TERRIFYING TERMINOLOGY

Use the link in the chat to access this list of terms

Active Directory (AD) – Microsoft's database and services that connect users with network resources. Systems administrators use AD Domain Services to support processes, objects, and services within a domain, and AD Sites and Services to configure and control user behaviors, computers, groups, IDs, and file and access permissions.

Artificial intelligence (AI) – Technology that enables a computer to think or act in a "human" way using reasoning, perception, problem solving, planning, and other aspects of machine learning. Cybercriminals are now using AI for threats like mass phishing and "smarter" malware.

Cloud – A technology that allows us to access our files or services through the internet from anywhere in the world. It is a collection of computers with large storage capabilities that remotely serve requests.

Credentials – Tools such as a Username and Password to verify a user's identity or authentication for an email account, Office 365, etc. Credentials can also confirm a user's identity in relation to a network address or other system ID.

Domain – The collection of users and computers on a local network or remote networks.

Domain controller (DC) – A server that responds to security authentication requests within a computer network domain, allowing host access to domain resources, authenticating users, storing user account information, and enforcing security policy for a domain.

Endpoint detection and response (EDR) – A cybersecurity technology that monitors an endpoint device, such as a mobile phone, laptop, or iPad to detect and respond to malicious cyber threats. EDR solutions are designed to detect and remove malware or any other form of malicious activity on a network.

Encryption – The process of encoding data so that it can be accessed only with a key.

Firmware – A type of software embedded into a device by the manufacturer to make the device run. Firmware often acts as a device's complete operating system, performing all control, monitoring and data manipulation functions.

Infrastructure – Also referred to as IT, local, or internal infrastructure; encompasses the hardware, servers, applications, operating systems, and network components such routers, switches, domain controllers required to support IT and computing services.

Malware – An umbrella term describing all forms of malicious software designed to cause harm, disclose information, or disrupt the stability of an IT computing and data storage system. Ransomware, viruses, worms, trojans, and spyware are common forms of malware.

Multi-factor Authentication (MFA) – An electronic method requiring a user to present two or more pieces of evidence, or factors, to an authentication mechanism to gain access to a website or application. MFA is also sometimes referred to as two-factor authentication.

Patch – A set of software changes that quickly resolves a bug or security vulnerability in software currently in use. A patch is also often called a "fix" or "bugfix."

Phishing – A form of social engineering-based scamming in which hackers deceive online victims into revealing sensitive information or installing malware of some kind. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted.

Security strategy – A set of cybersecurity measures to prevent unauthorized access to organizational assets such as computers, networks, and data. Such strategies often include regular system and application updates, plus management programs to ensure that security updates and patches are made as scheduled to protect sensitive information.