

OCTOBER IS CYBERSECURITY MONTH

SEE YOURSELF IN CYBER



ARTICLE HIGHLIGHTS



1

**LIMIT SOCIAL
MEDIA POSTS**

2

**INTERNET OF THINGS
(IoT)**

3

**CLOUD
SERVICES**

4

**SMART
PHONES**

WEEK 4: WHAT'S YOUR "APP-TITUDE?"

With the exponential rise in technological advancements, our world is becoming more connected than ever before. These connections allow us to have better communications which accelerate how we exchange information and data, in both the personal and business sectors of our lives. In this week's post, we are going to focus on the connected world and how to keep good cyber hygiene:

CONTACT US



304-201-7485



salesgroup@alpha-tech.us



www.alpha-tech.us



Hurricane, WV

TIS THE SEASON, TO BE SECURE ONLINE!



1.) **LIMIT SOCIAL MEDIA POSTS** – Social media allows us to connect with friends and relatives, find groups that share the same hobbies, and provide entertainment more tailored to your interests. These platforms have seen a substantial growth of users and are rapidly continuing to expand, even into virtual reality. It is important to remember that not only can your friends and family see what you are posting, but so can cybercriminals. Social media pages are generally the first result when looking up a name on a search engine. From there, hackers can see your information and use that knowledge to attempt a social engineering attack on you or even try to impersonate you. To stay safe, minimize posting and oversharing your personal life. Additionally, setting social media pages to “private” can limit unwelcome viewers. _

2.) **INTERNET OF THINGS (IOT)** – The Internet of Things (or IoT) is a term for appliances that have access to the internet such as smart watches, thermostats, security systems, TVs, etc. One major flaw of IoT devices is that manufacturers will use the same username and password for each device created. While this makes it more convenient for mass production, it also makes life much easier for attackers. If a hacker is successful at logging in using the default credentials, they would have access to your network and potentially be able to monitor you or cause serious harm. Therefore, is it VERY important that when you receive an IoT device to IMMEDIATELY change the login credentials and update to the latest firmware to ensure you stay protected.

3.) **CLOUD SERVICES** – We hear the term “the cloud” all the time, but do you know what the cloud is? Simply put, the cloud is a server, or servers, that hosts your files or applications so you can access them from any devices. One problem is that if you are able to access your data remotely, then so can a hacker. If an attacker were to get into your cloud account, he or she could steal all of your data and back it up onto their device. To ensure protection, be sure to turn on multi-factor authentication and use strong and unique passwords.

4.) **SMART PHONES** – Since their inception, smartphones have become such an integral part of our everyday lives. Recent polls have suggested that the average user spends 4-5 hours a day on their smart phone! Attackers can use various methods such as sending fraudulent text messages, utilizing malicious applications (even the App Store and Google Play store can fall victim to letting these bad apps on their platforms), and having your data leaked if you allow too many permissions for your applications. Jailbroken devices can be another cause for concern. Jailbreaking is a term for when a smart phone is hacked to remove restrictions that the manufacturer has put into place,

like changing the appearance of icons, downloading an app not in your smart phone store, or other system related functions. While appealing, this can lead to devastating effects due to the number of vulnerabilities that can be exploited by a hacker. To reduce your risk of being victim to an attack, never respond to texts or phone calls you do not recognize, read over what permissions the application is asking for before accepting (your puzzle game doesn't need access to your microphone or camera settings, for example), and avoid jailbreaking your phone.

That wraps up week 4. Tune in next week for our 5th and final installment of our Cybersecurity Awareness Month blog posts where we will be talking about keeping our critical infrastructure secure. Stay safe, everyone!



CRIME HATES SECURITY; WE DON'T.

CALL TODAY FOR YOUR FREE SECURITY ASSESSMENT

304-201-7485 OPT 2