CYBER SECURITY AWARENESS UPDATE

HIGHLIGHT OF COMMUNICATION AND INFORMATION SYSTEM EVENT

1. The National Cyber Security Authority has declared October as Cyber Security Awareness Month. Highlights of activities include Child Online Protection Reporting Portal, Forum on Impact of COVID-19 on Ghana's Digitalisation Agenda, Cyber security Forum with Industry Players. The department, therefore, encourages personnel to patronized the online educational programmes as published on the National Cyber Security website (https://www.cybersecurity.gov.gh/). A few common threats will be highlighted in this update.

2. Facebook goes down with Instagram and WhatsApp. On 4 and 8 Oct 21, Facebook, Instagram, and WhatsApp users experienced difficulties accessing the apps. The global network failure is reportedly due to configurations errors. Many social media users were left distraught. The company, however, denied that any user data was at risk of compromise. In order to provide alternate means of communication in the event of recurrence of such disruptions, the department recommends slack apps.

SOME COMMON CYBER THREATS AND VULNERABILITIES

3. **Social Engineering Attack**. Attackers employs social engineering techniques and phycology in their interactions with individuals, posing as employee, maintenance personnel, customer service personnel etc and deceive the targeted individuals to assume some trustworthiness. Confidential or secret credentials like Bank, email or other account names/numbers, social security numbers, service numbers, PINs, Password breach security or conduct cyber attacks. Attacker can gather information from several sources, over a period. Some preventive measures include the following:

a. Be suspicious of unsolicited phone calls, visitors, or email messages from individuals asking about personnel or other classified personal or corporate information.

b. Do not provide personal or corporate GAF information including internal working structures, network or data infrastructure to unauthorized persons. When in doubt consult your superior or the appropriate department depending on the issues at stake.

c. Do not reveal your personal credentials or financial information in an email and do not respond to email solicitations for such information.

5. **Phishing Attack**. Phishing attackers use emails embedded with malicious codes or websites with links to the malicious codes. An email purported from a fake user but disguise to seem like a credible source, requests some personal information, account credentials, GAF number or other details often providing some financial or other gains as incentive. Clicking on the malicious link often enables the attacker gain access to the victim's device, system or computer and then harvest the required classified information required which is then frequently misused. The attackers frequently take advantage of current events and specific issues such as disasters, epidemics/health scares, economic or financial concerns or similar too good to be true stories. Some of the common indicators of phishing attack include the following:

a. **Suspicious Sender's Address.** The sender's address may imitate a legitimate institution, corporate or individual's address. Cybercriminals often use email addresses that closely resemble reputable company.

b. **Generic Greetings and Signature.** Generic greetings such as "Dear Valued Customer" or "Sir/Ma'am" are often used without contact information in the signature block. A trusted organization will typically address you by name and provide their contact information.

c. **Spoofed Hyperlinks and Websites.** The malicious links are often spoofed and If one hovers the cursor over that link provided it frequently different from the one indicated in the body of the email. Such spoofed links often also do not match the text that appears when hovering over them.

d. **Spelling and Layout**. Other indicators or observations that give out phishing email include bad grammar, poor sentence structure, misspellings, and inconsistent formatting.

e. **Suspicious Attachments.** An unsolicited email requesting a user to download or open an attachment is one common delivery mechanism for malware. Ccybercriminals use a false sense of urgency or importance, huge financial gain, or familiar person/institution to help persuade the user to download or open the malicious attachment without examination.

AVOID BEING A VICTIM

6. Pay attention to details and check the following:

a. Uniform Resource Locator (URL) of a website address and look out for those beginning with "https" (indication that such sites are secure). The "http" are not secured and must not be used especially for financial transactions.

b. Look for a closed padlock icon which is an indication that one’s information will be encrypted or secured during the transmission to the destination.

c. If you are unsure whether an email request is legitimate or not, try verifying it by contacting the source establishment directly.

d. Do not use the contact information provided on a website connected to the request; instead, check previous statements for contact information.

e. Install and maintain licensed anti-virus software, firewalls, and email filters to reduce some of this traffic coming into your system.

h. Take advantage of any anti-phishing features (embedded in your browser or contact specialist in GHQ(DIT)) offered by your email client and web browser.

i. Enforce or enable multi-factor authentication (MFA) or at least two-factor authentication that is available in the application, system or device.

WHAT TO DO IF YOU SUSPECT YOU ARE FALLEN VICTIM

7. Depending on the circumstance or issue at stake, you should take actions to mitigate or recover if you suspect that you have fallen victim to a cyber attack (social engineering, phishing or hacking).

a. If you suspect that you might have revealed sensitive information about your GAF, report immediately to network administrators at GHQ(DIT) or Duty Officer Defence Intelligence as appropriate for necessary help.

b. If you suspect that your financial account may have been compromised, contact your financial institution immediately and close any accounts that may have been compromised.

c. Immediately change passwords or PINs that might have been revealed. Do not used the same password for multiple accounts, and ensure your passwords are not less than 8 characters. Ensure your passwords are strong (The password should contain alphabets, numerals and special keys).

d. Check and monitor for other signs of identity theft or breach of personal accounts.