Incident response: what do you do in the first 24 hours?

This month, confirm that Microsoft 365 auditing is on, keep sign-in logs for at least a year and agree who leads, who decides and whom you call. When something looks wrong, isolate accounts and devices without wiping them, export the logs in the first hours and, if the GDPR requires it, notify within 72 hours[1].

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.1**	**IT and security teams in small and mid-size organizations without a 24/7 SOC, many on Microsoft 365 and Entra ID**

Latest version
sheets.einblick.dev/incident-response/

If you only do five things

1. **Check that the audit log is on and reaches back far enough.**
   Run `Get-AdminAuditLogConfig` in Exchange Online PowerShell: auditing isn't on by default for Business Basic, Standard or Premium[2]. Audit (Standard) keeps records for 180 days[3], but Entra ID keeps sign-in logs for only 7 days on Free and 30 days on P1 or P2, so route them to an Azure storage account[4] or your SIEM.
2. **Line up outside help before you need it.**
   Sign an incident response retainer, or find out which firm your cyber insurer sends and what it needs from you first. The NCSC advises UK organizations of any size to use an assured provider, and notes that insurance may include one[5]; in Germany, the BSI lists qualified APT response firms[6].
3. **Set up a channel the attacker can't read.**
   Email and Teams may be down or untrusted, so agree a secure alternative and keep an offline contact list for staff, suppliers and partners[7]. Microsoft's own security operations team uses a separate, non-production Microsoft 365 tenant[8].
4. **Decide now who may pull the plug.**
   Name who can disconnect or shut down systems, call in outside help and speak publicly, with deputies for nights and holidays. NIST lists that authority in the incident response policy[9], and the NCSC warns that critical response roles should never rely on one person[7].
5. **Rehearse a stolen mailbox once a year.**
   Business email compromise complaints to the FBI reported $3.05 billion in losses in 2025[10]. Set up and rehearse procedures to revoke sessions, isolate devices, reset credentials and check related accounts[11]. The NCSC's free Exercise in a Box includes phishing scenarios[12].

The first hours

1. **Name a lead and a note-taker.**
   Record what was found and when, and each decision with who made it and why, in one time zone[13]. A paper logbook is fine[9].
2. **Can you trust email and Teams?**
   If an admin account or a mailbox may be compromised, assume the attacker can read them and move to your other channel. Communicating over the network under investigation is a common mistake[14].
3. **Isolate first, and don't wipe.**
   Disconnecting a system preserves evidence that shutting it down can lose, though shutting down may halt active processes[13]. Defender for Endpoint, including Plan 1, isolates a device but keeps it connected to Defender, and lifts isolation after seven days[15]. Stop backup jobs and protect the backups from further changes[16].
4. **Export the logs now.**
   Search the audit logs from just before the first suspicious activity, without filtering by activity at first[17]. On Entra ID Free, sign-ins older than 7 days are already gone[4]. Keep the original phishing email with its headers[8].
5. **Call your responders, insurer and lawyer before big changes.**
   Let the investigation run before you restore systems: the NCSC warns that rushing recovery can significantly increase risk[13].
6. **One account or a wider intrusion?**
   Lock a single compromised account at once (see below). If the attacker has admin rights, plan one coordinated cleanup: partial remediation often tips the attacker off[8], and they likely hold other credentials[14].
7. **Which clocks have started?**
   The GDPR's 72 hours start once you are reasonably certain that personal data was compromised, and you can notify in phases[1]. For NIS2, DORA and the CRA, see the EU security laws sheet. In the UK, a report to the NCSC doesn't meet your legal duties[13]. To report the crime in Germany, contact your state police's cybercrime contact point (ZAC)[18].

If a Microsoft 365 account is compromised

- **Disable the account and revoke sessions.** In the Entra admin center, clear **Account enabled** and select **Revoke sessions**, or run `Revoke-MgUserSignInSession`. Apps that aren't CAE-capable keep access until their access token expires, by default after 1 hour[19].
- **Reset the password through another channel.** Don't email it to the user. Reset synced accounts twice in Active Directory, and replace app passwords, which a reset doesn't revoke[17].
- **Remove what the attacker added.** Check MFA methods and devices, admin roles and consented apps[17]. Disable a malicious app rather than delete it, or another user's consent can bring it back[20].
- **Check forwarding and inbox rules.** Run `Get-InboxRule -Mailbox <user> -IncludeHidden` and check the mailbox's forwarding addresses. Rules that forward mail or move it to Notes, Junk Email or RSS Subscriptions are typical signs[17].

What changed in 2026

- **Voice phishing went mainstream in Teams.** Microsoft saw confirmed malicious voice phishing over external Teams calls rise 502% in a year; once a victim grants remote access, attackers finish reconnaissance in two minutes or less[11]. Mandiant ranks voice phishing second among initial vectors, at 11%[22]. If someone gave a caller remote access, treat it as an incident and isolate the device.
- **Hand-offs take seconds.** Mandiant measured a median of 22 seconds in 2025 between initial access and hand-off to a second group, down from more than 8 hours in 2022, and advises treating routine malware alerts as high priority[22].
- **More intrusions are found in-house, but they last longer.** Organizations found 52% of Mandiant's 2025 intrusions themselves, up from 43%, while median dwell time rose to 14 days from 11. Mandiant calls standard 90-day log retention insufficient[22].

- **Find out what was read.** MailItemsAccessed is logged by default for E3 and E5 users. If the attacker synced mail to their own client, Microsoft says to assume the entire mailbox is compromised[21].
- **Warn the people it wrote to.** Check Sent Items and message trace for changed bank details and phone the recipients. If money left, ask your bank at once to recall it; the FBI says time is of the essence[10].

What you can skip

- **Rewriting your plan to NIST's new model.** SP 800-61 Rev. 3 maps incident response to the CSF 2.0 functions, but NIST says to use whichever life cycle model suits you[9]. Names, numbers and authority matter more.
- **Buying tools during the incident.** Microsoft sees tools bought under pressure go unused and advises deferring any you can't deploy during the investigation[8].
- **Imaging every machine.** Analyze the systems the attacker used or changed[8]. NIST notes that most malware incidents won't be prosecuted, so formal chain of custody isn't always used[9].
- **Naming the attacker.** Attribution rarely changes the first day's actions. Spend the time on which accounts, devices and data are involved.

- **The NCSC published a first-hours checklist.** Its July 2026 guidance on disruptive attacks covers incident command, outside responders, the disconnect-or-shut-down decision and a central record[13]. Check your plan against it.

Mistakes that cost the most

- **Wiping before collecting evidence.** It loses memory and other host artifacts, and the attacker may notice and change tactics[14]. You may then be unable to show what was taken.
- **Tipping off the attacker.** Don't upload samples to online scanners, which attackers watch[8], or ping and browse their servers[14].
- **Fixing only the symptom.** Blocking an IP address without learning what the malware is and how it got in lets the attacker keep access[14].
- **Resetting every password at once.** Reset the accounts you know are compromised first, then others in stages[8].
- **Waiting for the forensic report to notify.** Start the short initial investigation at once; detail can follow in a phased notification[1].

What this looks like at your size

Small team, no security staff

- Put your IT provider's incident duties and what it may do on your behalf in the contract[9], with a response time.
- Hang up the BSI's IT emergency card with your IT contact's number: staff report at once and act only on instruction[23].
- Note your insurer's incident number and keep the policy details offline[5].

Growing, with IT or security staff

- Keep Entra and Microsoft 365 audit logs in a SIEM or storage account for at least a year, CISA's minimum for log data[14].
- Exercise with the retainer team that would come on site[5].
- Write one-page playbooks for a stolen account, a lost laptop and payment fraud, and test them twice a year.

Enterprise or regulated

- Set up incident command, such as Gold, Silver and Bronze[13], with delegated authority out of hours[7].
- With E5 or an add-on[4], Audit (Premium) keeps Entra, Exchange, OneDrive and SharePoint records for 1 year by default[3].
- Give each reporting clock an owner and draft the notices in advance, using the EU security laws sheet.

Version history

5 Nov 2026, version 1.1	Reviewed for company readers: the UK-only advice on assured responders now sits next to the BSI's list of qualified APT response firms for German companies.

Sources

1. Guidelines 9/2022 on personal data breach notification under GDPR, version 2.0. European Data Protection Board, 28 Mar 2023. edpb.europa.eu
2. Turn auditing on or off. Microsoft Learn, 19 Jun 2026. learn.microsoft.com
3. Learn about auditing solutions in Microsoft Purview. Microsoft Learn, 18 May 2026. learn.microsoft.com
4. Microsoft Entra data retention. Microsoft Learn, 6 Jan 2026. learn.microsoft.com
5. Preparing for highly disruptive cyber incidents: 3. Prepare your technical recovery capability. NCSC (UK), 1 Oct 2026. ncsc.gov.uk
6. Qualifizierte APT-Response-Dienstleister. BSI, 1 Jun 2026. bsi.bund.de
7. Preparing for highly disruptive cyber incidents: 2. Prepare your people. NCSC (UK), 1 Oct 2026. ncsc.gov.uk
8. Incident response overview. Microsoft Learn, 6 Nov 2024. learn.microsoft.com
9. SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST, Apr 2025. nvlpubs.nist.gov
10. 2025 IC3 Annual Report. FBI Internet Crime Complaint Center, Apr 2026. ic3.gov
11. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
12. Exercise in a Box. NCSC (UK), checked 3 Nov 2026. ncsc.gov.uk
13. Recovering from a highly disruptive cyber attack: 1. Immediate activities. NCSC (UK), 28 Jul 2026, reviewed 1 Oct 2026. ncsc.gov.uk
14. Technical Approaches to Uncovering and Remediating Malicious Activity (AA20-245A). CISA and the cyber security centres of Australia, Canada, New Zealand and the UK, updated 24 Sep 2020. cisa.gov
15. Take response actions on a device in Microsoft Defender for Endpoint. Microsoft Learn, 23 Jul 2026. learn.microsoft.com
16. TOP 12 Maßnahmen bei Cyber-Angriffen. BSI (Allianz für Cyber-Sicherheit), BKA and partners, Sep 2019. allianz-fuer-cybersicherheit.de
17. Respond to a compromised email account in Microsoft 365. Microsoft Learn, 3 Jul 2026. learn.microsoft.com
18. Zentrale Ansprechstellen Cybercrime (ZAC). Polizei (BKA), checked 3 Nov 2026. polizei.de
19. Revoke user access in an emergency in Microsoft Entra ID. Microsoft Learn, 19 Jun 2026. learn.microsoft.com
20. App consent grant investigation. Microsoft Learn, 12 Mar 2025. learn.microsoft.com
21. Use MailItemsAccessed to investigate compromised accounts. Microsoft Learn, 19 Jun 2026. learn.microsoft.com
22. M-Trends 2026 Executive Edition. Google Cloud (Mandiant), Mar 2026. services.google.com
23. IT emergency card "Verhalten bei IT-Notfällen". BSI, checked 3 Nov 2026. bsi.bund.de