Volume #4 - Issue #182
October 19th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Digital Identity Spoofs

Digital Identity spoofs happen when someone uses your identity to create fake social media sites or accounts with other services pretending to be you. (Note that after the Ashley Madison hack, it was found that thousands of people had opened accounts under a friend or colleges name. Many sites ask for an email address, but never verify the email actually belongs to that person.) This can actually be accomplished even though you have very little information on the person you are spoofing, many times a name, address and birthday is all that is needed. (They can even get your photos

by creating screenshots your existing pages or doing a google search for images of you.) Once these accounts are created third parties use someone else's name, photos, or other information, for improper purposes. The imposter may have a growing network of friends on the fake account, which was accessed using the victim's own friends list. To the unsuspecting individual who gets the Friend Request, this account looks like your friend and has the same friends. If you are a Facebook user you may have noticed a recent scam where people were receiving posts that their page had been spoofed.

Why would someone want to proof your identity? There are several possible reasons. They might be using their friend status to data mine your page to learn more about you. They may plan to target your friends with an Emergency Scam, for example, "This is Katherine. I'm in Cancun and I've been mugged and need money to get home." They may be spamming your friends' news-feeds without your knowledge…you've probably seen those where your friend posts "I've lost 18 pounds in two weeks!" By far the most dangerous reason may be either blackmail you or get revenge on you. Scammers may threaten to post damaging information about you if you don't pay them something or do something for them. Or they may go ahead and post this information as revenge.

Tips to prevent Identity Spoofing:

It is difficult to fully guard against identity spoofing, as services such as Facebook and Twitter allow anyone to set up an account in any name. To report a spoofed Facebook page, you need to first have a Facebook account: then go to the spoofed profile, click the button next to "Message" and select "Report/Block." Then click "This profile/timeline is pretending to be someone or is fake" and then "Pretending to be me" and finally "Continue."

To avoid having your own Facebook or Twitter account hacked into, never share your password with anyone and make sure to sign out of each service before you close the tab or window.

Your IP address is most at risk when you are using public Internet hotspots at places such as airports or coffee shops. When using these, it is a good idea to use a Virtual Private Network, which will be explained in an upcoming newsletter.

Thank you for subscribing to our email!