Cyber fraud terms you should know

Cyber criminals are getting more creative and less obvious—which means we need to stay vigilant and educated. We put together this list of some top fraud terms to help you stay up to date on cybersecurity terminology.

1. Advanced persistent threat (APT)

A targeted attack that penetrates a network without detection and maintains access for a period of time, all while monitoring information or stealing resources. APTs may continue for years.

2. Business email compromise (BEC)

Also known as email account compromise (EAC), this is a sophisticated scam that targets both businesses and individuals and exploits the fact that so many of us rely on email to conduct business—both personally and professionally. In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request and prompts payment to an unauthorized recipient. They attempt to bypass inbound email security controls and ensure successful delivery of malicious email campaigns. Tactics are also used to obtain sensitive information that may result in identity theft and financial loss.

3. Data exposure

Occurs when sensitive data is either intentionally or unintentionally available to the public. This form of compromise is often the result of a threat actor publishing data obtained illegally or a negligent systems administrator or developer simply leaving data in public view.

4. Exfiltrated data

Illegal transfer of an organization's data as the result of a cyberbreach, such as a ransomware attack.

5. Malware

A generic term for several different types of malicious software that perform malicious activity. This may include stealing sensitive information, locking the computer and demanding a ransom (see **Ransomware**), or even giving the attacker complete control over the affected system.

6. Multifactor authentication (MFA)

A method of verifying a user's identity that relies on more than one set of security credentials. There are three categories of credentials: something you either know, have or are. In order to gain access, your credentials must come from at least two different categories.

7. Phishing

Social engineering through emails using known information about the target to acquire other data such as usernames, passwords or financial information. **SMiShing** via text (SMS) and **Vishing** via phone (voice) are other forms of attack.

8. Ransomware

A type of malware that restricts access to data and demands that a payment be made to the attacker to restore access.

9. Spear phishing (see also BEC/EAC)

An email scam that uses social engineering to steal information or install malicious software on a system.

10. Zero-day vulnerability (and exploit)

A previously unknown software security flaw that has been discovered by malicious actors before legitimate security researchers have had a chance to find and fix it. A "zero-day exploit" is a method for using a zero-day vulnerability to attack a victim's computer.

TD Bank

America's Most Convenient Bank®

Member FDIC | TD Bank, N.A.