L2

Auxiliary Leadership Link

To: All Auxiliarists
Dated: 4 February 2025

Dear Members,

The Cybersecurity Directorate (Y) has received reports of fraudulent spear phishing emails impersonating the National Commodore, COMO Mary Kirkwood. These emails claim to have a "secure message" attached. If the attachment is opened, it directs recipients to a website requesting their email address and password. This is a scam designed to steal your login credentials.

What You Should Do:

- If you entered your credentials: Change your password immediately to secure your account. While you should not use the same password for multiple systems, you should now change the password for ANY other account you have that uses the same password. We request that you notify the Y Directorate Incident Response Team at cyber-incidents@cgauxnet.us if this occurred.

- If you received the email but did not interact with it: Delete the email. Do not open or forward the attachment. No additional reporting is necessary.

For more guidance on phishing scams, cybersecurity best practices, and reporting cyber incidents, visit the Cybersecurity (Y) Directorate page:
https://wow.uscgaux.info/content.php?unit=Y-DEPT&category=publications

Stay Safe Online:

- Be cautious of unexpected emails, even if they appear to come from known contacts.

- Never click on links or attachments unless you verify their legitimacy.

- If an email looks suspicious, delete it immediately.

Thank you for your attention to this matter.

Very respectfully,

Cliff Neve, DIR-Y