

Cyber Security

We are becoming more and more reliant on computers and the internet with everything from banking and paying bills to shopping and entertainment. With this, I wanted everyone to be aware of some basic tips and information on how to better protect yourself online.

Malware and Viruses

Malicious code, also called malware, and viruses are becoming quite common. The purpose of this type of attack can range from mischief to identity theft. There is nothing that will protect you 100%, but here are some things that you can do to reduce your risks and be more aware:

- Anti-Virus software – Make sure that you are running an Ant-Virus software on your Windows based computer. Microsoft offers a free Anti-Virus program call Microsoft Security Essentials. No matter what AV program you use, make sure it's always up to date to get its maximum protection.
- Anti-Malware software – There is a free program call Malwarebytes Anti-Malware that is available at www.malwarebytes.org for Windows-based computers. This can be used to scan for malicious software. The free version will scan and clean known malicious software.
- Program Updates – Regardless of your Operating System, always keep it up to date with patches. All the major OS providers consistently release updates to plug known holes and issues, make sure you download and install these regularly.
- Mail Attachments – Be cautious of any email that you do not expect. A common way that viruses spread is by a computer becoming infected and automatically emailing the virus to everyone in someone's address book. So, even if you receive an email from someone that you know, if there's a weird attachment or an attachment that you weren't expecting to receive, it could be malicious.
- Websites – Recently a large number of viruses have spread through small websites. These are generally smaller market websites that are not well protected against viruses. Once these get infected, they can infect everyone that visits them. To avoid this, try to stay away from unknown sites while on the internet. Also, if you visit a site and receive a popup message stating that you could be infected, do not click on the scan now link. Close all web browsers without clicking in the window and reboot your computer. Authorizing a scan will install a virus. If you receive a pop up message that is asking you to purchase a virus scanner or removal tool, do not purchase; it's not legitimate.
- Social Networking – Be cautious of shared content on large social networking sites. Currently, facebook.com is the number 1 source for viruses being transmitted. Stay away from content that you do not know or expect.

Phishing

Phishing attacks use email or malicious websites to solicit personal information by posing themselves as a trustworthy source. These attacks can range from an email claiming to be your mail provider and asking for your username and password to update their records to a credit card company claiming that there has been an attempt to hack your account and you need to click a link and provide your Social Security Number. These fraudulent emails spoof the e-mail address. This means that they appear to be from well-known companies or addresses. The from field can be altered to look like it was sent from any e-mail address. Here are a few ways to avoid being a victim:

- Fake contact - Be suspicious of unsolicited phone calls and email messages. If you are in doubt, look up legitimate contact information for that company, and call them back.
- Personal Info - Do not provide personal information over email. Legitimate companies will never ask for your Social Security Number, Credit Card number, or password over an email.
- Fake Links - Pay attention to the URL of a website especially links that are emailed to you. A common attack is someone claiming that your account has been compromised and you should click a link to login or your account will be canceled. But, the link is altered taking you to a malicious website. In a URL, there is a vast difference between www.bankofamerica.com and www.bankof-america.com and bankofamerica.server1-net.com. The domain name should always come right before the suffix, ie. .net, .com, org, .tv etc. In the above examples, only the first link is legitimate. The dash in the second link makes it a different domain. And the third example will take you to the server1-net.com domain not bankofamerica.com. These subtle changes can be used to take advantage of you.
- Unsafe Sites - Make sure you are entering your credit card number on a secured site. Anytime that you are providing sensitive information on the internet, the site should be secured. You can tell by looking at the url at the top. The url should start with https, the s stands for secure, not http. Also, there will be a lock icon either to the right or left of the url.

Passwords

Here are a few tips on making sure the passwords that you use on the Internet are strong.

- Don't use all numbers! A computer can crack a password that is all numbers in less time than it took to read this sentence.
- Don't use password. And, password1 isn't any better.
- Make sure your password can't be found in the dictionary. Common words and names are easily hacked by dictionary attack programs.
- People commonly use a pet's name or child's name as their password. Anyone attempting to crack your password would start with these.
- Don't reuse the same password on every account. If someone steals your password from a small boutique website, then it could be used to access more personal information if the password is the same for your bank or email.

Here's a few simple ways to make your password more secure. Change the password to keep it from a common word. Try to have 8 characters and use a mix of letters, numbers and special characters. An easy example is changing a to @, l to !, e to 3, and o to 0(zero), so instead of using password1, p@ssw0rd! is much more secure and won't be cracked with a dictionary attack.

If you have any questions, please feel free to ask!

