biondit.

MFA Vulnerability Diagnostic & Priority Fix Checklist

12 Questions to Diagnose MFA Vulnerabilities

1. What type(s) of MFA does your organisation use?
2. Do you rely on SMS or email OTPs as primary or fallback MFA methods?
3. Is your MFA vulnerable to adversary-in-the-middle (AiTM) phishing attacks?
4. Do you use push-based MFA (e.g., "Approve" prompts) without controls?
5. Have users reported approving MFA prompts they didn't initiate?
6. Can users access corporate systems from unmanaged devices with weak MFA?
7. Do you monitor for anomalous MFA patterns (e.g., repeated prompt failures, location anomalies)?
8. Are any of your MFA methods shared across critical systems (e.g., email + VPN + admin console)?
9. Do you perform regular phishing simulations to test MFA resilience?
10. Is your MFA solution resistant to replay or man-in-the-middle attacks?
11. Have you tested MFA fallback or recovery paths for abuse?
12. Do you use phishing-resistant MFA methods like FIDO2 security keys or passkeys?

Priority Fix Checklist

Priority	Action Item	Why It Matters
🔴 High	Eliminate SMS and email OTPs from your MFA options	These are the weakest links and easily phished or hijacked
🔴 High	Disable push notifications or limit retries	Prevents MFA fatigue and push bombing attacks
🔴 High	Adopt phishing-resistant MFA (e.g., FIDO2, passkeys, biometric keys)	Strong protection against AiTM, phishing, and session hijacking
🔴 High	Enforce device trust and contextual access policies	Helps block suspicious or unmanaged device login attempts
🟠 Medium	Run phishing simulations targeting MFA workflows	Identifies vulnerable users and improves awareness
🟠 Medium	Monitor for MFA anomalies and failed authentication patterns	Early detection of brute force, fatigue, and phishing attempts
🟡 Low	Simplify secure login with passwordless options	Reduces user friction while increasing security
🟡 Low	Audit MFA recovery and fallback processes	Ensures attackers can't exploit "forgot MFA" paths