CYBER SECURITY AWARENESS

The DO's and DO NOT's of Cyber Security

DO
Use the Ship's computer only for Ship Related work.
Make sure that the anti-virus protection on your computer is always up to date.
Ensure that back-up of all data is taking place at scheduled intervals.
Prior using any data storage device (e.g. USB, Hard Drive etc.), ensure that you do a Virus scan.
Be smart when browsing / surfing the internet. Always access website which have a valid security certificate. Check if the web address is beginning with "https://"
Ensure that you log out from your accounts prior leaving the workstation and that you keep the computer locked when not in use.
Always use strong passwords. Use passwords that include a mix of Upper & Lower case letters, including special characters.
Change your password frequently.
Report any suspicious activity to your Ship Security Officer.

DON'T
DO NOT Use unauthorized Data Storage devices like USB's, Hard Drives etc.
DO NOT Install or Download any unauthorized software on the Ship's computer.
DO NOT Use the same password for all login's or applications.
DO NOT Keep passwords which will be simple to crack for example your wife's name, your birthday etc.
DO NOT Enter your password in front of anyone.
DO NOT Share confidential data over public network.
DO NOT Click on any suspicious link or any link which is from an unknown source.
DO NOT Open an email or attachment from an unknown or suspicious sender.
DO NOT Fall prey to clicking a link for a Malicious Web Site that load Malware into your computer.
DO NOT Reply to emails which promise you lots of money or free gifts.
DO NOT Use the auto sign in feature or the save passwords feature in your web browser.
DO NOT Fall prey to Phishing. Phishing is the practice of sending emails which appear to be from a reputable company or organization in order to induce an individual into revealing confidential information.