Cybersecurity Glossary of Terms

Protect Your Business: Essential Cybersecurity

AwareSecureCo

Simple Definitions That Help You Take Action

Multi-Factor Authentication (MFA)

- **Definition:** A security process requiring two or more verification methods (e.g., password + code) to access an account.
- **Why It Matters:** Adds an extra layer of security, reducing the risk of unauthorized access.

Phishing

- **Definition:** A cyberattack where attackers trick users into providing sensitive information through fake emails, messages, or websites.
- **Why It Matters:** Phishing is one of the most common ways businesses get hacked–training employees to spot phishing attempts is critical.

Firewall

- **Definition: A security tool that filters and blocks unauthorized network traffic.**
- **Why It Matters:** Protects company systems from cyber threats by blocking malicious activity.

Ransomware

- **Definition:** Malicious software that locks files or systems and demands a ransom for their release.
- **Why It Matters:** Ransomware attacks can cripple businesses, leading to financial and reputational damage.

Social Engineering

- **Definition:** A manipulation technique where attackers trick individuals into revealing confidential information.
- **Why It Matters:** Cybercriminals often exploit human psychology rather than technical vulnerabilities to gain access to sensitive data.

Encryption

- **Definition:** The process of converting data into a coded format to prevent unauthorized access.
- **Why It Matters:** Protects sensitive information from hackers, especially during data transmission.

Document 8 of 8 - Cyber Sorted: Foundations

VPN (Virtual Private Network)

- **Definition:** A tool that encrypts internet traffic, making online activities more private and secure.
- **Why It Matters:** Essential for securing remote work and protecting company data from cyber threats.

Zero Trust Security

- **Definition:** A security model that requires continuous verification for all users and devices, assuming no one is automatically trusted.
- **Why It Matters:** Prevents unauthorized access by ensuring only verified users can access business systems.

Brute Force Attack

- **Definition:** A hacking method where attackers try multiple password combinations until they guess correctly.
- **Why It Matters:** Weak passwords make businesses an easy target–using strong, unique passwords helps prevent this type of attack.

Malware

- **Definition:** Malicious software designed to harm or exploit systems, including viruses, worms, and spyware.
- **Why It Matters:** Can cause system failures, steal data, and allow attackers to control company devices.

Patch Management

- **Definition:** The process of updating software to fix security vulnerabilities.
- **Why It Matters:** Regular updates prevent cybercriminals from exploiting outdated systems.

Insider Threat

- **Definition:** A security risk posed by employees, contractors, or vendors who intentionally or unintentionally compromise company security.
- **Why It Matters:** Insider threats account for a significant number of security incidents, making employee awareness crucial.

Data Breach

- **Definition:** An incident where sensitive information is accessed or exposed without authorization.
- **Why It Matters:** Data breaches can lead to financial loss, legal issues, and reputational damage for businesses.