May 2023

MARKET REPORT

2023 spear-phishing trends

Key findings about the impact of attacks and the challenges of threat detection and response »

Barracuda®
Your journey, secured.

Table of Contents

Key findings

50% of organizations were victims of spear phishing in the last 12 months

An average of **10 suspicious emails** are reported to an organization's IT department on a regular workday

A typical organization receives **5 highly personalized spear-phishing emails** per day

It takes nearly **two days** on average to detect an email security incident

1 in 4 organizations had at least one email account compromised in 2022

Hackers send an average of **370 malicious emails** from each compromised account

Introduction

Spear phishing remains low volume but high impact

While cybercriminals seek to take advantage of many different attack vectors, email remains among the most popular. The 13 email threat types identified by Barracuda researchers, including spear phishing, continue to evolve. Due to widespread email-based security attacks, businesses are suffering monetary losses, reputational damage, and other negative impacts.

Spear phishing is a highly personalized form of email attack. Hackers research their targets and craft carefully designed messages, often impersonating a trusted colleague, website, or business. Spear-phishing emails typically try to steal sensitive information, such as login credentials or financial information, which is then used to commit fraud, identity theft, and other crimes.

Methodology

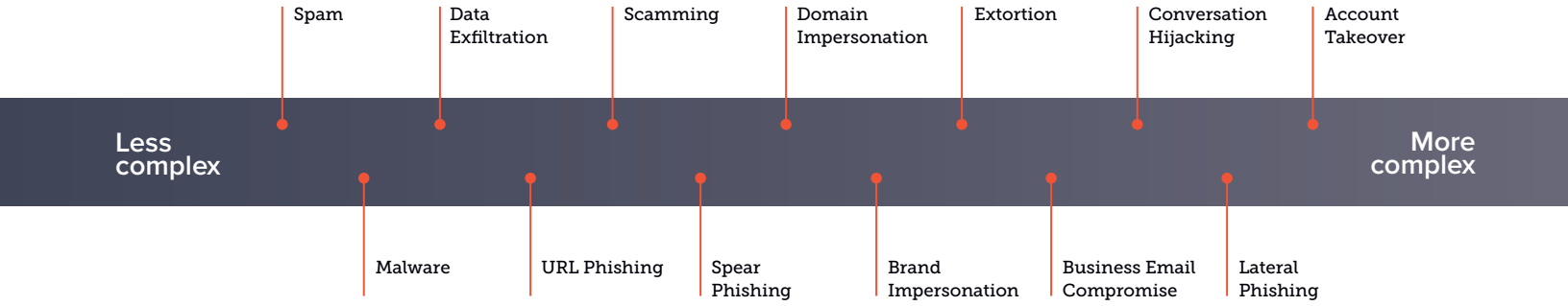
This report presents proprietary spear-phishing data and analysis from Barracuda researchers, drawing on a dataset that comprises 50 billion emails across 3.5 million mailboxes, including nearly 30 million spear-phishing emails.

The report also features survey findings from Barracuda-commissioned Vanson Bourne research. Independent market researcher Vanson Bourne conducted a global survey of 1,350 IT managers and technical IT professionals, senior IT security managers, and senior IT and IT security decision makers representing organizations of all sizes from a broad range of industries. Survey participants were from the U.S., Australia, India, and Europe. In Europe, respondents were from the United Kingdom, France, DACH (Germany, Austria, Switzerland), Benelux (Belgium, the Netherlands, Luxembourg), and the Nordics (Denmark, Finland, Norway, Sweden). The survey was fielded in December 2022.

Designed to evade traditional email security, including gateways and spam filters, spear-phishing attacks are often sent from high-reputation domains or already-compromised email accounts. Spear-phishing emails do not always include malicious links or attachments. Since most traditional email-security techniques rely on blocklists and reputation analysis, these attacks get through. Attacks typically use spoofing techniques and include "zero-day" links — URLs hosted on domains that haven't been used in prior attacks or that have been inserted into hijacked legitimate websites — so they are unlikely to be blocked by URL-protection technologies.

Cybercriminals also take advantage of social-engineering tactics, including urgency, brevity, and pressure, in their spear-phishing attacks in order to increase the likelihood of success.

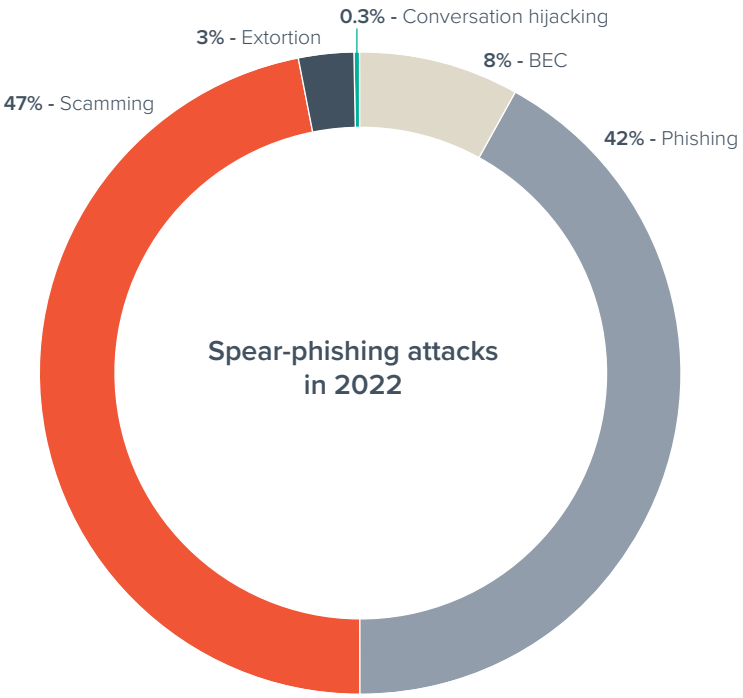
13 email threat types



Barracuda detection and analysis of spear-phishing attacks in 2022

In an analysis of 50 billion emails across 3.5 million mailboxes, Barracuda researchers uncovered nearly 30,000,000 spear-phishing emails. While these emails make up less than 0.1% of all emails sent, they greatly impact organizations when attacks are successful. (For comparison, high-volume attacks, such as spam and malware, make up about 16% of emails, but their impact is not as high.) The average cost of a data breach caused by business email compromise was nearly $5 million in 2022, according to IBM. And no business is immune.

Barracuda's research shows that the average organization gets roughly 5 spear-phishing emails per day — that's more than 1,700 each year. Perhaps the worst news of all is that Barracuda's analysis shows that spear-phishing emails have an average click-through rate of 11%. Considering just one successful attack can be devastating, it's critical to have multilayered protection against these email-based threats.



Barracuda researchers identified five main types of spear-phishing attacks:

Scamming

Scamming represents 47% of the spear-phishing emails analyzed, making it the most common attack. Scamming attacks can take many shapes and forms, but they are all designed to capture private, sensitive, and personally identifiable information, such as bank accounts, credit cards, and Social Security numbers. Attackers trick victims into disclosing the information and then use it to defraud them, steal their identities, or both. Attacks are executed using a variety of hooks, such as lottery winnings, unclaimed packages, fake job postings, donation solicitations, and other tactics.

Brand impersonation

This type of spear phishing, designed to impersonate well-known companies and commonly used business applications, makes up 42% of all attacks. They are one of the most popular types of attacks because they are well designed as an entry point to harvest credentials and carry out account takeover. Brand impersonation attacks are typically used to steal account login information, but they are sometimes used to steal personally identifiable information, such as credit card and Social Security numbers. Attackers impersonate large businesses and popular applications, such as Microsoft, DHL, DocuSign, WeTransfer, and others.

Business email compromise

Also known as CEO fraud, whaling, and wire-transfer fraud, business email compromise makes up only a small 8% of spear-phishing attacks, but it has caused billions of dollars in losses. Scammers impersonate an employee, a partner, a vendor, or another trusted person in an email, requesting a wire transfer or personally identifiable information from finance department employees or others with access to sensitive information. These highly targeted attacks are particularly difficult to detect because they rarely include a URL or malicious attachment.

Extortion

Extortion attacks account for 3% of the total number of targeted phishing attacks. Most of the attacks are sextortion email threats. Cybercriminals claim to have compromising videos, images, or other sensitive or embarrassing content allegedly recorded from the victim's computer. They threaten to share it with all their email contacts unless a ransom is paid. Demands typically range from a few hundred to a few thousand dollars and need to be paid in bitcoin, which is difficult to trace.

Conversation hijacking

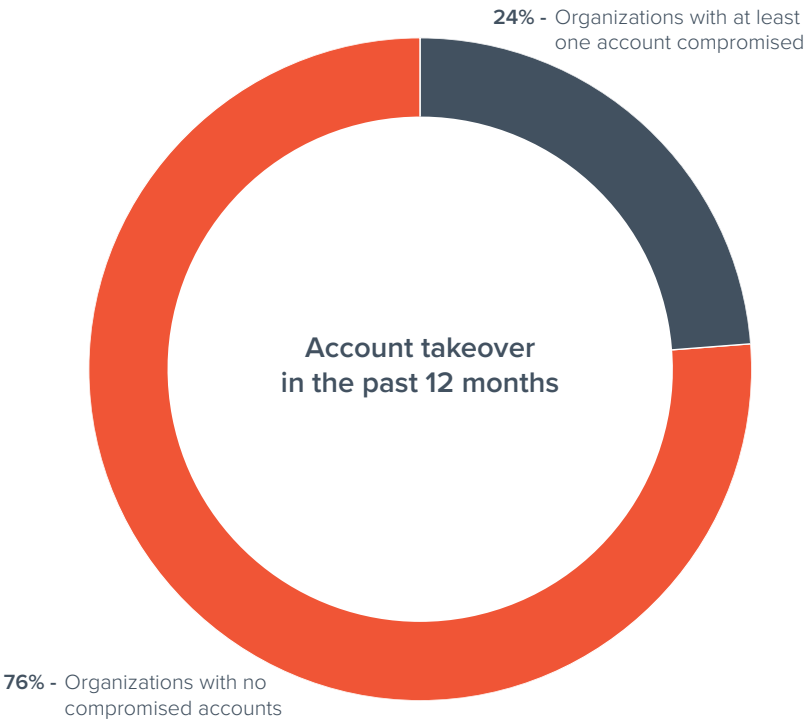
Conversation hijacking, also known as vendor impersonation, can be devastating. In these elaborate attacks, which make up just 0.3% of all spear-phishing emails, cybercriminals insert themselves into existing business conversations or initiate new conversations based on information they've gathered from compromised email accounts or other sources.

Conversation hijacking is typically part of an account-takeover attack. Attackers use phishing attacks to steal login credentials and compromise business accounts. They read through emails and monitor the compromised account to understand business operations and learn about deals in progress, payment procedures, and other details. Criminals leverage this information, including internal and external conversations between employees, partners, and customers, to craft convincing messages, send them from impersonated domains, and trick victims into wiring money or updating payment information.

Account compromise or account takeover is often the result of phishing attacks. Hackers use social engineering tactics to trick users into disclosing their login credentials, which are then used to get inside an organization's network. Once inside, hackers can spread laterally within an organization, compromising more valuable accounts or using compromised accounts as launch pads for further attacks.

In 2022, based on Barracuda's data and analysis, nearly one in four organizations (24%) had at least one email account compromised through account takeover. Hackers sent an average of 370 malicious emails from each compromised account.

The rest of this report looks at the experience of spear-phishing around the world, the impact of attacks, detection and response challenges, and a variety of related issues.



The impact and costs of spear-phishing attacks

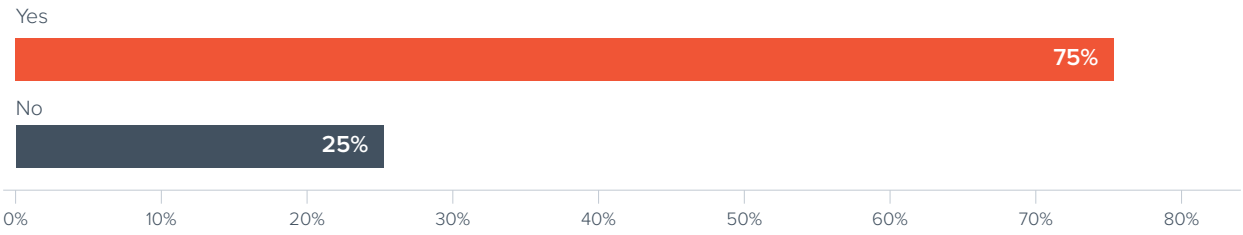
While spear-phishing attacks are low volume, they are widespread and highly successful compared to other types of email attacks.

The success of spear-phishing attacks

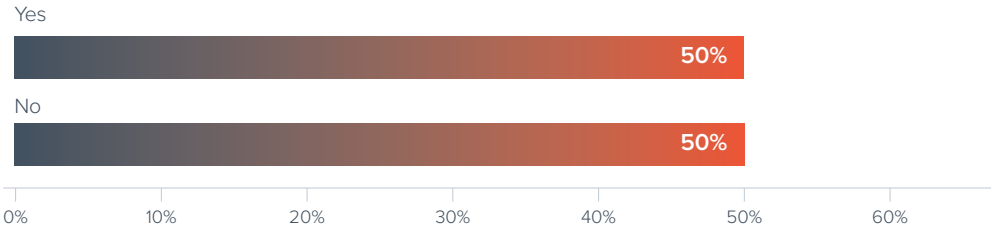
Three-quarters of respondents surveyed said they fell victim to an email attack in the last 12 months. Half said they were the victims of spear phishing. That means 2 out of 3 successful email attacks are spear-phishing attacks that use personalized messages, social engineering, and other tactics.

This is significant because these attacks make up only 0.1% of all email-based attacks according to Barracuda's data but are responsible for 66% of all breaches. On the other hand, high-volume attacks such as spam and malware, make up 16% of emails but are only responsible for one-third of breaches. Spear-phishing protection is critical because even just one successful attack can be devastating.

Has your organization faced any successful email-based attacks in the past year? (n=1,350)

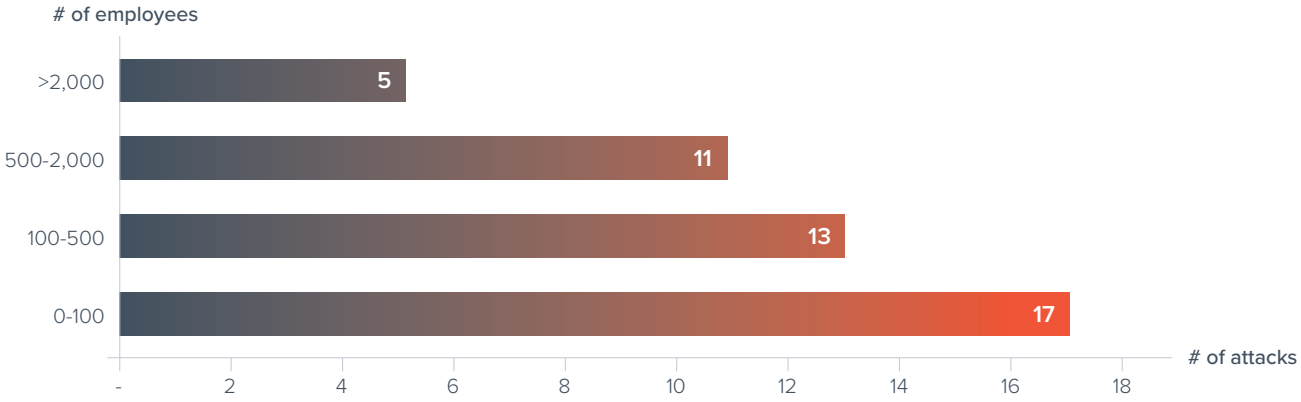


Was your organization a victim of spear phishing in the past 12 months? (n=1,350)



While smaller organizations report fewer successful email attacks caused by spear phishing (42%), Barracuda's 2022 report, Spear Phishing: Top Threats and Trends (Volume 7), showed that smaller businesses are being disproportionately attacked, with a higher average number of social engineering attacks per mailbox. Smaller organizations don't often have the tool necessary to identify and block sophisticated attacks or even identify and respond to attacks in progress. Many may not be aware of the volume of threats already in their users' inboxes.

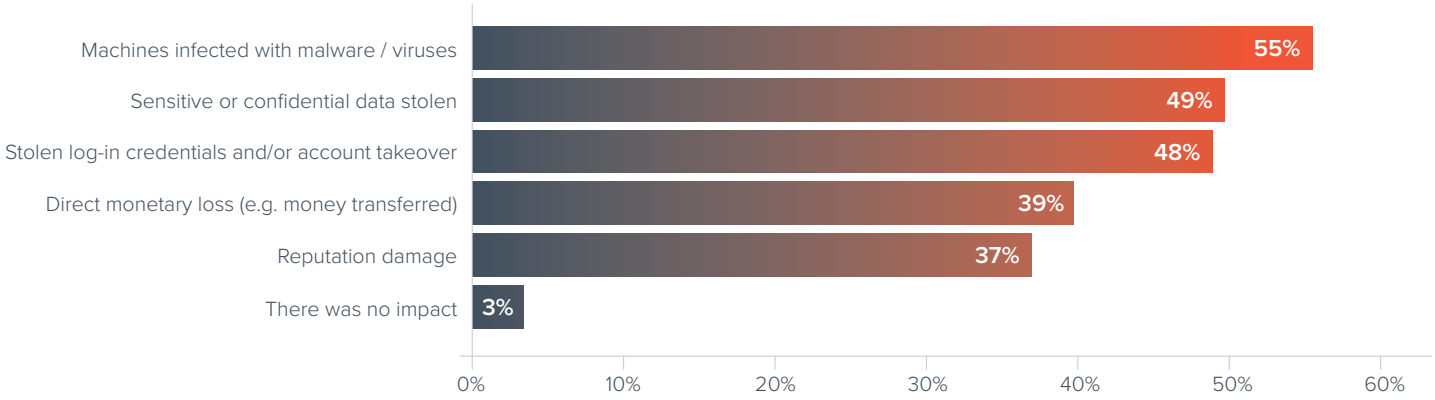
Average number of social engineering attacks per mailbox



According to our recent market survey, organizations using Gmail are more likely to report falling victim to spear-phishing attacks than those using Microsoft 365 — 57% of organizations using Gmail reported a successful spear-phishing attack, compared to 41% for those using Microsoft. In the Microsoft environment, there are many security options available to layer on, which provides better protection.

The impact of spear-phishing attacks

What was the imapct of the spear phishing attacks that occured in your organization in the past 12 months? (n=678)

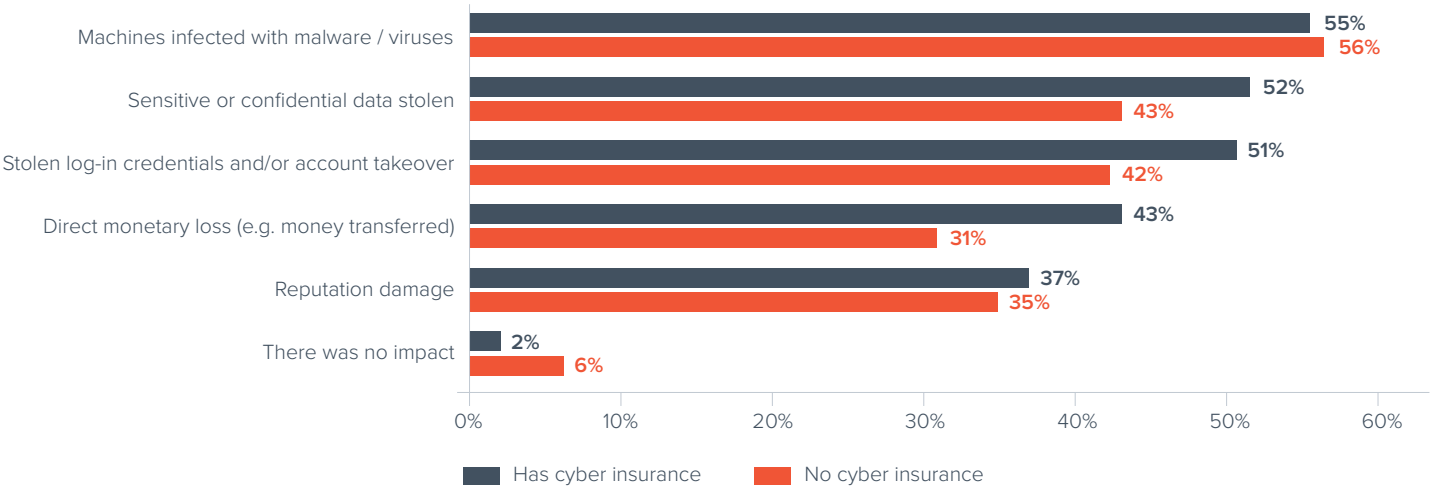


Nearly every victim of a spear-phishing attack in the last 12 months saw impacts on their organization, including malware infections, stolen data, and reputational damage. While a direct monetary loss is one of the effects, all the other impacts could also result in some financial damage for an organization as a result of an attack.

Hackers looking to launch malware attacks, such as those involving ransomware, often rely on phishing to get inside an organization. Stealing credentials is also a common goal of these attacks, as scammers are increasingly relying on spear-phishing tactics to gain access and then execute account takeover attacks. Of those who reported being a victim of a spear-phishing attack in the last 12 months, nearly half said they were the victims of stolen log-in credentials and/or account takeover.

For organizations with no cyber insurance in place, infected machines were the most frequently cited impact of spear-phishing attacks. While those that have cyber insurance also experienced this impact, they were more likely to experience other effects, including stolen information, stolen credentials, and direct monetary losses. The difference could be that only companies with sensitive information to steal would cite that as an impact. It's also possible that companies aren't aware of these problems and aren't looking for impacts, like the loss of sensitive information or stolen credentials.

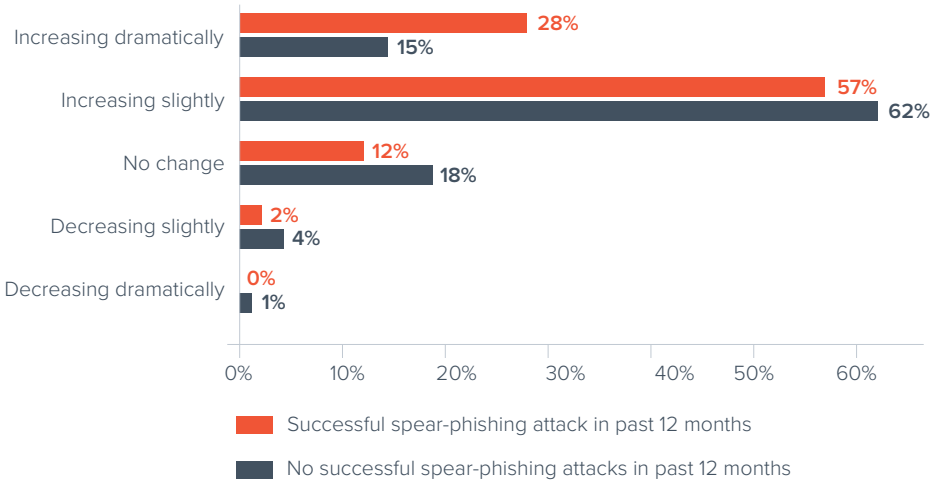
What was the impact of the spear phishing attacks that occured in your organization in the past 12 months? (n=678)



The costs of spear-phishing attacks

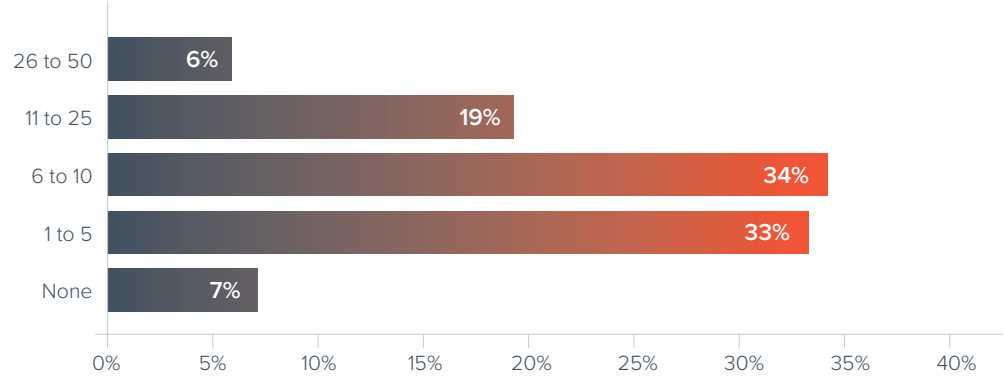
Organizations hit with a spear-phishing attack were more likely to say the costs associated with an email security breach had increased dramatically in the last year — 28% versus 15% of those who hadn't been victims of spear-phishing. These organizations are also more likely to have higher overall recovery and impact costs for the most expensive attack they suffer — an average of $1.1 million compared to $760,882 for those who were the victims of other types of email-based attacks.

How has the total cost of email security breaches changed over the past 12 months? (n=1,003)



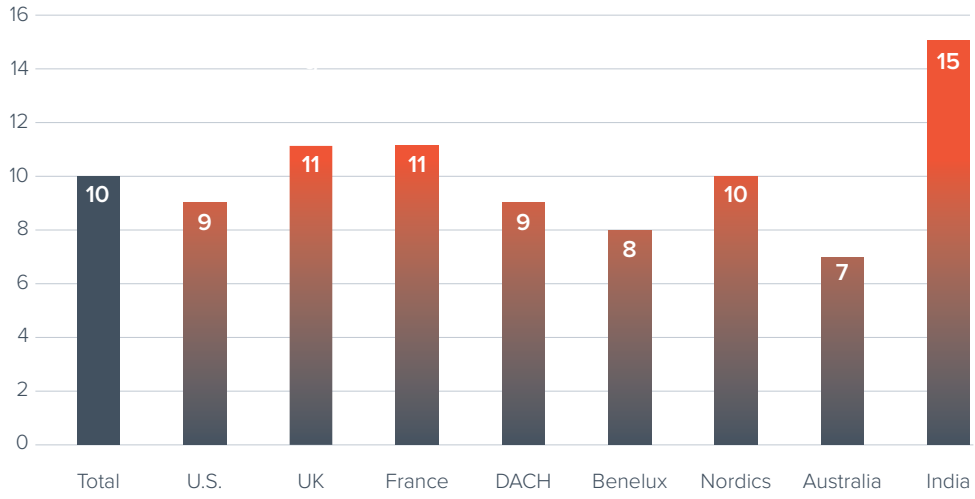
93% of organizations had users report suspicious messages post-delivery

Approximately how many suspicious emails are reported to your organization's IT on a typical work day? (n=1,350)



An average of 10 suspicious emails are reported to IT on a typical workday

Approximately how many suspicious emails are reported to your organization's IT on a typical work day? (n=1,350)



By region, users in India report the highest average number of suspicious emails per day — 50% more than the global average. This could be evidence that organizations are struggling to prevent email-based attacks or that organizations in India are placing a higher focus on suspicious emails and are discovering and reporting a higher average as a result. However, a large number of messages being reported is not always a good thing; it could also mean users are reporting a lot of gray mail or unwanted messages rather than malicious emails.

7% of organizations worldwide don't have any emails being reported by their users. In DACH and Australia, the numbers are particularly high, with 14% saying no emails are reported. These regions also have below-average levels of adoption of computer-based security awareness training. While the global average is 42%, in Australia, it's 28%, and in DACH, it's 37%. Lower investment in security awareness may have contributed to users being less vigilant or less able to recognize a potential email threat.

Based on the highly personalized nature of spear-phishing emails and the potentially severe impacts of a successful attack, every organization, regardless of size and location, should take the appropriate precautions to prevent these attacks.

Proportionately, users in larger organizations report fewer suspicious emails

The number of attacks being reported by users isn't proportionate to the size of their organizations. Organizations with 100-249 employees have an average of 7 suspicious emails reported per day, while at businesses with 1,000-2,500 employees, users report an average of 12 per day. As we have seen previously, smaller organizations actually receive a larger volume of spear-phishing attacks proportionate to their size.

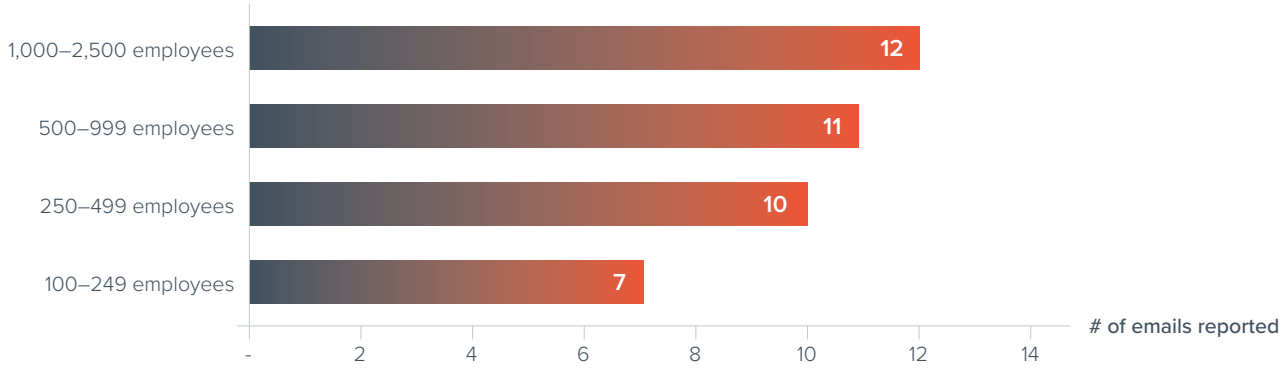
This larger volume of attacks and some potentially overzealous reporters could mean that IT teams need to process a larger number of messages. Unfortunately, smaller organizations have smaller IT teams, so they don't always have enough tools and resources to process all potential incidents.

Larger organizations are more likely to leverage tools and resources to help prioritize incidents that need to be addressed and quickly determine the difference between benign and malicious emails.

Users in companies with more than a 50% remote workforce report higher levels of suspicious emails — 12 per day on average, compared to 9 per day for those with less than a 50% remote workforce. Due to the dispersed nature of their employees, organizations with larger remote workforces are more sensitive to potential threats. Given that they are more likely to fall victim to a spear-phishing attack, they may welcome some overreporting from their users.

At organizations hit with multiple ransomware attacks, employees also report higher levels of suspicious emails — a daily average of 17 suspicious emails for businesses hit with three or more ransomware attacks. Security awareness among users in organizations is likely to increase after ransomware attacks, possibly leading to users overreporting

Approximately, how many suspicious emails are reported to your organization's IT on a typical work day? (average) (n=1,350)



Threat detection and response challenges

No security is effective 100 percent of the time. When a threat gets through, security teams need to act fast to identify and respond before it spreads and causes extensive damage. Faster detection and response times lower the risk of a security breach.

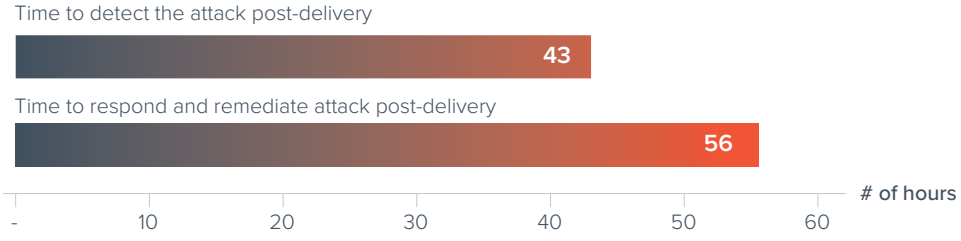
On average, organizations take nearly 100 hours to identify, respond to, and remediate a post-delivery email threat

With an average detection time of 43 hours and an average response and remediation time of 56 hours for post-delivery email threats, organizations take almost 100 hours to deal with an email security incident.

For 1 in 5 organizations (22%), it takes longer than 24 hours to identify an email attack. This long period gives users ample time and opportunity to click on a malicious link or respond to an email. When that happens, hackers are able to use the compromised account to get inside the network and potentially compromise additional accounts. If long detection times aren't concerning enough, 38% of respondents reported taking more than 24 hours to respond to and remediate attacks once they become aware of them.

Detection, response, and remediation times are shorter on average for larger organizations, which typically have more resources available and can respond more quickly. While the larger size has the potential to make the company susceptible to more threats, a larger team is likely available to help with efforts to detect, respond to, and remediate any impacts from attacks.

Thinking about your detection and response times of post-delivery or reported email incidents, aproximately how long does it take for your organization to do the following? (hours) (n=1,350)

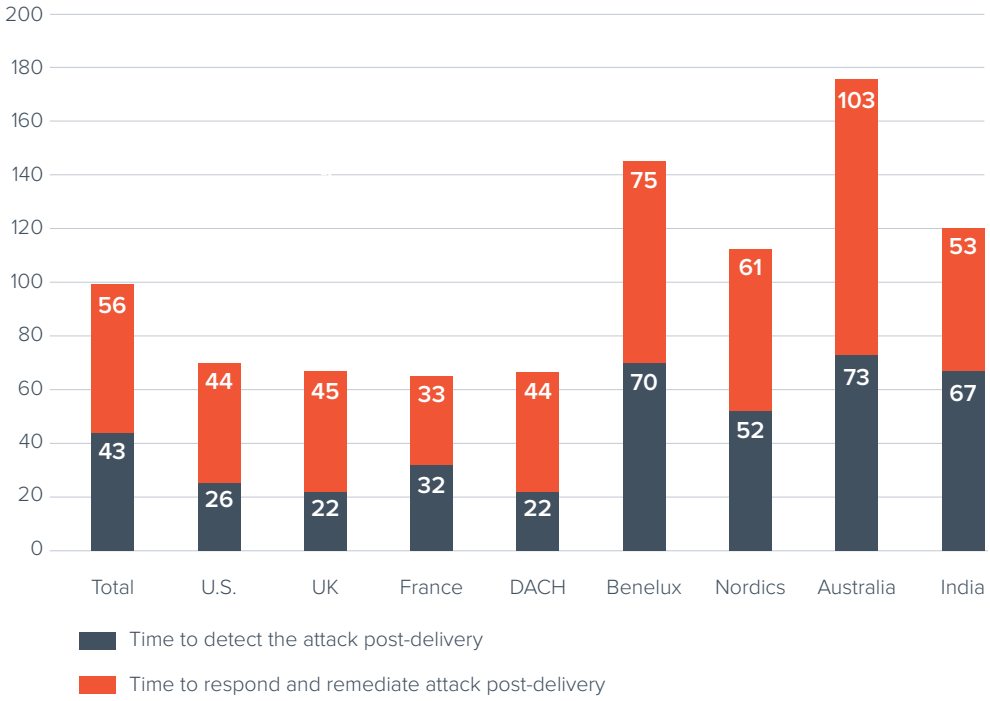


Investment in automation and security training cuts response times

Australia's low adoption rate (24%) for automated incident response may very well be a factor for their long response times. Australia also has the lowest adoption rates of computer-based security awareness training. The responsibility to uncover and respond to post-delivery threats falls mostly on IT, which takes too long without the necessary tools — 175 hours on average in Australia.

On the other hand, 36% of organizations in the United States use automated incident response, and 45% use computer-based security awareness training. They also report faster response times on average, which means they are using fewer IT resources and those resources can focus on other tasks.

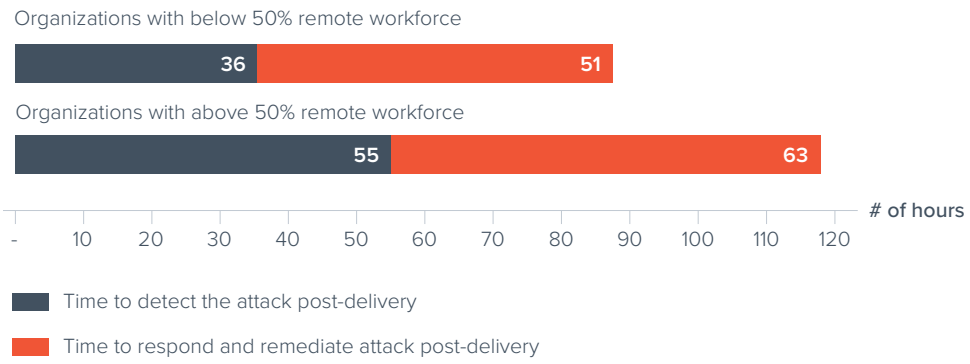
Thinking about your detection and response times of post-delivery or reported email incidents, aproximately how long does it take for your organization to do the following? (hours) (n=1,350)



Having more remote workers slows detection and response time

It takes organizations with more remote workers longer to both detect and respond to email security incidents. Organizations with less than a 50% remote workforce had average detection times of 36 hours, while those with more than a 50% remote workforce took an average of 55 hours to detect an email security incident. Likewise for remediation: Those with less than a 50% remote workforce had an average response and mitigation time of 51 hours, while those with more than a 50% remote workforce took an average of 63 hours to respond to and mitigate an email security incident.

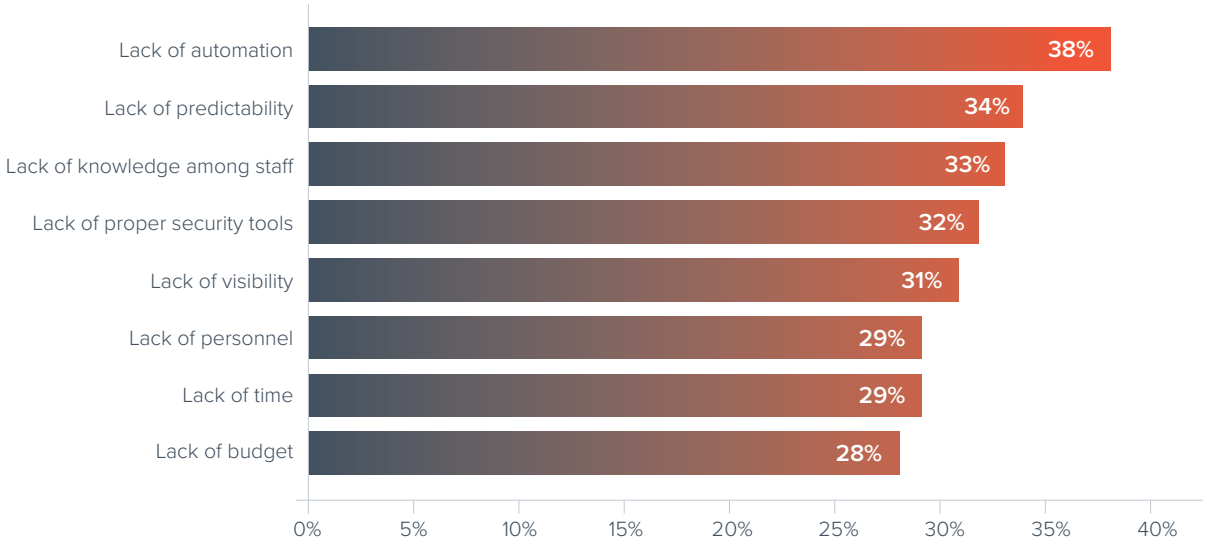
Thinking about your detection and response times of post-delivery or reported email incidents, aproximately how long does it take for your organization to do the following? (hours) (n=1,350)



Lack of automation is a top obstacle

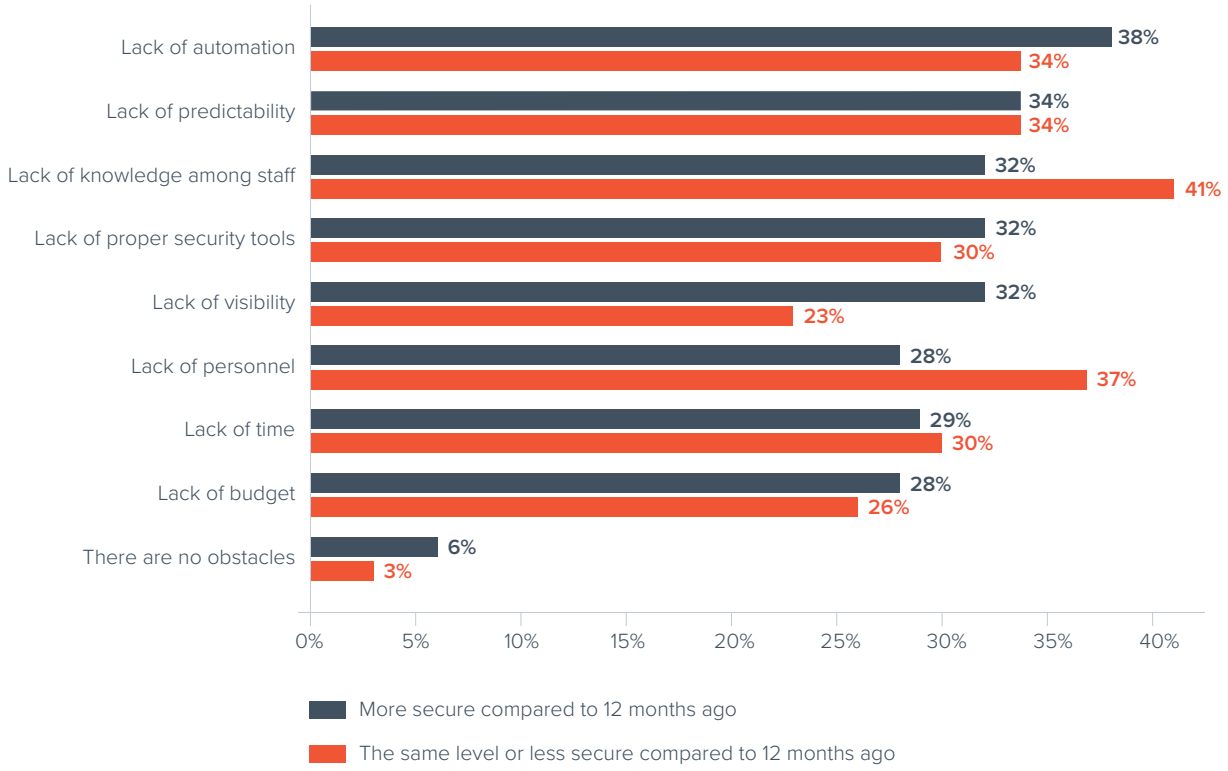
Larger organizations cite lack of automation as the most likely obstacle preventing a rapid response to an incident — 41% for organizations with more than 250 employees, compared to 28% for organizations with 100–249 staff. These smaller companies cite additional reasons almost equally, including the lack of predictability (29%), knowledge among staff (32%), and proper security tools (32%). Smaller companies appear to be still in the process of adopting appropriate tools and appear to have difficulty hiring and retaining knowledgeable staff. Once organizations have the right people, processes, and technology in place, they can take advantage of accelerators available to expedite response work, including automation.

What are the main obstacles that prevent fast detection and response to post-delivery email threats in your organization? (n=1,350)



Companies that feel more secure also say lack of automation is the most likely obstacle to fast incident response. In contrast, companies that feel less secure cite a lack of knowledgeable staff. Having knowledgeable staff is a prerequisite to having a strong incident response program, and automation can help significantly accelerate that response.

What are the main obstacles that prevent fast detection and response to post-delivery email threats in your organization? (n=1,350)



Best practices to defeat spear phishing

As email attacks evolve and become more sophisticated, organizations are facing serious threats from targeted spear-phishing attacks. The impact of just one successful attack can be devastating. To protect your business, you must invest in technology that blocks attacks and in training that helps people act as the last line of defense.

Technology

- **Take advantage of artificial intelligence.** Scammers are adapting email tactics to bypass gateways and spam filters, so it's critical to have a solution in place that detects and protects against spear-phishing attacks, including business email compromise, impersonation, and extortion attacks. Deploy purpose-built technology that doesn't solely rely on looking for malicious links or attachments. Use machine learning to analyze normal communication patterns in your organization and to spot anomalies that may indicate an attack.

- **Deploy account-takeover protection.** Ensure scammers aren't using compromised accounts in your organization to launch spear-phishing attacks. Use technology with artificial intelligence to recognize when accounts have been compromised and that remediates in real time by alerting users and removing malicious emails sent from compromised accounts.

- **Monitor inbox rules and suspicious logins.** Use technology to identify suspicious activity, including logins from unusual locations and IP addresses, a potential sign of a compromised account. Be sure to also monitor email accounts for malicious inbox rules, as they are often used to hide or delete emails sent as part of an account-takeover attack.

- **Use multifactor authentication.** Provide an additional layer of security above and beyond username and password, such as an authentication code, thumb print, or biometric authentication.

- **Implement DMARC authentication and reporting.** This helps defeat domain spoofing, one of the most common techniques used in impersonation attacks. Stop domain spoofing and brand hijacking with DMARC authentication and enforcement. Accurately set enforcement rules for your organization with the help of DMARC reporting and analysis.

- **Automate incident response.** With an automated incident response solution, you can quickly clean up any threats found in inboxes and make remediation more efficient for all messages going forward.

- **Train staffers to recognize and report attacks.** Educate users about spear-phishing attacks by making it a part of security awareness training. Ensure staffers can recognize these attacks, understand their fraudulent nature, and know how to report them.

- **Maximize data-loss prevention.** Use the right combination of technologies and business policies to ensure emails with confidential, personally identifiable, and other sensitive information are blocked from leaving the company.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level

Get more information at barracuda.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research in the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision-makers across technical and business functions in all business sectors and all major markets.

For more information, visit vansonbourne.com.

Barracuda®
Your journey, secured.