Multi-Factor Authentication (MFA)	A security measure requiring multiple forms of verification (e.g., password + mobile code).
Zero Trust Network Access (ZTNA)	A model that assumes threats exist inside and outside a network, requiring continuous verification.
Phishing	A type of cyberattack where criminals use deceptive communication, such as emails, to trick individuals into revealing sensitive information such as passwords, credit card details, or personal information [Bonus: Vishing is a similar type of attack where a scammer calls the victim and pretends to be from a legitimate source.
Firewall	A security solution that monitors and controls incoming/outgoing network traffic. Often offered "as-a-service" and managed by an IT partner.
Malware	Short for malicious software, refers to any intrusive software designed to harm or exploit IT networks or devices.
Ransomware	Malware that encrypts files and demands payment for decryption.
SIEM (Security Information and Event Management)	A system that collects and analyzes security data for threat detection.
EDR (Endpoint Detection and Response)	Security software that detects and responds to threats on endpoints such as laptops and servers.
XDR (Extended Detection and Response)	A security solution integrating multiple sources (endpoints, networks, cloud) for advanced threat detection.
MDR (Managed Detection and Response)	A security service providing continuous monitoring and response to cyber threats. Often paired with a SOC for additional protection.
IAM (Identity and Access Management)	A framework ensuring only authorized users can access sensitive systems and data.
Security Operations Center (SOC)	A team that monitors client environments and cybersecurity alerts to more quickly identify and stop cyber attacks.
CASB (Cloud Access Security Broker)	A security enforcement point that sits between an organization's on-premises infrastructure (or user devices) and cloud service and acts as a gatekeeper between the two.
DMARC	Domain-based Message Authentication, Reporting & Conformance is an email authentication protocol designed to protect organizations from email spoofing and phishing attacks.
SAT (Security Awareness Training)	Employee training that helps teach your team how to ID and respond to potential phishing and other social engineered threats.
Dark Web	Hidden, unindexed part of the internet where bad actors typically trade in stolen data.
Email Filtering	Automatically sorting and managing emails based on predefined criteria, identifying spam and malware, and preventing malicious content from reaching inboxes.