AUK Cyber - Top 18 Cyber Safety Tips

Practical cybersecurity guidance for employees, students, business owners, and remote workers.

1. Use strong, unique passwords

Create passwords with at least 12-16 characters. Avoid reusing the same password across email, banking, work, and social accounts.

2. Enable multi-factor authentication

Turn on MFA for email, cloud storage, banking, admin portals, and social media. Authenticator apps are safer than SMS when available.

3. Think before clicking links

Check sender address, spelling, urgency language, and unexpected attachments. When in doubt, visit the official website directly instead of clicking.

4. Keep software updated

Apply updates for Windows, browsers, phones, plugins, routers, and business applications to close known security weaknesses.

5. Back up important data

Maintain offline or cloud backups for key documents. Test restoration periodically so backups work during ransomware or device failure.

6. Secure your Wi-Fi network

Use WPA2/WPA3 encryption, change default router passwords, and separate guest Wi-Fi from business or personal devices.

7. Avoid public Wi-Fi for sensitive work

Use a trusted VPN or mobile hotspot for banking, business email, admin panels, or file transfers when outside your trusted network.

8. Lock devices when unattended

Use screen locks, PINs, biometrics, and automatic timeout. Never leave laptops or phones unlocked in public or shared spaces.

9. Limit admin privileges

Use standard user accounts for daily work. Reserve administrator accounts only for tasks that require elevated permissions.

AUK Cyber - Top 18 Cyber Safety Tips

Practical cybersecurity guidance for employees, students, business owners, and remote workers.

10. Verify payment or bank detail changes

Confirm invoice, payroll, or banking changes using a known phone number or separate communication channel before processing.

11. Protect customer and business data

Store sensitive information only where approved. Avoid sharing confidential files through personal email or unapproved apps.

12. Watch for social engineering

Attackers may impersonate executives, vendors, delivery teams, banks, or IT support. Verify unusual requests before acting.

13. Use trusted downloads only

Install apps from official websites or app stores. Avoid cracked software, unknown browser extensions, and random download links.

14. Monitor accounts regularly

Review account activity, sign-in alerts, bank statements, and admin logs. Report suspicious activity quickly.

15. Encrypt sensitive devices and files

Use device encryption and secure file sharing for confidential documents, laptops, removable drives, and backups.

16. Create an incident response plan

Know whom to contact, how to isolate affected devices, and how to preserve evidence during a suspected cyber incident.

17. Train users continuously

Run awareness sessions, phishing simulations, and role-based security training. People are a key line of defense.

18. Review security posture often

Schedule regular vulnerability assessments, penetration testing, cloud configuration reviews, and policy updates.