United States Coast Guard
U.S. Department of Homeland Security

10 OCT 2024
FM: CHDIRAUX
TO: ALAUX
ALAUX 033/24

Subj: NATIONAL CYBERSECURITY AWARENESS MONTH

---

1. October 2024 is the twenty-first annual National Cybersecurity Awareness Month. Since 2004, the President of the United States and Congress have declared October to be National Cybersecurity Awareness Month, helping individuals and organizations protect themselves online as threats to technology and confidential data become more commonplace. All Auxiliarists are strongly encouraged to remain vigilant against cybersecurity threats and to actively apply strong countermeasures in their personal and Auxiliary activities.

2. According to the Identity Theft Resource Center, there have been more than one billion reported victims of cyberattacks in the United States during the first half of 2024 as well as a 490% increase of data breach victims compared to 2023. The Coast Guard noted an 80% increase in ransomware attacks impacting the maritime environment in its latest annual Cyber Trends Report. In 2024, the average data breach cost grew to $4.88 million per attack - a 10% increase and the highest ever according to a report released by IBM. The Cybersecurity and Infrastructure Security Agency estimates that 90% of cyberattacks are initiated as a result of phishing emails emphasizing the importance of promoting good cybersecurity practices even down to the end user.

3. The Cybersecurity Awareness Month campaign theme - "Secure Our World" - focuses on our increasingly connected world where more of our sensitive information is online. Online convenience comes with risks. Each of us has a part to play in adopting cybersecurity habits and improved online safety behaviors to keep ourselves and others safe whether at work, home, school, or in the Auxiliary. The following four practices are highly effective methods to achieve a strong cybersecurity posture:

- Use Strong Passwords - Create long, random, unique passwords with a password manager for safer accounts.

- Enable Multifactor Authentication - You need more than a password to be safe. Turn on multifactor authentication to protect online accounts.

- Update Software - Fix security risks by installing updates and turning on automatic updates.

- Recognize and Report Phishing - Recognize phishing attempts, resist the temptation to click on untrusted links or attachments, and delete unwanted messages. Guidance for reporting cybersecurity incidents including Auxiliary related phishing attempts can be found at https://wow.uscgaux.info/content.php?unit=Y-DEPT&category=submit-incident-report.

4. More details on these as well as other cybersecurity guidance and best practices are available in the latest U.S. Coast Guard Auxiliary Cybersecurity Awareness presentation. The presentation and other guides are available on the Cybersecurity Directorate webpage. (https://wow.uscgaux.info/content.php?unit=y-dept).

5. Internet release is authorized.

For many reasons including the value of keeping communication lines clear and open as well as facilitating access to training and educational tools, all Auxiliarists are urged to have their own email address and to keep it updated in AUXDATA.

---

*All ALAUX's are posted on the Chief Director of Auxiliary website located at: CHDIRAUX ALAUX

If you have a question regarding this ALAUX, please seek resolution within your Chain of Leadership and Management (COLM) including up to your servicing District Director of Auxiliary (DIRAUX). If your question still cannot be resolved after that, then please email CGAUX@uscg.mil.