

31 DAYS OF CYBERSECURITY:



1. Register your organization to become an Oklahoma Champion.
2. Lock your phone with a PIN or enable biometric security.
3. Update your devices to the latest software.
4. Enable multifactor authentication.
5. Back up your files to an external drive or on a secure cloud.
6. Test your backup and make sure you can restore your files.
7. Check if your email has been part of a data breach.
8. Find an example of a phishing email and analyze it.
9. Check your credit report for signs of identity theft.
10. Change the default password of your home router.
11. Create a passphrase for your home Wi-Fi.
12. Uninstall unused apps from your devices.
13. Set up automatic software updates.
14. Run an antivirus or security scan.
15. Use a password manager to store your credentials.
16. Review your app permissions and remove excessive access.
17. Submit a cybersecurity meme to OK-ISAC's meme contest!
18. Learn about a new ransomware, what it is and how to avoid it.
19. Review your social media privacy settings.
20. Talk to a friend or family member about online safety tips.
21. Check your accounts for suspicious login activity.
22. Attend the OK-ISAC Symposium at InnoTech Oklahoma!
23. Create a recovery plan for key accounts and lost/stolen devices.
24. Clean up your email inbox. Report any suspicious senders.
25. Review privacy settings on your smart home devices.
26. Use a privacy-focused search engine for a day.
27. Update all account passwords.
28. Research a current cybersecurity threat.
29. Delete unused online accounts.
30. Change a weak password to something complex and unique.
31. Celebrate your progress and make a plan to keep these cybersecurity habits going!



OKLAHOMA
OMES OK-ISAC