Identity Fraud eNewsletter

Spring Edition 2012

BELLCO

Banking for Everyone.

Protect Your Mobile Phone

If you're like most people in this tech-savvy world, you use your smartphone to send text messages, check your e-mail, access your financial accounts, and store data such as contact address lists. Even though this technology makes lives easier, make sure you are taking the necessary precautions to protect those messages and information from Web-based threats such as viruses and spyware, or the possibility of loss and theft.

Here are some helpful hints to keep the information on your smartphone out of the hands of cybercriminals:

Setting up PINs and passwords. PINs are usually a four-digit password. Try not to use common passwords such as your birth date, mother's maiden name, or pet names. Check your phone manual for instructions on how to create a PIN or password.

Use caution when downloading apps. Use sources you are familiar with and that are reputable, such as Apple's App Store, Google's Android Market, and Amazon's Appstore. Be sure to research the requested permissions from each app before completing your download. Watch this video for more information.

Use a security service. Many smartphone makers have over-the-air backup; remote phone locating; remote phone locking; and data-erasing capabilities. Apple makes a free Find My iPhone app for iPhone 4 and later versions; for an Android or BlackBerry, try an app called Lookout. This software allows you to lock the phone or even erase data remotely.

Disable your browser's autofill feature. Android and iPhone mobile Web browsers will remember your username and password for websites you visit often, making it easy for anyone who finds your lost phone to log into your sensitive accounts. Check your phone's manual; autofill can be disabled in your phone's web browser settings to ensure your information is kept safe.

Turn off your Bluetooth when it's not in use. Turning off Bluetooth is an important security step that is easy to do and may also save you some battery life on your mobile device. Other individuals could pair their device to yours and hack your personal information.

Although these tips are about the device itself, the number-one rule of mobile security is to not connect to public Wi-Fi networks or networks you aren't familiar with to do important tasks. Open Wi-Fi connections do not encrypt or encode data passing back and forth. This lack of security allows anyone in the area to pick up the signals and watch the data — even save it to their hard drive to gather your personal data later. Tools such as "Firesheep" demonstrate that, if you are logged into sites like Facebook, your cookies can be captured and used by others. In an instant, you could lose control of your online identity.

In general when accessing personal information online that requires a username and password over a WiFi network, a best practice is to use WiFi networks that are password protected.

Safe Online Shopping Tips

Considering all of the transactions that take place online each day, the percentage of those that are fraudulent or illegitimate is very small. Nonetheless, it is important that you take appropriate precautions to make sure you protect your personal information.

When it comes to safe online shopping and credit card fraud protection, simply knowing what to look for can help prevent fraud.

Check the website's security level. You can check the level of the security on each site in two ways. Look at the web address. If it begins with "https" then the site has been registered and received a certificate of credibility. You can also look for a padlock symbol in your browser. If this symbol is on the page, you should be able to click on it and it will tell you if the security certificate of the website is current and to what web address/company the certificate was issued. Checking these two safety features can help you filter out those companies you may not be able to shop with safely.

Another important component of online security is simple common sense. Most online shoppers can tell the difference between a legitimate site and one that is potentially unsafe. These differences can often be seen in claims a site makes about its products. When a site offers a product for significantly less than its competitors, be wary and remember the old adage, "If it's too good to be true, it probably is." You may end up paying for the merchandise, but might not receive your order.

Bellco has partnered with Identity Fraud, Inc. to offer protection to Bellco members at a discount. Visit www.bellco.org/IDFraud.asp for full details.

Bellco Credit Union
7600 East Orchard Road, Suite 400N
Greenwood Village, CO 80111
303-689-7800 or 1-800-BELLCO1

EQUAL HOUSING LENDER

CREDIT UNIONS

NCUA

Federally Insured by NCUA