Software Troubleshooting

CompTIA A+ certification, Core 1 (220-1201) and Core 2 (220-1202)

23% of the exam · 4 exam objectives · 220-1202

Domain 3 is about diagnosing software problems from their symptoms: Windows stop errors, boot and performance problems, services, profiles and time drift; mobile apps, updates, battery, connectivity and rotation; and the signs of malicious software on phones and PCs, from unofficial apps and rooted devices to ransomware, scareware and browser hijacking. The skill is to read the symptom, find the likeliest cause and choose the smallest fix that solves it.

You should be able to: A PC shows certificate warnings on every secure site, and an Android phone reboots at random but runs normally in safe mode. What should you check first on each?

Every exam objective: the key point and the trap

3.1 Given a scenario, troubleshoot common Windows OS issues.

A blue screen of death (BSOD) is a stop error. One that starts after a driver or update change points to that change: start in Safe Mode, then roll back the driver or uninstall the update. Repeated BSODs with no change point to hardware such as memory or the drive.

Trap: Jumping to a reset or reinstall of Windows when the symptom points to one driver, one service, one app or one profile. Match the size of the fix to the size of the problem.

3.2 Given a scenario, troubleshoot common mobile OS and application issues.

An application that fails to launch, close or update: force close it, clear its cache, restart the device, then update or reinstall it. Whole-device resets come last.

Trap: Recommending a factory reset for a problem limited to one app or one setting. Most mobile issues are fixed by a setting, a restart, free storage or reinstalling one app.

3.3 Given a scenario, troubleshoot common mobile OS and application security issues.

Security concerns: apps from unofficial stores or sideloaded skip the store's review; developer mode exposes settings such as USB debugging; root access (Android) or a jailbreak (iOS) bypasses the OS's protections.

Trap: Treating a security symptom as a performance one, for example buying more data or clearing the cache when the high traffic is coming from a malicious app.

3.4 Given a scenario, troubleshoot common personal computer (PC) security issues.

Common symptoms of malware on a PC: unable to access the network, desktop alerts, false alerts about antivirus protection, altered system or personal files (missing or renamed files, inability to access files), unwanted notifications within the OS and OS update failures.

Trap: Trusting a security alert because it looks official. A pop-up that sells an unknown antivirus product is the problem, not the solution.

Key terms

BSOD: Blue Screen of Death

UEFI: Unified Extensible Firmware Interface

NTP: Network Time Protocol

RAM: Random-access Memory

USB: Universal Serial Bus

NFC: Near-field Communication

MDM: Mobile Device Management

PUP: Potentially Unwanted Program

UAC: User Account Control

DNS: Domain Name System

ExamDragon, examdragon.com/aplus. Independent exam preparation, written in our own words to the 220-1202 exam objectives. CompTIA and A+ are trademarks of CompTIA, Inc.