CYBERSECURITY AWARENESS MONTH 2022

PROTECT YOURSELF ONLINE

PHISHING - WHAT IS IT?	WHY SHOULD YOU CARE?
Phishing is when a threat actor poses as a trusted source and sends fraudulent digital messages, such as emails, with the intent of manipulating individuals into revealing personal information and gaining unauthorized access to a system through a download or link.	Phishing attacks are some of the most commonly successful types of attacks. Learning how to recognize fraudulent messages by paying close attention to detail and never clicking on embedded hyperlinks, as well as remembering to report phishing attempts when you are targeted, are the best ways to defeat this kind of cyber attack. Ensure that URLs begin with "https:" when clicking on links. The "s" indicates encryption is enabled to protect users' information. Learn the signs of these types of attacks and think before you click. Check that emails and links are legitimate. Verify all attachments come from a trusted source.
MALWARE - WHAT IS IT?	**WHY SHOULD YOU CARE?**
Malware, short for "malicious software," is software intended to damage, disable or give someone unauthorized access to your computer or other internet-connected device. This includes adware, botnets, ransomware, rootkits, spyware, viruses, worms and numerous others.	Malware can disrupt networks, interrupt business operations or lead a person to malicious sites to scam them for money or harm their reputation.
RANSOMWARE - WHAT IS IT?	**WHY SHOULD YOU CARE?**
Ransomware is a type of malware in which the attacker encrypts the victim's data to make it as inaccessible as possible, often by locking a person completely out of their computer. The hacker then demands a ransom to release or unencrypt that information.	The fees extorted by ransomware can be extreme or prohibitive — not to mention that there is no guarantee that your data will be returned after a ransom is paid! In addition to keeping your software and antivirus programs up to date, regularly back up your system on the cloud or on an external hard drive. That way, you always have a spare copy of the information that is most important to you or your business.
BOTS - WHAT ARE THEY?	**WHY SHOULD YOU CARE?**
Bots can carry out useful functions or be invasive and harmful. Bots are automated with pre-defined tasks that can imitate or replace human user behavior.	Bots can come as malware and gain total control over a computer system. They can scan or obtain contact information, send spam or perform other harmful acts.
SOCIAL ENGINEERING - WHAT IS IT?	**WHY SHOULD YOU CARE?**
Sometimes threat actors do not need computers to gain access to your information. With social engineering, threat actors gather common information about you to trick you into giving unauthorized access to information systems. Social engineering attacks can be quite sophisticated and are not always easy to recognize. This includes attacks such as phishing, swatting and more.	Social engineering attacks do not require sophisticated programming skills to be successful. The information you post on social media and other sharing platforms may make you especially vulnerable to these attacks.

Ready PA
www.Ready.PA.gov