



CYBER AWARENESS:

Mitigation Checklist

Location	
Date	
Completed by <i>(name and signature)</i>	

Control area	Do we as a business...	Actionable guidance	Current status
Phishing-Resistant MFA	Prioritise FIDO2/ WebAuthn or PKI-based MFA?	Deploy hardware security keys (e.g., YubiKeys) or platform authenticators (e.g., Windows Hello) using FIDO2/WebAuthn. For high-risk users (admins, execs), enforce phishing-resistant MFA by default.	
	Avoid SMS and basic push-based MFA?	Disable SMS and OTP-based MFA where possible. Replace push-based MFA with number matching or biometric-based MFA to reduce MFA fatigue and push bombing risks.	
	Phase implementation based on risk?	Start with high-value targets (admins, finance, IT) and expand to all users. Use risk-based conditional access policies to enforce stronger MFA where needed.	
	Plan to deploy MFA in legacy systems?	Identify legacy apps that don't support modern MFA. Use compensating controls like VPN enforcement, jump hosts, or legacy MFA gateways (e.g., Duo for RDP).	
SSO and IdP Configurations	Regularly audit federated identity providers?	Review all configured IdPs quarterly. Validate trust relationships, metadata, and certificate expiry. Remove stale or unused IdPs.	
	Disable unused or suspicious IdPs?	Immediately disable any IdP not in active use. Investigate any IdP with unusual configuration or login patterns.	
	Monitor for unauthorised changes to authentication flows or MFA settings?	Enable logging for all IdP configuration changes. Use SIEM alerts for changes to SAML/OIDC settings, MFA policies, or conditional access rules.	

Control area	Do we as a business...	Actionable guidance	Current status
Password Policies	Require minimum 16-character passwords?	Enforce long passphrases or pa (e.g., "correct-horse-battery-staple") via policy. Educate users on creating memorable but strong passwords.	
	Avoid periodic resets unless compromise is suspected?	Follow NIST guidance: only require resets after suspected compromise. Frequent resets lead to weaker passwords and reuse.	
	Use password managers and avoid reuse across systems?	Provide enterprise password managers (e.g., 1Password, Bitwarden). Train users to generate unique passwords per system, or have IT manage this for them.	
Remote Access	Implement application control policies to block unauthorised software?	Use allowlisting tools (e.g., AppLocker, WDAC) to block unapproved RMM tools and scripts. Monitor for shadow IT.	
	Maintain a list of approved remote access tools?	Maintain an inventory of sanctioned RMM tools. Block all others at the firewall or endpoint level.	
	Require RMM access only through VPN or VDI?	Enforce RMM access via secure channels. Use VDI or jump servers with session recording and MFA.	
	Monitor logs for unexpected RMM activity?	Set up alerts for RMM tool usage outside business hours or from unusual geolocations. Correlate with user behavior analytics.	
Detection and Response	Deploy and tune EDR/XDR solutions?	Use EDR/XDR with behavioral analytics (e.g., CrowdStrike, SentinelOne). Regularly tune detection rules to reduce false positives.	
	Configure EDR tools to detect credential dumping?	Enable detections for tools like Mimikatz, LSASS access, and suspicious PowerShell. Block known TTPs (e.g., PPL bypass)	
	Set up alerts for multiple MFA prompts in short succession?	Detect MFA fatigue attacks by alerting on rapid or repeated MFA requests. Investigate anomalies identified or staff members targeted.	
	Utilise threat intelligence and threat hunting?	Subscribe to threat intel feeds (e.g., MISP, commercial TI). Conduct regular hunts for TTPs (e.g., Okta abuse, SIM swapping).	
Incident Preparedness	Store backups in physically separate or cloud-isolated environments?	Use immutable cloud storage or offline backups. Ensure backups are not accessible from production networks.	
	Ensure backups are encrypted and immutable?	Encrypt backups at rest and in transit. Use WORM (Write Once Read Many) storage or backup immutability features	

Control area	Do we as a business...	Actionable guidance	Current status
Incident Preparedness <i>(continued)</i>	Test restoration procedures regularly?	Conduct quarterly restoration drills. Validate RTO/RPO objectives and document lessons learned.	
	Isolate critical systems and take steps to restrict lateral movement?	Use network segmentation, tiered admin models, and just-in-time access. Monitor for lateral movement indicators (e.g., Pass-the-Hash).	
User Awareness	Train staff to recognise phishing and smishing attempts?	Teach users to verify sender domains, avoid clicking links, and report suspicious messages.	
	Train staff to recognise vishing tactics?	Educate on voice-based social engineering. Encourage verification of caller identity and escalation of suspicious calls.	
	Train staff to recognise MFA fatigue?	Explain MFA bombing tactics. Instruct users to deny unexpected prompts and report them immediately.	
	Require multi-step identity verification for helpdesk actions?	Implement callback procedures, identity verification questions, and supervisor approvals for sensitive helpdesk requests.	