SaskTel News

June 2014 Issue 68

Understanding Wireless Roaming Charges

Even if you are not actively using your 4G wireless device, if your data features are turned on, your device is still using a data service.

To avoid data usage roaming charges, you can turn off the data feature on your wireless device so that only voice and text messaging services work. Please review your device manual. If you need access to data services while travelling, using Wi-Fi networks can allow access to data for no charge or for a nominal fee to the provider of the service.

If you lose the Wi-Fi connection, or there are no Wi-Fi networks available, please ensure you are aware of the data usage rates that you will be billed, depending on your location. Examples of activities that use data: email usage, browsing the internet, downloading or using applications like Google Maps, posting to social media like Facebook or Twitter, watching or listening to streaming video or music, and playing online games.

To help manage your wireless bill SaskTel offers U.S. and International data travel add-on packages.

To learn more please go to www.sasktel.com.

Lost or Stolen Device Service

SaskTel launched its Lost and Stolen Mobile Device Service on September 30, 2013. The purpose of the service is to reduce the number of thefts of these devices by making it difficult to reconnect a lost or stolen device to our wireless network.

SaskTel, along with all Canadian wireless carriers and participating U.S. carriers, will interconnect with the GSMA database to black-list reported devices. The CWTA website www.ProtectYourData.ca will allow anyone to check the International Mobile Equipment Identifier (IMEI), a unique registered number imbedded in the device, to see if the device has been black-listed in Canada. If the IMEI number has been black-listed, that device will not be able to be used on any Canadian network.

SaskTel has deployed an Equipment Identity Register (EIR) on its network to keep its own internal list of black-listed IMEIs. The EIR will connect to the IMEI database to share the latest list of black-list devices with other carriers.

The IMEI database takes black-list data from U.S. and Canadian carriers that subscribe to the GSMA and compiles it into one national black-list registry.

When the SaskTel EIR downloads the latest black-list, all devices reported as lost or stolen share the most current information to the IMEI database. In this way any device reported lost or stolen by other carriers, up to the previous day, would also be capable of being blocked on the SaskTel network.

Customers may call 1-800-727-5835, visit a Corporate Store, or visit a SaskTel Authorized Dealer to inquire as to whether or not a mobile device has been black-listed, add a device to the black-list should it be lost or stolen, or remove a device from the black-list should it be found.

Additional information can be found at: http://support.sasktel.com/app/answers/detail/a_id/10944.

SaskTel
Your Life. Connected.

Internet Protection

Internet users must remember that although the Internet is a valuable tool, it also presents unintended risks that need to be guarded against. Sophisticated spyware/malware, delivered via email or unintentionally installed by surfing a website, can automatically activate functions ranging from theft of personal or financial information, to damaging installed software, the operating system, or computer hardware.

Spamming and phishing attacks are an everyday occurrence with email, but can also occur via instant messaging, mobile phones, and social networking websites. Spam is unsolicited bulk messages, usually attempting to sell a product or service or promote a website. Phishing is a message pretending to be from a trustworthy source such as a bank, or other reputable company, trying to acquire sensitive information such as usernames, passwords, credit card details or other personally identifiable information.

SaskTel strongly suggests that you be wary of the contents of all email, even when you recognize the sender, as many spammers today are “spoofing”, or pretending to send email from valid email addresses. SaskTel strongly suggest that you not open any email where you do not recognize the sender, if the email appears to be in a strange language or has jumbled characters, or if extra letters have been added into words, or there is an attachment with a .VBS, .EXE, or .PIF extension or an unsolicited attachment with a .DOC, .DOCX, or .PDF extension. Do not open the attached file and delete the email immediately. Please be aware that files of virtually any extension may carry malware.

Do not accept unsolicited downloads through instant messaging systems or Peer to Peer file-sharing applications. Be aware that file-sharing could deliver malware to your computer or mobile phone.

SaskTel highly recommends that users install and maintain up to date anti-virus and anti-malware/spyware programs and that operating system updates and critical security patches are applied as soon as they are available. If you access the Internet using Wi-Fi, SaskTel strongly recommends that you encrypt your wireless connection using WPA2 encryption to reduce the likelihood of security or privacy issues. If your wireless network is currently encrypted using WEP encryption, please be aware that WEP is no longer considered a secure form of encryption and is easily compromised, potentially resulting in a breach of your home network and resulting in a loss of security or privacy. WPA2 can substantially increase the security of your wireless network.

If you need assistance making the change to WPA2, instructions are provided on sasktel.com/support by searching for “Wi-Fi Security” in the search bar on the support page.

Security is a priority at SaskTel. The "Support" section of our website, at www.sasktel.com, provides information about new email threats and security issues as they may arise.

Customer Privacy

SaskTel would like to assure its customers that all information about a customer is safeguarded and considered confidential, with the exception of a listed or published name, address and telephone number.

Customer information, other than a published name, address and telephone number is only provided to law enforcement agencies or agencies with legislative authority through defined legal processes (eg. subpeona, formal demand under statute). The only exception to this is in the case of a declared emergency.

Customer privacy is of utmost importance to SaskTel.