CYBER BOOTCAMP QUESTIONS

FUNDMENTALS OF RANSOMEWARE QUESTIONS:

1. ***If I only visit trusted websites. Am I still at risk? (*YES)**
   - Ransomware is distributed in different ways, and not just delivered by bad sites.
   - Spammed messages with poisoned attachments is most effective ransomware distribution methods making for a significant portion of attacks annually.
   - Cybercriminals have mastered how to pique users' interest by way of effective social engineering lures to entice them click on a bad link or an attachment in an email.
   - Other methods include compromised software and hacking, while compromised websites, malwertisements and exploit kits are viable sources of ransomware.
2. ***Can I just rename my files and regain access to them after it gets encrypted? (No)***
   - Ransomware uses cryptography to ensure data becomes unusable unless the ransom is paid to obtain decryption key.
3. ***What are bitcoins? Are there other ways to pay? (YES)***
   - Bitcoin is electronic currency which uses peer-to-peer (P2P) networks to track and verify transactions.
   - Its anonymity and the lack of a central authority to control this form of currency makes this the payment method of choice for cybercriminals.
   - Recent ransomware variants have also listed alternative payment options such as iTunes and Amazon gift cards, which are easily monetized.
4. ***Do I really have to pay to regain access to my files and system? Will they decrypt my files after I pay?***
   - Ransomware relies on making users think paying is the only option to regain access to their files, which is why files have been duly decrypted following settlement of payment.
   - Paying should never be the only option authorities recommend victim's not pay.
   - The FBI has identified cases payment was made and no decryption key was provided.
   - Important: Even if the key is provided it will still be difficult to access systems in situations where large portion of a network as impacted.
5. ***Ransomware infections are only for PCs right? Is my smartphone safe? (*NO)**
   - Smartphones are also being targeted.
   - Ransomware has been used to attack Android mobile to devices.
   - The FLocker (short for "Frantic Locker", detected as ANDROIDOS_FLOCKER.A) with over 1,200 variants is an example they ask for iTunes gift cards as payment.
   - FLocker also can infect Android-based smart TVs.
6. ***Can antivirus software remove ransomware from my infected system? (NO)***
   - Specialized Online tools have recently been made available to remove ransomware infections and to decrypt files.
   - Removing ransomware and decrypting files are two different things, files encrypted ransomware will remain unusable even if the malware is removed.
   - Unfortunately, ransomware is constantly updated with stronger encryption algorithms, and existing tools are unlikely to work on every single ransomware variant.
   - Prevention is the key to stop ransomware.
7. ***How can I make my computer ransomware-proof?***
   - Use a multi-layered approach to prevent it from reaching networks and systems and minimize risk to endpoints.

CYBER BOOTCAMP QUESTIONS

- Use protection via email and web gateway solutions the key is know and understand infection techniques

8. **What is the ultimate protection against ransomware?**

- Anti-malware vendors recommend using backup solutions.
- Remember, cybercriminals now are also attacking backup solutions.
- Use caution when selecting backup software.
- Better yet get applications that can detect and provide a robust self-protection functionality in case bad actors try to take down your backup process.

9. **Why is Ransomware so effective?**

- It creates fear and panic in their victims, causing them to click on a link or pay a ransom.
- Ransomware uses intimidating messages to achieve their aim:

10. **What do I do if I believe my system has been infected by Ransomware?**

- Signs your system may have been infected include locking of **y**our web browser or desktop with a message about how to pay to unlock it and/or your file directories contain a "ransom note" file that is usually a **.txt** file
- All files have a new file extension appended to the filenames
    - Examples of Ransomware file extensions: .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc, .good, .LOL!, .OMG!, .RDM, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, .LeChiffre, .keybtc@inbox_com, .0x0, .bleep, .1999, .vault, .HA3, .toxcrypt, .magic, .SUPERCRYPT, .CTBL, .CTB2, .locky or 6-7 length extension consisting of random characters

- **Steps to take:**
    1. Disconnect From Networks
        - Unplug Ethernet cables and disable WiFi or any other network adapters.
        - Put your device in Airplane Mode
        - Turn off Wi-Fi and Bluetooth.
        - This can aid in preventing the spread of the ransomware to shared network resources such as file shares.
    2. Disconnect External Devices
        - USB drives or memory sticks
        - Attached phones or cameras
        - External hard drives.
        - Any other devices
    3. Report the Incident
        - As early and as promptly as possible so damage and cost of recovery can be minimized.