CYBERSECURITY

December 2023

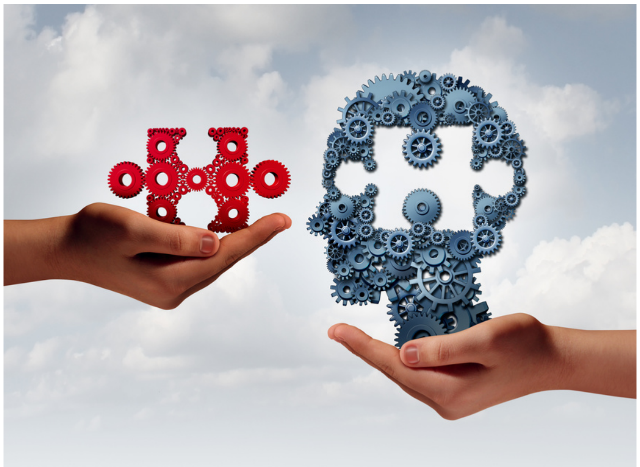
SECURITY NEWS

Department of Information Technology

FBI, DHS WARN OF HEIGHTENED THREAT THROUGH THE HOLIDAYS

Three federal agencies have issued a public safety warning extending through the holiday season. In their statement, they stated the threat of violence, particularly by lone actors is the highest its been since September 11, 2001. In their statement, they did not mention information related to any specific threat or plotting efforts, rather that, since the October 7 attacks in Israel, there has been a heightened calling from terrorist media organizations, to carry out lone wolf attacks. Threats can also be in the form of cyber attacks so remember to follow the best practices for home security. Be vigilant this holiday season and if you see something, say something.

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY



SAT TRAINING COMPLETION

Did you know that security awareness training is mandated by law for all Maryland state employees? (Md. Code, State Fin. & Proc. § 3.5-2A-4). The purpose is to ensure that all state employees are aware of, and in compliance with, the latest policies and best practices on information security. We are currently achieving an 86% completion rate of our quarterly cybersecurity training. Ensure your personal completion rate is 100%!

Did you know?

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering. “Verizon 2023 Data Breach Investigations Report”

Here are some of the top human errors that can cause malware infections

1. Falling for Phishing messages and other Social Engineering attempts

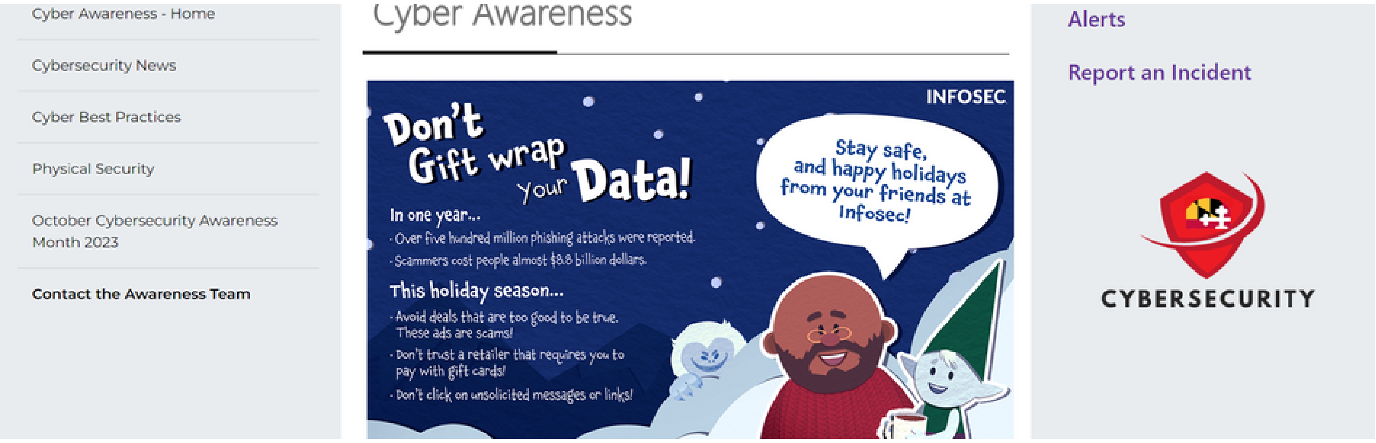
The Department of Information Technology security awareness team repeatedly trains employees and contractors on the threat of phishing because it is that important for you to understand. Whether it is email based, SMS text, phone call, social media, QR codes, or any other means, the threat actor is using psychology, and now artificial intelligence, to create realistic looking messages designed to entice you into clicking on links, attachments or follow guidance that results in malware being installed on systems. Do not take the bait!!

2. External Devices

Whether it is preparing for a presentation or just sharing photos and entertainment on a USB device, external devices that are moved between systems have an increased chance of becoming infected with malware that may be on someone else’s system. Plugging an infected device into a State of Maryland system, could result in state systems becoming infected and that could cause service disruptions or information loss.

3. Web Browsing, plug-ins and Apps, Oh My!

A certain percentage of the internet contains malicious content designed to infect systems. There are malicious domains that attackers set up and try to lure you to, there are domains used as proxies that have a high likelihood of compromise if visited such as browsing for: 1. Adult content, 2. Hacking, 3. Online gambling and free gaming. Be careful what you search for! Also, malware writers like to use browser plug-ins to deliver malware. Consider disabling plug-ins be default and only specifically allow plugins that you know and trust. And always check the apps you install on your phone, read the terms of use, check the feedback on the app and the developer.



Don't Gift wrap your Data!

In one year...

- Over five hundred million phishing attacks were reported.
- Scammers cost people almost $8.8 billion dollars.

This holiday season...

- Avoid deals that are too good to be true. These ads are scams!
- Don't trust a retailer that requires you to pay with gift cards!
- Don't click on unsolicited messages or links!

STAY INFORMED ABOUT THREATS, SCAMS AND BEST PRACTICES BY VISITING OUR NEW SECURITY AWARENESS WEBPAGE!

HOME CYBERSECURITY REMINDERS

1. Educate your family: Knowledge is your first line of defense. Make sure your family members are aware of the existence of cyber threats and the tactics used by scammers like phishing. Stress the importance of skepticism when receiving unexpected phone calls or messages.
2. Update all systems connected to your home wifi: Laptops, mobile devices, tablets, and other devices connected to your home wifi should be updated to reduce system vulnerabilities.
3. Keep social media accounts private: Information that is easy to access can be used by scammers to know more facts about a person or family making their social engineering work much easier.
4. Take Advantage of Call Blocking Tools: The Federal Communications Commission offers a wealth of call-blocking resources for both mobile and landlines.
5. Verify the Caller's Identity: When someone contacts you or a family member asking for personal or financial information, always verify their identity. Ask for a callback number, then look up the official contact information of the organization in question and reach out directly to confirm the request. Remember, the State of Maryland will not reach out proactively to request personal or financial information.
6. Use MULTI-Factor Authentication (MFA): Enable MFA on financial and email accounts to add an extra layer of security. This helps prevent unauthorized access even if a scammer gains access to your credentials.
7. Don't Share Sensitive Information: Remind your family members only to share personal or financial information if they are certain of the requester's identity.
8. Report Suspicious Activity: If you or a family member encounters a suspicious call, report it to the appropriate authorities, such as the Federal Trade Commission (FTC) or the local police.
9. Secure Home Assistants: If you use home assistants like Alexa or Google Home, secure them with strong, unique passwords. Also, disable voice purchasing and limit the information these devices can access.
10. Password Security: Do not write your passwords down anywhere and make sure your passwords are unique so that if one password is compromised, your exposure is limited. Using a password manager can help create long, strong passwords for you and help with not having to remember them.

Always Report Security Incidents, Issues, and Concerns

- Phone: 410-697-9700
- Email: SOC@maryland.gov

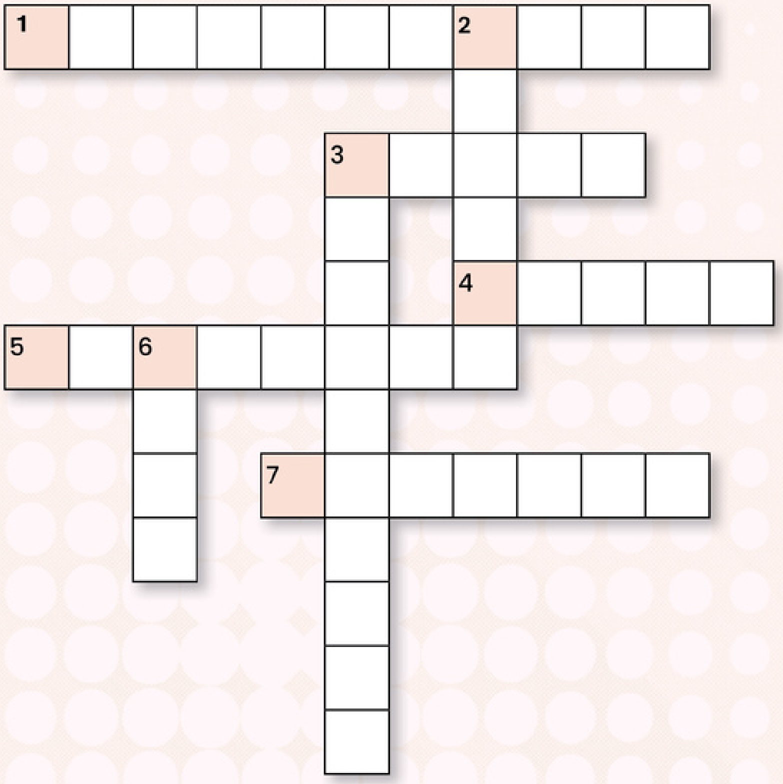
- 24/7 Security Operations Center
- Anti-retaliation policy
- Confidentiality Protection
- Keep Maryland Safe

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

PASSWORD SECURITY

CROSSWORD PUZZLE

HOW TO PLAY: Solve the clues to complete the crossword puzzle. All answers are things related to password security. As you place each word into the puzzle, you'll get more and more hints for the clues that are hardest to solve.



ACROSS

1. Something you are, something you know, or something you have combined are __________ authentication.
3. Shorter, weaker passwords that are closely tied to you on a personal level can be easy for an attacker to ________.
4. As well as, difficult to ________. (see 6 and 7)
5. Avoid using the same password/PIN across _______ accounts, or else you risk all accounts being compromised if any one is.
7. Also _________. (see 6)

.DOWN

2. If you suspect your password is compromised, you should ____ it.
3. Attackers want to ________ your password.
6. You want to make sure your password is ______.

ANSWERS

1. Multifacto **2.** Change **3a.** Crack **3d.** Compromise

4. Guess **5.** Multiple **6.** Long **7.** Complex

CYBERSECURITY HEROES

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY