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

04 OCT 2023
FM: CHDIRAUX
TO: ALAUX
ALAUX 037/23

Subj: NATIONAL CYBERSECURITY AWARENESS MONTH

---

1. October 2023 is the twentieth 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. In 2022, the average data breach cost grew to $4.45 million per attack. That is a 15% jump over the past three years. Further, it takes an average of 277 days to identify and contain a data breach according to a report released by IBM. The Anti-Phishing Working Group, an international coalition of counter-cybercrime responders, reported that it observed 3 million phishing attacks in the third quarter of 2022, the most ever tracked in a three-month period. Cyber-attacks on supply chains continued to grow, with a projection by Gartner, a technological research and consulting firm, indicating that 45% of organizations worldwide will have experienced cyber-attacks on their supply chains by 2025, a three-fold increase from 2021. Threats like these are prevalent and dangerous, and it is critical that we all take the necessary steps to prevent an attack.

3. This year's 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
- Enable Multi-Factor Authentication
- Keep Your Software Updated
- Recognize and Report Phishing

4. More details on these as well as other cybersecurity guidance and best practices are available in the updated U.S. Coast Guard Auxiliary Cybersecurity Awareness presentation. To view the presentation and other guides, click here.

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 II.

---

*All ALAUX's are posted on the Chief Director of Auxiliary web site 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.