GoSecure

EMAIL SECURITY EBOOK

Fight the Phishing Epidemic and Win

The 5 Biggest Challenges and How to Attack Back

Phishing is one of the most devastating threats hitting organizations every day.

And it's the most dangerous and costly cyber threat across the globe. A single successful phishing attempt against your employees provides the foothold cyber criminals need to access your corporate network. A joint study between Google and UC Berkeley looked at the various ways accounts are compromised. The result: phishing attacks were identified as the greatest risk to users.

It's clear. One successful phishing event is one too many.

This guide details the top five challenges organizations face in fighting phishing threats and how a new approach can finally solve your biggest corporate inbox risk.

Table of Contents

CHALLENGE 1

The Phishing Epidemic

We've all seen the favored email phishing lures: an urgent security alert from IT, a revised vacation policy from HR, someone wants to share a Google doc—you name it.

Given its cheap cost and high success rate, phishing remains cybercriminals' favored method-of-choice to gain access to your employee's desktops. Coming in with 40% of the votes, phishing won top ranks as the threat with the most significant impact entering the organization.[2]

Not only is phishing common, it's getting worse. Criminals are innovating their tactics, such as next-gen phishing, spear phishing, and business email compromise (BEC) to steal data and credentials across virtually every network.

And it's working...

93%

Of breaches in 2018 had phishing or social engineering at the center of the attack according to according to Verizon's Data Breach Investigations Report.

$1.7 billion

According to the FBI's 2019 Internet Crime Report, there were $1.77 billion in losses in 2018 due to BEC scams.

$1.4 million

Average cost of phishing and social engineering attacks for companies in 2018.[3]

85%

OF COMPANIES EXPERIENCED PHISHING AND SOCIAL ENGINEERING CYBERATTACKS IN 2018[1]

CHALLENGE 2

The Security Gap

For decades organizations have adopted the most advanced security controls—firewalls, email and web gateways, as well as next-gen anti-malware solutions—that feature innovations like artificial intelligence engines and global threat research analytics to combat phishing.

There's no doubt these solutions are a critical part of any company's security arsenal against phishing attacks. But the reality is, no solution is 100% perfect all the time. These security gaps in detecting phishing threats open the door to dangerous payloads like ransomware.

Even newer approaches like DMARC (Domain-based Message Authentication, Reporting, and Conformance), which lets email server administrators put policies in place that can detect when an incoming email is lying about its real "From:" address, are not being enforced. Almost 80% of organizations worldwide have not implemented DMARC.[5]

This means phishing threats will continue to bypass your current defenses to arrive into your employee inboxes.

Misplaced Confidence

More than **80%** of participants said they were "confident" or "very confident" that traditional email gateways will protect their organizations from targeted phishing attacks yet

42%

reported they fell victim to a recent phishing attack.[4]

NO COMBINATION OF SECURITY SOLUTIONS IS PERFECT

100% OF THE TIME THERE'S A GAP THAT STILL NEEDS TO BE FILLED

CHALLENGE 3

Employees: The Weakest Link

Phishing is on the rise, and your security defenses aren't bullet proof. So now what?

With the knowledge that some phishing attacks will reach corporate inboxes, it's surprising to find that the majority of organizations do not have an IT policy on how employees should deal with them. That's a big disconnect.

Most often companies tell their employees not to click on links or open attachments in suspicious emails. But this advice goes against how technology works for employees to get their job done. Employees are desensitized to all the noise and are often much more willing to click on links, which can prove dangerous.

Even a moderately well-crafted phishing email will almost certainly succeed in getting at least one employee to click on it. Once your employees get tricked, they unwittingly open the door to malware that captures and exports your customer data, confidential information, credentials—or installs ransomware that takes control of your systems.

ACCORDING TO EMAIL SECURITY CONFIDENCE SURVEY

The human element is the fastest growing driver in breaches today. The only two top threat actions in data breaches that have grown in the past 7 years were both human based.[7]

CHALLENGE 4

Security Awareness Training

It isn't enough.

Of course, knowledge is power, and it's natural to turn to security awareness and education training to test employees' responses to simulated phishing attacks. But this does little to effectively close the security gap and disrupts productivity.

Phishing simulation tests also upset staff and break trust within the organization. Telling employees they failed the test and need additional training makes them feel bad about their performance, despite their best intentions.

Human nature kicks in, and ultimately the trainings condition employees to: ignore legitimate emails, avoid reporting when they've clicked on a real phishing email and send any and all suspicious emails to IT for investigation.

Launching security awareness programs can also cost a lot of resources, time, and money—with unclear results. While organizations might see short term improvements, retention quickly drops in the following years. And the program needs sustained support. Your IT security practitioners need to become behavior and learning experts, and it places more resource constraints on the team with helpdesk inquiries and ongoing training management as staff turnover.

Employees spend ages pondering emails instead of priority tasks at hand.[8]

The average employee spends...

16 Minutes each day

80 Minutes each week

5.5 Hours each month

69.3 Hours each year

managing spam email.

Security is not getting better for many organizations[9]

Change in the Ability to Deal with Various Threats Over the Past Three Years

Phishing attacks reaching end users is getting worse or staying the same	58%
Ransomware infections on our network is getting worse or staying the same	59%
CEO Fraud/BEC Emails reaching senior executives is getting worse or staying the same	59%
CEO Fraud/BEC Emails reaching lower-level employees is getting worse or staying the same	63%

CHALLENGE 5

IT Resource Constraints

The phishing inbox risk has squarely fallen on IT's shoulders to burden, and the current best practice approaches of employee training, email investigations, and remediation are creating significant IT resource constraints.

Many employees play it safe and send every suspicious email to IT for investigation. This puts a heavy burden on IT to run a testing lab and become experts in email threat analysis.

Estimate of Cost Analysis: IT Self-Remediation

	Number of End User Seats	# of Suspicious Emails Reported to IT / month	Cost Per Year of IT Remediation
In-house IT	**750**	**375**	**$52,500**

Based on estimate of $70/hr for In-house IT costs. Does not include savings of reduction in successful attacks, remediation of an actual attack, hardware costs, etc.

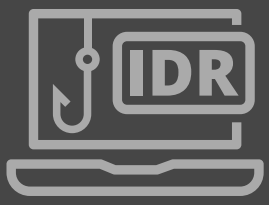
On top of investigation costs, it's a well-know fact many organizations simply do not have experienced cybersecurity staff in place. According to the 2019 ISC2 Cyber Security Workforce Study, it is estimated that an additional 4 million trained workers would be needed to close the skills gap and properly defend organizations. Unfortunately, it takes years to develop the skills and experience to be effective.

Cybersecurity Workforce Study*

4 Million	500,000	65%	>1/3
gap of trained workers needed to close the skills gap and properly defend organizations.	US workers alone needed to fill the shortage.	of organizations report a shortage of cybersecurity staff.	of organizations say that skilled personnel is a top concern.

** 2019 ISC2 Cyber Security Workforce Study*

A New Approach: GoSecure Inbox Detection & Response



GoSecure Inbox Detection & Response empowers you to close the phishing gap and take advantage of your organization's most important asset at the endpoint: your employees.

Inbox Detection & Response (IDR) is an automated email incident response service where employees can seamlessly report suspicious emails for threat investigation with a click of a button. IDR processes the email through machine learning and human expert analysis to check the email's true intent. In minutes, the email is analyzed and removed, if malicious.

By providing your employees instant access to IDR, you remove their guesswork of identifying phishing threats and enable your staff to be a part of your organization's security defense.

GoSecure Inbox Detection and Response also saves valuable IT resources by reducing the volume of email investigations and eliminating phishing remediation. With IDR, you can finally close the phishing inbox security gap and improve your security effectiveness.

Trust it. Or Test it.
Never guess on phishing emails again.

No email security gateway completely protects you from advanced social or phishing attacks.

Inbox Detection & Reponse upgrades you to the world's safest inboxes

- Resolves phishing incidents in minutes without IT
- Activates employees as a final level of endpoint security
- Dramatically reduces the role of IT in resolving threats
- Saves lots of time and money on remediation and follow-up
- Lowers need for employee security awareness training
- Dramatically reduces your risk of breaches and vital data loss

How Inbox Detection & Response Works

Closing the loop

1. Employee notices suspicious email in Outlook Inbox and clicks GoSecure IDR button to launch review
2. Flagged email is automatically quarantined and routed through the GoSecure Active Response Center
3. GoSecure automated machine learning engines investigate suspicious email
4. Live security experts join the investigation of suspicious email with multi-faceted analysis
5. Within minutes the suspicious email is returned, either verified or removed
6. Real-time reporting gives IT clear visibility into every incident and its resolution

The key?

GoSecure's Active Response Center

GoSecure's IDR email analysis is not only fueled by GoSecure's gauntlet of advanced threat filtering engines, but by our labs of expert human analysts. Across the globe, our analysts spend 24/7 reviewing and categorizing email-borne attacks. This expert human layer is unique to IDR and is essential to successfully thwarting social attacks with the highest levels of accuracy.

In Summary

For most organizations, finding the best way to detect phishing threats in the inbox is top of mind. Current approaches are falling short. Organizations need an automated, accurate process to identify phishing emails that empowers employees and takes the cost and hassle of investigations and remediations away from IT until it's necessary for their involvement

Organizations are turning to GoSecure Inbox Detection and Response to eliminate uncertainty and close the phishing security gap.

GoSecure IDR helps you:

Resolve phishing attacks in minutes

Empower your employees to be part of your defense

Make IT's job dramatically easier

Gain savings on investigation and recovery costs

Decrease your risk of data loss

Learn more at gosecure.net

References

1 - Accenture/Ponemon. "Cost of Cybercrime" Study, 2018
2 - SANS Institute. "2017 Threat Landscape Survey: Users on the Front Line." 2018.
3 - Accenture/Ponemon. "Cost of Cybercrime" Study, 2018
4 - GoSecure Email Security Confidence Survey, 2019
5 - ZDNet. "DMARC's abysmal adoption explains why email spoofing is still a thing", 2019.
6 - GoSecure Email Security Confidence Survey, 2019
7 - Verizon. "2019 Data Breach Investigations Report." 2019
8 - Legal Workspace, "The True Cost of Spam Email"
9 - Osterman Research, "New Methods for Solving Phishing, Business Email Compromise, Account Takeovers and Other Security Threats", 2019

GoSecure