Protect Yourself from Cyber Attacks

94% of Malware is delivered via email.

80% of incidents are initiated via phishing messages.

What can you do to keep from becoming a victim of a cyber attack?

1) Be Suspicious

- Be wary of unsolicited demands, requests, or offers.
- Be on the lookout for phishing (email)/Vishing (voice)/Smishing (SMS/text) attempts.
- Don't take the bait – attackers will use a sense or urgency, scarcity, emergency, or fear to get victims to act quickly and unsafely.
- Research any apps or tools before downloading them to a device and download them only from authorized distributors

2) Scrutinize

- Examine the sender's email address or contact information for sneaky variations.
- Examine all URLs/links for variations from actual websites.
- Do not click on links provided in unsolicited texts/email messages, even if they seem to come from a legitimate source. Always go to the company's website to log into your accounts.
- Take a close look at the name and file type of any attachments; do not open any attachment unless you are expecting the file and have verified the sender's email.

3) Protect Your Data

- Set-up and use multifactor authentication for any accounts where it is available; if attackers steal login credentials, they may not be able to use them.
- Only log-in to official sites/call official numbers; avoid following links.
- Back-up your data regularly and secure the backup by disconnecting it from your computer and networks, store in a secure location.
- Do not overshare on social media; use privacy settings and encourage family to limit information they share about you.

4) Protect Your Devices and Accounts

- Regularly patch and update software on all devices.
- Install, regularly update, and periodically run an anti-virus program.
- Set-up long and complex passwords, use different passwords for different accesses, and change them regularly.
- Consider using a password manager to keep track of all your passwords.

SUNSTATES SECURITY

Sources:
-NCIS
-CSO
-Verizon