



CYBERSECURITY TIPS



Strong Passwords and MFA

Use strong, unique passwords. Consider using a password manager to store and generate passwords securely. Enable MFA (multi-factor authentication) on all your important accounts. MFA adds a second layer of protection.



Updates and Backups

Keep your software up to date. Install updates regularly. Back up your data consistently. Have recent copies of important files stored in two places like an external drive and the cloud. Test that you can restore from the backup.



Verify

Don't click on links or open attachments from unknown or suspicious sources. Verify the sender by checking the email address, phone number, or business. When in doubt, go to the website directly instead of following the link.



Use Secure Wi-Fi

Avoid using public Wi-Fi for sensitive tasks such as banking or shopping. If you must use public Wi-Fi, use a VPN (Virtual Private Network) for added protection. At home, make sure your Wi-Fi has a strong password.



Think Before You Share

Don't overshare personal information like birthdays, location, or vacation plans on social media. People can use this info to guess passwords or scam you. Make sure to review your privacy settings on your accounts.

Resources:

- cisa.gov
- ftc.gov
- cyberhouserock.info