THIS IS AN IT SUPPORT GROUP

CompTIA A+ Practice Pack

50 exam-style practice questions with answer explanations, plus two help-desk checklists you can use at work today.

Part 1 Hardware Troubleshooting — 12 questions

Part 2 Networking Troubleshooting — 10 questions

Part 3 Mobile Devices — 10 questions

Part 4 Security — 8 questions

Part 5 Operational Procedures — 10 questions

Key Full answer key with explanations

Bonus Windows Update + Phishing Response one-page checklists

How to use this pack

These are scenario questions, not trivia. Every one of them is built the way the A+ exam (and real help desk work) actually tests you: a symptom, one clue most people skim past, and four answers where two are plausible.

- **Commit to a letter before checking the key.** All answers and explanations are in the Answer Key at the back, so you can work straight through a section without spoilers.
- **The explanation matters more than the letter.** If you got it right for the wrong reason, you got it wrong.
- **Look for the pattern, not the fact.** Most questions reward the same instincts: check the simplest cause first, separate hardware from software, change one thing at a time, and confirm the fix.
- **Drill in short sets.** Ten questions after reviewing a topic beats fifty in one sitting.

> **Scoring yourself:** 40+ correct — you're ready for full-length practice tests. 30–39 — solid, review the domains you missed. Under 30 — go back to concept review before drilling more questions; question-grinding won't fix a concept gap.

CORE 1 (220-1201)

Part 1: Hardware Troubleshooting

Boot problems, overheating, bad RAM, storage failures, display issues, and the classic "it worked yesterday" ticket. Check the simplest cause first, separate hardware from software, and confirm the fix.

1 Desktop has power lights but no display

A user reports their desktop turns on, fans spin, and the power LED lights up, but the monitor says “No signal.” The monitor works with another computer. What should you check first?

- A Replace the motherboard
- B Reseat the video cable and verify the correct monitor input
- C Reinstall the operating system
- D Replace the CMOS battery

2 Laptop shuts down during video calls

A laptop works normally for basic browsing but shuts down during long video calls. The bottom feels hot and the fan is loud. What is the most likely cause?

- A Failing cooling system or blocked airflow
- B Incorrect display resolution
- C Loose keyboard ribbon cable
- D Corrupt user profile

3 Random blue screens after a memory upgrade

A technician installed new RAM in a desktop. Since then, the computer randomly crashes with blue screens. What should the technician do next?

- A Run a memory diagnostic and verify RAM compatibility/seating
- B Replace the power button
- C Disable Windows updates
- D Format the storage drive

4 Clicking sound from a desktop tower

A user says their desktop is slow to open files and sometimes freezes. You hear a repeated clicking sound from inside the case. What is the best next step?

- A Defragment the drive immediately
- B Back up data and check drive health
- C Replace the monitor cable
- D Increase the screen brightness

5 Computer powers on, then immediately powers off

A desktop powers on for two seconds, then shuts off. This repeats every time the user presses the power button. Which cause is most likely?

- A Bad wallpaper file
- B Power supply, short, overheating protection, or improperly seated component
- C Expired antivirus subscription
- D Incorrect time zone

6 External keyboard works on another laptop

A USB keyboard does not work on one laptop, but it works on another. Other USB devices work in the same port on the original laptop. What is the best next step?

- A Replace the laptop motherboard
- B Check Device Manager, drivers, and keyboard settings
- C Replace the laptop battery
- D Reimage the computer immediately

7 Printer works for everyone except one user

One user cannot print to the shared office printer. Other users print fine. The printer test page works from the device panel. What should you check first?

- A The user's print queue, default printer, and connection to the shared printer
- B The building's electrical service
- C The printer's fuser assembly
- D The office router firmware

8 New SSD is not detected

A user installed a new internal SSD, but it does not appear in the OS. What should you check early in the process?

- A Whether the drive appears in BIOS/UEFI and Disk Management
- B Whether the user has enough desktop icons
- C Whether the monitor supports HDR
- D Whether the mouse battery is full

9 Laptop battery drains unusually fast

A laptop battery that used to last several hours now dies quickly. The user recently started carrying it in a backpack and using it in meetings all day. What should you check first?

- A Battery health, power settings, and high-usage apps
- B The office printer queue
- C The desktop monitor refresh rate
- D The network switch VLAN

10 System date and time reset after unplugging

A desktop loses date/time settings whenever it is unplugged from power. What component is the likely cause?

- A CMOS/RTC battery
- B CPU fan
- C HDMI cable
- D RAM heat spreader

11 Faint image on a laptop screen

A laptop screen appears almost black, but when you shine a flashlight at an angle, you can faintly see the desktop. What is the likely issue?

- A Backlight or display assembly problem
- B Bad Ethernet cable
- C Incorrect printer driver
- D Expired browser cache

12 Computer is slow only when opening large files

A workstation boots normally, browses normally, and runs email fine, but becomes painfully slow when opening large local project files. What should you investigate first?

A. Storage performance and free disk space

B. The user's keyboard layout

C. The webcam privacy shutter

D. The office Wi-Fi password

CORE 1 (220-1201)

Part 2: Networking Troubleshooting

Connectivity failures, DNS problems, IP configuration, and Wi-Fi complaints. Work out what layer is broken before touching settings.

13 Laptop shows a 169.254 address

A user says their laptop is connected by Ethernet but cannot access the internet or internal sites. `ipconfig` shows an IPv4 address starting with `169.254`. Other users are online. What should you check first?

- A Whether the laptop received a valid DHCP lease
- B Whether the user's monitor supports HDMI 2.1
- C Whether the browser cache is full
- D Whether the public website is down

14 Websites fail by name but work by IP

A desktop can ping `8.8.8.8`, but browsing to normal websites by name fails. What is the most likely area to investigate?

- A DNS configuration
- B Monitor refresh rate
- C Printer toner level
- D CMOS battery

15 One conference room has weak Wi-Fi

Users report that Wi-Fi is fine in most of the office, but calls drop in one conference room. What is the best first troubleshooting step?

- A Reinstall Windows on every laptop
- B Check signal strength, access point placement, interference, and client density in that room
- C Replace the company's firewall immediately
- D Tell users to stop using video calls

16 VPN connects, but internal file shares do not work

A remote user says the VPN client shows “connected,” but mapped drives and internal file shares fail. Email and public websites work. What should you check next?

- A VPN routes, DNS suffix/search behavior, and access permissions
- B The user's laptop wallpaper
- C The office coffee machine
- D Whether the mouse is paired by Bluetooth

17 Everyone on one switch loses network access

Several users sitting near each other report no network access at the same time. Users in the rest of the office are fine. What is the most likely first area to check?

- A The access switch, uplink, power, or cabling for that area
- B Every user's browser history
- C The public DNS record for the company website
- D The CEO's email signature

18 Printer is online, but one subnet cannot print

A network printer works for users on the first floor, but users on the second floor cannot print. The printer web page opens from the first-floor subnet but not the second-floor subnet. What should you investigate?

- A Routing, firewall rules, printer IP/subnet settings, or ACLs between subnets
- B Whether the printer has enough paper
- C Whether every second-floor user has bad RAM
- D Whether the printer display brightness is too low

19 User can reach websites but not a shared folder

A user can browse the internet and access email, but cannot open a mapped drive. Coworkers can open the same share. What should you check first?

- A The user's permissions, mapped drive path, credentials, and name resolution to the file server
- B The ISP's backbone routing
- C Replace all office switches
- D Disable DNS for the entire company

20 New desk phone has no power

A newly installed VoIP phone does not power on. The same network jack works with a laptop. What should you verify early?

- A Whether the switch port provides PoE or whether the phone needs a power adapter
- B Whether the phone has the right ringtone
- C Whether the user's Outlook signature is synced
- D Whether the browser default search engine changed

21 Wi-Fi connects but says “No internet“

A laptop connects to the office Wi-Fi SSID, receives a normal private IP address, but cannot reach websites. Other users on the same Wi-Fi are online. What should you check next?

- A Gateway/DNS settings, captive portal, proxy/VPN client, and local firewall on that laptop
- B Replace every access point
- C Assume the entire internet is down
- D Change the user's keyboard

22 After moving desks, Ethernet is dead

A user moved to a new desk. Wi-Fi works, but wired Ethernet shows disconnected. The same laptop and cable worked at the old desk. What should you check first?

- A Patch panel/switch port mapping and whether the wall jack is active
- B Reinstall the operating system
- C Replace the user's keyboard
- D Reset the user's email password

CORE 1 (220-1201)

Part 3: Mobile Devices

Laptops, phones, and tablets: charging, batteries, Bluetooth, displays, and lost-device response. Mobile questions reward knowing what to check before what to replace.

23 laptop will not charge

A user says their laptop battery is at 7% and will not charge. The same wall outlet powers a monitor. The user recently switched to a different USB-C charger from another desk.

What should you check first?

A. Reinstall the operating system

B. Verify the charger, wattage, cable, and charging port for compatibility or damage

C. Replace the laptop system board

D. Disable Wi-Fi to save power

24 swollen battery

A technician notices that a laptop trackpad is raised and the bottom case is bulging. The user says the laptop still runs if they press the case down.

What is the best response?

A. Keep using it until the next maintenance window

B. Stop using the device, follow battery safety procedures, and replace the battery through the approved process

C. Put heavy books on the laptop overnight

D. Puncture the battery to release pressure

25 Bluetooth headset will not pair

A user cannot pair a Bluetooth headset with their laptop. The headset pairs with their phone. The laptop paired with another headset last week.

What should you try early in the troubleshooting process?

A. Confirm Bluetooth is enabled, remove stale pairings if needed, put the headset in pairing mode, and try again nearby

B. Replace the laptop SSD

C. Change the user's email password

D. Disable all wireless radios permanently

26 phone has Wi-Fi but no company mail

A user’s phone can browse websites on Wi-Fi, but company email stopped syncing after they changed their password.

What is the most likely next step?

A. Replace the phone antenna
B. Update the saved account credentials or mail profile, then test sync
C. Factory reset the phone immediately
D. Tell the user Wi-Fi is broken

27 external monitor works, laptop screen does not

A laptop powers on and displays normally on an external monitor. The built-in screen stays very dim, but you can faintly see the desktop if you shine a light at an angle.

What does this most likely suggest?

A. Internal display backlight or display assembly issue
B. DNS misconfiguration
C. Bad keyboard layout
D. The operating system is definitely corrupted

28 touchscreen is inaccurate

A tablet registers touches slightly away from where the user taps. The screen protector was installed yesterday.

What should you check first?

A. Remove or inspect the screen protector and test touch input again
B. Replace the wireless access point
C. Rebuild the user's mailbox
D. Disable device encryption

29 mobile hotspot is slow

A field technician uses a phone hotspot to connect a laptop. The connection works, but it is slow and drops when the phone is moved to the inside of a metal equipment cabinet.

What is the best explanation?

A. The hotspot signal is being weakened by placement and interference
B. The laptop needs more RAM to see the hotspot
C. The phone must be factory reset
D. The technician should delete the browser cache

30 lost company phone

A user reports that a company-managed phone was lost during travel. It contains work email and authenticator apps.

What should IT do first?

- A Follow the mobile device management policy to lock, locate, wipe, or disable access as appropriate
- B Wait a week in case it turns up
- C Ask the user to post about it on social media
- D Delete the user's desktop profile

31 laptop camera does not work

A user says their laptop camera works in one meeting app but not another. The app that fails shows a privacy warning.

What should you check?

- A App camera permissions and privacy settings
- B Replace the battery
- C Change the Wi-Fi channel
- D Delete the user's documents

32 NFC tap-to-pay fails

A user says tap-to-pay stopped working after they installed a thick rugged phone case. The payment app opens normally.

What should you try first?

- A Remove the case and test NFC again
- B Replace the office router
- C Reinstall the laptop operating system
- D Disable all biometrics forever

CORE 2 (220-1202)

Part 4: Security

Authentication, permissions, malware symptoms, and safe handling of security incidents at the help desk level.

33 Unexpected MFA prompts

A user calls the help desk because their phone keeps showing MFA approval prompts they did not start. They ask you to reset MFA because the prompts are annoying.

What should you do first?

A. Reset MFA immediately so the user can keep working

B. Tell the user to approve one prompt and change the password later

C. Treat it as possible account compromise, verify identity, review sign-in activity, and follow escalation policy

D. Disable MFA for the user because MFA is causing the issue

34 Request for admin rights

A user says a vendor application will only install if they are made a local administrator. They want permanent admin rights because “this keeps happening.”

What is the best response?

A. Add the user to local administrators permanently

B. Use an approved elevation, software deployment, or temporary admin process after validating the business need

C. Give the user the domain admin password for five minutes

D. Tell the user to download a cracked installer that does not need admin rights

35 Lost company laptop

A remote employee reports that their company laptop was stolen from a car. The laptop had access to email and cloud storage. The employee thinks the laptop was locked when it was stolen.

What should IT do next?

A. Wait to see if the laptop turns up

B. Confirm encryption/device management status, lock or wipe the device if policy allows, revoke sessions, and document the incident

C. Delete the user's mailbox

D. Tell the user that a lock screen is enough protection

36 Shared folder permissions

A manager asks you to give one employee access to a finance folder. The employee needs to view invoices but should not edit or delete files.

Which permission approach is best?

A. Give the employee full control so they do not call back later
B. Add the employee to the correct read-only group after approval
C. Share the manager's password with the employee
D. Copy the finance folder to the employee's desktop

37 Public Wi-Fi support call

A user is working from a hotel and says they cannot connect to an internal app. They ask whether they should connect to an open Wi-Fi network named “Free Hotel Internet 2” because it has a stronger signal.

What is the safest guidance?

A. Use the open network and ignore browser warnings
B. Use approved remote access from a trusted network, avoid unknown open Wi-Fi, and report suspicious captive portals or certificate warnings
C. Turn off the firewall to improve connectivity
D. Email their password to the help desk so you can test it

38 Browser popups after installing “free” software

A user reports that their browser now shows constant popups after they installed a free PDF tool. They also see a new extension they do not recognize.

What is the best next step?

A. Isolate the device if needed, remove suspicious software/extensions, run approved scans, update, verify, and document
B. Tell the user popups are normal
C. Disable all security tools because they slow down the browser
D. Delete random system files until the popups stop

39 BitLocker recovery after a motherboard replacement

A laptop asks for a BitLocker recovery key after hardware service. The user is frustrated and wants you to bypass it because they have a meeting.

What is the correct approach?

- A Bypass encryption with an online tool
- B Retrieve the recovery key from the approved location after verifying the user/device, then document the recovery
- C Disable encryption permanently
- D Reinstall Windows immediately without checking backups

40 Password reset request from chat

Someone messages the help desk from a personal chat account claiming to be an executive. They say they are locked out and need a password reset immediately.

What is the best response?

- A Reset the password because executives are important
- B Verify identity using the approved reset process before changing credentials
- C Ask them to send their old password first
- D Create a second account with no MFA

CORE 2 (220-1202)

Part 5: Operational Procedures

Documentation, change management, safety, ticket handling, and professionalism. The "easy" domain people lose points on because they answer with habits instead of procedure.

41 Before replacing a failing drive

A user's laptop drive is showing signs of failure. The user says the laptop contains important local files that may not be synced to cloud storage. What should you do before replacing the drive?

- A Replace the drive immediately because failing drives are urgent
- B Confirm backup status and preserve user data according to company policy
- C Delete temporary files to make the drive run faster
- D Reinstall the operating system without asking about data

42 A change during business hours

You found a firmware update that might fix random docking station problems for a group of users. The update requires a reboot and could affect many laptops. What is the best next step?

- A Push it immediately while everyone is online so you can see results
- B Create or follow a change request, test on a small group, and schedule the rollout
- C Email users after the reboot happens
- D Skip documentation because firmware updates are routine

43 Ticket notes after fixing email

You fixed an Outlook issue by recreating the profile, confirming mail sync, and showing the user how to reopen shared mailboxes. What should your ticket notes include?

- A “Fixed”
- B “Outlook issue resolved”
- C Symptoms, steps taken, result, user confirmation, and any follow-up
- D Nothing, because the user is happy

44 Handling a user's personal files

While troubleshooting a laptop, you notice personal photos and tax documents on the desktop. The files are not related to the ticket. What should you do?

- A Open them to check whether they are causing disk space problems
- B Ignore unrelated personal data and only access what is required for the support task
- C Copy them to your USB drive in case the user needs a backup
- D Mention interesting file names to a coworker

45 ESD safety while replacing RAM

You are replacing RAM in a desktop. Which action best reduces electrostatic discharge risk?

- A Work on carpet because it is softer for parts
- B Wear an ESD strap or use an approved ESD mat while handling components
- C Keep the computer plugged in and powered on
- D Hold the RAM by the gold contacts

46 A user reports unexpected MFA prompts

A user calls because they are receiving MFA prompts they did not initiate. They want you to “just reset MFA.” What is the best response?

- A Reset MFA immediately so the user can keep working
- B Treat it as a possible account compromise, verify identity, review sign-in activity, and follow escalation policy
- C Tell the user to ignore the prompts
- D Disable MFA because it is annoying the user

47 Disposal of old drives

Your team is retiring old laptops. Some drives may contain company data. What should happen before disposal or recycling?

- A Delete the Documents folder
- B Format the drive quickly and recycle the laptop
- C Sanitize or destroy storage media according to company policy and document the chain of custody
- D Give the laptops away because they no longer boot

48 Lifting a heavy UPS

A rack-mounted UPS needs to be moved. It is heavy and awkward. What should you do?

- A Lift it alone if you are in a hurry
- B Drag it by the power cable
- C Get help or use proper lifting equipment, and follow safety guidance
- D Remove random parts until it feels lighter

49 After employee termination

HR notifies IT that an employee has been terminated and access must be removed immediately. Which action is most appropriate?

- A Disable accounts, revoke sessions, remove access, document actions, and coordinate with HR/security
- B Wait until the end of the week so the user can finish personal tasks
- C Delete every mailbox and file immediately
- D Only reset the password

50 A fix causes a new issue

You changed a printer driver to fix slow printing, but now several users cannot print duplex. What should you do next?

- A Close the ticket because the original issue improved
- B Document the change, verify scope, roll back if needed, and communicate the impact
- C Blame the users for printing too much
- D Keep trying random drivers without notes

ANSWER KEY

Answer Key & Explanations

Score yourself first, then read the explanations — including for the ones you got right. If you got it right for the wrong reason, you got it wrong.

Part 1: Hardware Troubleshooting

1 B — Reseat the video cable and verify the correct monitor input.

Start with the simplest external causes. A working monitor plus a “No signal“ message points to connection, input selection, graphics output, or GPU seating before it points to the OS. Reinstalling Windows will not fix a display signal that fails before Windows matters.

2 A — Failing cooling system or blocked airflow.

The clue is heat under load. Video calls can push CPU, GPU, camera, and network activity at the same time. Clean vents, check fan operation, confirm the device is on a hard surface, and run hardware diagnostics if needed.

3 A — Run a memory diagnostic and verify RAM compatibility/seating.

The recent change is the flashing neon sign. Bad seating, mismatched specs, unsupported capacity, or a defective module can create random crashes. Test one module at a time if needed.

4 B — Back up data and check drive health.

Clicking plus file access problems can indicate a failing mechanical hard drive. Your first instinct should be data protection, not heroic repair attempts. Check SMART status and replace the drive if diagnostics support it.

5 B — Power supply, short, overheating protection, or improperly seated component.

Very short power cycles usually happen before the OS is involved. Check power connections, motherboard standoffs, RAM/GPU seating, CPU cooler installation, and use a known-good power supply if appropriate.

6 B — Check Device Manager, drivers, and keyboard settings.

The keyboard works elsewhere, and the port works with other devices. That points away from simple hardware failure and toward device-specific software, driver, or policy issues. Reimaging is overkill before basic checks.

7 A — The user's print queue, default printer, and connection to the shared printer.

The scope is one user. That usually means a local queue, default printer selection, stale driver, permissions, or mapping issue. For a full workflow, use the printer troubleshooting checklist.

8 A — Whether the drive appears in BIOS/UEFI and Disk Management.

If BIOS/UEFI does not see the drive, think cable, port, seating, compatibility, or failed drive. If BIOS sees it but the OS does not show it in File Explorer, the disk may need initialization, partitioning, or a drive letter.

9 A — Battery health, power settings, and high-usage apps.

Battery complaints need both hardware and usage checks. Look at battery health reports, power mode, screen brightness, background apps, and whether the laptop is sleeping properly in the bag.

10 **A — CMOS/RTC battery.**

A weak CMOS battery can cause BIOS settings and clock information to reset when the machine loses power. This is one of the few times the little coin-cell battery is not just trivia.

11 **A — Backlight or display assembly problem.**

A faint image means the GPU may still be sending video, but the display is not lighting correctly. Test with an external monitor to separate graphics output from the built-in display assembly.

12 **A — Storage performance and free disk space.**

Performance problems are about scope. If the slowdown appears during local file access, inspect storage health, free space, disk type, indexing, and whether the files are actually local or synced from a cloud client.

Part 2: Networking Troubleshooting

13 **A — Whether the laptop received a valid DHCP lease.**

A `169.254.x.x` address is an APIPA address. It usually means the device did not receive an address from DHCP. Check the cable, switch port, adapter status, VLAN/port configuration, DHCP availability, and whether another device works on the same jack. Do not start with browser settings when the IP address is already telling you the network setup failed early.

14 **A — DNS configuration.**

If IP connectivity works but names do not resolve, DNS moves to the top of the list. Check DNS server settings, whether the DNS server is reachable, VPN DNS behavior, and whether only one site or all names are failing. This is a classic exam pattern and a real support pattern.

15 **B — Check signal strength, access point placement, interference, and client density in that room.**

The scope is physical: one room. That points to RF coverage, interference, roaming, or overloaded access points before it points to a company-wide network problem. Look for distance from the AP, walls, metal, neighboring networks, Bluetooth-heavy rooms, and whether too many clients are pinned to one access point.

16 **A — VPN routes, DNS suffix/search behavior, and access permissions.**

“VPN connected“ only tells you the tunnel came up. It does not prove the user can resolve internal names, route to the file server, or access the share. Check whether internal resources work by IP, whether split tunneling is expected, whether DNS changes after connection, and whether the user account has permission. For a longer workflow, use the VPN troubleshooting checklist.

17 **A — The access switch, uplink, power, or cabling for that area.**

Again, scope gives it away. Multiple nearby users failing together points to shared infrastructure: switch, patch panel, uplink, PoE/power, or a local cabling issue. Do not troubleshoot each laptop as a separate mystery novel until you rule out the common point of failure.

18 **A — Routing, firewall rules, printer IP/subnet settings, or ACLs between subnets.**

When one network segment can reach a device and another cannot, think routing and filtering. Check the printer's IP, subnet mask, gateway, VLAN, firewall rules, and whether the second-floor subnet is allowed to reach printer services. If the issue were paper, everyone would have the same bad day.

19 **A — The user's permissions, mapped drive path, credentials, and name resolution to the file server.**

The network is not fully down. The problem is specific to one user and one resource. Check whether the user can reach the server, whether the path is correct, whether credentials are stale, whether the account is locked or removed from a group, and whether the drive mapping points to an old server. The network share troubleshooting checklist covers the full version.

20 **A — Whether the switch port provides PoE or whether the phone needs a power adapter.**

Many VoIP phones use Power over Ethernet. A laptop working on the jack proves network connectivity, not PoE availability. Check switch port PoE settings, power budget, cabling, phone power requirements, and whether a power brick is needed.

21 **A — Gateway/DNS settings, captive portal, proxy/VPN client, and local firewall on that laptop.**

The laptop associated with Wi-Fi and received an IP address, so do not stop at "Wi-Fi bad." Check whether it can ping the gateway, resolve names, reach IP addresses, pass a captive portal, or is being trapped by a stale VPN/proxy/security client. One device failing while others work usually means local configuration or policy.

22 **A — Patch panel/switch port mapping and whether the wall jack is active.**

The recent change is the desk move. Check the physical path: wall jack, patch panel, switch port, cable, port status, and whether that jack is actually patched. This is exactly the kind of ticket where a ten-second cable path check beats an hour of software fiddling.

Part 3: Mobile Devices

23 **B — Verify the charger, wattage, cable, and charging port for compatibility or damage.**

Start with the obvious physical and compatibility checks. Many USB-C chargers fit the port but do not provide enough power for a laptop under load. The cable can also matter. Reinstalling the OS will not fix an underpowered charger. Replacing the board before checking power basics is how repair queues become expensive fiction.

24 **B — Stop using the device, follow battery safety procedures, and replace the battery through the approved process.**

A swollen battery is a safety issue, not a "try rebooting" issue. Stop using the device and follow the organization's handling process. Do not compress, puncture, bend, or keep charging it. The exam may not be dramatic here, but real lithium battery failures can ruin your day in a very smoky way.

25 **A — Confirm Bluetooth is enabled, remove stale pairings if needed, put the headset in pairing mode, and try again nearby.**

This is a pairing problem until proven otherwise. Check whether Bluetooth is enabled, whether the headset is already paired to something else, whether the device is discoverable, and whether old pairings are confusing the process. Jumping to storage replacement is not troubleshooting. It is interpretive dance with a screwdriver.

26 **B — Update the saved account credentials or mail profile, then test sync.**

The phone has network connectivity. The clue is the password change. Mobile mail apps often keep old credentials until the user updates the account, signs back in, or refreshes the managed profile. A factory reset might be a last resort for a broken device, but this scenario is begging you to fix the account configuration first.

27 **A — Internal display backlight or display assembly issue.**

If the external display works, the laptop is booting and graphics output is at least partly functional. A very faint internal image points toward the screen, backlight, display cable, or display assembly. DNS has nothing to do with whether photons are showing up on the panel, which is rude but useful.

28 **A — Remove or inspect the screen protector and test touch input again.**

The timing matters. If touch issues started right after a screen protector was installed, inspect that first. Dirt, bubbles, thickness, or poor alignment can affect touch behavior. You can still check updates and diagnostics later, but do not ignore the giant clue sitting on top of the glass.

29 **A — The hotspot signal is being weakened by placement and interference.**

Wireless troubleshooting still applies when the access point is a phone. Distance, placement, building materials, power-saving behavior, cellular signal, and interference can all matter. A metal cabinet is not a friendly radio environment. It is basically a tiny Faraday cage with worse cable management.

30 **A — Follow the mobile device management policy to lock, locate, wipe, or disable access as appropriate.**

A lost managed device is a security event. The exact action depends on policy and tooling, but the exam-friendly answer is to use MDM or approved controls to protect data: lock, locate, wipe, revoke tokens, or disable access when required. Waiting around is not a control.

31 **A — App camera permissions and privacy settings.**

If the camera works in one app, the hardware is probably not dead. Modern operating systems and managed environments can block camera access per app. Check permissions, privacy settings, browser permissions if it is a web meeting, and any organization policy. This is also a good reminder that “camera broken” often means “permissions are doing their job loudly.”

32 **A — Remove the case and test NFC again.**

NFC requires very short-range communication. A thick case, metal plate, wallet attachment, or bad placement can interfere. Since the app opens, start with the physical change. Not every mobile problem is a cloud identity crisis. Sometimes it is just a case built like a tank.

Part 4: Security

33 **C — Treat it as possible account compromise, verify identity, review sign-in activity, and follow escalation policy.**

Unexpected MFA prompts can mean an attacker already has the password and is trying to get the second factor approved. Do not treat that like a normal “new phone” request.

A safe flow is: verify the caller using approved methods, tell them not to approve unknown prompts, check sign-in logs if you have access, revoke sessions or force a password reset if policy requires it, and escalate suspicious activity. Our MFA reset checklist covers this workflow in more detail.

34 **B — Use an approved elevation, software deployment, or temporary admin process after validating the business need.**

Least privilege is the pattern. Users should have the access needed to do their jobs, not permanent power because one installer is annoying.

In real support work, this may mean deploying the software through Intune, SCCM, Jamf, a managed app catalog, a privileged access tool, or a documented temporary elevation process. If the software is not approved, the answer may be "not yet," not "sure, enjoy your new attack surface."

35 **B — Confirm encryption/device management status, lock or wipe the device if policy allows, revoke sessions, and document the incident.**

A lock screen helps, but it is not the whole response. The security question is whether company data and active sessions are protected.

You want to know whether BitLocker or another full-disk encryption tool was enabled, whether the device is managed, when it last checked in, and whether remote lock or wipe is allowed. Also revoke cloud sessions and document what happened. If this becomes a breach review, "probably fine" will not be a fun ticket note.

36 **B — Add the employee to the correct read-only group after approval.**

This is least privilege again. If the user needs read access, do not grant modify or full control just because it is easier.

Groups are cleaner than one-off permissions because they are easier to audit and remove later. Also remember that Windows file access may involve both share permissions and NTFS permissions. If you need the ticket version of this flow, see our shared mailbox access checklist and network share troubleshooting checklist. Different systems, same access-control habit: approve, scope, grant, verify, document.

37 **B — Use approved remote access from a trusted network, avoid unknown open Wi-Fi, and report suspicious captive portals or certificate warnings.**

A+ security is practical. Open Wi-Fi, fake SSIDs, certificate warnings, and sketchy captive portals are all normal ways users wander into trouble.

The best answer points them back to approved remote access and safe network behavior. If your environment allows hotspot use, VPN, ZTNA, or managed remote access, follow that policy. Do not train users to click through warnings just because a ticket is inconvenient.

38 **A — Isolate the device if needed, remove suspicious software/extensions, run approved scans, update, verify, and document.**

This is the malware-removal pattern in a browser-shaped jacket. Check installed applications, extensions, startup items, browser settings, and endpoint protection alerts. Use approved tools. If there is evidence of credential theft, data exposure, or spreading malware, escalate. For more reps, use the A+ malware removal practice questions.

39 **B — Retrieve the recovery key from the approved location after verifying the user/device, then document the recovery.**

Encryption is doing its job. Hardware changes can trigger recovery, and the support response should follow policy. Common approved locations might include Microsoft Entra ID, Active Directory, an MDM platform, or a documented recovery portal. Do not invent shortcuts around encryption. Our BitLocker recovery key troubleshooting checklist walks through the practical support flow.

40 **B — Verify identity using the approved reset process before changing credentials.**

Help desk password resets are a favorite social engineering target. Urgency plus authority is not proof. Use the approved identity verification path. The important part is that the reset process is not “whoever sounds the most annoyed wins.”

Part 5: Operational Procedures

41 **B — Confirm backup status and preserve user data according to company policy.**

Operational procedure questions love this trap. Yes, the hardware problem matters. No, you do not get bonus points for speed-running data loss.

Before invasive work, verify whether the data is backed up, whether the user has unsynced local folders, and what the approved recovery path is.

42 **B — Create or follow a change request, test on a small group, and schedule the rollout.**

Change management exists because “probably fine” has ruined many afternoons. For anything that affects multiple users, production systems, firmware, network settings, identity, security, or business availability, use the change process.

Good change notes include the reason, affected devices, risk, backout plan, test group, schedule, and owner.

43 **C — Symptoms, steps taken, result, user confirmation, and any follow-up.**

Good notes help the next tech, your future self, and sometimes your manager when a repeat issue shows up. They do not need to be a novel, but they need enough detail to be reusable.

A practical note might look like this:

> User reported Outlook stuck at loading profile after password change. Confirmed webmail worked. Recreated Outlook profile, re-added shared mailbox, verified send/receive and calendar access. User confirmed mail synced normally. No escalation needed.

For more examples, see our help desk ticket notes templates.

44 **B — Ignore unrelated personal data and only access what is required for the support task.**

Privacy is not optional just because you have admin rights. Access the minimum data needed to solve the ticket, avoid browsing personal content, and follow company policy for backups or transfers.

If user data must be moved, use approved tools and document what happened. Do not use personal USB drives, personal cloud storage, screenshots in chat, or “I was just helping” as a policy.

45 **B — Wear an ESD strap or use an approved ESD mat while handling components.**

ESD precautions are basic, but they show up because they matter. Power down equipment, disconnect power when appropriate, ground yourself with approved tools, handle components by the edges, and store parts in antistatic bags.

46 **B — Treat it as a possible account compromise, verify identity, review sign-in activity, and follow escalation policy.**

Unexpected MFA prompts can mean someone has the password and is trying to get through the second factor. That is not a normal convenience reset.

Verify the user through approved methods, check sign-in logs if you have access, revoke sessions or force password reset if policy requires it, and escalate suspicious activity. Our MFA reset checklist covers the safer workflow.

47 **C — Sanitize or destroy storage media according to company policy and document the chain of custody.**

Deleting files is not the same as sanitizing media. For business equipment, follow the approved disposal process: encryption status, wipe method, destruction vendor if used, asset tag, date, and who handled it.

This is boring paperwork until it becomes a breach conversation. Then everyone suddenly loves paperwork.

48 **C — Get help or use proper lifting equipment, and follow safety guidance.**

Safety questions are usually straightforward: do not hurt people. Heavy batteries, servers, monitors, printers, and racks can injure you if you try to be a hero.

Use team lifts, carts, rails, gloves, eye protection, and lockout/tagout procedures where appropriate. If you are not trained for electrical or facilities work, escalate.

49 **A — Disable accounts, revoke sessions, remove access, document actions, and coordinate with HR/security.**

Offboarding is a security process, not just a password reset. Depending on policy, you may need to disable the identity account, revoke cloud sessions, remove group membership, preserve mailbox/data, collect devices, and document the timeline.

Use a checklist. We have one here: employee offboarding for IT support.

50 **B — Document the change, verify scope, roll back if needed, and communicate the impact.**

A fix that creates another outage is not finished. Document what changed, who is affected, whether there is a rollback path, and what users should expect.

This is where operational procedures connect to troubleshooting. You are not only solving the technical problem. You are managing risk while solving it.

BONUS CHECKLIST 1

Windows Update Troubleshooting — One-Page Checklist

The ticket-ready version. Full walkthrough with repair-tool order and restart-loop handling: thisisanitsupportgroup.com/blog/windows-update-troubleshooting-checklist-it-support-2026

1 · Capture evidence before retrying

- [ ] Device name, Windows edition, version, and OS build
- [ ] Update name or KB number, exact error code and wording
- [ ] Failure stage: detection, download, install, restart, or post-update
- [ ] Scope: one device, one site, or many devices in the same ring
- [ ] Recent changes: VPN, proxy, security tool, storage, driver, policy

2 · Check management state

- [ ] Personal, domain joined, Entra joined, or RMM/MDM managed?
- [ ] Update approved for this deployment ring? Any deferral, pause, or maintenance window?
- [ ] Are peer devices in the same ring succeeding?
- [ ] Many devices failing together → stop one-off fixes, escalate as a shared incident

3 · The boring prerequisites (these close the most tickets)

- [ ] Stable AC power — never start firmware or feature updates on a weak battery
- [ ] Network path: personal VPN off, required corporate VPN on, proxy auth OK
- [ ] Free storage on the system drive (clean known-safe items only)
- [ ] Correct date, time, time zone, and sync source
- [ ] Save work, do ONE normal restart to clear pending operations

4 · One controlled retry, then supported repairs in order

- [ ] Retry from Settings once; capture the new error if it changes
- [ ] Run the built-in update troubleshooter; record what it changed
- [ ] Component health: `DISM.exe /Online /Cleanup-Image /RestoreHealth` then `sfc /scannow`
- [ ] Cache resets are a runbook step, not a first move — capture evidence first
- [ ] Restart loop? Check BitLocker recovery-key availability BEFORE entering recovery

5 · Close it properly

- [ ] Verify the update shows successful in update history
- [ ] Test sign-in, network, audio, and the user's primary application
- [ ] Restore any temporary changes and write notes another tech can continue from

BONUS CHECKLIST 2

Phishing Email Response — One-Page Checklist

First response for help desk, not full forensics. Full version with response lanes and copyable ticket notes: thisisanitsupportgroup.com/blog/phishing-email-response-checklist-it-support-2026

1 · Ask one question first: what did the user DO?

- [ ] Saw it only → low risk: preserve and report the message
- [ ] Clicked, entered nothing → medium: capture URL/time, check endpoint and browser alerts
- [ ] Entered password or MFA code → high: reset credentials, revoke sessions, escalate
- [ ] Opened or ran an attachment → high: isolate the endpoint, escalate
- [ ] Approved an unexpected MFA prompt → critical: contain the account immediately
- [ ] Sent money or banking changes → critical: contact finance through known channels

2 · Tell the user what NOT to do

- [ ] Stop interacting: no re-clicking, replying, forwarding, QR-scanning, or deleting
- [ ] If credentials or a file were involved: leave the device on and available
- [ ] Never ask the user to "show me exactly what you clicked"

3 · Preserve evidence

- [ ] Original email with full headers, message ID, sender and reply-to
- [ ] URLs (defanged — do not browse to them), attachment name/type/hash
- [ ] Exact timestamps for click, sign-in, MFA prompt, reply, or execution
- [ ] Use the report-phishing button or security mailbox, not normal forwarding

4 · Contain the right thing

- [ ] Credentials exposed: verify identity, reset password, revoke sessions and tokens, review MFA methods, check mailbox rules/forwarding/delegates/app consent
- [ ] Code ran: isolate via endpoint tooling; do NOT power off unless security directs it
- [ ] A password reset alone does not evict an attacker with a valid session token

5 · Check for wider impact, then close the loop

- [ ] Search other mailboxes for the same sender, subject, URL, or attachment
- [ ] Multiple users affected → it is an incident, not a single-user ticket
- [ ] Tell the user the outcome in plain language, and thank them for reporting

Want the rest?

This pack covers five A+ domains. There are more free practice sets, ranked practice-test reviews, and study plans on the site:

A+ study plan — thisisanitsupportgroup.com/blog/comptia-a-plus-study-plan-complete-guide-2026

Best A+ practice tests, ranked — thisisanitsupportgroup.com/blog/comptia-a-plus-practice-tests-ranked-2026

More practice questions (malware removal, operating systems, software troubleshooting, virtualization, Windows command line) — thisisanitsupportgroup.com/topics/it-certifications

More help-desk checklists (VPN, printers, slow computers, MFA resets, onboarding…) — thisisanitsupportgroup.com/blog

You're on the newsletter now, so new practice sets and checklists land in your inbox weekly. Found this useful? Forward it to a coworker who's studying.