CYBER SECURITY AWARENESS UPDATE 18 – 24 OCTOBER 2021

HIGHLIGHT OF COMMUNICATION AND INFORMATION SYSTEM EVENT

1. As part of the Cyber Security Awareness Month, the National Cyber Security Authority (NCA) will feature special guests from Auburn University to do a presentation that will seek to bring technical innovation and measures to counter cyber attacks directed towards users of mobile phones and palmtops. Personnel are encouraged to join the meetings via zoom using the link https://auburn.zoom.us/j/89660421634 to gain insight to improve the security of their devices.

2. It is estimated that Cyber Fraud makes up 45% of all cybercrime, and in terms of the amount lost to criminals, cyber fraud is the second highest. Therefore, personnel are encouraged to put pragmatic measures to secure their online banking and avoid being victims of cyber-attacks. In view of the above, our department this week will seek to create awareness on Ransomware, a common means cyber attackers employ, making their victims vulnerable.

CYBER THREATS AND VULNERABILITIES

3. Ransomware. Ransomware is extortion software cyber criminals employ to lock your computer and its resources and then demand a ransom before its release. It can take the form of a computer virus. The virus first gains access to your device depending on the type of ransomware; either the entire operating system or individual files are encrypted. A ransom is then demanded from the victim.

4. Ransomware infection. Ransomware infection means that your data has been encrypted or your operating system is being blocked by cybercriminals. These criminals usually demand a ransom in return for decrypting the data. The malware can find its way onto your device in many different ways. The most common routes include infections from malicious websites, unwanted add-ons in downloads and spam**.** Ransomware poses a significant threat to us users and our organization, Ghana Armed Forces in all its forms and variants.

DETECTING RANSOMWARE IN YOUR SYSTEM

5. The following are ways a user can use to detect a ransomware attack:

a. Anti-virus scanner sounds an alarm. If your device has a virus scanner, it can detect ransomware infection early. An unlicensed anti-virus makes you a target to cybercriminals.

b. Check file extension. The standard extension of an image file is ".jpg" and that of the word file is “.doc or .docx”. If this extension has changed to an unfamiliar combination of letters, there may be a ransomware infection.

c. Name change. The malicious program often changes the file name when it encrypts data.

d. Dubious Network Communication. Software interacting with the cybercriminals or with the attacker's server may result in suspicious network communication. Avoid connecting your system to unknown public Wi-Fi.

f. Encrypted Files. A late sign of ransomware activity is that your files cannot be opened.

OPTIONS TO VICTIMS OF RANSOMWARE ATTACK

6. Ransomware is generally divided into two types: locker ransomware and crypto ransomware. A locker ransomware virus locks the entire screen, while crypto ransomware encrypts individual files. Regardless of the type, victims usually have three options:

a. To pay the ransom and hope the cybercriminals decrypt the data.
b. Try to remove the malware or virus using available tools.
c. To reset the computer or device to factory settings.

Serial 6(b) and 6(c) are to be employed by ICT specialists. Therefore personnel are encouraged to contact GHQ(DIT) for the necessary assistance. Since the cybercriminals are computer Developers, personnel are to desist from paying ransom without getting an appropriate specialist for help.

PROTECTION AGAINST RANSOMWARE

7. The following are some measures to prevent your systems from becoming a potential target of ransomware attacks:

a. Never Click on Unsafe Links. Avoid clicking on links in spam messages, an unknown website or unknown WhatsApp links.

b. Avoid Disclosing Personal Information. Do not reply if you receive a call, text message, or email from an untrusted source requesting personal information. Cybercriminals planning a ransomware attack may conduct social engineering, which they then use to tailor phishing messages specifically to you.

c. Do Not Open Suspicious Email Attachments. Ransomware can also find its way to your device through email attachments. To ensure the email is trustworthy, pay close attention to the sender and check that the address is correct.

d. Never Use Unknown USB Sticks. Never connect USB sticks or other storage media to your computer if you do not know the source. Cybercriminals may have infected the storage medium and placed it in a public place to entice somebody into using it.

e. Keep Your Programs and Operating System Up to Date. Regularly updating programs and operating systems helps to protect you from malware.

f. Use Licensed Software. Cracked software in our systems exposes or give traces to cybercriminals to enter into our systems. The attackers create the cracks to leave traces to their server to attack you.

g. Use Only Known Download Sources. To minimize the risk of downloading ransomware, never download software or media files from unknown sites. Visit websites with "**https**" instead of "**http**". A shield or lock symbol in the address bar can also indicate that the page is secure. Download applications from Google Play Store or the Apple App Store instead of a third-party store.

h. Ransomware Protection Software. If you want to minimize the risk of a ransomware attack**,** you should rely on high-quality ransomware protection software. A number of ransomware protection software are available to users, but personnel are advised to contact GHQ(DIT) before they purchase or download any protection software for their systems.