# Cybersecurity

March 2026

Cliff Neve, DIR-Y

# Why are we here

You've received an secure message from **Mary Kirkwood** of **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: [redacted]

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 Kirkwood,**

**National Commodore,**

© 2026 **U.S. Coast Guard Auxiliary**.

*February 2026 spear-phishing attack impersonating National Commodore Mary Kirkwood to harvest Auxiliarist credentials.*

# What the nefarious actor does

Email impersonates leadership

↓

User opens attachment

↓

Fake login page appears

↓

User enters email + password

↓

User receives error message (even if password correct)

↓

Attacker logs in as the user (hopefully MFA stops it)

↓

Attacker goes to Walmart.com, Amazon.com, etc, etc, etc and attempts credentials harvested

***Actors aren't HACKING into accounts. They are harvesting credentials and LOGGING in. As you.***

# Best case

User identified that it was a phishing email and reported it to phishing@cgauxnet.us

one of my members reported receiving this and it looks sketchy to both of us.

A scam email below using a Canada email.

Scott

**User recognized the phishing email and reported it.**

# Bad Case

Hello,

I am an AUP graduate, and I clicked the phishing link from Mr. Brady T Marking this morning. Will I be ok? I clicked it while I was on my phone, and not my computer. I have entered no passwords or information into the link, and clicked away right away.

I deleted the email, so I am unable to forward it.

**User clicked link but did not provide credentials, and reported it.**

# Worse Case

Unfortunately I fell for this one last week.

I entered my Auxiliarist Member Number and my password the Auxiliary websites. I use it nowhere else.

I have attempted to change my password but have been unsuccessful. I would appreciate your help to do so.

**User clicked link and provided credentials…once…and reported it.**

# Really Awful Case

Sir, or ma'am,

I think I went through every one of my passwords for that email! What do I do now?

I feel so stupid. Why would the national Commodore send me an email?

**User clicked link and provided credentials…then more credentials…then more credentials….**

# Scenario #2: Gift Card Fraud
## (Classic Social Engineering Attack)

**From:** James E [redacted] Thomas <[redacted]
**Date:** January 2, 2026 at 07:09:42 EST
**To:** [redacted].uscgaux@gmail.com
**Subject: New Beginning**

Hello [redacted]

I hope you're doing well. I'm currently out of town and wanted to reach out regarding an assistance.

I need you to get me some gift vouchers (cards) for a charitable cause on behalf of the District 5SR East District Southern Region, to support veterans receiving hospice care especially during this season of sharing.

I'll refund you the cost as soon as I settle in or I can send you a check to get them if you are low in funds.

Could you please let me know if you're able to assist with this request?

Thank you for considering this

James Everette Thomas
District Commodore (DCO)
District 5SR
East District

# Scenario #2: Gift Card Fraud

Thank you [redacted] It is an individual charity but I will be presenting it on behalf of  District 5SR East District Southern Region

I need you to kindly purchase 7pcs x $100 of either Apple, eBay or Target or Amazon gift cards which totals $700.

You can purchase them at any of  Kohl's,CVS, Kwik, Macy's, Walmart, or Walgreen's Stores. Due to the time frame of the pledge, I will be glad if you get them early enough today.

E-mail me once you buy them. Let me know if a check will be fine for refund. Thank you.

# Urgency

I can't stay glued to the computer waiting all day ******.

If you are busy, let me know when you would be able to do it.

I am in Limbo.. Please reply whenever you see my messages.

----- Forwarded Message -----
**From:** "James Everette Thomas" <odebb8805@gmail.com>
**To:** "jason_wilmoth@yahoo.com" <jason_wilmoth@yahoo.com>
**Sent:** Sat, Jan 3, 2026 at 11:50
**Subject:** Did you receive my messages?
Hello Jason,

Can you please acknowledge my messages?

James Everette Thomas

I will be watching over my e-mail. Let me know if you have get home .
Thank you.

Hello *****,  Do you have the cards now? Let me know what is happening.

When are you sending pictures of the codes of the real cards and not the pack?

# Did it work?

----- Forwarded Message -----

**From:** "[redacted]@yahoo.com>

**To:** "[redacted]@gmail.com>

**Sent:** Fri, Jan 2, 2026 at 20:38

**Subject:** Re: New Beginnings

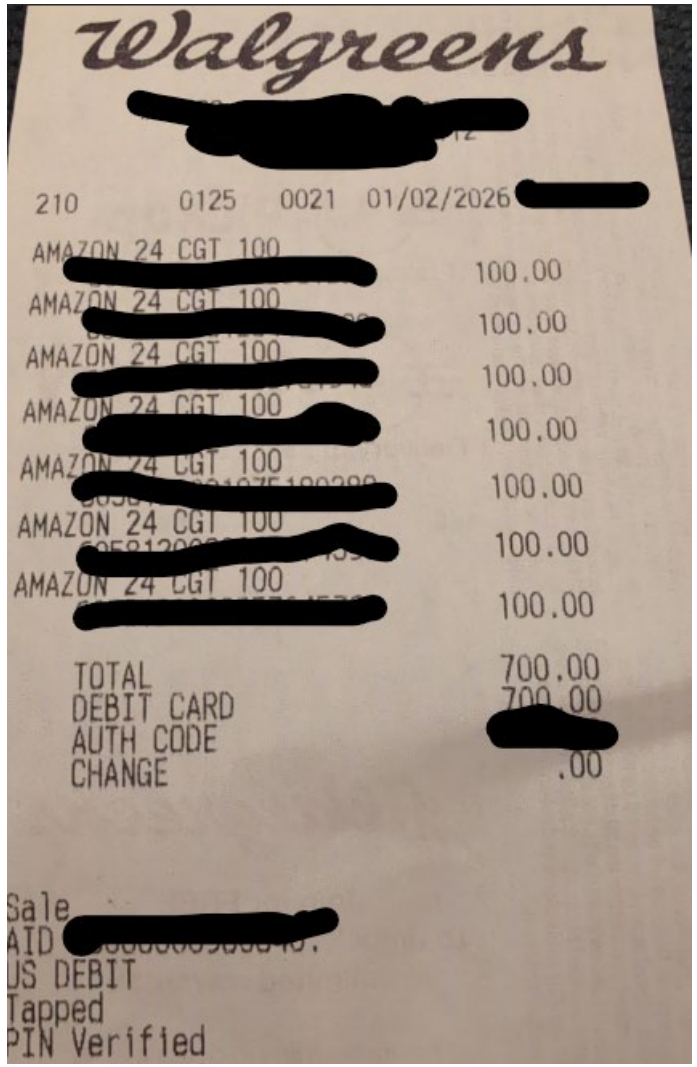
DCO

I got the cards tonight.

$700.00

[redacted]

Mail to: [redacted]



# What do these have in common

**1. Trust**
The message appears to come from someone you know.

**2. Urgency**
The attacker pushes you to act quickly.

**3. Authority**
The message appears to come from leadership.

***These attacks are <u>not</u> about hacking computers. They are about <u>manipulating people.</u>***

# Why the Auxiliary is a Target

## 1. Trust-Based Culture

- Volunteer organizations are built on **trust and cooperation**.
- Attackers exploit that.
- Members are more likely to:
- respond to leadership
- help fellow members
- act quickly when asked

## 2. Distributed Workforce

- Auxiliarists operate from:
- personal computers
- personal email accounts
- home networks
- This creates a **large and decentralized attack surface**.

# Why the Auxiliary is a Target (continued)

## 3. Limited Security Controls

- Unlike large enterprises:
  - devices are not centrally managed
  - cybersecurity training is inconsistent
  - technical protections are limited
- So **awareness becomes the primary defense**.

## 4. Access to Valuable Information

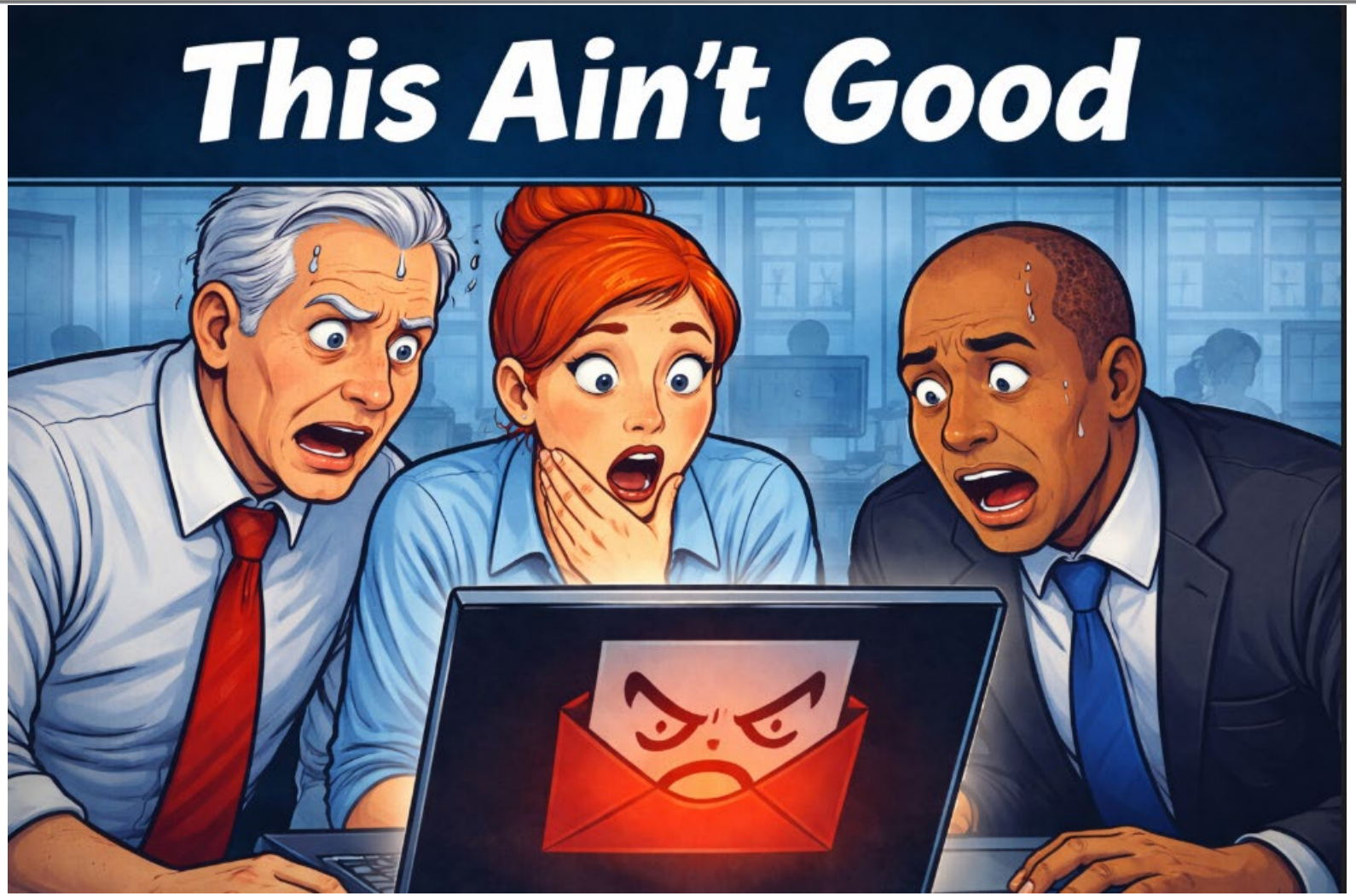
- Auxiliarists interact with:
  - Coast Guard personnel
  - maritime industry partners
  - federal systems and data
- Compromising one account can create credibility and access.

# The Challenge

- Auxiliarists use their own unmanaged computers for Aux business
- Most use their own personal email accounts
  - Email administered by Gmail, Yahoo, AOL(!), Compuserv(!), Earthlink(!)
- I cannot help with technical controls or prevent emails from being sent from or to these accounts

**Auxiliarists, even those who use cgauxnet.us email, aren't required to take any kind of cybersecurity awareness training**

# What Does That Mean For DIR-Y?



# If I Can Only Impart One Thing…..

**When contacted (email, text, or phone):**

- **Do NOT share any information**
- **Verify independently — YOU initiate the contact**

**Trust nothing. Verify everything.**

# General Best Practices

- Never provide sensitive information on an incoming call or email
- 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

**Skepticism is your best defense.  Slow down!**

# 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'.

# Questions

**Cliff Neve**
Director, Cybersecurity Directorate (DIR-Y)
U.S. Coast Guard Auxiliary

# Backup Slides

# 4 Easy Ways to Stay Safe Online

**Use Strong Passwords and a Password Manager**

**Turn on Multifactor Authentication**

**Recognize and Report Phishing Attacks**

**Update Your Software**

# Use Strong Passwords

## CREATE STRONG PASSWORDS:

- **Long**
  - At least 16 characters
- **Unique**
  - NEVER reuse passwords
- **Random**
  - Upper- and lower-case letters
  - Numbers
  - Special characters
  - Spaces
  - Consider pass-phrases

# Use a Password Manager

## WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy
- It won't fall for a phishing website, even if you do!

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks.

# Turn on Multifactor Authentication

## WHAT IS IT?

- **A code sent to your phone or email**
- **An authenticator app**
- **A security key**
- **Biometrics**
  - Fingerprint
  - Facial recognition

# Turn on Multifactor Authentication

## WHERE SHOULD YOU USE IT?

- **Email**
- **Accounts with financial information**
  Ex: Online store
- **Accounts with personal information**
  Ex: Social media

# Recognize and Report Phishing

## PHISHING RED FLAGS:

- **A tone that's urgent or makes you scared**
  *Ex: "Click this link immediately or your account will be closed"*
- **Sender email address doesn't match the company it's coming from**
  *Ex: Amazon.com vs. Amaz0n.com*
- **Unexpected communications such as an email you weren't expecting**
- **Requests to send personal info**
  *Legitimate organizations don't ask for personal information through email or an unexpected call.*
- **Misspelled words, bad grammar and odd URLs can still be a sign of phishing.**
  *Be aware that AI will make spotting these more challenging. Be diligent.*

# Recognize and Report Phishing

## WHAT TO DO IF YOU SPOT A PHISH

### Do NOT

- Don't click any links you don’t trust. Delete the email/text.
- Don't click any attachments you were not expecting or recognize.
- Don't send personal info online or share over the phone.

### Do

- Verify that the communication is real and contact sender directly through known phone numbers or emails.
- Report it to your IT department or email/phone provider.
- Use email filters
  - Many email services have filters that can help prevent many phishing messages from ever reaching your employees’ mailboxes.
- DELETE IT.

# Update Your Software

## WHY?

- Updates ensure your devices and apps are protected from the latest threats
- Don't click "remind me later", it could leave you vulnerable to cyber threats
- Automatic updates are the easiest way to stay secure

# Update Your Software

## WHERE TO FIND AVAILABLE UPDATES

- Check for notifications to your phone or computer
- Look in your phone, browser or app settings
- Check the upper corner of your browser for any alerts