URCYBERSECURITY

EDUCATE. SECURE. THRIVE

KNOW THE LINGO!

CYBERSECURITY

/ˈsībərsəˌkyo͝orədē/ **noun**

The practice of protecting your devices, DATA (Bold), and online activities from hackers, viruses, and other digital threats.

Use Strong, Unique Passwords:

Why? Weak or reused passwords make it easy for hackers to access your accounts.

Tip: Create 12-16 character complex passwords using a mix of letters, numbers, symbols, or passphrases. 'wFGWg)n3CEA4'

Bonus: Use a password manager to keep track of them securely.

Keep Your Software Up to Date:

Why? Software updates often include security patches to protect against new threats.

Tip: Turn on automatic updates for your devices and apps.

Example: Regular updates help fix vulnerabilities that hackers might exploit.

Enable Multi-Factor Authentication (MFA):

Why? MFA adds an extra layer of security beyond just a password.

Tip: Always enable MFA for your important accounts (banking, email, social media).

Example: MFA might require a code sent to your phone after you enter your password.

Use a VPN (Virtual Private Network):

Why? A VPN encrypts your internet connection, protecting your data from hackers.

Tip: Always use a VPN when connected to public Wi-Fi networks (cafes, airports).

Example: A VPN makes it harder for cybercriminals to intercept your data while browsing.

urcybersecurity.com

Backup Your Data Regularly:

Why? Cyberattacks like ransomware can lock your files, and having a backup helps you recover.

Tip: Use cloud storage or external drives to back up important files.

Bonus: Schedule automatic backups to save time and reduce risk.

Protect Your Devices with Antivirus Software:

Why? Antivirus software helps detect and remove malicious programs before they can harm your system.

Tip: Install antivirus software and run regular scans on your devices.

Example: Good antivirus software can spot harmful malware before it infects your device.

Secure Your Wi-Fi Network:

Why? Unsecured Wi-Fi can allow strangers to access your personal information.

Tip: Set a strong, unique password for your Wi-Fi and enable encryption (WPA3).

Bonus: Turn off your router's admin access from the internet for extra protection.

Educate Yourself on Common Cyber Threats:

Why? Awareness is the first step to staying safe online.

Tip: Stay informed about the latest cybersecurity threats and trends.

Example: Familiarize yourself with terms like phishing, malware, and ransomware to recognize potential dangers.

Think Before You Share Personal Information:

Why? Oversharing on social media can lead to identity theft or social engineering attacks.

Tip: Avoid sharing too much personal information online, especially publicly.

Bonus: Regularly check your social media privacy settings.