7 Top Email Security Terms You Should Know

2FA: 2 Factor Authentication

Also known as MFA (multi-factor authentication). Any combination of 2 or more tangible authenticators to allow access to private online accounts or devices.

Even if a password has been compromised, these additional steps will prevent immediate access.

APT: Advanced Persistent Threat

An APT is a systematic cyberattack using multiple tactics to overload existing security measures over time. Hacking into email accounts is a common method used. Basic security strategies are usually not enough to stop these kinds of attacks.

Data Loss Prevention

The proactive efforts to detect and dismantle security threats and violations before they result in compromised accounts and data loss.

Encryption

Emails sent from one user to another and other types of private data are scrambled until they are incomprehensible, only to be reassembled with the use of a key. There are several different types. Email encryption is helpful for keeping emails safe while they are sent, transferred, and received. Every organization should have an encryption system in place to prevent hacks and data loss.

Phishing

Hackers use this method to obtain sensitive information and data, usually through emails that seem legitimate, but trick recipients into clicking links or replying with private information or passwords.

Ransomware

Cyberattacks that encrypt files on a device, rendering them unreadable and unusable, then demand money in exchange for decryption. Often activated when users open an attachment that compromises their files and data.

Spoofing

A cyber attack that uses fake information that seems legitimate, such as email addresses or domain names, to get users to divulge important information or wire money, etc.

CNP TECHNOLOGIES