IronVest

Protect your Employees. Secure your Enterprise.

Active Phishing Prevention: Equip Employees to Recognize and Stop Phishing Attacks

Table of Contents

Active Phishing Prevention: Equip Employees to Recognize and Stop Phishing Attacks

If you're in charge of your business's cybersecurity, you're well aware of the threat posed by phishing attacks. These attacks are difficult to defend against, targeting employees with ever more sophisticated social engineering ploys that trick individuals into unintentionally,and sometimes unknowingly, giving up access to your internal systems.

Since this is such a clear and present threat, many businesses invest in traditional email security solutions. But what many leaders don't realize is that this approach no longer offers sufficient protection.

With phishing attacks now occurring at such high volumes and levels of sophistication, a tool like a secure email gateway that claims to stop up to 75% of attacks from reaching your employees' inboxes isn't enough. The damage from these attacks can be severe. In response, businesses need a multi-layered approach to actively prevent phishing attacks.

Read on to learn about how your business can adopt active phishing prevention techniques to equip your employees to recognize and stop phishing attacks. We'll cover:

- The Threat of Phishing
- Recognizing Phishing Attacks
- Traditional Approach to Prevent Phishing (& How They Fall Short)
- Adopting a Multi-Layered Approach
- Active Training: The Effective Way to Prevent Phishing Attacks

The Threat of Phishing

Phishing poses a major threat to businesses of all shapes and sizes. Every business, from mid-market enterprise companies to Fortune 500 firms, is at risk of phishing attacks.

In some industries, the stakes are particularly high. Following a 2021 phishing attack on UC San Diego Health, attackers were able to access private patient and employee data, including SSNs and financial records. One of the biggest phishing attacks of all time occurred in the financial services industry, with Belgian bank Crelan losing $75 million.

As you can see, without the right level of protection, the consequences of a phishing attack can be devastating.

What exactly is phishing, and what threat does it pose?

A phishing attack is a social engineering attack. In this type of cyber attack, someone poses as a reliable and trustworthy entity in order to convince an employee to disclose sensitive information.

These attacks can take many routes to trick employees like encouraging them to click a malicious link that installs malware or prompting the employee to send sensitive information. The link is often sent via email and appears to come from a legitimate source.

In recent years, the methods used by phishing attackers have become much more sophisticated. Attacks are becoming increasingly personalized, with attackers harvesting business information from various online sources to create compelling messages that trick employees. Attackers are creating fake social media profiles, impersonating software tools used every day by employees, and using times such as tax season or the holidays to trick employees with seemingly relevant messages.

The Impact of Phishing Attacks

A phishing attack is often the opening salvo of a much wider attack. In fact, 91% of cyber attacks that result in data breaches originate in a phishing email.

You can think of a phishing attack as a means for outside attackers to obtain access to your system. Once they get that access by stealing your employees' credentials, there's no telling what havoc they might unleash on your business: from installing ransomware that locks your systems to stealing customer data.

Needless to say, this can have wide-reaching implications. The impact of an attack can be thought of in several buckets:

- **Financial Losses**: if an attack brings down your business's internal systems, you may struggle to process sales. That lost revenue comes in addition to potential ransom payments, legal costs, or fines your business might face. In late 2021, Singaporean Bank OCBC lost $13.7m after falling victim to a phishing attack.
- **Data Breaches & Ransomware**: credential breaches can often lead to extremely damaging data breaches that expose your business's proprietary data. Alternatively, attackers may deploy ransomware that locks employees out of key business systems.
- **Productivity Decline**: while your systems are locked down by a cyber attack, your employees remain on the clock. Until the security issue is resolved, your teams will fall behind on deadlines. Some estimates put this cost at as much as $3.2m in lost employee productivity, per attack.

- **Mitigation Costs**: incident response is often far more expensive than investing in tools that prevent phishing attacks in the first place. Fall victim to a phishing attack and you may have to bring in highly specialized consultants to remedy the issue.
- **Reputational Damage**: security incidents don't just affect your business: they affect your customers and partners. If that disruption is a major issue, your reputation will take a hit and customers may start to look for alternative solutions.

Of course, the consequences of each attack are entirely situational and depend on the sophistication of the attackers and the strength of your business's internal security controls.

Curious about your business's current level of protection against phishing attacks? Get an honest, data-driven assessment of your internal environment with a Free Phishing Audit and Vulnerability Report from IronVest today.

Recognizing Phishing Attacks

It can be tempting to stick your head in the sand and hope this doesn't happen to your business. The statistics, however, show that's not a good idea. In the first six months of 2022, there were an astounding 255 million phishing attacks – a 61% increase on the same period in 2021.

With employees continuing to work remotely and in hybrid environments, the threat of phishing attacks remains high. One study, from Microsoft, found 80% of security professionals reported an increase in security threats since the

widespread adoption of remote work, with 62% reporting that phishing attacks had increased faster than any other form of attack.

Effectively defending your business against phishing attacks requires more than just basic technology. Many businesses are already using Secure Email Gateway (SEG) solutions, but alone, these aren't enough.

Studies have shown that 25% of bad emails get through SEGs and land in employee inboxes. When that happens, additional layers of security and employee awareness play a critical role in keeping internal systems secure.

So, what are the main forms of phishing attacks, and how can employees recognize them?

Five Main Types of Phishing Attacks

The cybersecurity industry is a little like an arms race. As security solutions become more sophisticated, so do attackers, resulting in ever more complex attack vectors that can be extremely challenging for security teams to keep up with.

New types of attack continue to proliferate, but the most widely-used types of phishing attacks include:

1. Brand Spoofing Attacks

What Are They? These attacks impersonate legitimate senders with branded emails that include familiar logos, colorways, and fonts. Common examples include password reset emails, emails from file-sharing platforms, or fake invoices. Their goal is to encourage recipients to click a malicious link or download an attachment.

How Can Employees Recognize Them? Employees should carefully inspect all suspicious emails to determine whether they are from a legitimate source. Encourage employees to check sender email addresses and closely examine links. Deceptive phishing emails often have spelling and grammatical errors and may be formatted unusually. Security awareness training, in addition to continuous, contextual training provided in real-time, equips employees with the required knowledge.

2. Spear Phishing Attacks

What Are They? Spear phishing attacks are much more focused. They target specific employees and use information gained from public sources, such as social media sites, to convince employees that the sender is legitimate. The goal is the same: to trick employees into downloading a file attachment or clicking a malicious link.

How Can Employees Recognize Them? A robust security awareness training program helps educate employees on best practices. However, the reality is that many spear phishing attacks are very convincing and can fool even well-trained employees.

Businesses should adopt a more layered approach to phishing prevention that pairs existing SEGs with complementary tools such as IronVest InboxGuard that provide contextual training and active inbox alerting to employees.

3. Whaling Attacks

What Are They? These attacks are even more targeted than spear phishing attacks. They tend to target senior executives, such as CEOs, CFOs, and COOs, who have significant access to internal systems with little oversight. Executives receive an email that appears to come from a colleague and seems legitimate. Whaling emails typically convey urgency and encourage readers to either click on a link or take a secondary action, such as initiating an external wire transfer.

How Can Employees Recognize Them? Make sure that all employees routinely complete phishing training, including your organization's most senior leaders. These individuals often have much greater access to important internal systems, making them an attractive target for attackers..

4. Smishing Attacks

What Are They? A smishing attack takes place over text message, rather than email. Attackers aim to trick employees into unwittingly sharing personal information through a text message. Smishing attacks are becoming more common since text messages have a much higher open rate than emails. Smishing attacks are often grouped with vishing attacks: phishing attacks that take place through phone calls or voicemails.

How Can Employees Recognize Them? The signs of a smishing attack are similar to those of a regular phishing attack; the only difference is that the attackers use SMS messages instead of email. Make sure that employees know they should apply the same judgment to suspicious text messages as they would to suspicious emails.

Phishing training, while helpful, is something employees often forget once the training course is complete, underscoring the importance of a more active approach to phishing prevention.

For an additional layer of security, businesses should invest in more robust anti-phishing cybersecurity software. This can protect against these emails landing in employees' inboxes in the first place.

5. Credential Phishing Attacks

What Are They? These attacks aim to trick employees into giving up their account credentials to a key business system. Employees receive an email that looks legitimate and invites them to log in to a system. The employee clicks to navigate to this page and enters their credentials, unwittingly sharing their login details to any number of business systems.

How Can Employees Recognize Them? Credential phishing attacks are sophisticated and they can be very effective. Educate your employees on what to watch out for and take additional steps to strengthen account security, like adding two-factor authentication on all accounts.

Some studies estimate that the click-through rate on a credential phishing email can be over 10%, emphasizing the importance of blocking these emails from arriving in employee inboxes in the first place.

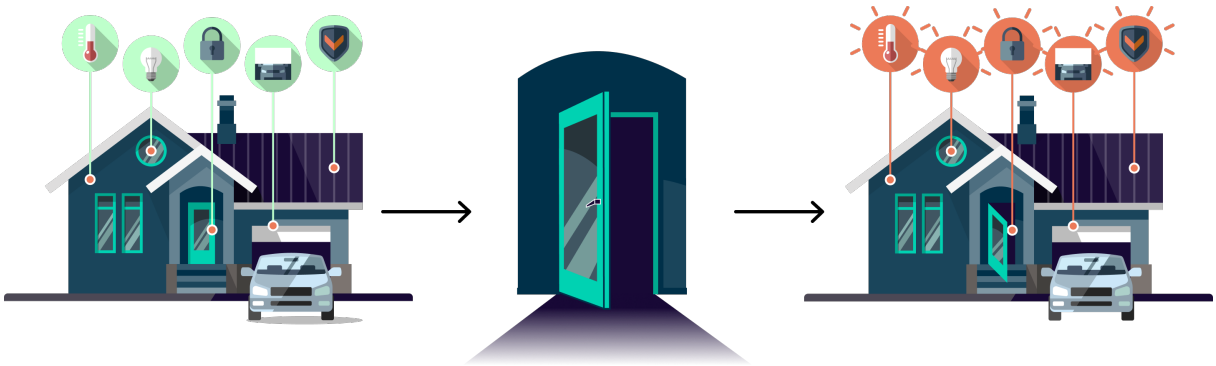
Attackers continue to experiment with new types of phishing attacks and it's likely that new attack vectors will continue to emerge. With such high stakes, it's vital for businesses to invest in technologies and training to prevent phishing.

Traditional Approaches to Prevent Phishing (& How They Fall Short)

Today, the majority of businesses are already taking steps to prevent phishing attacks from harming their organizations. But all too often, these approaches fall short. After all, upwards of 90% of all data breaches begin with phishing attacks.

That begs the question: what's wrong with businesses' current approach to preventing phishing attacks?

One answer: businesses dedicate a lot of resources to protecting their infrastructure, but comparatively few resources to protecting their employees. Think about it: your business probably has a range of cybersecurity tools from basic antivirus software to advanced network security monitoring technologies.



All of these technologies protect your systems, but they don't protect the individuals that control access to all of those systems: your employees. Think of your business as a house. You can have all the alarm systems and cameras you want, but if your employees are tricked into inviting an intruder in, the damage is already done.

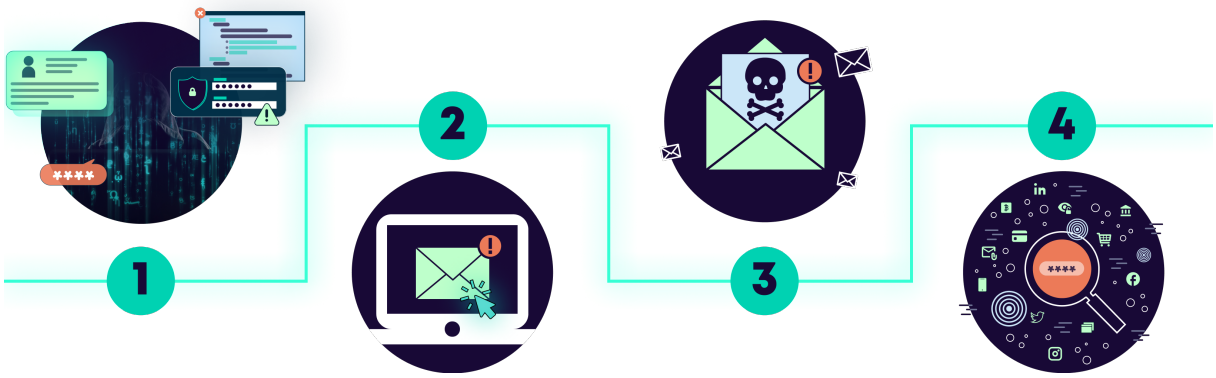
The numbers don't lie: 82% of data breaches involve a human element. Employees are any business's first line of defense against cyberattacks, and it's vital that leaders invest in turning their teams into human firewalls. The traditional way most businesses approach that? Security awareness training.

Security Awareness Training

Many organizations provide employees with basic cybersecurity training on a periodic basis. These training programs almost always feature modules on phishing, exploring the warning signs of a phishing attack and explaining how employees should respond to suspicious emails.

In many cases, these programs also offer simulated phishing attacks that businesses can use to assess employee awareness, identify areas of weakness, and qualify the impact of the training program.

While security awareness training has been shown to reduce the chances of a business falling victim to a phishing attack, it does not eliminate it entirely. While security awareness training offers simulated phishing attacks, it does not offer real-time prompts on an ongoing basis when employees receive suspicious emails.



In the days following the training, awareness might be top of mind, but in the weeks and months after this, the lessons learned fade and employees lower their guard. Remember, all it takes for a phishing attack to be successful is one employee out of hundreds or thousands to click on a suspicious link.

With attackers continuing to experiment with new forms of attack, even the best security awareness training leaves your business vulnerable to the latest threats. Instead of leaving your business's security solely in the hands of employees, many security teams also invest in anti-phishing technologies. The most common of these technologies is Secure Email Gateways (SEGs).

Secure Email Gateways (SEGs)

A Secure Email Gateway, also known as a SEG, is an email security tool that filters all incoming and outgoing emails from a business. The SEG scans emails for malicious content including malware, phishing attacks, and even spam. Suspicious emails are quarantined and are not delivered to the employees' inboxes.

SEGs have been in use for many years. They act as the first layer of defense against email-based cybersecurity attacks. By scanning emails and preventing suspicious messages from being delivered to individual users, SEGs dramatically cut down on the volume of spam and potential cyberattacks that employees are exposed to.

Depending solely on an SEG to protect your employees can be a major mistake. Today, 25% of bad emails make it through SEG solutions without being flagged, exposing employees to major risks. Given that 3 billion phishing emails are sent every day, failing to adopt additional layers of email security leaves businesses at increased risk of suffering a data breach.

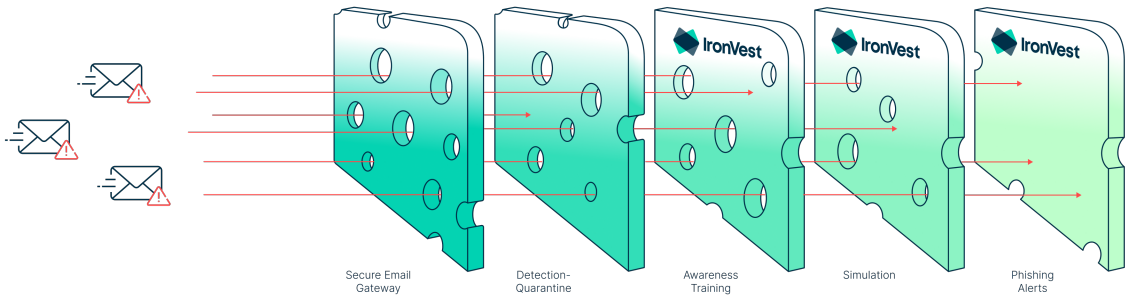
Adopting a Multi-Layered Approach to Email Security

You can think of your existing email security infrastructure as being similar to layers of swiss cheese. Each layer might stop a large percentage of attacks, but some still leak through to the next layer.

To effectively minimize the disruptive impact of a phishing attack, businesses must embrace a more comprehensive approach to email security. In addition to adding new layers of email security including employee training and Secure Email Gateways, businesses should also adopt a fail-safe solution, such as InboxGuard from IronVest.

InboxGuard is a powerful security tool that labels potential phishing emails which make it through existing security measures, providing employees with the additional security information they need to identify potential phishing scams. By combining InboxGuard's active alerting capabilities, phishing simulations, and other security technologies, businesses can promote a more secure infrastructure.

Adopting InboxGuard as part of a more sophisticated approach to email security reinforces existing barriers that potential phishing attacks must overcome in order to be successful. This results in a multi-layered approach to email security that resembles the below diagram:



This approach essentially offers businesses a safety net for when existing email security technologies let attackers slip through the cracks. When employees do receive a suspicious email, they receive situational training that provides real-time education on phishing attacks with micro-learning modules.

Active Training: The Effective Way to Prevent Phishing Attacks

Considering the deficiencies in existing anti-phishing strategies, it's extremely likely that harmful phishing emails will bypass your business's current security infrastructure and land in your employees' inboxes. When (not if) that happens, it's crucial that you give employees the tools to protect themselves against these attacks.

IronVest InboxGuard is a cloud-based anti-phishing solution that delivers security training both contextually and in real-time on actual phishing emails that your organization might receive. We layer our solution with an immersive security training program that offers consistently updated, relevant, and highly engaging content that is specifically designed to change employee behavior and promote a strong security culture throughout your enterprise.

InboxGuard uses powerful AI technology to seamlessly run a series of advanced checks on every email. When potential phishing emails are detected, InboxGuard educates employees in real-time, actively warning users of red flags and providing a series of warnings about the content of each email.

By adopting InboxGuard as part of a multi-layered approach to email security, businesses can detect 99.99% of phishing emails and give employees the tools to effectively respond, dramatically improving overall cybersecurity.

InboxGuard can be deployed in minutes with no interruption to your employees' workflow. The tool integrates seamlessly with existing email security tools, including Secure Email Gateways, and features a 1-click install with leading email clients such as Microsoft Office 365. Security teams also benefit from advanced reporting capabilities that give security teams insights into weak spots at an individual or department level.

Curious about how your organization's current approach to email security and phishing prevention stacks up?

Get a free phishing vulnerability audit and report today and discover how IronVest InboxGuard can upgrade your email security posture.