Cybersecurity Best Practices

YOU are the first line of defense in protecting your personal information.

DO

Use complex passwords

- At least eight characters long.
- At least one uppercase letter, one lowercase letter, one number and one symbol.

Update regularly

Updates are pushed to fix vulnerabilities that hackers **WILL** exploit.

Back up your files

Back up your files at least weekly on an external hard drive or cloud. This protects you against ransomware and other threats.

Check website URLs

- Make sure the websites you visit start with **“https://”**.
- **"http://"** is not guaranteed to be secure.

Disable Bluetooth

- Disable your Bluetooth when not in use.
- Your device can be hacked and your private info can be stolen via Bluetooth.

DON'T

Mix personal and state devices

DO NOT use your personal device for official means or state device for personal means.

Open suspicious emails

- Avoid opening suspicious emails, and links/attachments that come with them.
- If you have a bad feeling ask the HelpDesk.

Use public networks

- Home, work network, your phone's Hotspot = **Private.**
- Hotel, restaurant, coffee shop, church WiFi, etc. = **Public.**

Trust every USB drive

- Treat USB drives as if they are infected with malware when bought.
- Run a virus scan of the USB drive when you first plug it into a device.

OKLAHOMA

OMES Cyber Command