Respond Quickly to Identity Compromise

Challenge

Empowering your employees in data security

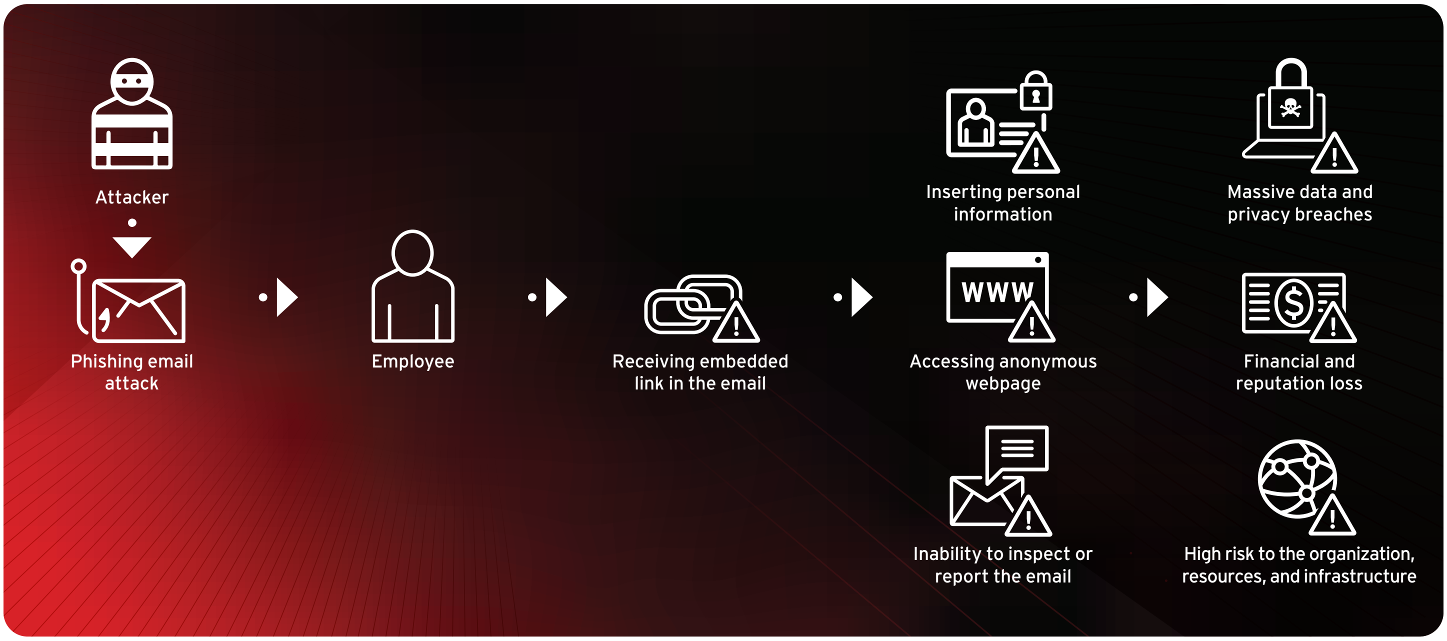
Employee risk is evolving at an accelerated rate. To protect their digital footprint from web- and cloud-enabled threats, businesses have been investing in modern security awareness solutions as part of organizational culture. The priority, when starting at an employee level, is to identify and understand the high-risk threats of phishing emails that include clickable attachments, cloned websites, fake social posts, and instant messaging invites.

Phishing attempts, social engineering, and malicious attachments introduce a high risk to your company. Educating your employees with proper knowledge on handling such events, such as properly reporting possibly malicious emails immediately, is the first step towards reducing cyber risk. However, no amount of prevention is 100% bulletproof. Your IT team needs modern technology to inspect loaded pages and scan all attachments for threats without causing friction within your organization's environment.

Phishing attacks on the rise

The advancement of social engineering and artificial intelligence (AI) has made phishing emails look more legitimate than ever before. Techniques have become more personalized, targeting specific individuals across your organization, including executive management and their assistants, directors, managers, as well as departmental staff across IT, legal, and HR, and partner channels. The primary focus is to persuade your unsuspecting employees to divulge sensitive information or install malware.

The simplest yet most effective phishing email attack includes a malicious message containing a link that directs your employees to a webpage where they are prompted to insert their personal information (ID, username, password) or credit card number. Such cyberattacks are highly coordinated, advanced, and executed in multiple steps. This can lead to massive data and privacy breaches, infected devices and systems, and in turn, ransomware payouts for the threat actor.


Attacker
Phishing email attack
Employee
Receiving embedded link in the email
Inserting personal information
Accessing anonymous webpage
Inability to inspect or report the email
Massive data and privacy breaches
Financial and reputation loss
High risk to the organization, resources, and infrastructure

The phishing attack process

IT security risks

Phishing attacks are designed to gain access to sensitive information or infrastructure. Even if the attacker compromises a low-privileged individual, it opens the door for them to perform attack techniques by convincing your employees to launch malware or an internal phishing attack to gain high-level privileges. Internal phishing is attractive to threat actors because it leverages the trust others already have in the compromised user. Using a legacy approach of only deploying email scanning with an email gateway bypasses all internal email traffic and, thus, is ineffective at catching internal threats.

IT security risks increase when your employees cannot accurately differentiate between marketing and phishing emails, while your IT team are unable to view and successfully filter email threats. A multi-layered email security approach with rules to holistically track traffic and stop malicious actions in real-time is needed to mitigate these risks.

To support ongoing business operations, your IT team needs to instill a balanced approach. An overly restrictive acceptable use policy (AUP) will prohibit productivity. Instead, embedding a notification at the top of incoming emails to notify your employees if their communication is coming from an "internal" or "external" source can strengthen awareness without limiting productivity. This approach requires modernizing and constantly reviewing IT security operations and access policy controls with zero trust-providing flexibility for employees and business needs and ensuring effective communication as part of employee security awareness and training initiatives.

Capabilities

Modernizing business approach with robust security

The objective is to allow your business to thrive while keeping it safe from cyber threats. This includes securing employee information through various digital communications, like emails, web browsing, and applications accessed over the internet. However, this becomes more difficult as your company grows and your organization's threat surface widens—for example, from an increased work-from-home labor force. Therefore, multi-layer security measures with unified policies and simplified controls are essential. Besides the growth and change in workforce practices, the rising complexity of email phishing and web threats have shifted the solution against internet threats from a traditional security operations approach to advanced architectures such as zero trust. Applying this modern approach allows businesses to lower employee and IT security risks, constantly assess access control, gain insights into traffic, set permissions, and increase awareness.

Becoming proactive in threat detection

Trend One, our unified cybersecurity platform, introduces proactive security measurements and control, so your organization can detect, filter, track, and stop actions before and after an incident occurs. This is achieved by leveraging our email gateway, cloud application access control, and secure web gateway (SWG) capabilities to support strategic employee security awareness and training initiatives. IT effectiveness can be achieved with help from the following tools, capabilities, and best practices:

- **Visibility and control**: Leveraging the secure web gateway (SWG) and cloud access security broker (CASB) technologies, provides a view into all web traffic, as well as web application usage details, including files stored or the emails sent.
- **Performance**: Global points of presence (PoPs) on a powerful cloud infrastructure increases the speed of inspecting SSL traffic, scanning for malware at download, and recognizing data loss prevention (DLP) infractions—with minimal latency.
- **Agility and scalability**: Our cloud-native web gateway technology allows you to scale faster than traditionally available on-premises web gateways—and with no downtime. This enables you to handle large virtual events or to support work-from-home initiatives without compromising security, visibility, and control.
- **Layered security**: Our integrated capabilities provide protection at multiple layers, both in transit and at rest, against phishing, spam, and potentially risky messages with multiple techniques, including sender content and image analysis and machine learning.

Moving beyond the boundaries

By leveraging proven technology through the lens of Trend Vision One™, not only are the email gateway, cloud application access control, and SWG capabilities present, but the wider ecosystem is able to provide additional data. This allows for the identification of compromised accounts, automated access decision-making, rich telemetry, reporting visibility, and API integrations, along with simple and consistent policy control.

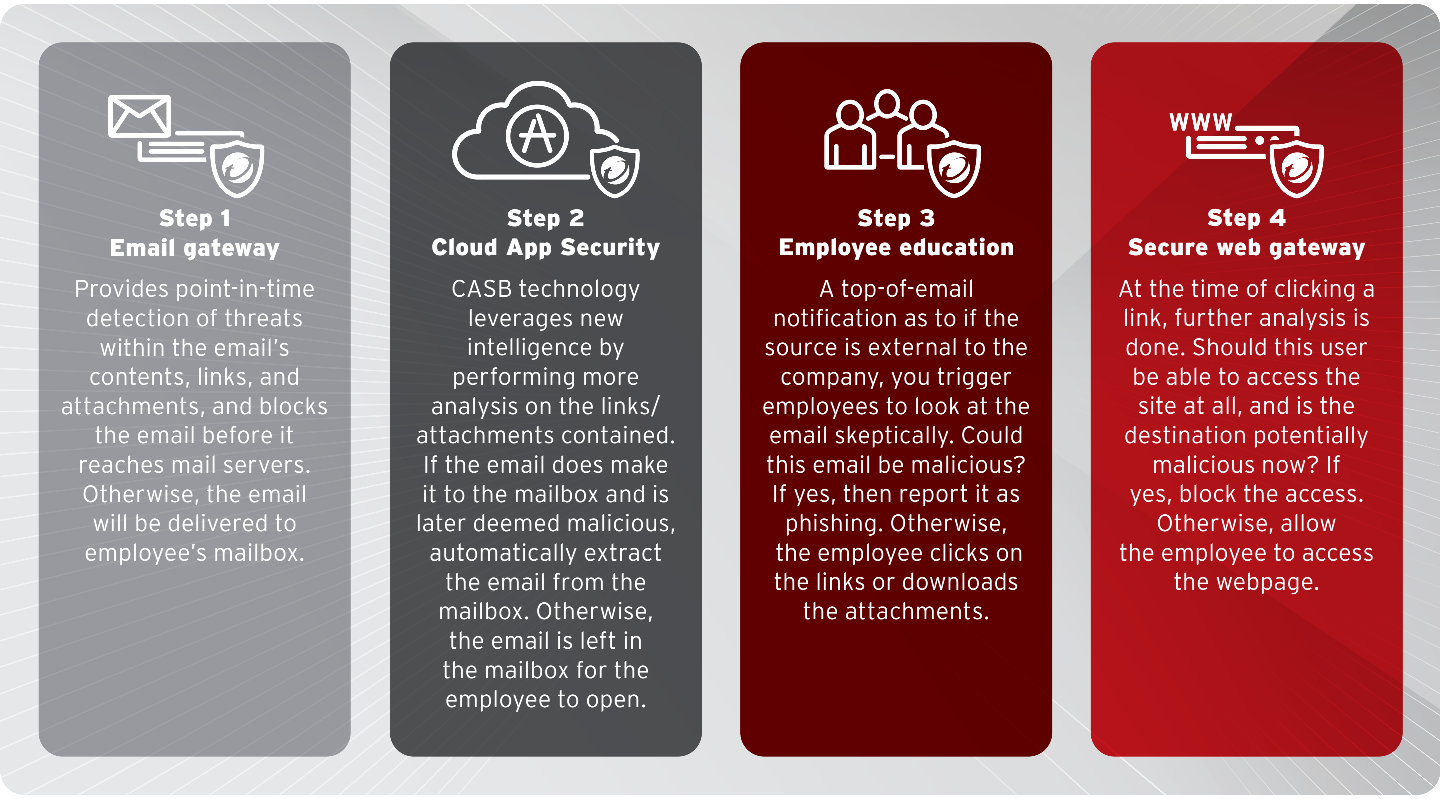
Implementation

Gateway and security solutions

For incoming messages, your organization requires immediate inspection via an email gateway. Trend Micro™ Email Security (TMES) provides a "point in time" detection of threats that stem from business email compromise (BEC), potential phishing attacks based on content, and known malicious links and files. TMES protects Microsoft Exchange, Microsoft 365, Gmail™, and other hosted or on-premises email solutions.

Next, if an email makes its way to the mail service/server, it will be assessed again using Trend Micro™ Cloud App Security. By scanning the email "at rest," further intensive scanning can be done without impacting email delivery. It also enables retroactive response, making it possible to delete malicious emails when new intelligence is received. Cloud App Security can also scan emails between peers, preventing compromised accounts from phishing other employees.

By using our cloud-based SWG at the "point of click," Trend Micro™ Zero Trust Secure Access filters web and internet traffic at the application level. This includes assessing if the destination being accessed or the file being downloaded is malicious. With an AUP in place, access to unsanctioned applications is restricted, preventing your employees from inputting sensitive information. SWG sits between the end user and the internet, inspecting traffic inline across multiple security techniques, including TLS/SSL.



Step 1
Email gateway

Provides point-in-time detection of threats within the email's contents, links, and attachments, and blocks the email before it reaches mail servers. Otherwise, the email will be delivered to employee's mailbox.

Step 2
Cloud App Security

CASB technology leverages new intelligence by performing more analysis on the links/attachments contained. If the email does make it to the mailbox and is later deemed malicious, automatically extract the email from the mailbox. Otherwise, the email is left in the mailbox for the employee to open.

Step 3
Employee education

A top-of-email notification as to if the source is external to the company, you trigger employees to look at the email skeptically. Could this email be malicious? If yes, then report it as phishing. Otherwise, the employee clicks on the links or downloads the attachments.

Step 4
Secure web gateway

At the time of clicking a link, further analysis is done. Should this user be able to access the site at all, and is the destination potentially malicious now? If yes, block the access. Otherwise, allow the employee to access the webpage.

Steps to detect, analyze and stop phishing emails

Next Steps

By implementing a multi-layer security solution, your organization can modernize its approach and provide employees with the appropriate level of protection as they grow their digital footprint. Trend Micro offers your business the following free trials. Benefit from an integrated solution to mitigate the most common form of cyber risk.

Email Security Advanced 30-Day Trial

Cloud App Security 30-Day Trial

Trend Vision One Test Drive