GLOSSARY OF TECHNOLOGY TERMS

(#)

301 MOVED PERMANENTLY - This error code is used for permanent URL redirection. It indicates that the requested resource has been moved to a new location permanently...

302 FOUND (Moved Temporarily) - This error code indicates a temporary URL redirection. It tells the client that the requested resource can be found at a different location temporarily...

400 BAD REQUEST - This error code indicates that the server cannot understand or process the client's request due to malformed syntax or invalid parameters...

401 UNAUTHORIZED - This error code indicates that the request requires user authentication. The user needs to provide valid credentials, such as a username and password, to access the requested resource...

403 FORBIDDEN - This error code indicates that the server understood the request, but the user does not have permission to access the requested resource...

403.14 FORBIDDEN - This error code is specific to Microsoft Internet Information Services (IIS) and indicates that the web server is configured to deny access to the requested resource...

404 NOT FOUND - This error code indicates that the requested web page or resource could not be found on the server...

408 REQUEST TIMEOUT - This error code occurs when the server did not receive a complete request within the expected time frame. It can happen due to slow network connections or server overload...

429 TOO MANY REQUESTS - This error code indicates that the user has sent too many requests in a given amount of time. It is often used in rate-limiting scenarios to prevent abuse or excessive usage...

500 INTERNAL SERVER ERROR - A generic error message indicating that there was an issue with the server while trying to fulfill the request. It usually indicates a problem with the server configuration or an unexpected error occurred...

502 BAD GATEWAY - This error code typically occurs when a server acting as a gateway or proxy receives an invalid response from an upstream server. It indicates a temporary issue with the server communication...

503 SERVICE UNAVAILABLE - This error code indicates that the server is currently unable to handle the request due to being overloaded or undergoing maintenance. It is a temporary condition...

504 GATEWAY TIMEOUT - Similar to the 502 error, this code indicates a communication issue between servers. It occurs when a server acting as a gateway or proxy did not receive a timely response from an upstream server...

5G - The fifth generation of cellular network technology, offering significantly faster speeds, lower latency, and higher capacity compared to previous generations. 5G enables advanced applications like autonomous vehicles, remote surgery, and massive IoT deployments...

(A)

AIRPLANE MODE - A smartphone setting that disables all wireless communication features, including cellular, Wi-Fi, and Bluetooth...

ALGORITHM - A set of rules or instructions designed to solve a specific problem or perform a specific task. In the context of technology, algorithms are often used in programming and data analysis to process and manipulate data, make decisions, or automate tasks...

ANTIVIRUS - Software designed to detect, prevent, and remove malware from a computer system. Antivirus programs scan files and processes for known patterns and behaviors of malicious code...

APP (Application) - A software program designed to perform specific tasks or provide specific services on a smartphone. Apps can be downloaded and installed from an app store, offering a wide range of functionalities, such as social media, games, productivity tools, and more...

ARTIFICIAL INTELLIGENCE (AI) - The simulation of human intelligence in machines that are programmed to think and learn like humans. AI enables machines to perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and problem-solving...

ASCII (American Standard Code for Information Interchange) - A character encoding standard that represented alphanumeric characters, symbols, and control characters using a 7-bit binary code. ASCII was widely used in early computer systems...

AUGMENTED REALITY (AR) - A technology that overlays digital information, such as images, videos, or 3D models, onto the real world. AR enhances the user's perception and interaction with their environment by blending virtual elements with the physical world...

(B)

BACKDOOR - A hidden entry point or method intentionally built into a software or system to bypass normal authentication or security controls. Backdoors can be used by hackers to gain unauthorized access...

BASIC - Short for Beginner's All-purpose Symbolic Instruction Code, Basic was a

popular programming language used in the early days of personal computing. It was known for its simplicity and ease of use, making it accessible to novice programmers...

BATTERY - The power source of a smartphone that provides electrical energy to operate the device. Battery life refers to the duration a smartphone can function before requiring recharging...

BBS (Bulletin Board System) - A computerized system that allowed users to connect and interact with each other by posting messages, downloading files, and playing online games. BBSes were a precursor to modern online forums and communities...

BIG DATA - Extremely large and complex datasets that cannot be easily managed or processed using traditional data processing methods. Big data involves high-volume, high-velocity, and high-variety information, requiring advanced tools and technologies for analysis and extraction of valuable insights...

BIOMETRIC AUTHENTICATION - A security mechanism that uses unique biological or behavioral characteristics, such as fingerprints, iris patterns, facial recognition, or voiceprints, to verify and authenticate an individual's identity...

BLACK HAT HACKER - A malicious hacker who exploits vulnerabilities in computer systems and networks for personal gain, unauthorized access, data theft, or disruption. Black hat hackers engage in illegal activities...

BLOCKCHAIN - A decentralized digital ledger that records transactions across multiple computers. Each transaction, or block, is securely linked to the previous one, forming a chain. Blockchain technology provides transparency, security, and immutability, making it useful for various applications beyond cryptocurrencies...

BLUETOOTH - A wireless technology that enables smartphones to connect and communicate with other Bluetooth-enabled devices, such as headphones, speakers, smartwatches, and car audio systems, for data transfer and control...

BOOT DISK - A floppy disk or other storage media that contained the necessary files to start a computer and load the operating system. Boot disks were used when a computer failed to boot from its internal storage...

BOTNET - A network of compromised computers, often called "zombies" or "bots," under the control of a hacker or group of hackers. Botnets are commonly used for launching distributed denial-of-service (DDoS) attacks or spreading malware...

BROWSER - A software application used to access and view websites on the internet. Popular web browsers include Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari...

BSOD (Blue Screen of Death) - An error screen displayed by Microsoft Windows operating systems when a fatal system error occurs. It usually requires a system restart to resolve the issue...

(C)

CAMERA - The built-in digital camera on a smartphone, allowing users to capture photos and videos. Smartphones often have front and rear cameras with various features, such as autofocus, image stabilization, filters, and editing tools...

CELLULAR DATA - The wireless connectivity provided by a cellular network, allowing smartphones to access the internet, send and receive data, make calls, and send text messages when Wi-Fi is not available...

CENTRAL PROCESSING UNIT (CPU) - The primary component of a computer that performs most of the processing inside the computer. It executes instructions, performs calculations, and manages data movement...

CGA (Color Graphics Adapter) - A graphics standard used in early IBM-compatible computers to display color graphics. CGA supported a limited color palette and lower resolution compared to later standards...

CLOUD COMPUTING - The delivery of computing services over the internet, allowing users to access and utilize shared resources, such as storage, servers, databases, software, and applications, without the need for local infrastructure or physical storage...

CLOUD STORAGE - Online storage space that allows users to store and access files, photos, videos, and other data from their smartphones. Cloud storage services provide convenient backup, synchronization, and sharing options...

COMMAND LINE INTERFACE (CLI) - A text-based interface used to interact with a computer by typing commands. Users would enter specific commands to perform tasks or execute programs...

COMMAND PROMPT - A text-based interface in early operating systems where users could enter commands to interact with the computer. Command prompts provided direct access to the system's functionality and utilities...

CRACKER - A term sometimes used interchangeably with "hacker," but more commonly refers to individuals who break or circumvent software protections (e.g., copy protection, licensing systems) with malicious intent...

CRT MONITOR - Short for Cathode Ray Tube, a CRT monitor was the standard display technology used in older computer systems. It used electron beams to produce images on a glass screen...

CRYPTOCURRENCY - Digital or virtual currency that uses cryptography for secure financial transactions and control the creation of additional units. Cryptocurrencies, such as Bitcoin and Ethereum, operate independently of a central bank and rely on blockchain technology for transparency and security...

CYBERSECURITY - Measures and practices designed to protect computers, servers, networks, and data from unauthorized access, theft, damage, or disruption.

Cybersecurity aims to safeguard against various threats, such as malware, phishing, hacking, and other cybercrimes...

(D)

DATA ANALYTICS - The process of examining and interpreting large datasets to uncover patterns, trends, and insights. Data analytics involves using various techniques, such as statistical analysis, machine learning, and data mining, to extract valuable information from raw data...

DATA BREACH - The unauthorized access, acquisition, or disclosure of sensitive or confidential information held by an organization. Data breaches can lead to identity theft, financial loss, or reputational damage...

DATA MINING - The process of discovering patterns, correlations, and insights from large datasets. Data mining involves extracting useful information from raw data using various techniques, such as statistical analysis, machine learning, and pattern recognition...

DEEP LEARNING - A subfield of machine learning that focuses on artificial neural networks with multiple layers. Deep learning models learn from vast amounts of data and can recognize complex patterns and features, enabling advanced applications like image and speech recognition...

DENIAL-OF-SERVICE (DoS) ATTACK - An attack that aims to overwhelm a computer system, network, or website with an excessive volume of traffic or resource requests, rendering it inaccessible to legitimate users...

DIAL-UP MODEM - A device that allowed computers to connect to the internet through a telephone line. Dial-up modems used audio tones to establish a connection and offered slow data transfer speeds...

DNS_PROBE_FINISHED_NXDOMAIN - This error code indicates that the DNS server could not resolve the domain name requested by the client...

DOS (Disk Operating System) - An early computer operating system used in PCs, primarily in the 1980s and early 1990s. DOS required users to type commands into a command prompt to perform various tasks...

DOT MATRIX PRINTER - A type of printer that used a matrix of small pins to strike an ink ribbon and produce printed output. Dot matrix printers were noisy and produced low-resolution, dot-based characters...

(E)

EDGE COMPUTING - A computing paradigm that brings computation and data storage closer to the source of data generation, reducing latency and bandwidth usage. Edge computing enables real-time data processing and analysis at or near the edge of the network, enhancing efficiency and responsiveness...

ENCRYPTION - The process of converting data into a format that can only be read or understood by authorized parties. Encryption ensures the confidentiality and security of data, protecting it from unauthorized access or interception...

ERR_CONNECTION_TIMED_OUT - This error code indicates that the client's connection attempt to the server has timed out. It can happen due to network issues or unresponsive servers...

ETHERNET - A widely used standard for wired local area network (LAN) connections. Ethernet allows devices to communicate and share data through a network using cables and network adapters...

ETHICAL HACKER - Also known as a white hat hacker, an ethical hacker is a computer security professional who legally and responsibly identifies vulnerabilities and weaknesses in computer systems and networks to improve their security...

EXPANSION CARD - A circuit board that could be added to a computer to provide additional functionality or upgrade existing capabilities. Expansion cards were commonly used for tasks like adding extra memory, graphics, sound, or networking capabilities...

EXPLOIT - A piece of software or code that takes advantage of a vulnerability in a system or application to gain unauthorized access, control, or perform malicious actions...

(F)

FACTORY RESET - A process that restores a smartphone to its original factory settings, erasing all user data, settings, and apps. Factory resets are often performed to troubleshoot issues or prepare a device for resale...

FILE SYSTEM - The method used by an operating system to organize and store files on a storage device. It manages file naming, organization, access, and metadata, ensuring efficient storage and retrieval of data...

FIREWALL - A security device or software that monitors and filters incoming and outgoing network traffic based on predefined security rules. Firewalls protect networks and devices from unauthorized access and potential threats...

FLOPPY DISK - A portable magnetic storage medium that was used to store and transfer data in early computer systems. Floppy disks were flexible, square-shaped disks encased in a protective sleeve...

(G)

GPS (Global Positioning System) - A technology that uses satellite signals to determine the precise location of a smartphone. GPS enables navigation, location-based services, and mapping applications...

GRAPHICAL USER INTERFACE (GUI) - A visual interface that allows users to interact

with a computer using graphical elements, such as windows, icons, menus, and buttons. GUIs provide a user-friendly way to navigate and control software applications...

GREEN SCREEN - A monochrome computer display that used a green phosphor for text and graphics. Green screens were commonly found in early computer terminals and systems...

GREY HAT HACKER - A hacker who falls somewhere between the ethical and malicious spectrum. Grey hat hackers may exploit vulnerabilities without authorization but do so with the intention of notifying the affected organization or helping them secure their systems...

(H)

HACKER - An individual who explores and manipulates computer systems and networks to gain unauthorized access, exploit vulnerabilities, or acquire sensitive information. Hackers can be categorized as ethical (white hat), malicious (black hat), or somewhere in between...

HARD DISK DRIVE (HDD) - A storage device that uses magnetic storage to store and retrieve digital information. HDDs offer large storage capacities but are slower compared to solid-state drives (SSDs)...

HOME SCREEN - The main screen of a smartphone that displays app icons, widgets, and shortcuts. Users can customize their home screens by rearranging icons, adding widgets, and changing wallpapers...

HTML - Short for "Hypertext Markup Language," HTML is the standard markup language used for creating web pages. It defines the structure and content of web documents, including text, images, links, and multimedia...

(I)

INTERNET OF THINGS (IoT) - A network of interconnected physical devices, vehicles, appliances, and other objects embedded with sensors, software, and network connectivity, enabling them to collect and exchange data. IoT allows for seamless communication and automation between devices...

INTRUSION DETECTION SYSTEM (IDS) - A security system that monitors network traffic or system activities for potential security breaches or unauthorized access. IDS alerts administrators when suspicious activities are detected...

INTRUSION PREVENTION SYSTEM (IPS) - A security system that monitors network traffic in real-time and actively blocks or prevents unauthorized access or malicious activities. IPS goes beyond detection and takes proactive measures to protect the network...

(J)
N/A

(K)

KERNEL PANIC - A critical error that occurs in Unix-like operating systems when the kernel encounters an unrecoverable error. It often results in a system crash or freeze...

KEYLOGGER - A type of malware that records keystrokes on a computer or mobile device. Keyloggers capture sensitive information, such as passwords, credit card numbers, or other confidential data...

(L)
N/A

(M)

MACHINE LEARNING (ML) - A subset of artificial intelligence that enables computer systems to automatically learn and improve from experience without being explicitly programmed. Machine learning algorithms analyze and interpret data to make predictions or take actions, improving their performance over time...

MALWARE - Short for "malicious software," malware is a broad term encompassing various types of malicious software, including viruses, worms, Trojans, ransomware, and spyware. Malware is designed to harm or exploit computer systems and users...

MOBILE PAYMENT - The ability to make payments using a smartphone, typically through a mobile payment app or a digital wallet. Mobile payment services use Near Field Communication (NFC) or QR codes to facilitate transactions...

(N)

NETWORK SEGMENTATION - The practice of dividing a computer network into multiple smaller networks or subnetworks to enhance security. By isolating different segments, the impact of a security breach or unauthorized access can be limited...

NOTIFICATION - A message or alert displayed on the smartphone's screen to inform the user about new events, such as incoming calls, text messages, emails, social media updates, or app notifications...

(O)

OPERATING SYSTEM (OS) - 1. Software that manages computer hardware and software resources and provides common services for computer programs. Examples include Windows, macOS, Linux, and Android. 2. The software platform that manages the basic functions of a smartphone. Examples of smartphone operating systems include Android (Google), iOS (Apple), and Windows Phone (Microsoft)...

(P)

PAGE FAULT IN NONPAGED AREA - An error commonly encountered in Windows operating

systems when a program or process attempts to access a non-existent or invalid memory address...

PARALLEL PORT - A hardware interface that allowed computers to connect to peripheral devices, such as printers, using parallel communication. Parallel ports transmitted data in parallel, meaning multiple bits were sent simultaneously...

PASSWORD STRENGTH - The measure of the effectiveness of a password in resisting unauthorized access. Strong passwords typically include a combination of upper and lowercase letters, numbers, and special characters and are not easily guessable...

PATCH - A software update or fix released by vendors or developers to address security vulnerabilities, bugs, or performance issues in their software or operating systems. Regularly applying patches helps protect systems from known vulnerabilities...

PENETRATION TESTING - Also known as ethical hacking or white-hat hacking, penetration testing involves authorized attempts to identify vulnerabilities in a system or network by simulating real-world attacks. It helps organizations assess their security posture and identify areas for improvement...

PHISHING - A fraudulent technique where attackers impersonate legitimate entities or organizations to deceive individuals into revealing sensitive information, such as passwords, credit card details, or social security numbers...

PHREAKING - The act of manipulating or exploiting telephone systems to gain unauthorized access, make free calls, or engage in other fraudulent activities. Phreaking was prominent in the early days of telecommunications...

(Q)

QUANTUM COMPUTING - A type of computing that leverages quantum phenomena, such as superposition and entanglement, to perform complex computations at an exponentially faster rate than classical computers. Quantum computing has the potential to solve complex problems in fields like cryptography, optimization, and drug discovery...

(R)

RANDOM ACCESS MEMORY (RAM) - Temporary storage that holds data and instructions that are currently being used by the CPU. RAM provides fast access to data, allowing for efficient processing but is volatile, meaning it loses data when the computer is powered off...

ROBOTIC PROCESS AUTOMATION (RPA) - The use of software robots or artificial intelligence to automate repetitive, rule-based tasks and processes typically performed by humans. RPA aims to improve efficiency, accuracy, and productivity by reducing manual labor and human error...

(S)

SECURE SOCKETS LAYER (SSL) / Transport Layer Security (TLS) - Protocols that provide secure communication over the internet. SSL/TLS encrypts data transmitted between a web server and a user's browser, ensuring confidentiality and integrity...

SECURITY INCIDENT RESPONSE - The process of managing and responding to a security incident or breach. It involves detecting, analyzing, containing, eradicating, and recovering from security threats or incidents to minimize their impact...

SERIAL PORT - A hardware interface used to connect peripheral devices to a computer using serial communication. Serial ports transmitted data one bit at a time and were commonly used for devices like mice, modems, and early digital cameras...

SIM CARD - A small chip inserted into a smartphone that identifies the subscriber and provides cellular network connectivity. SIM cards store data such as phone numbers, contacts, and network settings...

SMARTPHONE - A mobile phone that offers advanced features and capabilities beyond traditional calling and texting. Smartphones typically provide internet access, multimedia capabilities, app support, and touchscreens...

SOCIAL ENGINEERING - The psychological manipulation of individuals to trick them into revealing sensitive information or performing actions that compromise security. Social engineering techniques include impersonation, deception, and exploiting human psychology...

SOLID-STATE DRIVE (SSD) - A storage device that uses flash memory to store data. SSDs are faster, more durable, and consume less power than HDDs, making them a popular choice for primary storage...

SQL INJECTION - A type of attack where an attacker injects malicious SQL (Structured Query Language) code into a vulnerable website's database query. SQL injection can lead to unauthorized data access or manipulation...

(T)

TOUCHSCREEN - The primary input method on most smartphones, where the screen detects and responds to the user's touch. Touchscreens allow users to navigate through menus, interact with apps, and input text by tapping, swiping, or using gestures...

TRACKBALL - An input device that resembled an upside-down mouse with a stationary ball on top. Users would roll the ball with their fingers or palm to move the cursor on the screen...

TWO-FACTOR AUTHENTICATION (2FA) - A security measure that requires users to provide two different types of identification or verification to access a system or account. It typically combines something the user knows (e.g., password) with something the user possesses (e.g., a unique code sent to their mobile device)...

(U)

URL - Short for "Uniform Resource Locator," a URL is a web address that specifies the location of a resource on the internet...

USER EXPERIENCE (UX) - The overall experience and satisfaction a user has when interacting with a product, system, or service. UX focuses on factors such as ease of use, intuitiveness, efficiency, and delight, aiming to enhance the user's interaction and meet their needs...

USER INTERFACE (UI) - The means by which a user interacts with a computer system, software, or application. UI encompasses visual elements, such as menus, buttons, icons, and graphical displays, as well as input methods, including keyboards, touchscreens, and voice commands...

(V)

VIRTUAL REALITY (VR) - A computer-generated simulation that immerses users in an interactive, artificial environment. VR typically involves wearing a headset that tracks the user's movements and displays a virtual world, creating a sense of presence and enabling realistic experiences...

VIRUS - Malicious software designed to infect computers and replicate itself. Viruses can cause damage to data, disrupt system operations, and spread to other computers...

VULNERABILITY - A weakness or flaw in a system's design, implementation, or configuration that can be exploited by attackers to gain unauthorized access or perform malicious activities...

(W)

WI-FI - 1. A wireless technology that allows devices to connect to a local area network (LAN) or the internet without the need for physical cables. Wi-Fi uses radio waves to transmit data between devices and access points. 2. A technology that allows smartphones to connect to local wireless networks for internet access. Wi-Fi offers faster speeds and is often used to conserve cellular data usage when a reliable Wi-Fi connection is available...

WORD PROCESSOR - A software application used for creating, editing, and formatting text documents. Early word processors, such as WordStar and WordPerfect, were popular before the emergence of graphical word processing software...

(X)
N/A

(Y)
N/A

(Z)

ZERO-DAY VULNERABILITY - A security vulnerability in a software or system that is

unknown to the software vendor or system administrator. Zero-day vulnerabilities can be exploited by hackers before the software developer can release a patch or fix...