SECURE NETWORK TECHNOLOGIES
(833) 974-0015

50 Popular Cybersecurity Terms Everyone Should Know

1. **Firewall**
   A network security device or software that monitors and controls incoming and outgoing traffic based on predetermined security rules.
2. **Antivirus**
   Software designed to detect, prevent, and remove malware such as viruses, worms, and trojans.
3. **Phishing**
   Fraudulent attempts to obtain sensitive information, like passwords or credit card numbers, by pretending to be a trustworthy entity via email or other communication.
4. **Ransomware**
   Malware that encrypts a victim's data and demands payment for the decryption key.
5. **Malware**
   Any software intentionally designed to cause damage to a computer, server, or network.
6. **Encryption**
   The process of converting information into a code to prevent unauthorized access.
7. **Two-Factor Authentication (2FA)**
   A security process requiring two forms of identification before granting access to an account or system.
8. **Data Breach**
   An incident where unauthorized individuals gain access to sensitive or confidential data.
9. **VPN (Virtual Private Network)**
   A tool that creates a secure, encrypted connection over the internet, masking your IP address and protecting your data.
10. **Social Engineering**
    Manipulative tactics used by attackers to trick people into giving away confidential information.
11. **Zero-Day Vulnerability**
    A software vulnerability unknown to the vendor, leaving it unpatched and exploitable by attackers.
12. **Patch Management**
    The process of updating software to fix vulnerabilities and improve security.
13. **DDoS (Distributed Denial of Service) Attack**
    An attack that overwhelms a server with traffic, causing it to crash or become inaccessible.
14. **Penetration Testing (Pen Test)**
    Simulated cyberattacks performed to evaluate the security of a system or network.

15. **SOC (Security Operations Center)**
    A team responsible for monitoring and responding to cybersecurity threats in real-time.
16. **MFA (Multi-Factor Authentication)**
    A security method requiring multiple forms of verification, such as a password and a smartphone code.
17. **XDR (Extended Detection and Response)**
    A unified solution that integrates multiple security tools to detect and respond to threats across endpoints, servers, and networks.
18. **MDR (Managed Detection and Response)**
    A service that combines technology and human expertise to identify, investigate, and respond to threats.
19. **IoT (Internet of Things) Security**
    Protection for internet-connected devices like smart TVs and thermostats to prevent unauthorized access.
20. **Botnet**
    A network of compromised computers controlled by attackers to perform malicious activities.
21. **Insider Threat**
    Security risks originating from within an organization, often involving employees or contractors.
22. **SIEM (Security Information and Event Management)**
    A tool that collects and analyzes security data to detect potential threats.
23. **TLS (Transport Layer Security)**
    A protocol ensuring secure communication over the internet, often replacing SSL.
24. **SSL (Secure Sockets Layer)**
    An outdated protocol used to secure communication online, replaced by TLS.
25. **DNS Spoofing**
    An attack that redirects a website's traffic to a fraudulent site.
26. **Spyware**
    Software that secretly gathers information about a user without their consent.
27. **Adware**
    Software that displays unwanted advertisements, often bundled with free programs.
28. **Keylogger**
    A tool that records keystrokes to capture sensitive information like passwords.
29. **Trojan Horse**
    Malicious software disguised as legitimate to trick users into installing it.
30. **Brute Force Attack**
    An attempt to gain access to an account by systematically guessing passwords.
31. **Dark Web**
    A part of the internet that requires special software to access, often associated with illegal activity.
32. **Cyber Hygiene**
    Best practices for maintaining the security and health of devices and systems.

33. **Backup**
    A copy of important data stored separately to recover information in case of a cyber incident.
34. **Access Control**
    Techniques used to restrict access to systems and data to authorized users only.
35. **Trojan Horse**
    Malicious software disguised as a harmless application to trick users.
36. **Sandboxing**
    Running suspicious files or applications in an isolated environment to prevent harm to the system.
37. **Pharming**
    Redirecting users from a legitimate website to a malicious one without their knowledge.
38. **Password Manager**
    Software that securely stores and manages passwords for multiple accounts.
39. **Incident Response**
    The process of identifying, managing, and mitigating a security breach.
40. **Privileged Access Management (PAM)**
    Security controls for managing and monitoring access to critical systems.
41. **Cyber Threat Intelligence (CTI)**
    Information about potential or current cyber threats used to prevent attacks.
42. **Worm**
    Malware that replicates itself to spread to other computers without human intervention.
43. **Rootkit**
    Malicious software that allows attackers to gain administrator-level control over a system.
44. **Cybersecurity Framework**
    Guidelines and best practices for managing cybersecurity risks, like NIST or ISO 27001.
45. **Third-Party Risk**
    Security vulnerabilities introduced by vendors or partners who have access to your systems.
46. **Attack Surface**
    The total number of points where an unauthorized user can try to enter or extract data.
47. **Security Awareness Training**
    Programs designed to educate users about recognizing and avoiding cyber threats.
48. **Purple Teaming**
    A collaborative approach in cybersecurity where red teams (attackers) and blue teams (defenders) work together to improve an organization's security by identifying vulnerabilities and strengthening defenses through shared insights.
49. **Deepfake**
    AI-generated fake images, videos, or audio used for deceptive purposes.
50. **Endpoint Protection**
    Security solutions focused on protecting devices like laptops, smartphones, and desktops from threats.