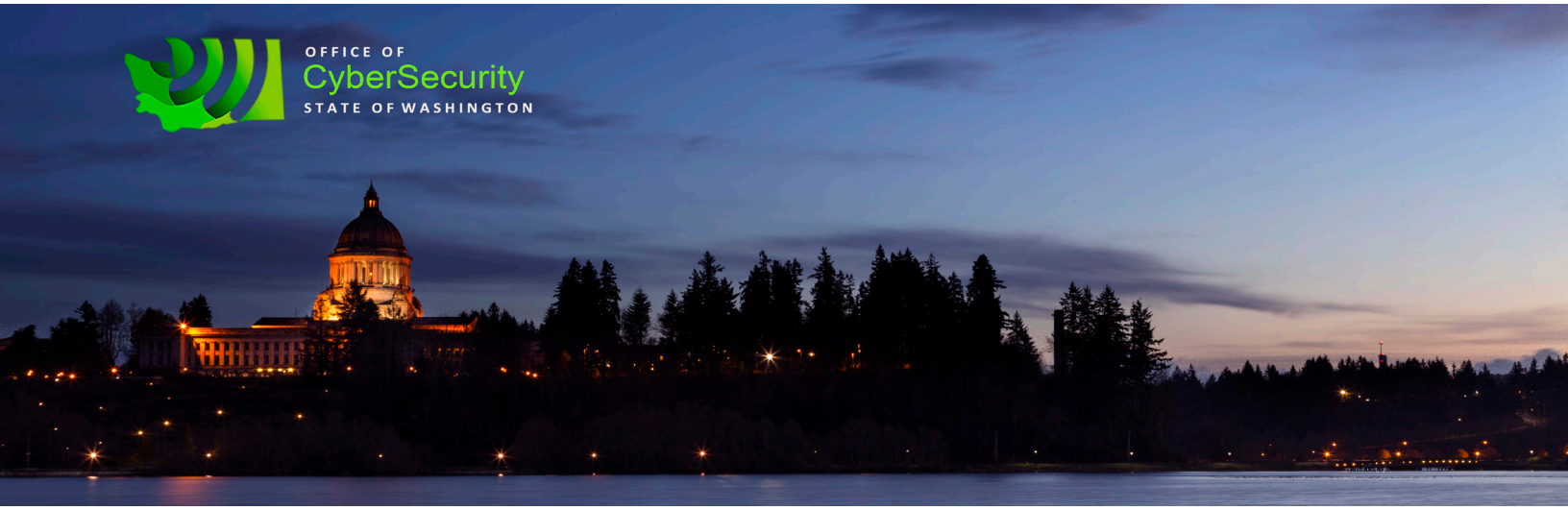

Office of CyberSecurity

2018 Hacktober Cyber Quiz

We had several requests this year for a list of all the Hacktober quiz questions and answers.

Here they are:

Day 1

Q: If you receive an unexpected phone call from someone who says they need remote access to your computer, should you allow them to access your computer?

A: No

Day 2

Q: You are at a coffee shop and would like to check files at work or make a personal banking transaction online. The coffee shop has free WiFi. You should:

A: Never use free WiFi services to conduct business or personal transactions

We realize this question deserved a more detailed answer. The best answer would be never to use the public WiFi because it could allow hackers to access your device. However, if absolutely necessary, you could use your cellphone as a hotspot to provide a more secure internet connection.

Day 3

Security Tip: Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time—no matter how short—lock it up so no one can use it while you're gone.

Day 4

Q: There are three types

of scanning involved in hacking. Which answer below best describes the type of scanning that discovers the presence of known weaknesses on target systems.

A: Vulnerability Scanning

Day 5

Q: How many times should you reuse a password?

A: Never

Day 6

Q: Connecting to a system without a username or password is considered what type of session?

A: Null

Day 7

Security Tip: Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically, and often silently, compromise your computer. If attachments or links in email are unexpected or suspicious for any reason, don't click on it.

Day 8

Q: You are walking into your building and see a USB flash drive on the ground that has your agency's logo on it. You should:

A: Take it to your IT security department so they can access it in a safe environment.

Day 9

Security Tip: Be careful about what you share on social networks. Criminals can easily gain access to a shocking amount of information—where you go to school, where you work,

"Two-step verification is one of the best steps you can take to secure any account. Two-step verification is when you require both a password and code sent to or generated by your mobile device."

when you're on vacation—that could help them gain access to more valuable data.

Day 10

Q: True or False: Hacking went Hollywood in the 1983 movie WarGames which was about a whiz kid who breaks into a Defense Department computer and, at one point, hi-jacks a pay phone by hot-wiring it with a soda can pull-ring.

A: True

Day 11

Q: When updating software on your computer, it is best to obtain the updates from: (Select all that apply)

A: Original vendor's website and your agency's IT Department

Day 12

Security Tip: Two-step verification is one of the best steps you can take to secure any account. Two-step verification is when you require both a password and code sent to or generated by your mobile device. Examples of services that support two-step verification include Gmail, Dropbox and Twitter.

Day 13

Q: True or False: British hacker Gary McKinnon broke into 97 U.S. Navy, Army, Pentagon, and NASA computers in 2001 and 2002.

A: True

Day 14

Security Tip: When you send an email, the message leaves your email provider's server and travels all over the internet. There is no way to know how many servers the message will pass through from the moment you send it, to when the recipient actually receives it. You also don't know who has access to those all those servers. The vulnerability of emails is the main reason why you should never exchange any sensitive information with this method, such as your credit card

information, Social Security number, etc.

Day 15

Q: How often should you expect someone to call or e-mail you to ask for your personal information such as your name, address, birthday, credit card or debit card numbers?

A: Never

Day 16

Q: Why should you enable 2-step verification?

A: If your password is stolen, your account is safe because they don't have access to your second layer of security information.

Day 17

Q: You receive a phone call from someone claiming to be from your bank. They tell you they suspect someone has fraudulently accessed your account, and they need your login credentials to verify that it was or wasn't you. You should:

A: Hang up and report the call to authorities if you have the caller's phone number

Day 18

Security Tip: Learn how to use your mobile device securely. Create strong passwords, use a pass code or biometric information to lock your screen, only install apps from trusted sources.

Day 19

Security Tip: Everyone is susceptible to getting hacked. The bad guys are very persistent and we can all make a mistake. If you believe you have been hacked, never try to fix the situation. Instead, report it right away. If you

"Hackers are more common then you think. It is extremely easy for a novice hacker to access files on your home computer if your WiFi network is not secured. WPA2 is currently the preferred encryption method. Go to cybersecurity.wa.gov for more information."

try to resolve the situation yourself, such as paying an online ransom or deleting the infected files. Not only could you still be hacked but you are most likely causing far more harm than good.

Day 20

Q: True or False: You should monitor your children's use of your computer or create separate logon accounts for them.

A: True

Day 21

Q: True or False: Your home network does not need to be secured with a password.

A: False

Hackers are more common then you think. It is extremely easy for a novice hacker to access files on your home computer if you WiFi network is not secured. WPA2 is currently the preferred encryption method. You find more information on how to protect your home network at cybersecurity.wa.gov.

Day 22

Q: Anti-Virus Scanning Software on your home and work computer performs what function?

A: Prevents, detects and removes malicious software from computers

Day 23

Security Tip: Phishing scams continue to proliferate at alarming rates and are becoming more and more difficult to detect. Be cautious about all communications you receive. Do not click on any links listed in untrusted messages and do not open any attachments contained in suspicious email.

Day 24

Q: True or False: Printed documents containing

personal information should be shredded or disposed of securely.

A: True

Day 25

Security Tip: As tax season comes closer, beware of emails purporting to be from the IRS claiming you have a refund. The IRS does not initiate taxpayer communications through email.

Day 26

Q: What can Malware do?

A: Malware can install applications on your computer that commandeer system resources or spy on user keystrokes, very often running without the user's knowledge. Malware can also considerably slow down computers, break vital system components and render a device inoperable.

Day 27

Security Tip: Pre-approving the videos and pictures your child posts is important. Children posting their face and other personal information to a public audience puts them at risk.

Day 28

Q: Data encryption helps protect files by:

A: Making a file unreadable unless you have a secret key or password that enables you to decrypt it.

Day 29

Q: Reporting malicious activity and files to your IT department is important because: (Check all that apply)

A: Reporting helps prevent wide spread malware in your agency and the state network. IT support can help stop the damage caused by malware on your computer, and also repair your computer.

Day 30

Security Tip: Erasing information or disposal of electronic media (e.g., PCs, CDs, thumb drives, etc.) often leads to a false sense of data security. Be aware of proper methods of sanitizing, destroying, or disposing of media containing sensitive or classified information.

Day 31

Thank you for playing! We would appreciate your feedback on our Hacktober game and suggestions for next year! Please email cybersecurity@ocs.wa.gov.