October 2021

#BeCyberSmart

Cybersecurity Awareness Month

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1 Keep your devices and software up to date.	2 Do not use the same passwords across multiple accounts.
3 Back up your data to prevent data loss.	4 Consider using a phrase to create a complex password.	5 Utilize multi-factor authentication when it is available.	6 Examine each email closely for signs of phishing.	7 Think twice before clicking links or advertisements.	8 Configure the security settings on your IoT devices. Do not use default passwords.	9 Do not leave mobile devices unattended.
10 Turn on auto-update when available.	11 Spoofed emails are phishing emails that appear to come from a known sender.	12 Read emails carefully. Phishing emails may be alarming or sound "too good to be true".	13 Do not share secure information via email unless it is encrypted.	14 Research before downloading software or apps to determine their legitimacy.	15 Verify that the person calling you is who they say they are.	16 If an unverified caller asks for sensitive information, disconnect and call the company back at a known, published number.
17 Delete unused software and apps to reduce your attack surface.	18 Require a password on web meetings so only those invited can attend.	19 Do not use easily researched answers to security questions such as a pet's name.	20 Do not interact with text messages, calls or emails from unfamiliar sources.	21 Regularly scan your devices with anti-virus software.	22 Report any suspicious emails, texts or calls to protect colleagues from falling victim.	23 Limit access to your social media to only those you know.
24 Limit the personal details you share online.	25 Keep track of your online accounts. Delete those that are no longer in use.	26 Verify the legitimacy of sensitive requests, even if it appears to come from someone in your organization.	27 Protect your mobile devices with strong authentication methods.	28 Secure your workspace and devices before stepping away for any length of time.	29 Do not connect unknown devices to your mobile device or computer.	30 Keep physical data safe. Do not leave it unsecured.
31 If you suspect one of your accounts is compromised, change all of your passwords.						