Good Habits for Staying Cyber Secure

Cybersecurity is not just the responsibility of IT departments—it's a shared responsibility that starts with individual behavior. Practicing consistent, smart security habits can significantly reduce risk and help protect both personal and organizational data from cyber threats. The goal is to build a “security-first mindset” where secure choices become second nature.

1. Use Strong, Unique Passwords

- Avoid common passwords and reuse across accounts.
- Use long passphrases (e.g. “Summer@River_2025!”).
- Consider using a **password manager** to generate and store credentials securely.
- According to **NordPass (2024)**, 64% of users still reuse passwords, making them vulnerable to credential stuffing attacks.

2. Enable Multi-Factor Authentication (MFA)

- MFA adds an extra layer of protection beyond your password.
- Microsoft (2023) states that MFA can block **99.9% of account takeover attempts**.
- Apply MFA wherever possible—especially for email, banking, and cloud services.

3. Think Before You Click

- Be cautious of unsolicited emails or messages asking for sensitive information.
- **Phishing accounts for 36% of breaches** (Verizon, 2023)—hover over links before clicking and verify senders.
- Report suspicious emails to IT/security teams instead of ignoring them.

4. Keep Software Up to Date

- Always install system and software updates promptly.
- Unpatched vulnerabilities accounted for **60% of cyber compromises** in 2024 (BankInfoSecurity, 2024).
- Enable auto-updates on all devices, browsers, and apps.

5. Lock Devices and Use Encryption

- Lock computers and mobile devices when not in use.
- Use encrypted services and VPNs when handling sensitive data, especially on public Wi-Fi.
- Data encryption helps protect information in case devices are lost or stolen.

6. Avoid Public Wi-Fi for Sensitive Tasks

- Public networks are often unsecure and vulnerable to man-in-the-middle attacks.
- Use a trusted VPN when accessing company systems or entering passwords on public networks.

7. Back Up Important Data

- Use automatic cloud or offline backups for critical files.
- Regular backups can help you recover from ransomware attacks, accidental deletions, or device failures.

8. Be Cautious with Personal Devices (BYOD)

- Ensure personal devices meet company security standards if used for work.
- Install security software and avoid mixing personal and business use on the same device.

9. Stay Informed About Current Threats

- Cyber threats evolve constantly. Follow trusted cybersecurity sources and complete regular training.
- Employees who receive regular cybersecurity training are **60% less likely** to fall victim to attacks (SANS Institute, 2024).

10. Report Incidents Promptly

- Even minor mistakes—like clicking a suspicious link—should be reported.
- Early reporting helps security teams respond quickly and contain threats before they escalate.

The Bottom Line

Cybersecurity is everyone's job. By developing and maintaining strong security habits, individuals can become the first line of defense against cyberattacks. Good habits aren’t about fear—they’re about empowerment: giving people the knowledge and tools to protect themselves and their organizations every day.