

# CYBER SECURITY GLOSSARY OF TERMS



**BEC (Business Email Compromise)** – Business Email Compromise, which heavily relies on social engineering tactics to trick unsuspecting employees and executives. BEC is common in a typical wire fraud scheme.

**Deepfakes** – Utilizing AI technology and machine-learning techniques to cunningly mimic videos, pictures, or sheer voices of actual people.

**Malware** – Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

**Man in the Middle Schemes** – A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

**Money Mules** – A money mule is someone who transfers or moves illegally acquired money on behalf of someone else. Criminals recruit money mules to help launder proceeds derived from online scams and frauds or crimes like human trafficking and drug trafficking. Money mules add layers of distance between crime victims and criminals, which makes it harder for law enforcement to accurately trace money trails. Money mules can move funds in various ways, including through bank accounts, cashier’s checks, virtual currency, prepaid debit cards, or money service businesses.

**Pharming** – Directing you to a bogus website that mimics a legitimate one.

**Phishing** – Sending fraudulent emails that purport to be from a legitimate source, and designed to trick you into revealing passwords or other sensitive information. Phishing messages are bulk emails, typically appearing to be from a reputable source, that ask you to take a specific action that can cause damage to you or your organization. These messages are malicious.

**Ransomware** – Attackers infiltrate the user’s computer using some type of malware that restricts access to the infected computer system in some way. The data is then encrypted and the user is asked to pay money in order to regain access to the computer. Best defense to this type of attack: back up system regularly.

**Data exfiltration:** A form of a security breach when data is copied, transferred or retrieved

**Double extortion:** Response “No thank you. Well, we’ve exfiltrated your data and will publish on the Internet.”

**Smishing** – Text messages designed to do the designed to do the same as phishing.

**Spoofing** – Sending fraudulent emails that purport to be from a legitimate source; A disguised form of communication, e.g., email, phone calls, or website, from a source that might be known or trusted on a specific file, e.g., source is known to the transaction but the email for the source has been changed (spoofed).

**Spam** – Unsolicited and unwanted email, typically sent to try to sell you something. While it is often annoying and misleading, it is rarely malicious. Phishing messages are bulk emails, typically appearing to be from a reputable source, that ask you to take a specific action that can cause damage to you or your organization. These messages are malicious. Spear phishing emails are targeted attacks on a person or organization, occurring after detailed research in order to make them seem especially real. These messages are extremely malicious and can lead to very damaging consequences. Simply delete them!



**Spear Phishing** – Emails are targeted attacks on a person or organization, occurring after detailed research in order to make them seem especially real. These messages are also extremely malicious and can lead to very damaging consequences.

**Vishing** – Telephone call or message designed to trick you, similar to phishing.

**Whaling** – A type of phishing attack specifically aimed at a high-profile target, like a senior executive or a high-ranking government official. Since these types of targets are more likely to have access to confidential information, the stakes can be much higher than a generic phishing attempt.

**For more information, reach out to your Agency Advisor today!**

building partnerships together

— The CATIC Family Of Companies —

