Trustifi

WHITE PAPER

Why Legacy Secure Email Gateways Can't Catch Phish

And how to keep your organization safe from email borne attacks

www.trustifi.com

Phishing scams account for 95% of businesses' losses from cybercrime. While SEGs (Secure Email Gateways) may claim to protect emails from all possible threats, they unwittingly send infected emails to users, just waiting for them to act. Since the invention of email, phishing has evolved continuously, and hackers have been finding new ways to infiltrate users' inboxes and trick secure gateways.

Why can't SEGs catch Phish? Here are a few reasons:

Focus on active, ongoing attacks

The purpose of secure email gateways is to prevent active, ongoing attacks. In the latest incarnation of phishing threats, however, the attacks are initiated and terminated instantly, before their profiles can be detected by the SEG.

Filter high-volume spam

SEGs are built to detect high-volume spam. Phishing attacks, on the other hand, tend to be low volume, targeted, and slow, which facilitates their penetration through the SEG.

Cannot recognize adept imposters

Imposter emails that don't appear to be malicious cannot be blocked or quarantined by SEGs. In a phishing attack, the attacker spoofs an identifiable sender, vendor, or website to trick the secure email gateway into believing they are a trusted source.

Species of Phish

Business Email Compromise (BEC)

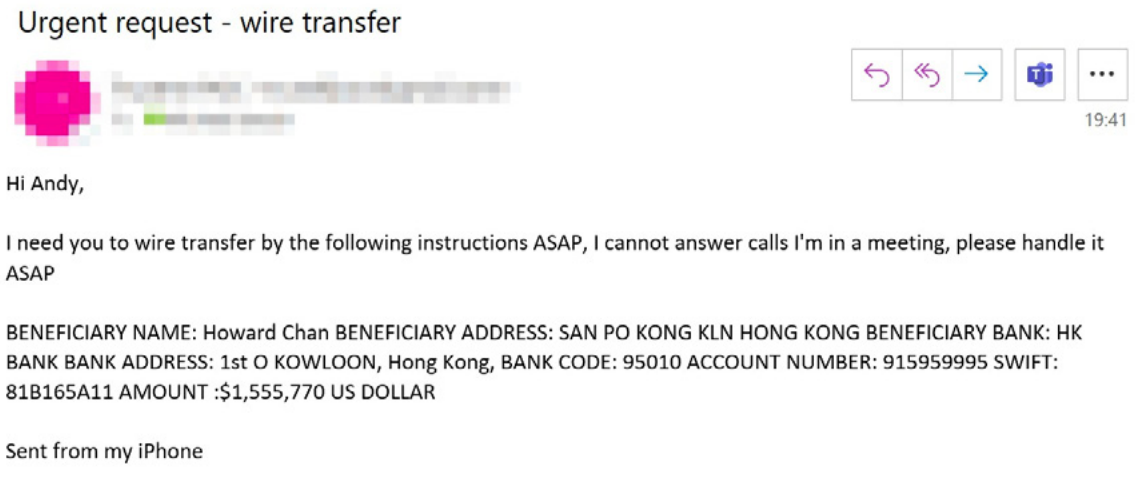
Business email compromise involves sending a fraudulent email to a business to defraud them. Businesses that conduct wire transfers with suppliers overseas are the most susceptible to BEC attacks. Through either keyloggers or phishing, an attacker spoofs or compromises the openly available email accounts of senior executives associated with finance or involved in wire transfers. Masquerading as an authorized individual, the attacker dupes the targeted user into making fraudulent transactions. Phishing attacks caused by BEC result in companies losing thousands of dollars.

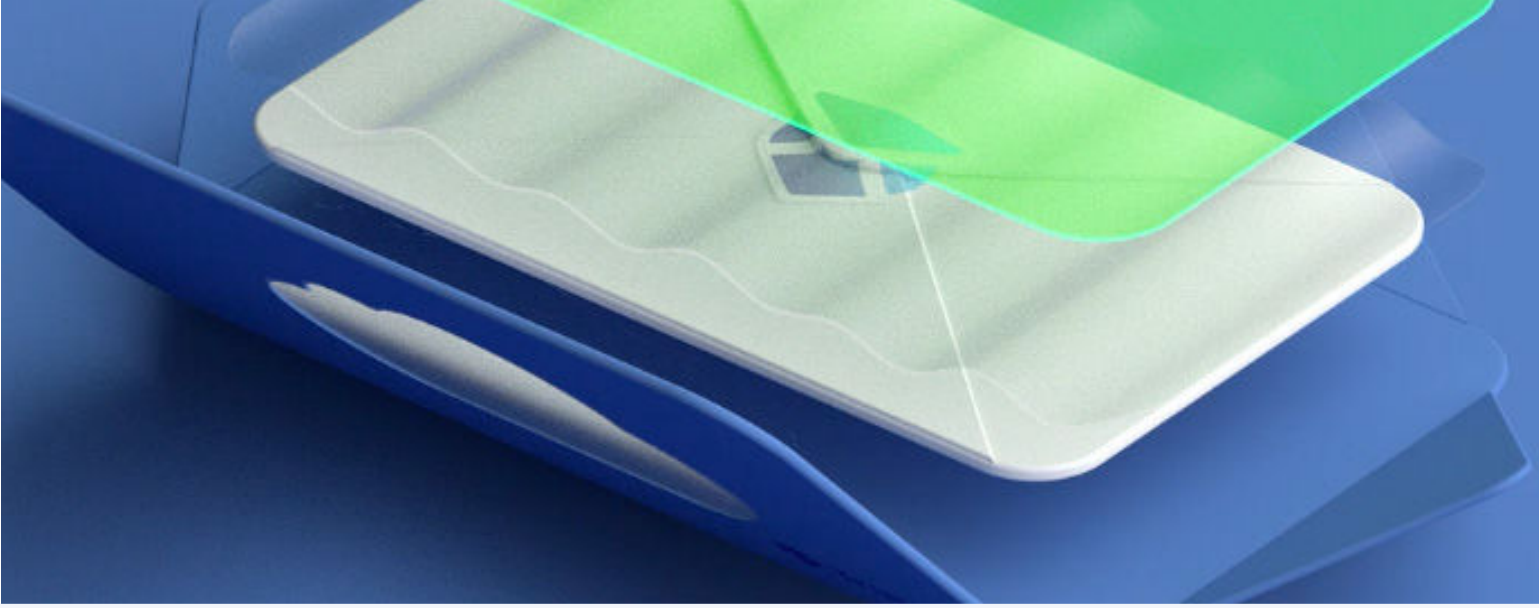
BEC Attack Examples

Example 1. An attacker impersonated a supplier to manipulate an employee of a company, persuading him to pay a $24.5 Million invoice. The attacker sent seven BEC phishing messages over a course of 20 days. SEG defenses at the company were not enough to stop the emails.

Example 2. The employees of Nikkei America, a subsidiary of one of Japan's largest publishing companies, were duped into making a wire transfer to a bank account the attackers controlled. Using fake information, the scammers posed as Nikkei executives. The company lost approximately $29 million.

Example 3: Urgent Request for a Wire Transfer:





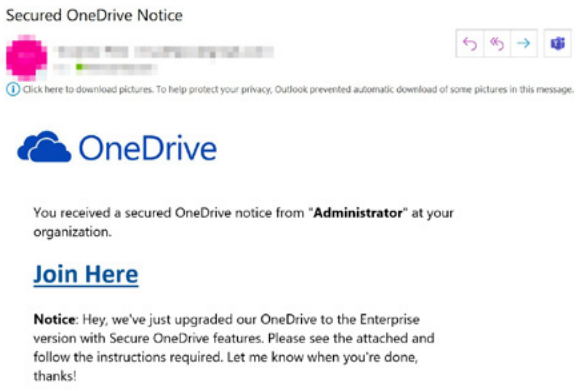
Spear Phishing

Spear phishing is a targeted email scam where an attacker attempts to steal sensitive information from a specific recipient, business, or organization for malicious purposes. The attack is often carried out using the victims' personal details, such as their friends, employers, hometowns, places they visit frequently, and their online shopping behavior.

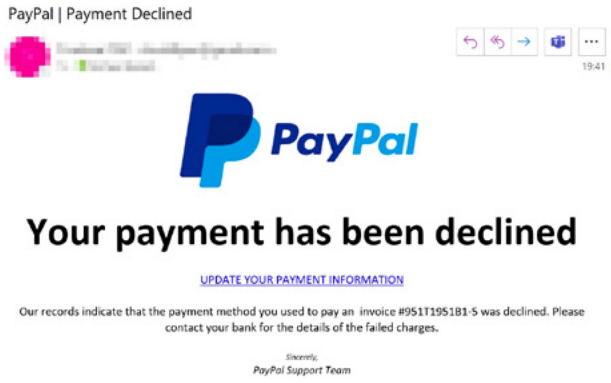
Spear Phishing Example

The Naples City Council claims a highly advanced spear phishing attack was responsible for a $700,000 hack. According to a news release, the attacker provided a fake bank account to receive the funds. The fake account was associated with a construction company working on a project in downtown Naples at the time.

Example: Microsoft OneDrive Phish Scam



Example: Paypal Phish Scam



Fighting Phishing Attacks

Even after spending millions on cybersecurity, most companies remain vulnerable to phishing attacks that penetrate all defenses and reach directly into the users' inbox These attacks result in monetary loss, data theft, and reputation destruction.

SEGs can't keep up with attack innovations

- **Signature-based detection**

  SEGs use signature-based detection, which is useless since the latest sophisticated malware is low-volume, multifaceted, and targeted.

- **Reputation-based detection**

  SEGs rely on reputation-based detection, which is ineffective due to the latest methods used by the threat actors. An imposter or spoofed email, domain, account, or website can be established within 24 hours, and the attack can be launched and terminated in just a few hours. Their sophistication is one of their biggest advantages.

  SEG add-on threat-protection services that scan attachments and URLs are expensive and delay user access to legitimate files and websites, reducing employee productivity.

Cloud-based SEGs Don't Scale

As inboxes move to the cloud, SEGs are moving there as well. Cloud-based SEGs, however, are basically virtualized appliances that are hosted and managed in the cloud. They share similar functionality and performance limitations with on-premises SEGs.

Humans Make Poor Firewalls

According to a recent study, 15% of highly trained employees fell for a simulated attack by opening suspicious emails and clicking the malicious links or attachments. Your defense solution must stop phishing attacks from getting into user inboxes, since a single slip can spell major trouble. Humans cannot be relied on to block every phishing attack. It is impossible to eliminate the phishing problem simply by educating your employees. You might reduce the attacks but not completely eliminate them with education. Even educated users take the bait once in a while. Therefore, you need to empower your education with advanced anti-phishing technology.

Defending against Malware and Ransomware

Malware-infected files can slip through cyber defenses because hackers use a variety of techniques. A victim can be tricked into clicking on a URL provided in a social post or email that downloads a malicious document containing malware.

Defenses against such attacks rely on the ability to retrieve remotely linked files and email attachments, accompanied by powerful algorithms that are able to detect malicious code hidden within files. More sophisticated defenses can also open compressed files and password-protected documents and examine their contents for malicious code.

Organizations that rely heavily on SEGs pay a lot for the service, but SEGs will not keep your company safe from constant phishing attempts. Today's attackers are so sophisticated that they make legacy defenses look comical.

A multi-layer anti-phishing solution is recommended by Gartner

Traditional email security solutions eliminate known phishing sites, but they aren't aware of the latest sophisticated or previously unknown malicious sites and malware. To protect your mailbox from advanced and complex phishing attacks, a multilayered anti-phishing solution is an absolute necessity. In a paper by Gartner® titled "*How to Build an Effective Email Security Architecture*" a multi-layered anti-phishing solution was recommended to reduce cyber threats.

The Gartner paper cites a Verizon study. According to Verizon, social incidents and security breaches are caused 98% by phishing and 93% by pretexting. A recommended architectural approach to deal with the magnitude of recent email threats is presented in the *Gartner paper*. The recommendation addresses BEC, suspicious URLs, malware, and credential phishing.

The New Solution to Phishing Attacks

Your technology must outsmart attackers. It can be a major challenge for organizations to protect themselves against advanced email threats. Outdated technologies like legacy systems and secure email gateways can be complex, expensive, and when used without an added layer of protection, will often struggle to block sophisticated malicious emails and social engineering attacks.

Keep your organization safe from targeted threats with powerful multi-layered scanning technology. Deeply analyze, detect, and classify the most advanced Phishing, Malicious, SPAM and even Gray emails. Easily deployable and convenient to use, Trustifi Email Security is the leading cloud-based email security solution.

Trustifi's Inbound Shield imposes a layer of protection between your email system and the outside world. Using Artificial Intelligence (AI) and dynamic engines, Inbound Shield readily identifies and blocks suspicious inbound emails. In addition to scanning and eliminating malicious content, the Inbound Shield looks for a host of anomalies, including:

- ✓ **Imposters sending messages from falsified domains.**
- ✓ **Requests for money transfers and confidential information.**
- ✓ **Links to impersonated websites.**

  - Phishing
  - Spoofing
  - Impersonation
  - Business Email Compromise
  - Malware
  - New Threats, like Zero-Day

Trustifi

While Trustifi's Inbound Shield keeps suspicious emails out of the users' inboxes, their Email Encryption and Data Loss Prevention services keep your company ahead of the criminals. **Contact Trustifi today** to see a demo and learn how quickly you can have state-of-the-art phishing protection.

www.trustifi.com
sales@trustificorp.com