SNO
A smarter tomorrow.

OPERATIONAL CHECKLIST

Phishing Incident Response Checklist

What to do in the first hour, the first day and the weeks after someone clicks. Built around the NCSC's four layers of phishing defence, with specific steps for credential-theft and adversary-in-the-middle (AiTM) attacks on Microsoft 365.

Prepare | Triage | Contain | Investigate | Recover | Report | Learn

How to use this checklist

Phishing is still one of the most common ways attackers get into organisations. No single control stops every phishing email, so the NCSC recommends layered defences and a practised, planned response. This checklist helps you check you're ready *before* an incident and gives your team a step-by-step response when one happens.

Two ways to use it

- **Readiness review:** work through section 1 now. Treat every **Partly** or **No / not sure** as an action.
- **During an incident:** use the first-hour card on the next page, then sections 2 to 7 in order. Note the time against each step.

Who needs a copy

- Your IT lead, service desk or managed service provider
- Whoever owns data protection (often your DPO or finance director)
- The director who will make decisions during an incident
- Finance, if payments or invoices could be affected

Why MFA alone is not enough

In an adversary-in-the-middle (AiTM) attack, the phishing page sits between the user and the real sign-in page. It captures the password *and* the one-time MFA code, then steals the signed-in session. The attacker can then use the account without needing either again. That's why containment means revoking sessions and checking MFA methods, not just resetting the password, and why the NCSC encourages phishing-resistant MFA such as FIDO2 security keys and passkeys where you can use it.

Important

This checklist is general guidance, not legal advice, and it doesn't replace your own incident response plan. Steps and timings will vary with your systems and contracts. If you think a crime has been committed, or personal data has been affected, follow the reporting steps in section 6 and take professional advice where needed.

The first hour: quick reference card

Print this page and keep it with your incident contacts.

When	Action	Done (time)
Minute 0	Thank the person who reported it. Ask them not to delete the email, not to forward it to colleagues and to keep the device switched on but disconnected from the network if they opened an attachment.	
0–15 minutes	Find out what happened: did they click a link, enter a password or MFA code, open an attachment or approve a sign-in prompt? Who else received the same email?	
15–30 minutes	If credentials may have been entered: reset the password, revoke all sessions and refresh tokens, and remove any MFA method the user doesn't recognise. Block the sender and the link.	
30–60 minutes	Isolate any device that opened an attachment. Remove the email from every mailbox. Check for new inbox rules, forwarding and app consents. Decide who needs to be told, and start the incident log.	

The times are suggested targets, not regulatory deadlines. SNO's 24/7 Operations Centre contained a real AiTM attack in under 30 minutes using these steps (see the SNO case study "Stopping an AiTM phishing attack").

1 Before an incident: are you ready?

Mapped to the NCSC's four layers of phishing defence. These are the controls that reduce how often phishing works, and how much damage it does when it does.

CHECK	YES	PARTLY	NO / NOT SURE
Layer 1: our email domains publish SPF and DKIM records and a DMARC policy, and we monitor DMARC reports. This makes it harder for attackers to spoof your domain. Aim to move DMARC towards a "quarantine" or "reject" policy once reports are clean.	☐	☐	☐
Layer 1: inbound email is filtered for malicious links and attachments, with links re-checked when they're clicked.	☐	☐	☐
Layer 2: staff know exactly how to report a suspicious email, for example with a report button, and reporting is quick and blame-free. The NCSC advises against punishing people who click. Fast reporting matters more than perfect detection.	☐	☐	☐
Layer 2: staff also know how to report if their own device or account is compromised and they can't use email, for example by phone to a named contact. NCSC guidance highlights this gap: a compromised user may not be able to use their normal channels.	☐	☐	☐
Layer 3: MFA is enforced on every cloud service, and phishing-resistant MFA (FIDO2 keys or passkeys) is used for admins and high-risk roles where supported.	☐	☐	☐

CHECK	YES	PARTLY	NO / NOT SURE
Layer 3: sign-in policies flag or block risky sign-ins, for example from unusual locations, unmanaged devices or legacy authentication. In Microsoft 365 this is typically Conditional Access with sign-in risk policies. Licensing varies.	☐	☐	☐
Layer 3: devices have up-to-date anti-malware, users don't work day to day with admin rights, and macros from the internet are blocked.	☐	☐	☐
Layer 4: sign-in and mailbox activity is logged and someone reviews alerts, including outside office hours. You can use built-in cloud security tools, an in-house team or a managed security monitoring service.	☐	☐	☐
Layer 4: we have a written incident response plan with named roles, and an up-to-date contact list for IT, our provider, insurer, bank and legal adviser.	☐	☐	☐
We've practised a phishing scenario in the last 12 months, for example with the NCSC's free Exercise in a Box.	☐	☐	☐

2 Triage: what happened?

Establish the facts quickly. The answers decide which containment steps you need.

CHECK	YES	PARTLY	NO / NOT SURE
We've kept the original email (as an attachment or via the report tool) rather than deleting it. Investigators need the full headers, links and attachments.	☐	☐	☐
We know whether the user clicked a link, entered a password or MFA code, opened an attachment, or approved an unexpected MFA prompt. Ask calmly and without blame. People are more accurate when they don't feel judged.	☐	☐	☐
We've identified every other person who received the same or a similar email, and whether any of them clicked. Search by sender, subject and link domain across all mailboxes.	☐	☐	☐
We've checked whether the email asked for a payment, a change of bank details or gift cards, and told finance immediately if so. Payment fraud is time-critical. Contact your bank straight away if money has moved.	☐	☐	☐
We've started an incident log recording times, decisions and who did what. This helps the investigation, insurance claims and any regulatory report.	☐	☐	☐

3 Contain: stop the attacker

If there's any chance credentials or a session were captured, act on the account and the device together.

CHECK	YES	PARTLY	NO / NOT SURE
The user's password has been reset **15–30 MIN** Choose a new, unique password. Don't reuse a variation of the old one.	☐	☐	☐
All active sessions and refresh tokens for the account have been revoked **15–30 MIN** A password reset alone doesn't end a stolen session in an AiTM attack.	☐	☐	☐
MFA methods on the account have been reviewed, and any method the user doesn't recognise has been removed. Attackers often register their own phone or authenticator app to keep access.	☐	☐	☐
The sender address, domain and malicious link have been blocked across email and web filtering.	☐	☐	☐
Copies of the phishing email have been removed from all mailboxes.	☐	☐	☐
Any device that opened an attachment or ran a file has been isolated from the network **WITHIN 1 HOUR** Keep it powered on if possible. Shutting down can destroy useful evidence.	☐	☐	☐
If the attacker may be active, the account has been temporarily disabled until containment is complete. Agree a temporary way for the user to keep working, if needed.	☐	☐	☐

4 Investigate: how far did it go?

Look for what the attacker did with the access. In Microsoft 365, most of this is in the sign-in logs and the unified audit log.

CHECK	YES	PARTLY	NO / NOT SURE
Sign-in logs have been checked for unfamiliar locations, IP addresses, devices or apps since the email arrived.	☐	☐	☐
Mailbox rules have been checked for new forwarding, redirect or delete rules, and suspicious ones removed. Attackers commonly hide replies or forward invoices to themselves.	☐	☐	☐
Third-party app consents (OAuth) granted by the user have been reviewed and anything unexpected revoked.	☐	☐	☐
We've checked whether the account sent emails to other staff, customers or suppliers, and warned anyone who received one.	☐	☐	☐
Files and data the account accessed have been reviewed, so we know whether personal or sensitive data was viewed or downloaded. This decides whether you have a reportable personal data breach (section 6).	☐	☐	☐

CHECK	YES	PARTLY	NO / NOT SURE
Any isolated device has been scanned, and rebuilt from a known-good image if malware was found. In SNO's AiTM case study, malware was found and the laptop was wiped and reinstalled.	☐	☐	☐

5 Recover: get back to normal safely

Restore access only when you're confident the attacker has been removed.

CHECK	YES	PARTLY	NO / NOT SURE
The user has been given access again with a new password and verified MFA, ideally phishing-resistant.	☐	☐	☐
The account is under closer monitoring for at least the next 30 days. Suggested period. Adjust to your risk.	☐	☐	☐
Any changes made by the attacker (rules, consents, MFA methods, forwarded data) have been reversed and recorded.	☐	☐	☐
Staff who received the email have been told what it looked like and what to do if they see it again.	☐	☐	☐

6 Report and notify

Some reports are legal obligations, others help stop the attacker reaching other people. Check your insurance policy too: many insurers require prompt notification.

CHECK	YES	PARTLY	NO / NOT SURE
We've decided whether personal data was affected and, if the breach is likely to put people's rights and freedoms at risk, reported it to the ICO within 72 hours of becoming aware of it. Under UK GDPR, the 72 hours includes weekends. You can report before you have every detail. Record your reasoning even if you decide not to report.	☐	☐	☐
Where the risk to individuals is high, we've told the people affected without undue delay.	☐	☐	☐
If a crime has been committed, such as fraud or financial loss, we've reported it to Report Fraud (reportfraud.police.uk). Report Fraud replaced Action Fraud as the UK's national reporting service for cyber crime and fraud in December 2025.	☐	☐	☐
For a significant incident, we've considered reporting to the NCSC (report.ncsc.gov.uk).	☐	☐	☐
The phishing email has been forwarded to the NCSC's Suspicious Email Reporting Service (report@phishing.gov.uk). Suspicious texts can be forwarded to 7726.	☐	☐	☐

CHECK	YES	PARTLY	NO / NOT SURE
Our cyber insurer, and any customers or partners with contractual notification terms, have been informed where required.	☐	☐	☐

7 Learn: reduce the chance of a repeat

Hold a short, blame-free review within two weeks while details are fresh.

CHECK	YES	PARTLY	NO / NOT SURE
We've recorded how the email got through, how it was spotted, and how long each stage took.	☐	☐	☐
Any gaps found in section 1 have owners and target dates.	☐	☐	☐
Our incident response plan and contact list have been updated with what we learned.	☐	☐	☐
We've thanked the people who reported it, and shared a short, anonymised summary with staff. Positive reinforcement makes people more likely to report next time.	☐	☐	☐

Need help now, or want to be ready?

SNO's UK-based 24/7 Operations Centre monitors client environments around the clock, detecting and responding to threats like the one in this checklist. If you'd like a clear view of how prepared you are, start with a Security Posture Review.

Ask an expert: sno.cloud/security-posture-review

01691 888 090 · sales@sno.cloud · www.sno.cloud

References

- NCSC, "Phishing attacks: defending your organisation" (four layers of mitigation): https://www.ncsc.gov.uk/guidance/phishing
- NCSC, "Responding to a cyber incident – a guide for CEOs": https://www.ncsc.gov.uk/guidance/ceos-responding-cyber-incidents
- NCSC, Exercise in a Box: https://www.ncsc.gov.uk/information/exercise-in-a-box
- NCSC, Suspicious Email Reporting Service: https://www.ncsc.gov.uk/collection/phishing-scams
- ICO, "72 hours – how to respond to a personal data breach": https://ico.org.uk/for-organisations/sme-web-hub/72-hours-how-to-respond-to-a-personal-data-breach/
- ICO, report a personal data breach: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/
- GOV.UK, "Report Fraud: new service from City of London Police" (4 December 2025): https://www.gov.uk/government/news/report-fraud-new-service-from-city-of-london-police
- SNO case study, "Fortifying against cyber threats" (AiTM phishing response).

General guidance only; not legal advice. © 2026 Specialist Network Operations. Version 1.0, November 2026.