31 DAYS OF CYBERSECURITY AWARENESS

CYBERSECURITY AWARENESS MONTH 2022 | STAYING SAFE ONLINE

Password Security

Never share your password with anyone

Password Security

Never store a password where it could be seen or accessed by another person

Password Security

Passwords should be at least 16 characters long

Password Security

Create complex passwords that use symbols and upper and lower case letters

Password Security

Never use personal information such as names or dates as passwords

Password Security

Use sentences and phrases rather than singular words for passwords

Password Security

Use a different password for every account

Password Security

Activate multi-factor authentication (MFA) on all accounts

Online Scams/ Phishing

Double check the senders email address for spelling errors

Online Scams/ Phishing

Hover over links before clicking on them to see where they are sending you

Online Scams/ Phishing

If it seems too good to be true - it probably is

Online Scams/ Phishing

If you are told that something must be done urgently or ASAP, be skeptical

Online Scams/ Phishing

Phishing attacks can imitate friends or family in attempts to trick you

Online Scams/ Phishing

Always be skeptical of claims of "missing payments"

Online Scams/ Phishing

When shopping online always double check the URL to be sure you're on the real website

Online Scams/ Phishing

Note when an email has a generic greeting and doesn't state your name

Staying Secure in Public

Never connect to unsecure public Wi-Fi networks

Staying Secure in Public

Do not log into private accounts in public

Staying Secure in Public

Consider using a VPN app for data encryption while in a public setting

Staying Secure in Public

On your mobile device, opt to use your data if you don't have an available secure network

Staying Secure in Public

Never view your private financial records in public

Staying Secure in Public

Always remember to sign out of personal accounts after using a public device

Staying Secure in Public

Make sure your devices are not set to automatically connect to nearby Wi-Fi

Staying Secure in Public

Look for "https" on a sites URL to make sure it is encrypted

Best Practices

Move away from session-based zero-knowledge security strategies

Best Practices

Find a security solution that focuses on protecting your data, since that is what hackers are after.

Best Practices

Use technology that verifies each endpoint connection

Best Practices

Look for data security technology that is FIPS 140-3 validated

Best Practices

Search for technology that will require no change to your user experience

Best Practices

Use data security that prevents SIM swapping and cloning attacks

MTE Technology

Implement MTE Technology into your system to prevent bad actors from stealing your data.

eclypses®

www.eclypses.com