Top 3 Phishing Attacks

And How to Defend Against Them

Phishing

What is Phishing?

Phishing is a technique used by hackers to impersonate a trustworthy entity in an email. Attackers use phishing emails to obtain sensitive information such as usernames, passwords, or banking credentials. They distribute malicious links and attachments to trick users into downloading malware or ransomware. These attacks are usually sent in large numbers to business users and consumers—more or less at random—with the expectation that only a small number will respond.

How to Block Phishing Attacks

Anti-phishing solutions use a combination of techniques to detect and prevent phishing attacks. They check the reputation of the domain and sender, see if a sender or link within an email was used in previous phishing campaigns, scan websites for malicious downloads, add link protection to block links that may become malicious over time, and compare the body of the email to previous messages that were categorized as malicious.

Spear Phishing

What is Spear Phishing?

Unlike mass phishing attacks, spear-phishing emails are carefully designed for a specific individual to get them to respond. Attackers invest time in researching these individuals and their organizations to craft a personalized message—and only send very few messages at a time. These attacks come from high reputation sender addresses or already compromised accounts and often contain zero-day, never used before links that don't appear obviously malicious to most security protection solutions. Hackers rely on these highly effective spear-phishing attacks to steal credentials or infect devices with malware.

How to Block Spear Phishing attacks?

Spear-phishing attacks often are able to bypass traditional security gateways, which mostly rely on reputation analysis, blacklists, and look for malicious payloads. To block spear-phishing attacks, a security solution needs to include an intelligent, context-aware technology to identify anomalies in the content of the email. These anomalies can include mismatch between sender identity and email address, expressions commonly used in phishing attacks, suspicious call to actions, and links that are anomalous to the context of the email.

Business Email Compromise

What is Business Email Compromise (BEC)?

BEC attacks—also known as CEO fraud, whaling, or wire transfer fraud—impersonate an employee within the organization in order to defraud the company, its employees, customers, or partners. In most cases, attackers will focus their efforts on employees with access to company's finances or personal information and trick individuals to perform wire transfers or disclose sensitive information. These attacks utilize socially engineered tactics, compromised accounts, and often have no attachments or links.

How to Block BEC?

Similar to spear phishing, relying on an email gateway is not enough to detect and block BEC. Organizations need technology that does not rely on static rules to detect these targeted attacks, rather a solution that provides analysis of its historical communication patterns and visibility into internal email communication. This helps to determine with a higher degree of accuracy whether a certain email is part of a BEC or account takeover.

Barracuda Solutions for Phishing, Spear Phishing and Business Email Compromise

Comprehensive, elegantly simple protection against phishing and other email-borne threats for your users, brand, and business.

ESS Barracuda Essentials + **SEN** Barracuda Sentinel + **PL** Barracuda PhishLine + **FIR** Barracuda Forensics