complus

Cyber Awareness
Checklist

Your IT Defences Before 2026

MANAGE. PROTECT. ASSURE.

www.complus-it.com

info@complus-it.com

Strengthen
Passwords and Authentication

Use unique, complex passwords for every service:

Use a passphrase of at least three different random words and aim for 16 characters or more; if a system enforces a minimum, do not go below eight characters and avoid mandating composition rules like forced symbols or mixed case, block common or breached passwords such as 123456 or password, avoid personal information, and enable MFA on important services

Adopt a password manager:

Password managers create and store strong credentials so you don't have to remember them all. Avoid letting your browser save passwords; if a device is lost, saved credentials can be exposed.

Enable multi-factor authentication (MFA) :

MFA adds a second verification step (e.g., one-time codes, biometrics) and significantly reduces the impact of compromised passwords. Use MFA for business-critical systems and consider physical security keys for administrative accounts.

© 2025 Complus IT. All rights reserved.

Keep software and devices up to date

Configure automatic updates for operating systems, applications and firmware:

Enable automatic updates so systems receive security patches promptly; centrally manage and schedule updates across servers, laptops, routers and firewalls, and verify compliance through periodic patch audits.

Download software from trusted sources:

Install apps only from official app stores or the vendors own site, not via ads or third-party mirrors; ignore update prompts in browser pop-ups or unsolicited emails and update through the app or system settings instead.

Invest in reputable security software:

Antivirus suites act as a last line of defence and can block malware, phishing and ransomware. Don't wait until after an infection to deploy antivirus; prevention is cheaper than remediation.

© 2025 Complus IT. All rights reserved.

Secure
data and maintain backups

Encrypt sensitive data at rest and in transit:

Classify critical information and apply strong encryption to files, databases and network traffic. Pair encryption with data-loss prevention (DLP) tools that monitor data movement and block unauthorised exfiltration.

Limit access on a need-to-know basis:

Implement the principle of least privilege and minimize the number of administrative accounts. Network segmentation creates “safe zones” that isolate sensitive data from the rest of the network.

Backup critical workloads regularly:

Categorize data by importance and back up essential systems frequently so they can be restored after ransomware or hardware failures. Use secure, encrypted cloud backups and test recovery procedures. Follow clear data-retention policies to avoid storing unnecessary information that could be stolen. Automatic cloud backup tools make this process easy for small teams.

© 2025 Complus IT. All rights reserved.

Defend against phishing and social-engineering

Teach staff how to spot phishing cues:

Phishing emails often contain urgent requests, suspicious domains, poor grammar or generic greetings. Legitimate organisations don't ask you to verify credentials or payment details via email.

Handle emails cautiously:

Avoid opening attachments or clicking links from unknown senders. Disable automatic email previews to prevent malicious content from loading automatically.

Deploy email security tools:

Use email encryption and threat-scanning gateways to block malicious attachments. Regularly train employees to report suspicious messages through an established escalation process.

© 2025 Complus IT. All rights reserved.

Secure networks and remote work

Avoid public Wi-Fi or use a trusted VPN:

Public networks are often poorly secured and can allow attackers to intercept data. If working remotely, connect through a reliable VPN so traffic is encrypted and anonymised.

Secure your business and home Wi-Fi:

Use WPA3 or at least WPA2 encryption, change default router passwords and disable Wi-Fi Protected Setup (WPS). Provide guest networks for visitors and isolate them from internal resources.

Implement remote-access policies:

Require all remote devices to connect via VPN or secure access software and block access from insecure public Wi-Fi. Automate delivery of security patches and antivirus updates to remote endpoints, maintain an IP allowlist and revoke access promptly if a device is lost.

Be cautious with location and proximity services:

Turn off Bluetooth, NFC and location services on mobile devices when they are not needed because these features can be exploited.

© 2025 Complus IT. All rights reserved.

Educate and empower your team

Run ongoing security awareness training:

Training should cover phishing recognition, safe browsing, social-media hygiene, password management and the proper use of company systems. Encourage employees to think critically before sharing personal or business information online.

Explain the reasons behind security controls:

Staff are more likely to follow policies when they understand why multi-factor authentication exists and how to use password managers. Store security policies in a central location and make them easy to access.

Promote a reporting culture:

Encourage employees to report suspected phishing, lost devices or unusual activity immediately. Provide clear channels for reporting and follow up with supportive feedback.

© 2025 Complus IT. All rights reserved.

Manage
third-party and supply-chain risks

Assess suppliers and partners carefully:

Before granting access, make sure third parties have strong security practices and are willing to adopt your access policies.

Use vendor identity-and-access management (IAM) tools:

Treat external accounts like internal users: add them to centralized IAM systems, limit privileges and monitor their activity. Require formal approval for all third-party access requests.

Retain oversight:

Document who has access to what and regularly review permissions. Third-party integrations can open back doors; restricting their privileges reduces the blast radius if a vendor is compromised.

© 2025 Complus IT. All rights reserved.

Establish an incident response and resilience plan

Prepare for the worst:

A robust incident response plan should outline steps for threat identification and containment, protection of critical data, eradication of malware, restoration of normal operations and post-incident review.

Run drills and table-top exercises:

Practise responding to ransomware, data breaches and DDoS attacks so every employee knows their role. Balance thoroughness and speed—respond quickly but adhere to your plan.

Engage cybersecurity professionals:

SMEs may not have in-house security teams, so consider engaging external experts for audits, penetration testing and threat-intelligence services. UK organisations can also draw on government resources like the National Cyber Security Centre (NCSC) and free planning tools such as the FCC's Small Biz Cyber Planner.

© 2025 Complus IT. All rights reserved.