OCTOBER IS CYBERSECURITY MONTH

SEE YOURSELF IN CYBER

alpha TECHNOLOGIES

ARTICLE HIGHLIGHTS

- **WATCH OUT FOR PHISHING ATTEMPTS**
- **VISHING/SMISHING ALSO IN THE MIX**
- **KNOW YOUR DEVICES**
- **ALWAYS LOCK YOUR DEVICE WHEN AWAY FROM IT**

WEEK 2: CYBER FROM THE BREAK ROOM TO THE BOARD ROOM

Welcome back to week two of our five-week series on cybersecurity awareness. This week we will be focusing on how to guard yourself and your organizations sensitive information while at work.

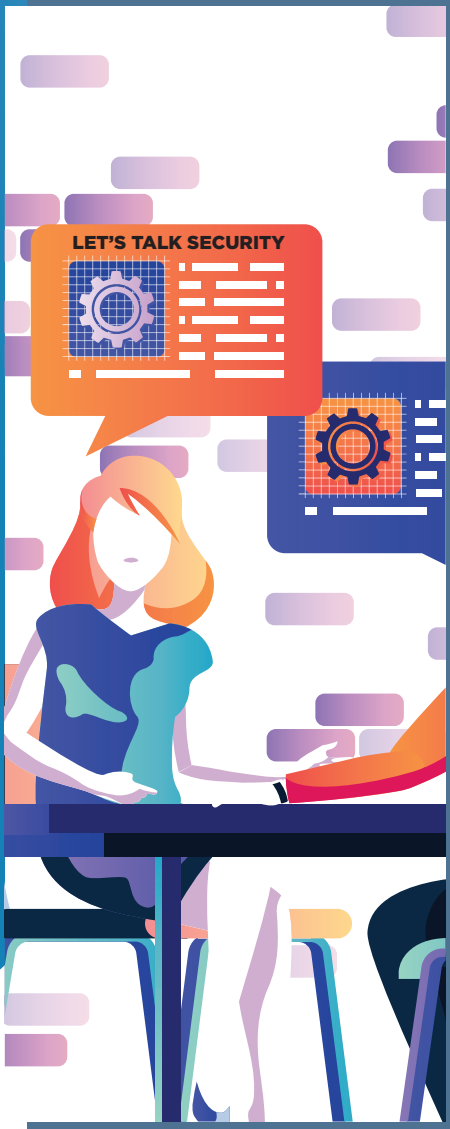
CONTACT US

304-201-7485

salesgroup@alpha-tech.us

www.alpha-tech.us

Hurricane, WV



1.) **WATCH OUT FOR PHISHING ATTEMPTS**: Malicious players know that billions of dollars are spent in cybersecurity each year, and it is becoming more difficult for them to break into systems. Because of this, they are turning their eyes on another resource: You. Attackers will use email to try and convince you to either click a dangerous link, open an attachment containing malware, or disclose sensitive information. To better defend yourself against a phishing attack, always read through emails carefully to ensure the genuine address of the sender as well as looking for typos, grammatical errors, or suspicious attachments. Never click on another URL link in an email without verifying where it goes. Hover over it and see what address shows; if it looks suspicious, report it to your IT department.

2.) **VISHING/SMISHING ALSO IN THE MIX**: Not only are attackers using email to try and steal data, they are also using voice and texting called vishing and smishing, respectively. Attackers will use deceptive social engineering tactics, such as urgency and intimidation, to try and obtain sensitive information from you. To thwart a vishing attempt, always verify who you are speaking with and do not disclose any account or personal identifiable information over the phone. For smishing attempts, never respond to unknown numbers and do not click links from unexpected texts.

3.) **KNOW YOUR DEVICES**: While antimalware applications are great at catching viruses and other harmful software, they cannot detect 100% of bad actors. It is important to pay attention to your devices and how they function with day-to-day operations. Signs of malware can include missing files, new programs, unexpected pop-up windows, or slowing of your device. If you notice any of these signs or other strange activities, they should be reported to the IT department immediately.

4.) **ALWAYS LOCK YOUR DEVICE WHEN AWAY FROM IT**: Just because you are at work does not mean that your guard should be down when stepping away from your device. When leaving your computer, always use the lock feature (Windows Key + L for Windows, Control + Command + Q for Mac) to password protect your device from wandering eyes and bad guys.

Next week we will be discussing growing cyber threats that can affect anyone so be sure to check it out. Stay safe, everyone!