OCTOBER IS CYBERSECURITY MONTH

SEE YOURSELF IN CYBER

alpha TECHNOLOGIES

ARTICLE HIGHLIGHTS

- **TRY TO AVOID PUBLIC WIFI**
- **USE A UNIQUE PASSWORD PER ACCOUNTS**
- **LIMIT YOUR LIFE ONLINE**
- **USE MFA (MULTI-FACTOR AUTH)**

WEEK 1: SIMPLE STEPS FOR ONLINE SAFETY

The month of October is Cybersecurity Awareness Month. For the next 5 weeks Alpha Technologies will be headlining different topics on cybersecurity. This week will be dedicated to staying safe online. The following page contains some tips and tricks that can not only protect yourself, but your organization as well.

CONTACT US

304-201-7485

salesgroup@alpha-tech.us

www.alpha-tech.us

Hurricane, WV

1.) Try to avoid public WiFi: Public Wifi is inherently unsafe and should be used with the utmost caution. The best way to send data is to use your mobile network on your phone. If you are using another device, use your phone as a mobile hotspot to send data through your cellular network. If you must connect to a public Wifi, be sure that the network you are connecting to is not spoofed. Malicious players will commonly broadcast a WiFi signal with the same SSID as the legitimate broadcast, as well as making their broadcast signal stronger, so you are more likely to connect to the spoofed WiFi network. Even if you are connecting to a legitimate broadcast, bad guys can still monitor the public network you are connected to and steal important and sensitive
information. The best way to overcome this is to always use a VPN when connecting to WiFi. This will ensure that your data is encrypted and prevent anyone monitoring the network from interpreting the material.

2.) Use a unique and complex password for each account: Malicious actors are continuously trying to break into servers' databases that contain login credentials. With this information, they will use a technique called "credential stuffing" where all of the stolen usernames and passwords will be tested on a variety of websites and applications. Unique passwords can stop the attackers from breaking into multiple accounts. Additionally, a unique username can be employed to enhance security further. A reputable password management application can be used to securely store login credentials.

3.) Limit your life online: Many people enjoy sharing themselves or their families on social media, such as a birthday, a vacation, or time spent with friends. Unfortunately, this can lead to major security vulnerabilities. Databases containing OSINT (Open-Source Intelligence) have detailed information about individuals such as their full name, date of birth, street address, etc. and are accessible to attackers. Much of this information is gathered simply by having a program scan search engines and social media pages for personal information. This data may seem harmless, but can be invaluable in the wrong hands and can lead to an identity theft vulnerability. To keep good Internet hygiene, do not disclose your sensitive data online and keep posts on social media to a minimum. Another good tip is to not post when you will be out of town or on vacation. This can be a major risk to not only cybersecurity but also your physical security. Posting pictures and sharing experiences of your vacations should wait until you get home.

4.) Use Multi-Factor Authentication (MFA): A great way to ensure an additional layer of security for your accounts is by using multi-factor authentication, or MFA. This can be conveniently set up on your smartphone and can be completed in seconds during a login attempt. Upon logging in with your credentials, a confirmation in the form of text, email, or push notification is generated to confirm identity. Malevolent players will have an even harder time trying to get into your account when you practice hardening of your authentication methods.

Tune in next week where we will discuss how to stay cyber-safe from the break room to the board room and talk about ways to promote best cybersecurity practices at work.