Article for December 3, 2014

Did you brave the crowds on Black Friday? Or did you hit the internet on Cyber Monday? There were definitely some crazy deals out there, if you were willing to fight the crowds or muddle through websites! With more and more customers wanting to avoid long lines and crowds in stores, online shopping is very popular! It certainly can be convenient to shop in the comfort of your own home in your favorite chair, but don't get complacent when shopping online, because it's likely that a crook is also in the comfort of their own home, in their favorite chair, just looking for a victim.

The three most common techniques to take advantage of online shoppers is targeting vulnerable computers, creating fraudulent sites and email messages, and intercepting insecure transactions. However, there are some things you can do to stay safe while shopping online. Here are just a few.

Always keep your personal information private and your passwords secure. Never use the same password on more than one site. Create unique, complex passwords for all of your accounts that include a combination of upper and lowercase letters, numbers and special characters.

Use secure websites for purchases. Look for the locked padlock icon at the bottom of the screen or "https" in the URL address. The "s" signifies that the website is secure. The presence of a closed padlock icon in your browser's window tells you the website's owners purchased a digital certificate proving that they own the domain and it is not a fake. A gray padlock guarantees the domain is valid and the connection to it is encrypted. A green padlock indicates not only a secure connection, but that the owners of the domain are who you would expect them to be. For example, XYZ.com is owned by XYZ Company. Clicking (or double-clicking) on a genuine padlock icon will display security information about the site. Note that some fraudulent websites display a non-functioning padlock image meant to fool you.

Shop with companies you know. Be cautious when shopping on sites you haven't used in the past. If you need to order from a website you haven't used before, you might consider using a pre-pay debit/credit card for the purchase, so that you protect your regular credit card, just in case.

Be sure to limit app permissions on mobile apps. Some apps access only the data they need to function, while others mine data that isn't related to the purpose of the app. Don't install apps that require excessive permissions to your personal data. Instead, search for alternative apps that provide the services you want without requiring you to name your next of kin!

Use anti-virus software, a firewall, and anti-spyware software on your computers, cell phones and tablets. Make use of these tools and make sure they are all up to date.

Finally, don't make purchases or log into your bank's website when using public WI-FI. These are breeding grounds for cyber criminals who monitor the networks and capture unencrypted data. We certainly don't want you be a victim! Make use of these suggestions and Be Safe Out There!