TECH+ Exam Glossary

Find more at BareMetalCyber.com

1. **Access control**
   Access control is the set of rules and mechanisms that decide who can use a system or resource and what they can do with it. On Tech+, it shows up when you must pick the right basic safeguard (for example, limiting accounts or permissions) rather than relying on "security through obscurity."

2. **Access point (AP)**
   An access point is a device that provides Wi-Fi connectivity so wireless devices can join a network. On the exam, it often appears in "small office/home" network scenarios where you need to identify the correct device role or troubleshoot weak coverage and interference.

3. **Adapter**
   An adapter is a piece of hardware (or sometimes software) that allows two different interfaces or standards to work together (for example, USB-C to HDMI). Tech+ questions use adapters to test practical interface knowledge and to catch mismatches between ports, connectors, and what a user is trying to connect.

4. **Authentication**
   Authentication is proving an identity (for example, confirming a user is who they claim to be). It matters because many security questions hinge on recognizing that "logging in" is authentication, while actions after login depend on authorization.

5. **Authorization**
   Authorization is granting an authenticated identity permission to access specific resources or perform specific actions. On Tech+, it commonly appears as the reason someone can sign in but still cannot open a file, install software, or change a setting.

6. **Backup**
   A backup is a copy of data (and sometimes system state) kept so you can restore after loss, corruption, or ransomware. The exam tests whether you can distinguish file vs. system backups and choose local vs. cloud approaches in simple scenarios.

7. **Bandwidth**
   Bandwidth is the maximum capacity of a connection to carry data, usually described as a rate (like Mbps or Gbps). Tech+ uses bandwidth to test performance

thinking, such as why video calls stutter, downloads are slow, or a network link becomes a bottleneck.

8. **Binary**
   Binary is a base-2 numbering system that represents values using only 0 and 1. It's high-yield because Tech+ expects you to recognize common notational systems and relate them to computing fundamentals, storage, and troubleshooting context.

9. **Bluetooth**
   Bluetooth is a short-range wireless technology used for peripherals like headsets, keyboards, mice, and some IoT devices. On the exam, it shows up in connection and pairing troubleshooting and in choosing the right interface for a given device scenario.

10. **Browser cache**
    A browser cache stores local copies of web content to speed up repeat visits. Tech+ frequently tests when clearing cache is an appropriate troubleshooting step (for example, fixing display issues, stale pages, or odd website behavior) versus when it will not help.

11. **Chatbot**
    A chatbot is software that uses conversational input and output to answer questions or perform simple tasks, often using artificial intelligence features. On Tech+, it appears as a practical example of AI tools and you may need to choose an appropriate use case or recognize limitations like accuracy and context.

12. **Cloud computing**
    Cloud computing is delivering computing resources and services over a network instead of running everything on local hardware. The exam commonly tests whether you can distinguish common service models and deployment choices in plain scenarios rather than memorizing buzzwords.

13. **Command line interface (CLI)**
    A command line interface is a text-based way to interact with an operating system by typing commands instead of clicking through a graphical interface. It matters on Tech+ because you may be asked to recognize when a CLI tool is appropriate for basic tasks or troubleshooting.

14. **Compiled language**
    A compiled language is a programming language where source code is translated into machine-readable form before it runs. On the exam, this is usually contrasted

with interpreted or scripting languages as a category question about how code is executed and deployed.

15. **Confidentiality**
    Confidentiality means preventing unauthorized access to information. It shows up on Tech+ when you must pick the control that keeps data private, and it is commonly confused with integrity, which is about preventing unauthorized changes.

16. **CPU (Central Processing Unit)**
    The CPU is the main processor that executes instructions and drives general system processing. Tech+ uses CPU basics in hardware identification and performance reasoning, like matching symptoms to a likely bottleneck or component role.

17. **Data at rest**
    Data at rest is data stored on a device or storage system, such as a hard drive, SSD, or cloud storage. On Tech+, it typically appears in security scenarios where you choose protections like encryption to reduce exposure if storage is lost or accessed improperly.

18. **Data in transit**
    Data in transit is data moving across a network connection between systems or devices. It matters on the exam because you are often asked to pick protections like HTTPS or VPNs when the risk is interception while data is traveling.

19. **Database**
    A database is an organized collection of data designed for storage, retrieval, and management. Tech+ focuses on foundational distinctions like relational versus non-relational structures and how databases support queries and reports.

20. **Decimal**
    Decimal is a base-10 numbering system commonly used in everyday counting and measurement. On Tech+, it is tested as part of notational systems, usually alongside binary and hexadecimal, to confirm you can recognize which representation is being used.

21. **Default gateway**
    A default gateway is the router address a device uses to reach networks outside its local subnet. On Tech+, it shows up in “no internet” troubleshooting where local devices can talk to each other but cannot reach external sites.

22. **DHCP (Dynamic Host Configuration Protocol)**
    DHCP automatically assigns IP settings like IP address, subnet mask, default

gateway, and DNS servers to devices. The exam often tests symptoms of DHCP failure, like an incorrect address range or devices that cannot join the network reliably.

23. **Digital certificate**
    A digital certificate is an electronic credential that helps prove identity for systems and enables encrypted connections using public key cryptography. On Tech+, it commonly appears in web security scenarios where you must recognize why certificate warnings happen and what they imply.

24. **DNS (Domain Name System)**
    DNS translates human-friendly names (like a website name) into IP addresses that computers use to connect. It's high-yield because many troubleshooting questions hinge on whether the problem is name resolution (DNS) versus connectivity (routing) or service availability.

25. **Documentation**
    Documentation is recorded information about systems, configurations, procedures, and changes, such as network diagrams or troubleshooting notes. Tech+ uses it as a "best next step" concept, because good documentation reduces repeat incidents and speeds up problem isolation.

26. **Driver (device driver)**
    A driver is software that allows an operating system to communicate with a specific hardware component. On the exam, driver issues appear as devices not working, missing features, or instability after updates, and the right fix is often to install, update, or roll back a driver.

27. **Encryption**
    Encryption transforms readable data into an unreadable form unless the correct key is used to decrypt it. Tech+ tests when encryption protects data at rest or in transit and when it does not help, such as if an attacker already has valid access.

28. **Endpoint**
    An endpoint is a user-facing device that connects to a network, like a laptop, desktop, phone, or tablet. It matters on Tech+ because many security and troubleshooting decisions start with identifying the endpoint's role and exposure.

29. **Ethernet**
    Ethernet is a wired networking standard used for reliable local area network connections. On Tech+, it comes up in cabling, switch/router basics, and

performance troubleshooting where wired connections behave differently from Wi-Fi.

30. **Firewall**
    A firewall is a control that allows or blocks network traffic based on rules. The exam often uses firewall scenarios to test whether you can match symptoms to blocked ports, incorrect rules, or the difference between host-based and network firewalls.

31. **Firmware**
    Firmware is low-level software stored on hardware devices that helps them start up and operate, like BIOS/UEFI in a computer or code in a router. On Tech+, it shows up in update and troubleshooting scenarios where the fix is not an “app update” but a device-level change that can improve stability or security.

32. **Folder permissions**
    Folder permissions are rules that control which users or groups can read, write, modify, or delete files in a folder. Tech+ commonly tests situations where someone can access a system but cannot open or change a specific file location because the permissions are wrong.

33. **Frequency (wireless)**
    Frequency is the radio band used by wireless networks, such as 2.4 GHz or 5 GHz. On the exam, frequency is tied to range, speed, and interference, and you may need to pick the best band for coverage versus performance.

34. **Full backup**
    A full backup is a complete copy of the selected data set at a point in time. Tech+ uses it to test basic backup strategy tradeoffs, like longer backup windows and larger storage needs but simpler restores.

35. **GUI (Graphical User Interface)**
    A graphical user interface is the visual way users interact with software using windows, icons, and menus. On Tech+, the GUI is often contrasted with the command line to test which interface is more efficient or appropriate for a task.

36. **Hard drive (HDD)**
    A hard disk drive uses spinning platters to store data magnetically. It matters on Tech+ because HDD symptoms, performance characteristics, and failure modes are different from SSDs, and many questions test those practical differences.

37. **Hexadecimal**
    Hexadecimal is a base-16 numbering system that uses digits 0–9 and letters A–F. On

Tech+, it typically appears in contexts like MAC addresses, memory dumps, color codes, or other places where compact representation matters.

38. **Hotspot**
    A hotspot is a method of providing internet access over Wi-Fi, usually by sharing a cellular connection from a phone or dedicated device. Tech+ tests hotspot use in connectivity scenarios, including security implications like using strong passwords and avoiding sensitive work on untrusted networks.

39. **Incident response**
    Incident response is the organized process for detecting, handling, and recovering from security events. On the exam, it shows up as “what should happen next” thinking: contain, preserve evidence, communicate appropriately, and restore normal operations.

40. **Integrity**
    Integrity means ensuring data is accurate and not changed without authorization. Tech+ often tests integrity by contrasting it with confidentiality and availability, especially in scenarios involving tampering, corrupted files, or untrusted changes.

41. **IP address**
    An IP address is a numeric identifier that lets devices find and communicate with each other on a network. Tech+ troubleshooting often depends on recognizing whether an address is valid for the network, whether it changes dynamically, and whether two devices are accidentally using the same address.

42. **ISP (Internet Service Provider)**
    An internet service provider is the company that delivers internet connectivity to a home or business. On Tech+, this term appears when you must decide whether an outage is internal (local network equipment) or external (the service provider link).

43. **Malware**
    Malware is software designed to harm systems, steal data, or gain unauthorized access, including viruses, worms, and ransomware. The exam tests recognizing common symptoms and picking the first best defensive move, such as isolating an affected device and reporting through the right channel.

44. **MFA (Multi-Factor Authentication)**
    Multi-factor authentication requires two or more different types of proof, such as something you know plus something you have. Tech+ uses MFA as a core security control choice, and questions often test why MFA reduces risk even when passwords are weak or reused.

45. **NAT (Network Address Translation)**
    Network address translation lets many internal private IP addresses share a single public IP address on the internet. On Tech+, NAT shows up in small-network design and troubleshooting, especially when a device can reach local resources but has issues reaching external services due to router settings.

46. **Operating system (OS)**
    An operating system is the core software that manages hardware resources and provides services for applications. Tech+ emphasizes basic OS functions like accounts, updates, drivers, and common troubleshooting steps rather than deep internals.

47. **Patch management**
    Patch management is the practice of acquiring, testing, deploying, and tracking updates that fix bugs and security issues. On the exam, it appears as a governance and risk decision point: knowing when updates reduce risk and when unplanned updates can introduce instability.

48. **Phishing**
    Phishing is a social engineering attack that uses deceptive messages to trick users into revealing information or taking harmful actions. Tech+ tests your ability to spot red flags, choose the safest response, and understand why reporting is as important as deleting the message.

49. **RAID (Redundant Array of Independent Disks)**
    RAID is a way to combine multiple disks to improve performance, increase fault tolerance, or both, depending on the level used. Tech+ questions often focus on the purpose and tradeoff, especially the common confusion that RAID is not the same thing as a backup.

50. **VPN (Virtual Private Network)**
    A virtual private network creates an encrypted tunnel between a device and a network or service to protect traffic over untrusted networks. On Tech+, VPNs appear in remote access scenarios where you must pick the right security option and understand that a VPN protects data in transit, not the security of the endpoint itself.