SaskTel News

September 2010 Issue 53

Voice Mail & Telemarketing Fraud

Voice mail has become an everyday communication 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. Residential users are far less vulnerable to hacking attempts because few have access to the "through-dialing" feature. Though this is not a new fraudulent activity, the number of instances was on the rise once again earlier this year, and can run into the thousands of dollars of unauthorized long distance calls.

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, then it's 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 the numbers on the keypad is also unsafe.

This spring some SaskTel customers received calls announcing that they had won a Cruise, or were being offered exceptional credit card rates, and were asked to push a number to get details. Dialing the number suggested may result in third party billing charges on your phone bill, usually ranging between $4.99 to $5.99 a minute, by an out of country provider. As well, these calls were spoofing a Saskatchewan number for the call display, leading customers to believe that these were local calls. These are not legitimate calls. SaskTel continues to work closely with Bell and other telephone providers to resolve these types of telemarketing scams as quickly as possible.

If you receive this type of call you should hang up immediately. Do not press any further numbers and do not redial or attempt to call the number back. SaskTel recommends that customers never dial a number that they do not recognize. Customers can register a complaint regarding a telephone or fax telemarketing call: online at http://www.LNNTE-DNCL.gc.ca or by phone at 1-866-580-3625.

Sask 1st Call : Dial Before You Dig

For free cable locates before you dig, contact Sask 1st Call at 1-866-828-4888. The cable path will be marked, but SaskTel cannot guarantee the cable depth since ground cover may have been removed by past work or by erosion. Requests must be made at least 48 hours in advance of the work start date so the locate can be scheduled. Locates are only valid for ten working days after which a new locate request must be submitted. It is the responsibility of the person or company requesting the cable locate to remove marking flags after the completion of the work. SaskTel appreciates your cooperation to help prevent cable damages.

SaskTel

Internet Protection

The internet is an invaluable resource for many SaskTel customers but unfortunately it can also be a source of unintended risk in the form of malicious software (malware) such as viruses, Trojan downloaders, worms, or spyware or malicious users such as those who send Spam or Phishing attacks. In the past malware was primarily delivered through email, while today any number of sites on the internet can be a source of malware which may be automatically executed with effects that range from personal information theft to the duplication of malware email to everyone in your address book, pop-up windows, serious damage to installed software, the operating system, or the hardware of the computer itself.

Spamming and Phishing attacks are especially prevalent on the internet. 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, attempting to acquire sensitive information such as usernames, passwords or credit card details or other personally identifiable information. The majority of Spam and Phishing is delivered via email, but can also occur via instant messaging, mobile phones, and social networking websites.

When using email, be wary of the contents, even when you recognize the sender, as many spammers today are spoofing email addresses; pretending to send email from valid email addresses. We also strongly suggest that 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 even 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 like, Yahoo Messenger, AOL Messenger, MSN Live, or Peer to Peer applications such as eDonkey, BearShare, Limewire, or BitTorrent. Be aware that if you participate in file-sharing, many of these files could be delivering malware to your computer or even to your mobile phone.

SaskTel highly recommends that users install and maintain up to date anti-virus and anti-spyware programs and that operating system updates and critical security patches are applied as soon as they are available. Security is a priority at SaskTel. The "Support" section of our website, at www.sasktel.com, provides information about new email threats and other security issues as they may arise.

Know Your Long Distance Plan

SaskTel reminds our customers that unlimited long distance plans apply to 'voice' calls only. 'Data' calls are not eligible for savings or discounts and will be charged at regular long distance rates.

A data call is any non-voice call, typically between electronic equipment, such as a fax transmission, or dialing any long distance internet service provider other than SaskTel. This includes calls from your modem at home, or dialing into a remote internet account.

It is also important to remember that when you download data from a web site for which long distance charges apply, you are responsible for those charges. Customers should also pay special attention to any dial-up internet usage to avoid unnecessary charges. It can be as simple as ensuring you log off of the internet when you have completed surfing, since internet charges continue as long as the dial-up internet connection is left on. If you would like information on long distance plans please call 1-800-727-5835.

Toll-Free Numbers

SaskTel would like to remind you that only numbers with the prefix 800, 866, 877, and 888 are toll-free. The prefixes, which are not interchangeable, are used by simply dialing 1, followed by the appropriate prefix, followed by the seven-digit number. Please note that other prefixes, including 809, are not toll-free prefixes and long distance charges will apply on your telephone bill.

SaskTel