Use multi-factor authentication when possible

If possible use a password and receive a text code accessing online accounts.

www.lockdownyourlogin.com

Don't overshare online and use privacy settings on social media

Don't display personal information on a social media account and update privacy settings periodically. Disable geo-tagging on social media accounts.

Create long passwords using phrases, numbers and symbols

Don't use a combination password that is obvious such as the name of your pet or birthdate.



Don't fall victim to a phishing scam. If it looks suspicious, don't risk opening an email or clicking on a link.

Remember to update your security software

Updated security software will prevent attacks from manipulating software vulnerabilities.



Do not leave cell phones, laptops, tablets etc. unattended in a public place to prevent theft. Always keep devices locked when not in use.



Secure your home wifi network

Always change the username and password to something you have created and not a factory default.

NATIONAL CYBERSECURITY ALUARENESS MONTH