U.S. Coast Guard Auxiliary
Computer Software & Systems Directorate
Cybersecurity Division

CYBERSECURITY AWARENESS BULLETIN

PROTECTING YOUR USER IDS & PASSWORDS

Serial:	CI-AWA-2020-194-01
Date:	12 JULY 2020

Scope
This bulletin provides best practices for protecting user credentials.

Summary
As an Auxiliarist you have access to sites and data that need to be protected. If you protect your ID and use a strong password, you will be doing your part to keep yourself and the Auxiliary safe. Supplementing your credentials with multi-factor authentication further strengthens your cybersecurity posture.

Details
Compromised user IDs or passwords can provide others with unauthorized access to Coast Guard and/or Auxiliary information systems. Compromised IDs and passwords can also be used to facilitate criminal or unauthorized activity. To prevent this from happening, it is highly recommended to follow best practices:

- Use passwords at least 14 characters in length (minimum length required for AUXLMS)
- Passwords should contain a combination of lower and upper-case letters, numbers, and special characters (e.g., @, #, ?, *, &, =)
- Change passwords at least every 4 months or immediately if you suspect your password is compromised
- Use pass "phrases," if you can, that include the criteria listed above. For example, 1GiantPurpleGorilla!
- Use different passwords on different systems and accounts
- Use a password manager to help you create and store unique complex passwords for all the sites you access
- Do not use a password that can be easily guessed, including personal information such as names, pets, birthdays, hobbies, or dates
- Do not use words that can be found in any dictionary of any language.
- Do not use your social security number as a password
- Do not share, reveal, post, or write down your User ID, passwords or PINs
- Do not include your password in an automated login process

Two Factor Authentication (TFA) or Multifactor Authentication (MFA)

There are three general types of authentication:

- Something you know - This includes user IDs, passwords, or pre-established answers to questions
- Something you have - This could be a small physical token such as a smart card, a special key fob, a special USB drive, or your smartphone
- Something you are - This includes biometric identification such as scanning of eyes (retinas or irises) or fingerprints, other facial recognition, or voice recognition

Two factor authentication refers to using two of these methods. Multifactor refers to using two or three of these as added levels of protection. Using TFA and MFA keeps your accounts safe in the event a hacker gets your login credentials. TFA and MFA come in different forms such as smart device apps or special codes that are sent to you via text message. Some websites require TFA or MFA. AUXDATA II is an example of a website that requires TFA. Even if a website does not require TFA, you should take advantage of it if the capability is offered to protect yourself and your data. Many email platforms, banking and investment sites, as well as shopping sites offer TFA. To see if a site offers TFA, visit https://twofactorauth.org/.

Protecting the Auxiliary in the Cyber Domain