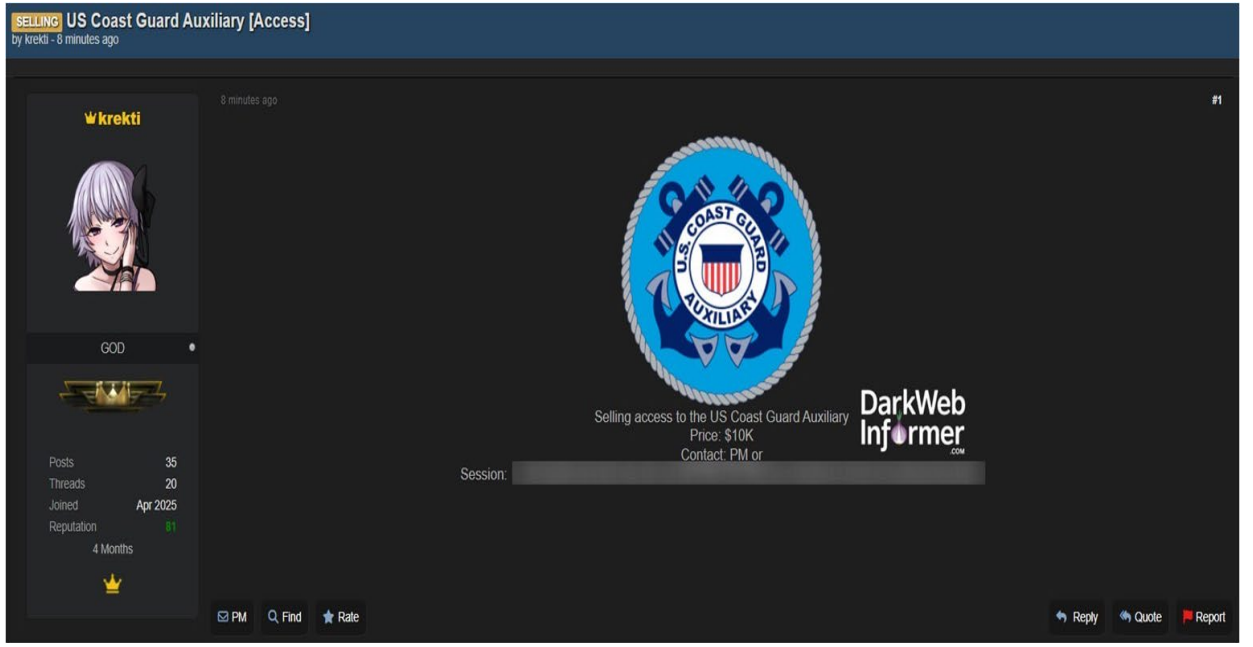
U.S. Coast Guard Auxiliary Cybersecurity Awareness

October 2025

U.S Coast Guard Auxiliary

Why Does Cybersecurity Matter?

- ***About 31% of maritime professionals reported at least one cyberattack in the year leading up to October 2024, up from 17% over the previous five years.***
- ***Attacks on our systems or our members' personal accounts can disrupt operations and damage the credibility of the Coast Guard Auxiliary as a trusted partner in national security.***
- ***What happens to one member can ripple out to affect their family, their finances, and the Auxiliary community***



Cybersecurity Hygiene

1. General Best Practices

2. Passwords & Identity Management

3. Phishing

4. Social Media

5. Responsible AI Use

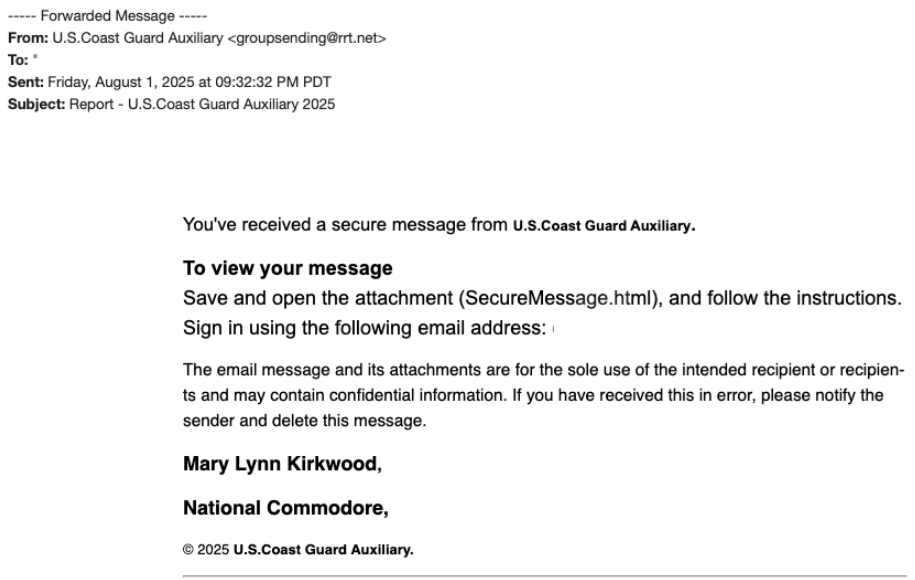
General Best Practices

- Use strong, unique passwords
- Utilize multi-factor authentication (MFA) wherever it is available
- Keep systems & software updated especially with security patches
- Turn on anti-virus & firewall protection
- Back-up your files securely to cloud-based data storage platforms
- Be cautious of pop-ups & alerts (always be on guard)

Passwords & Identity Management

- Use **multi-factor authentication (MFA)** whenever possible
- Create **strong, unique passwords**
- Use a **trusted password manager**
- Don’t **reuse or share passwords**
- Take a **risk-based approach by prioritizing your user accounts** with access to your most critical information (e.g., bank accounts)

Phishing



----- Forwarded Message -----
From: U.S.Coast Guard Auxiliary <groupsending@rrt.net>
To: *
Sent: Friday, August 1, 2025 at 09:32:32 PM PDT
Subject: Report - U.S.Coast Guard Auxiliary 2025

You've received a secure message from **U.S.Coast Guard Auxiliary.**

To view your message
Save and open the attachment (SecureMessage.html), and follow the instructions.
Sign in using the following email address:

The email message and its attachments are for the sole use of the intended recipient or recipients and may contain confidential information. If you have received this in error, please notify the sender and delete this message.

Mary Lynn Kirkwood,

National Commodore,

© 2025 **U.S.Coast Guard Auxiliary.**

- Be skeptical of unexpected emails or pop-ups
- Don’t click suspicious links or attachments
- Verify requests through trusted contacts (different communication channel)
- Use spam filters, antivirus, and anti-phishing tools

Social Media

- Think before you post — it lives forever
- Lock down privacy settings
- Be cautious with friend requests, apps & links
- Limit location sharing & personal info

Responsible AI Use

- Be cautious with personal data
  - Don’t feed sensitive info (SSNs, financials, work details) into AI tools
- Verify results
  - AI can hallucinate, or make things up
  - Always fact-check before sharing or acting
- Avoid harmful use (new regulations are and will continue to come into adoption)
  - Don’t use AI for deepfakes, disinformation, or impersonation
- Think before you share AI content
  - Treat AI outputs like any other online content
  - Check for accuracy, context, and source

Remember that Data Security is critical to AI Security –
don’t forget security foundations

Conclusion

The security of the Coast Guard and Coast Guard Auxiliary information systems and data that we are entrusted with is all our responsibility. By securing and protecting our own personal IT resources that connect to USCG and CGAUX systems, we help to reduce the overall attack surface.

Reporting cybersecurity incidents (such as the loss of sensitive data) and suspected phishing attempts to the respective emails below. If you See Something or Suffer Something, make sure you Say Something so it can be Secured.

Cybersecurity Incidents: cyber-incidents@cgauxnet.us

Phishing: phishing@cgauxnet.us

Key Takeaways (Reference Sheet)

Top 5 Cyber Hygiene Reminders

- Use multi-factor authentication (MFA) on every account where possible.
- Always use a complex and unique password for all user accounts.
- Apply all updates and security patches on your devices (e.g., update your iPhone iOS).
- Always take a risk-based approach and question unusual/urgent messages.
- Securely back-up your important data to a cloud-based data storage platform (e.g., Apple iCloud).

Top Signs of a Phishing Attempt

"If it feels off, then it is a sign of a potential phishing attempt." Always be on guard.

- An urgent email with threatening language is a common sign of a phishing attempt.
- Check for red flags in the email such as a slightly different sender email address, embedded links don't match the domain, and unexpected file attachments. These are all signs.
- Another common sign is the use of email itself as an unusual channel to ask for sensitive information such as a bank account password.

Key Points of Notification

Please contact the respective email accounts below for the following situations:

- For cybersecurity related incidents (e.g., loss of sensitive data such as through sending to the wrong email) - please notify cyber-incidents@cgauxnet.us
- For emails that are deemed to be suspicious - don't open/click or analyze yourself; please notify at phishing@cgauxnet.us for instructions to 'forward as attachment'.