source. Use caution when buying digital assistant or smart home devices second-hand as it can be difficult to verify that it hasn't been tampered with.
- Ensure your Wi-Fi router is secure and give it a unique name that doesn't give away clues about your identity or where you live (i.e. don't use your family name).

- Set a strong and unique password for each smart home device or Internet connected camera, ideally with a mix of letters, numbers and special characters. Many devices come with a default password that's easy for scammers to guess.
- Be alert for phishing emails or text messages asking for your username or password. These can often look convincing and closely mimic the logos and domain names used by legitimate sources.
- Keep your software up to date. There are always regular safety updates to protect your devices from viruses and other threats. While most updates will occur automatically, it's always wise to check to see if you have the most recent software version.

When you want to check your smart home devices while you're out, try to use a mobile VPN (Virtual Private Network) if accessing a public Wi-Fi network. They are easy to use and let you access the web safely and privately.

To enable VPN, use your smartphone settings by tapping under the Network & Internet section, then tap the Add VPN option and give the connection a name.

SaskTel smartHOME home monitoring systems use cutting edge technology that can safely automate your home with the benefit of 24/7 local monitoring. Customers can set their own alerts and reminders notifying them of any activity, whether the system is armed or not. To learn more, call 1-800-SASKTEL.

Checking Your Data

Streaming your favourite show is fun, but it can bring you closer to using the monthly data limit of your SaskTel wireless rate plan.

For customers who do not subscribe to an unlimited plan, SaskTel sends data notifications to your device to let you know when you are nearing or have reached 100% of your monthly allowance.

To avoid going over your limit, try to get in the habit of checking your usage regularly by visiting sasktel.com/myusage on your Android or iOS device or using the free mySASKTEL mobile app.

There are also many sensible ways to trim your data usage such as using Wi-Fi when available or accessing one of SaskTel's free and secure Select Wi-Fi hotspots across the province.

For more data-saving tips, visit sasktel.com/manageyourdata.

