CYBER SECURITY AWARENESS UPDATE **UPDATE NO. 3**

25 – 31 OCTOBER 2021

HIGHLIGHT OF COMMUNICATION AND INFORMATION SYSTEM EVENT

1. As part of the Ghana National Cyber Security Awareness Month (NCSAM 2021), the Cyber Security Authority (CSA) organized a virtual workshop on the "Impact of the Cybersecurity Act 2020 on CERT (Computer Emergency Response Team)". The workshop re-echoed the need for GAF personnel to be circumspect in their activities in cyberspace because the Act has spelt out the needed punishment for any cyber offence.

2. Multiples studies have revealed that users continue to ignore secure login best practices. This weak password policy is one of the top five cyber threats hackers use to exploit potential victims. It represents the most significant cyber threat Ghana Armed Forces Information Systems will face, especially in the new normal. Given the above, our department this week will seek to create awareness on Passwords, a common means cyber attackers employ, making their victims vulnerable.

CYBER THREATS AND VULNERABILITIES

3. Password Security. Passwords provide the first line of defense against unauthorized access to personal devices and GAF information systems. Poor password security has been identified as a critical vulnerability to GAF personnel devices and computer systems. The GAF is embarking on a digitalization agenda that will move certain key services and operations online. Therefore, it is essential for all GAF personnel, both military and civilian employees, to be aware of the threat implications on their devices and GAF systems by using weak and exposed password credentials. The more robust and secure passwords are, the more protected GAF personnel devices and systems are from cyber threats and attacks.

WRONG PASSWORD FORMAT

4. The following are ways a user's password becomes vulnerable to cybercriminals:

a. Use publicly accessible information about individuals: name, service number, date of birth, telephone number, dependents names, nicknames, and any other publicly accessed details.

b. Use of common phrases, famous quotations, and song lyrics.

c. Use the same password across multiple accounts such as email, online banking, social media, etc.

d. Avoid short passwords usually less than 8 characters and without numbers, special characters (@ # $ % - *?) and uppercase.

e. Avoid using predictable password generation strategies such as adding a letter(s) or character(s) to existing passwords to create new passwords.

a. A compromised password should never be used again.

RECOMMENDED PASSWORD MANAGEMENT PRACTICE

5. Personnel are advised to follow the following password management practices:

a. Attempt memorized password, never shared, written down or recorded along with corresponding account information or usernames on sticky pads or sent through email or any online means without encryption.

b. Enter your password without anyone looking.

c. Always sign out once you leave your browser or systems and never leave your handheld devices unattended.

d. Avoid entering passwords when connected to unsecured Wi-Fi connections, as hackers can intercept your passwords and data over unsecured connections.

e. When you suspect your password is compromised, change your password and contact GHQ(DIT) or a specialist for help.

f. Always select “never” when your Internet browser asks for your permission to remember your passwords.

g. Always use Multi-Factor Authentication (MFA) when available to reduce the impact of a compromised password.

h. Be wary of pranks and suspicious calls and emails requesting certain vital information from you, as hackers can use such details to reset your account.

i. Avoid clicking on promotional offers and click to win deals that are too good to be true. Always verify from the company’s website before you sign up for such offers.

j. Create a separate email account to use for logging in to online accounts or making purchases etc.

k. When in doubt of how vulnerable your password is to hackers, visit the site (https://www.security.org) and enter your password to check the duration of your password to a hacker to hack.