The Monthly Brief

Volume 5 Issue 11 November 2017

Public Wi-Fi Scams

If you like to take advantage of free public Wi-Fi, double check before connecting. Scammers are using Wi-Fi to steal personal information and gain access to your accounts. Here's how it works:

You are at a coffee shop, airport, hotel lobby, or other public place, and you want to connect to the Wi-Fi. You search for connections and find one nearby. It may be labeled something generic like "Free Public Wi-Fi." These connections are actually created by the scammer using a "Hot Spot" and can even include the business name you're at. When you access the connection the scammer can record all of the data being sent over the connection, including credit cards, user names and passwords.

In another version the scammer charges a small fee for access. Once the payment is made, all of your credit card info or login credentials have been stolen. The threat can even come from a scammer on a legitimate Wi-Fi network reading data sent by your device. To avoid these Wi-Fi scams:

Verify the Wi-Fi connection name with the business or location before connecting. **Look For https** Only login to accounts or make purchases on sites using secure encryption. To determine if a website is encrypted, look for https at the start of the web address as the "s" stands for secure. **Always Use Anti-Virus and Firewalls on your devices.** For more advice and tips on using public Wi-Fi safely visit the Federal Trade Commission's website and watch their very informative video.

Follow Us On Facebook

Subscribe: philarcher@sa18.org

Amazon Delivery Scam

With the holiday shopping season already underway, this scam targets Amazon Marketplace customers who purchase from 3rd party sellers. **(Click the photo to view our Facebook Video!)**

How It Works: A vendor who ships direct (not through Amazon) makes a sale. They provide the buyer (and Amazon) with a tracking number; however they ship an empty box to an accomplice at another address (not yours) who signs for it. Amazon's records show that the package was delivered so the crook gets paid. To avoid 3rd party seller scams, understand the 3 ways Amazon sells products:

Amazon Direct - products are sold and shipped by Amazon (**SAFE**)
Amazon Fulfillment - items are warehoused and shipped by Amazon (**SAFE**)
Amazon Marketplace - products are sold and shipped directly from 3rd party sellers. (**POTENTIALLY UNSAFE**). Beware these sellers but if you use them understand the risk and always check for a high number of sales and positive ***verified*** feedback.

2 Factor Authentication

The Equifax data breach has dominated the news for weeks and its no wonder. With the information stolen, crooks can gain access to virtually any online accounts (financial, email, social) by answering simple authentication and security questions and then taking control.

To combat this start by updating your account profiles with a new account notification email address (created after the Equifax breach). Because the email wasn't in the Equifax files, crooks won't know about it and prevent alerts from reaching you. Next activate "2 Factor Authentication" or 2FA. This is an extra login verification step using information you know like a password, combined with information only you will have, a single use access code sent to your phone.

With 2FA, whenever a login to your account is attempted, a short lifespan code is sent to you as a text message (SMS) or email and must also be entered to gain access. Even with your login credentials, crooks can't get in without the special code. 2FA can also protect any online account like email (Google 2FA) and cloud accounts (Apple iCloud & ID). Some iPhones even use fingerprint ID technology for greater login protection.

Visit twofactorauth.org to find companies that offer 2FA to their customers and use these links to visit popular bank 2FA set-up pages: Bank of America; Capital One; Chase; Discover; HSBC; USAA ; and Wells Fargo.