HOXHUNT

Why mitigating email threats should be your top priority?

Despite technological advances in email filtering, most cyberattacks still start with malicious emails.

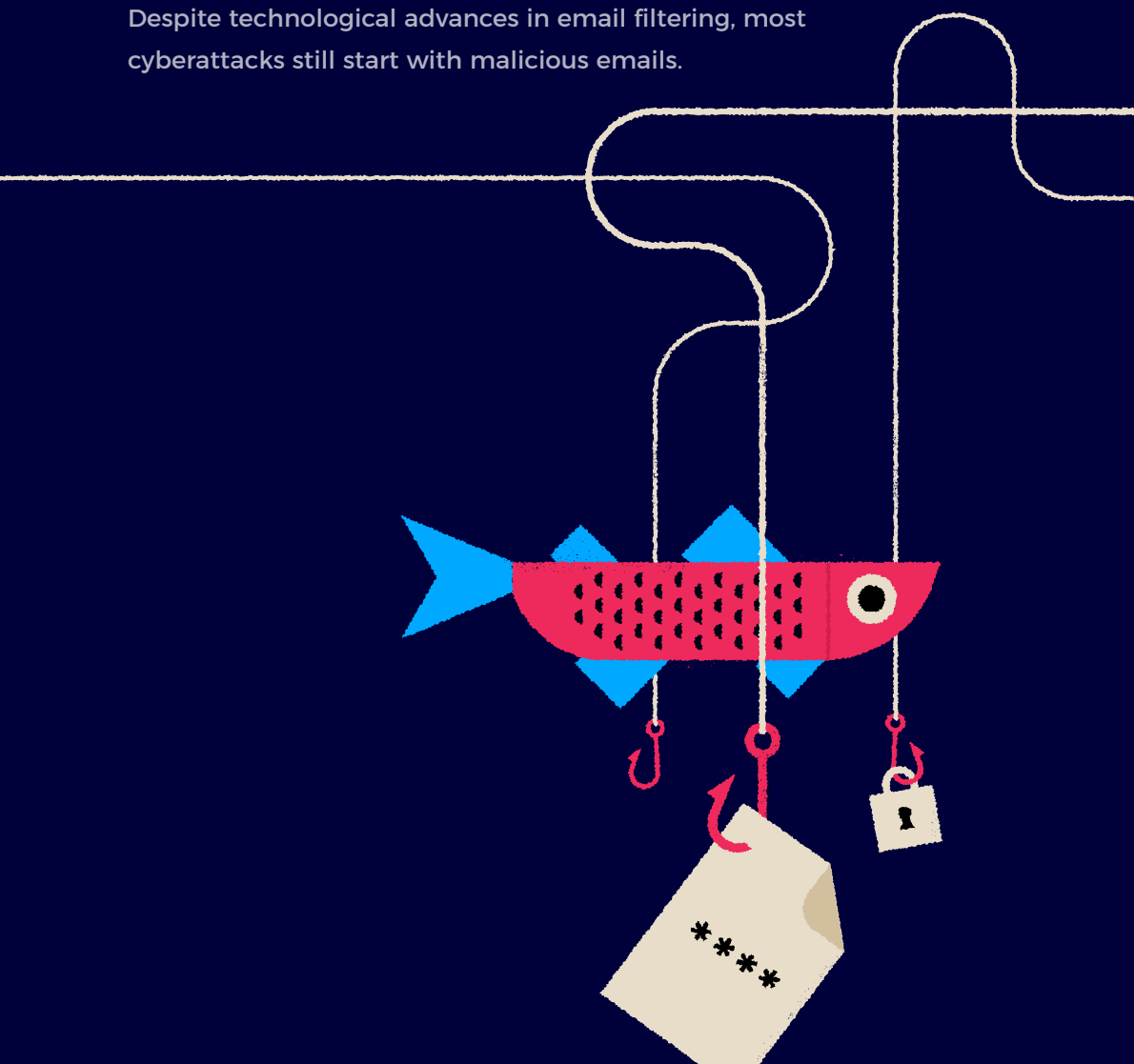


Table of Contents

Why email threats require special attention

Risk-based approach

Almost everyone - executives, boards, customers, and the general public agrees that cyber risks are significant contributors to enterprise risks and that they need to take cybersecurity seriously.

Cybersecurity departments in today's world face no shortage of challenges. Cyberrisks cover many areas and deciding which areas to focus on remains a struggle.

Chief information security officers (CISOs) need to balance resources across their different areas of responsibility while dealing with internal budget constraints, shortage of cybersecurity talent, and increasing compliance requirements.

The most sophisticated companies are moving to a risk-based approach for managing their cyberrisks (1). It means that to decrease enterprise risk levels, cybersecurity departments must identify and focus on the more critical elements of cyberrisk.

CISOs need to understand where their most significant risks lie. While companies are investing millions in technological solutions to protect their infrastructure, the expanding attack surfaces and sophisticated cyber threats make it more important than ever that individual employees understand their role in preventing attacks. And no matter how advanced the technical solutions, some attacks will always get through. It takes just one successful attack to bring down an entire organization.

Focusing on the technological defenses and adhering to compliance can give a false sense of security, while the most significant attack surface, the employees, may remain unprotected.

“

93% of Organizations Cite Phishing as Top Threat.

Infosecurity magazine

CISO Problem Space

PEOPLE

CISO

TECH

Device Management	Identity Management
Policy Bring your own device (BYOD) Stolen/lost devices	SSO 2FA Access Control Password management
Remote Access	**Security awareness**
VPN	Social engineering Phishing Continuous training Tools and techniques

Security Operations	Risk Management
Network / Application firewall Application Security Anti-malware DDoS Encryption Soc Operations Incident Response Forensics	Vulnerability Management Pen Testing Code Reviews Policies and Procedures
Compliance	**Security Architecture**
Audits Certificates	Network architecture Remote access Backups Application protection

Threat landscape

There are many ways for an attacker to infiltrate your organization.

It's not exactly news that email-based threats are the most common method used by attackers. Ninety-three percent of organizations cite email-based threats as a primary threat (2), and employees are the largest attack surface for a company.

According to the Verizon Data breach report, phishing is the most common first phase of the attack. Attackers use phishing emails, because they work. 30 percent of phishing attacks are opened, but only 3 percent are reported to the cyber security teams.

Because phishing is the most common technique intruders usie, solving it can have the highest impact on your organization's risk.

Still, many companies haven't taken adequate measures to protect their employees against these threats, thus leaving their most significant attack surface vulnerable.

Companies usually try to cover email based threats as part of their cybersecurity awareness training, educating employees on a range of different threats. They also set policies that try to force personnel to behavior securely.

While important, traditional cybersecurity awareness alone is not enough to mitigate risks across all areas.

Learning how to manage some aspects of the threat landscape, like phishing, require more than classroom training or video courses.

Examples of Email Threats

Phishing	Phishing is a type of social engineering where the attacker attempts to obtain sensitive data by impersonating a trusted entity.
Spear phishing	Spear phishing is a highly-targeted form of phishing attackers use to send personalized emails to well-researched targets (often to executives or people with access to money).
Malware	Malware can be harmful files or software, most typically delivered as an attachment or through a malicious link.
Ransomware	Ransomware is often delivered through emails. Ransomware encrypts the victim's data and systems and demands a fee to get the access back.
Spyware	Spyware infects the victim's systems to gather sensitive information.
Credential theft	Attackers are trying to harvest credentials, for example, by spoofing a trusted online website to get the victims to give away their login credentials.
Business email compromise	Attackers send an email message that appears to come from a trusted source, for example, they could be asking someone to conduct a wire transfer as soon as possible.

Did you know?

In 2015, hackers remotely accessed the control centers of three Ukrainian electricity distribution companies. This attack left more than 200,000 consumers without power. It started when attackers sent phishing emails with infected attachments to the companies' offices. The recipients' opening of the attachments activated macros embedded in the files, which enabled the hackers to gain remote access to the control centers.

Did you know?

In March 2016, the personal email account of John Podesta, a former Chief of Staff of the White House was compromised and his emails were hacked. Many of his emails were work-related and they shed light on the inner workings of the Clinton campaign.

The data breach was accomplished by a spear-phishing attack.

Kill chain and early prevention

The global average total cost of a data breach in 2020 was $3.86 million (3). This figure is why it's vital that you stop attacks before they can do significant damage.

The cyber kill chain describes the stages of a cyberattack, which can also help you figure out the best ways to prevent an attack.

The closer to the beginning of the kill chain that you can detect an attack, the less it will cost to resolve in terms of both time and resources. If you notice the attack only when it has reached your network, you'll have to spend more time investigating how far it has spread and what damage has occurred.

No matter how advanced, the technical layer will let some attacks through. If you can't prevent all attacks from reaching the employee, the best way to stop an attack is to make sure your employees know how to detect and react to attacks. Your employees can stop attacks even though they are already in the delivery phase.

Since even with the best training, it's possible some of your users still fall for an attack, it's essential that your phishing program also provides your employee with a simple way to report if they've already clicked on something they later realize was malicious.

Preventing attacks in the earliest stages has the highest return on investment (ROI).

Did you know?

"94% of malware was delivered via email."

Verizon Data Breach investigations Report 2019

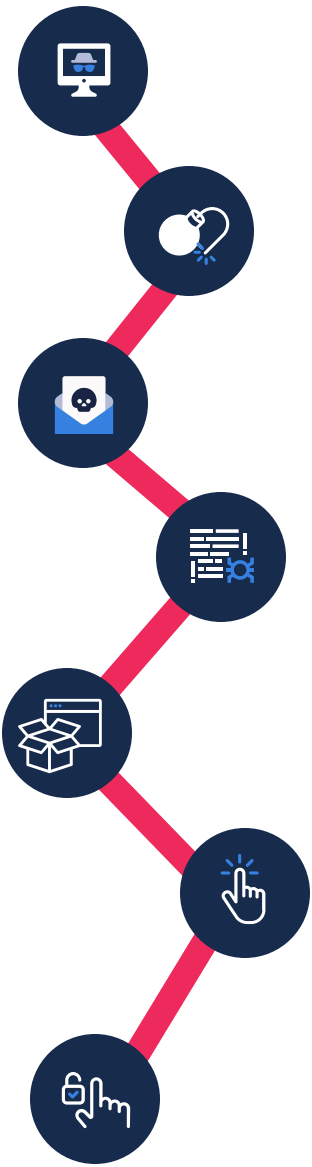
Kill chain

The cyber kill chain, created by Lockheed Martin, describes the phases of stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.

1

Reconnaissance

Attackers probe for a weakness. This might include harvesting login credentials or information useful in a phishing attack.



2

Weaponization

Build a deliverable payload using an exploit and a backdoor.

3

Delivery

Sending the weaponized bundle to the victim - for example, a malicious link in a legitimate-looking email.

4

Exploit

Executing code om the victim's system.

5

Installation

Installing malware on the target asset.

6

Command and control (C&C)

Creating a channel where the attacker can control a system remotely.

7

Actions

Attacker remotely carries out its intended goal.

Why do companies fail to mitagate email-based threats?

Why isn't technology enough to solve the problem?

Antivirus tools and email filters can identify and contain known threats. However, viruses and malware adapt and change, which means complete protection isn't possible. While the technological layer continually improves, malicious actors are also finding new ways to bypass these technical layers.

Also, when attackers use social engineering tactics like spear-phishing attacks, malicious programs can bypass these technologies. In addition to email, these attacks can also target you through different mediums such as text messages, WhatsApp, and social media, where the user is often unprotected.

These different attack vectors are the reason why it's essential to teach your employees to detect social engineering attacks as they will inevitably face them.

Why can't you solve phishing in a classroom?

Attackers use social engineering tactics to try to trick your employees. You can't effectively train users against social engineering tactics in a classroom. The purpose of social engineering tactics is to catch the victim off guard. They invoke emotions like curiosity, fear, and urgency in the emails, urging people to take action that will have negative consequences. The threat landscape is also continuously evolving, which means frequent and up-to-date training is crucial to stay one step ahead.

It's essential to make sure your training has similar elements that the real-life attacker would use. Sending realistic simulated attacks to your employees in the live email environment and using similar tactics that the attackers will employ can ensure they know what to do when facing a real attack.

Why can’t phishing be solved with quarterly simulations?

Some companies choose to test their employees with quarterly simulations, often enrolling those users who fail the initial test for this extra training.

While this method gives companies some degree of understanding of the failure rates, it fails to impact the long-term failure rate. It also does not take into consideration employees who missed the simulation completely.

For employees to develop the habit of recognizing and reporting threats, you need to train them frequently. Training them frequently in the live email environment reinforces this habit and helps them stay vigilant against malicious emails.

Did you know?

“Phishing accounts for 90% of data breaches.”

Retruster

Characteristic of a successful email threat mitigation program

A successful email threat mitigation program is human-first

A successful email threat mitigation program starts with a people-first approach. The training needs to be effective and motivating, giving the employees the skills and confidence to help protect your organization.

When you give employees the skills and confidence to know what to do when they encounter a threat, you'll create a positive cybersecurity culture where employees feel they play an essential part in protecting the organization.

Cybersecurity culture consists of attitude, behavior, and awareness. A successful phishing training program will positively impact these areas, helping you to create a positive cybersecurity culture.

Cognitions or Knowledge

The employees' awareness, verifiable knowledge, and beliefs regarding practices, activities, and self-efficacy are related to the veracity of your organizational security.

Behaviors

The actual or intended activities and risk-taking actions of employees can directly or indirectly impact the cybersecurity culture in the organization.

Attitudes

Employees' feelings and emotions about various activities that pertain to organizational security will affect the cybersecurity culture.

Protect - Detect - Respond

In addition to personalized training that will change your organizational behavior, you need to encourage your employees to report real threats and form a protective layer for your network. If one employee reports a threat, it might be enough to remove the threat before other employees can have the chance to fall for it.

As security teams have a range of different areas that they need to focus on, technology should ease some of the team's workload rather than add to it.

Protect

Personalized training that leads to behavior change.

Detect

Activate your organization to report incoming threats.

Respond

Respond to your most dangerous threats.

Did you know?

"Phishing is the top threat action."

Verizon Data Breach Investigations Report 2019

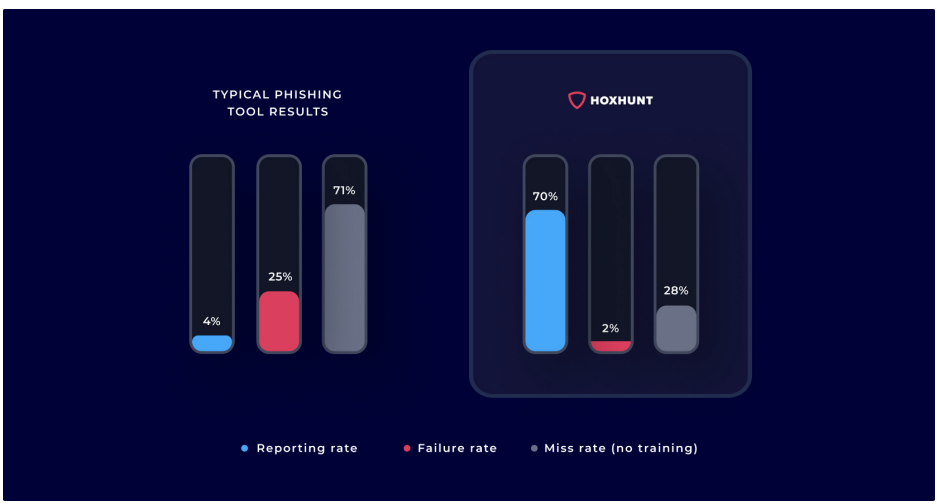
Results

A successful email threat mitigation program will help to reduce cyber risks. To reduce the risks, stopping attacks early in the kill chain is a must. To do that, make sure that your employees stay vigilant against these threats by educating them.

If you want to make an impact, make sure that you emphasize the need for behavior change throughout the organization. You can achieve this goal with the right training program that engages employees to protect your company by adapting safe online habits.

To measure the success of the program, introduce metrics and key performance indicators (KPIs). Measuring how many of your employees fall to simulated phishing attacks and how many employees report threats can be an excellent start in this process.

At Hoxhunt, we have worked with hundreds of organizations, and we have received millions of threat reports from our users. The starting position always depends a lot on each organization. Still, through our training, the companies we work with have been able to bring their failure rate down to around two percent and have achieved a reporting rate of seventy percent on average. While these numbers aren't directly comparable between individual companies, it provides a great benchmark on where your company should be heading to mitigate the risks appropriately.



References

(1)
https://www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity

(2)
https://www.infosecurity-magazine.com/news/93-of-organizations-cite-phishing/

(3)
https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

(4)
https://www.keepnetlabs.com/antivirus-tools-cant-stop-phishing-attacks-anti-phishing-solution-that-can-stop-phishing-attacks/


HOXHUNT