CERT Monthly Safety Tip

Some Tips To Be Safer Online

- Install latest release of software to get most up-to-date security patches. Turn on automatic updates.
- Consider using highly-rated utility and security software for extra safety.
- Use (different) strong passwords and/or a password manager
- Add 2-factor (TFA) or multi-factor (MFA) authentication to protect financial accounts or online shopping services
- Use Virtual Private Network (VPN) software on unprotected public WiFi systems
- Delete suspicious emails or texts, especially those seeking your urgent attention, or money, or personal account information.
- Check the sender's URL address for typos, foreign country codes or anything that seems odd. Don't click on any links or attachments.
- If an email appears to be legitimate, always go to the sender's official website to access your account rather than click on any included link.
- Be as anonymous as is practical on social media. Don't share personal or family information.
- Schedule automatic backups of important information to a cloud-based service and/or to an external USB or hard drive

For info on Del Webb CERT, contact CERTDelWebbLWR@gmail.com