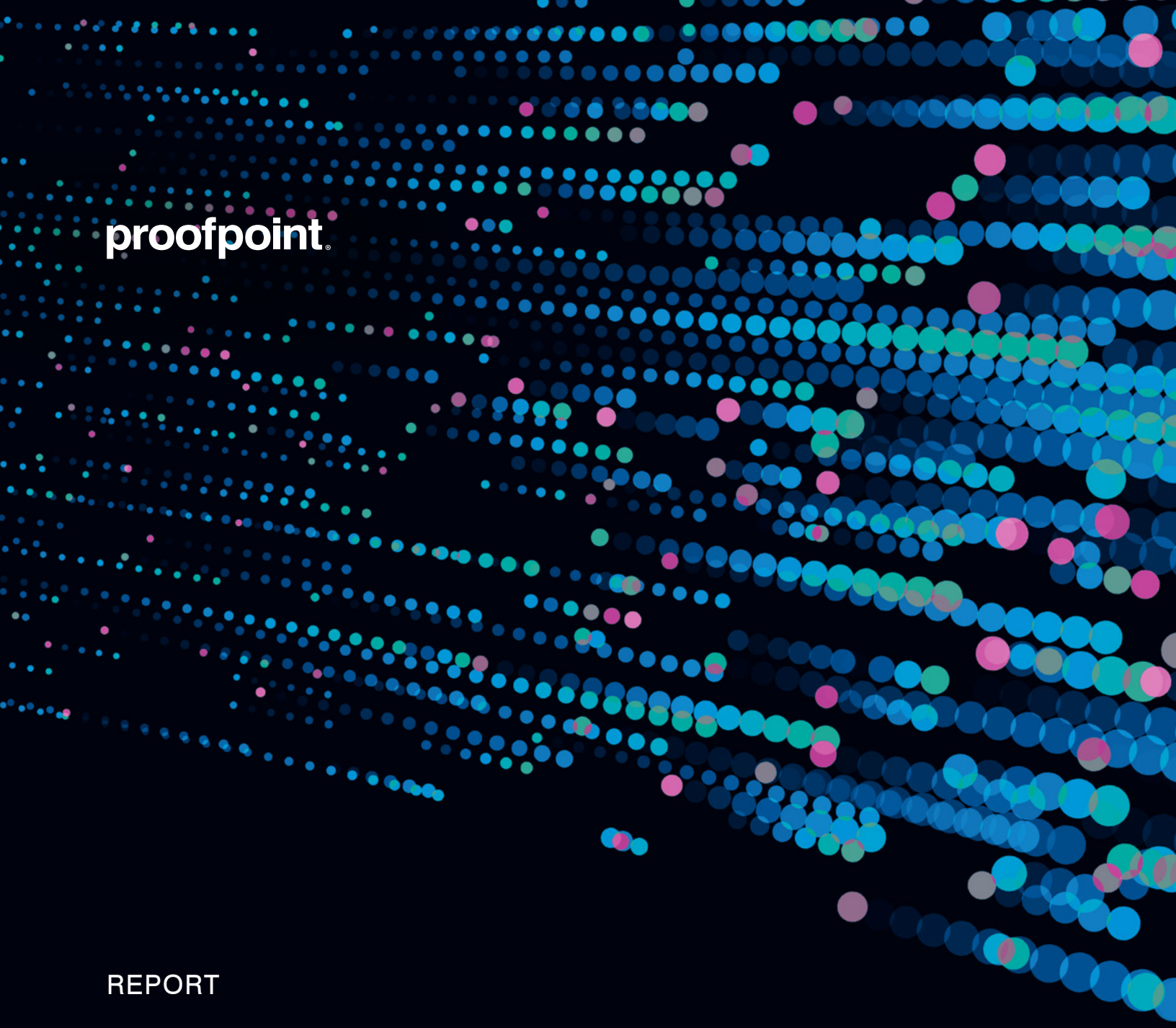


proofpoint

REPORT

2024 State of the Phish

Risky actions, real-world threats and user resilience in an age of human-centric cybersecurity

INTRODUCTION

Imagine a successful cyberattack against your organization. What does it look like? Maybe it involves a fiendishly clever piece of social engineering—a convincing lure that catches the recipient off guard. Or maybe it would take a smart technical exploit to get past your defenses. But in reality, threat actors don't always have to try that hard.

Often, the easiest way to breach security is to exploit the human factor. People are a key part of any good defense, but they can also be the most vulnerable. They may make mistakes, fall for scams or simply ignore security best practices. According to this year's State of the Phish survey, 71% of working adults admitted to taking a risky action, such as reusing or sharing a password, clicking on links from unknown senders, or giving credentials to an untrustworthy source. And 96% of them did so knowing that they were taking a risk.

When obliged to choose between convenience and security, users pick the former almost every time. So, what can organizations do to change this? In this report we'll take a closer look at how attitudes towards security manifest in real-world behavior, and how threat actors are finding new ways to take advantage of our preference for speed and expedience. We'll also examine the current state of security awareness initiatives, as well as benchmarking the resilience of people and organizations against attack.

The foundation of this report is a survey of 7,500 end users and 1,050 security professionals, conducted across 15 countries. It also includes Proofpoint data derived from our products and threat research, as well as findings from 183 million simulated phishing messages sent by our customers over a 12-month period and more than 24 million emails reported by our customers' end users over the same period.

TABLE OF CONTENTS

KEY FINDINGS

Over 1 million

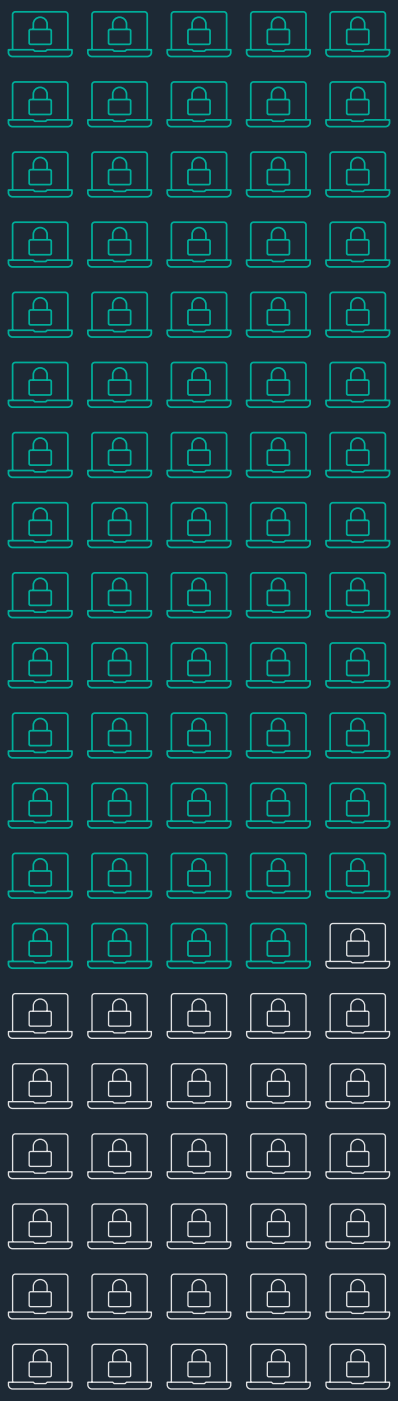
attacks are launched with MFA-bypass framework EvilProxy every month, but 89% of security professionals still believe MFA provides complete protection against account takeover.

of users took a risky action

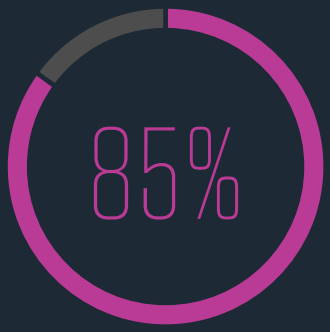
of them knew they were doing something risky

66 million

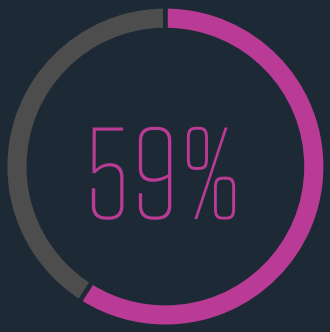
BEC attacks were detected and blocked on average per month by Proofpoint.



69% of organizations were infected by ransomware.



of security professionals said that most employees know they are responsible for security, but



of users either weren't sure or claimed that they're not responsible at all.

10 million

TOAD messages are sent every month.

Microsoft continues to be the most abused brand, with

68 million

malicious messages associated with the brand or its products.

58% of users who took risky actions engaged in behavior that would have made them vulnerable to common social engineering tactics.

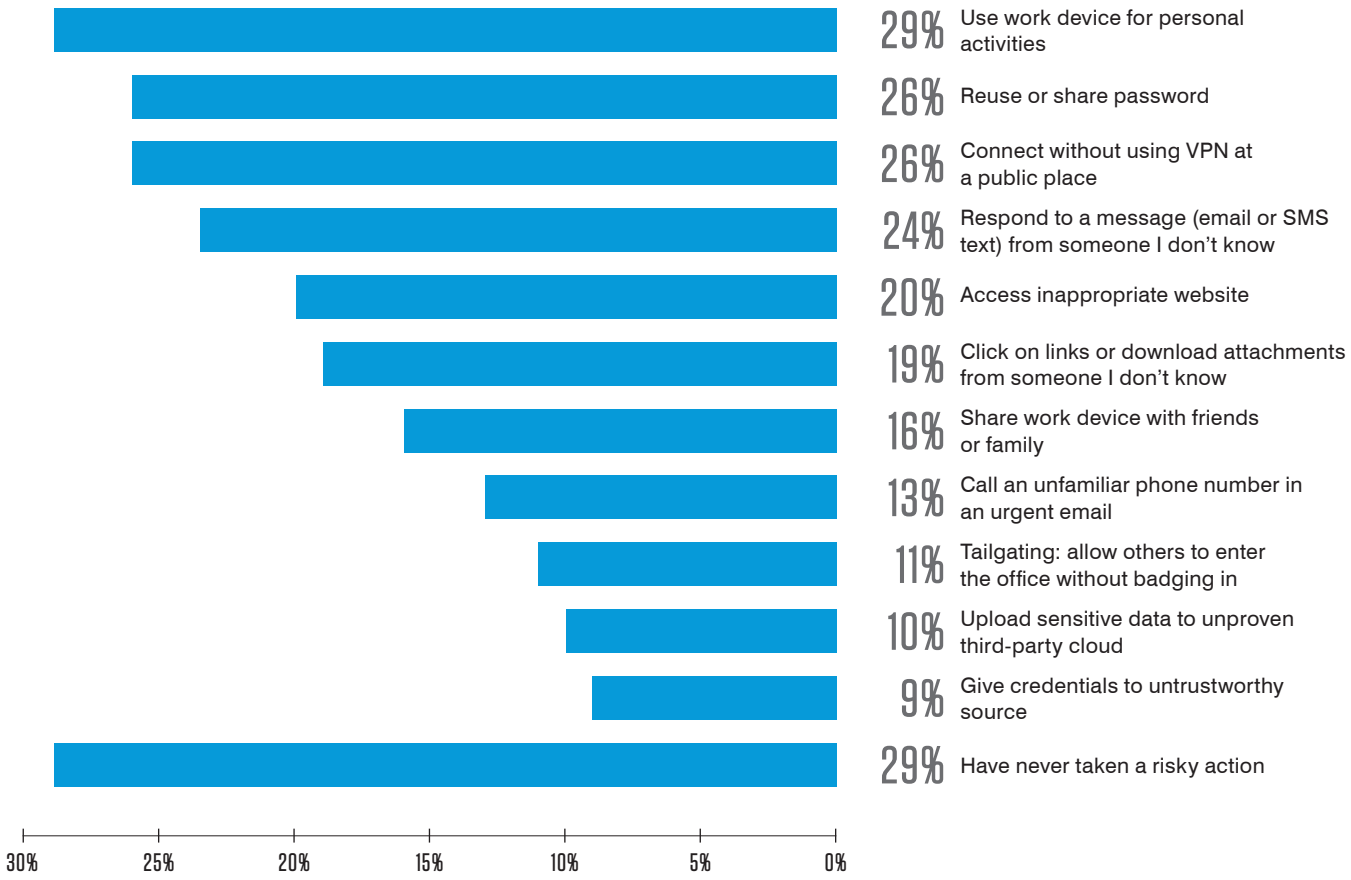
Security Behaviors and Attitudes

Even the best technical defenses can be undermined if users don't do the basics, such as avoiding suspicious links, verifying the sender's identity and setting a strong password and keeping it to themselves. However, many users fail to follow these simple rules, putting themselves and their organizations at risk.

End-user behavior and attitudes

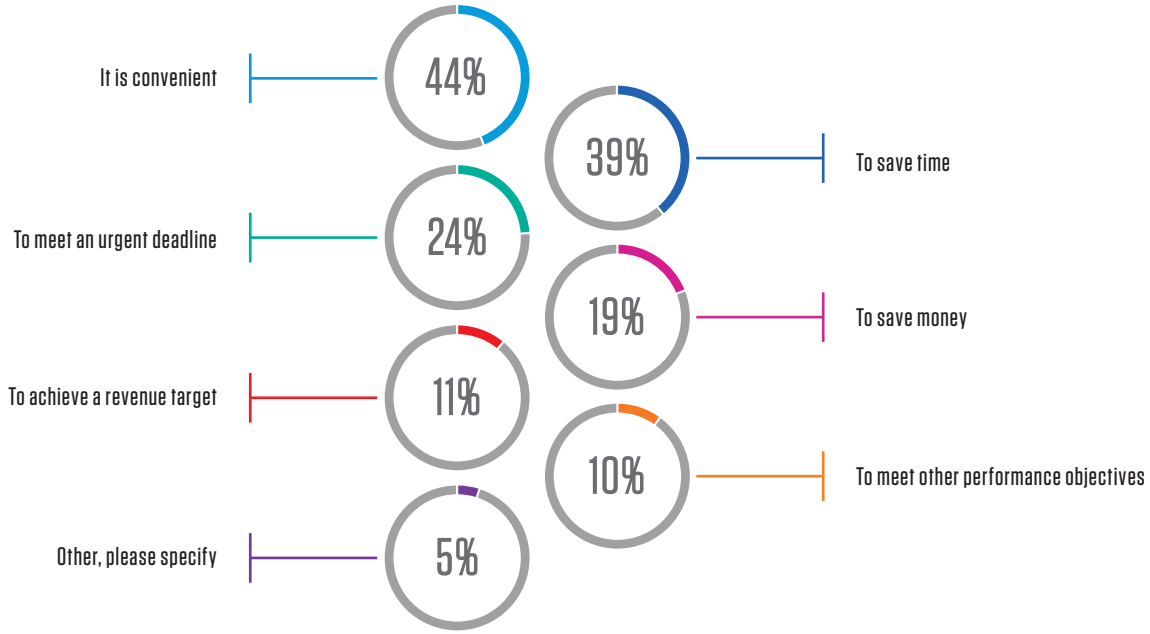
According to our survey, 71% of users said they took a risky action and almost all of them—96%—did so knowingly. Among that group, 73% said they'd taken two or more risky actions. And more than a third of the risks they took were rated by those users as either "extremely risky" or "very risky."

Risky Actions Taken



Users took risky actions for a variety of reasons: convenience, time saving and urgency being the most common answers. But a small cohort of 2.5% took risky actions purely out of curiosity. Either way, the message is clear: people aren't taking risky actions because they lack security awareness. Often, users know what they are doing when they take risks and are quite willing to gamble with organizational security.

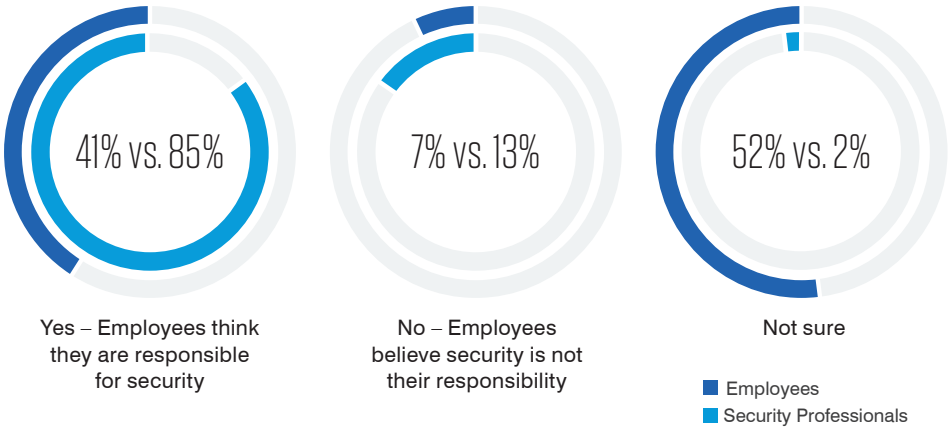
Why Risky Action is Taken



Nobody knows this better than the world's cybercriminals. They understand that people can be exploited, either through negligence, obliviousness or—in rare instances—malice. Social engineering is a part of almost every email threat analyzed by our researchers. And 58% of users who took a risky action said they engaged in behavior that would put them at risk of basic social engineering tactics, such as clicking on unknown links, responding to unfamiliar senders and sharing credentials with untrustworthy sources. These actions can lead to ransomware infection, malware, data breach or financial loss.

One of the reasons users take these risks is a lack of consensus about accountability and responsibility. Only 41% of users said they know that they bear responsibility for cybersecurity at their workplace. About 7% claimed that they aren't responsible at all, while the majority (52%) weren't sure.

Perception on Security Responsibility



This contrasts with the view among security professionals, 85% of whom say that most employees know they are responsible for security. This gap between perception and reality suggests that there is a need for clearer communication about shared responsibility, rather than just more training on security best practices and policies.

63%

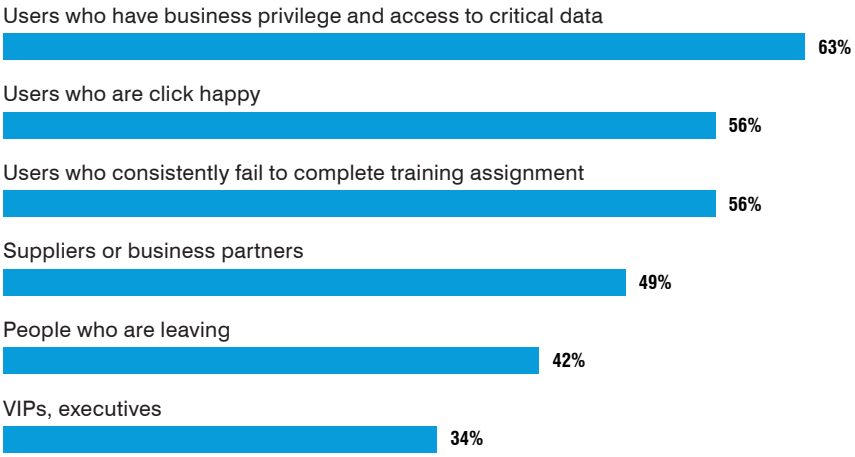
of security professionals rated users with access to critical business data as the top cybersecurity risk

The professional view

Security professionals understandably have a different perspective on security risks to end users. They are more aware of the threat landscape and the consequences of a breach. And they have a more nuanced understanding of the challenges that go into securing complex and dynamic environments. They also have the unenviable task of finding ways to balance the need for security with the need for unhindered productivity and efficiency.

According to our survey of security professionals, they rate users with access to business-critical data as the biggest security risk (63%)—a group that is inevitably hard to manage, as much of that access is necessary. But click-happy users and those who don't complete security awareness training are close behind in joint second place (56% each). These categories of user were all considered significantly more risky than executives/VIPs (34%), despite the latter group often having broad access to valuable data.

Users Who Represent Risk



Unfortunately, our survey reveals significant overlap between the riskiest behaviors identified by security professionals and the most common risky actions taken by end users. Reusing passwords, using work devices for personal activities and accessing inappropriate websites are among behaviors considered the most unsafe; all of them appeared in the top actions taken by users.

Rank	Top Risks Considered by Infosec	Top Risky Actions Taken by Users
1	Click on links or download attachments from someone I don't know	Use work device for personal activities
2	Reuse or share password	Reuse or share password
3	Access inappropriate website	Connect without using VPN at a public place
4	Upload sensitive data to unproven third-party cloud	Respond to a message (email or SMS text) from someone I don't know
5	Use work device for personal activities	Access inappropriate website

This overlap suggests that users may be taking some of these actions because they are unaware of just how risky they are considered by security teams.

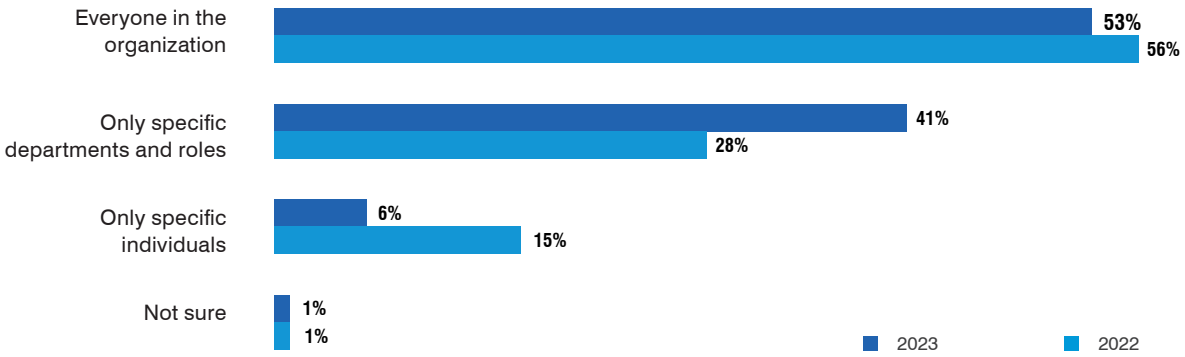
Security Awareness Trends

While training alone isn't enough to change unsafe behavior, teams that lack basic security awareness tools and knowledge are still much more likely to fall prey to cybercriminals. But as new social engineering lures and techniques appear on the threat landscape, awareness programs must be agile and broad-based to remain relevant.

Current state of security awareness

First some positive news: 99% of respondents said they have a security awareness program of some sort up and running. But while the basics may already be in place, many are struggling to drive real behavioral change. A possible reason for this is that only 53% say they train everyone in the organization (down from 56% last year). This means that some users may be left out of the loop or may receive inadequate or outdated training.

Security Awareness Activities Assignment



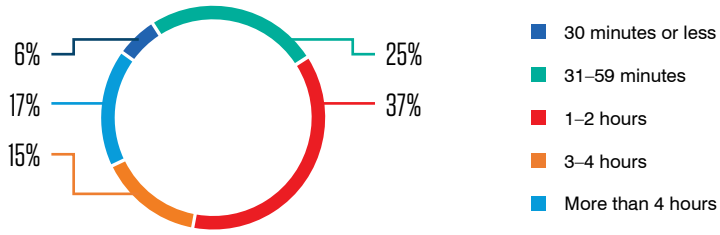
Another challenge is the coverage and relevance of training topics. Security professionals agree that remote work, password hygiene and internet safety are critical, but less than a third of security awareness programs cover all these topics. The top training topics cited by respondents were malware, Wi-Fi security, ransomware and email phishing, which are all important, but not sufficient to address the full spectrum of risks. And as we'll see later when we examine the latest cybercriminal tactics and techniques, emerging threats can quickly become commonplace, taking unprepared users by surprise.

41% from 28%

The percentage of organizations that trained specific roles jumped year over year

On the positive side, the survey shows some signs of improvement and innovation in security awareness tactics. Year over year, training of specific roles and departments has risen significantly (41% from 28%), indicating a more tailored and targeted approach. Time allocated to user education has also increased year over year, with more respondents dedicating over three hours per year to awareness training. Overall, the average amount of time dedicated to awareness training has increased for the first time in three years.

Time Allocated for Security Awareness Activities



The types of tactics being used are evolving, too, with a 23% increase in the use of contests and prizes to gamify and incentivize attention. This change can help increase user engagement and motivation, while also creating a positive and fun learning environment. Computer-based training remains the most common format (45%), but other methods such as simulated USB drops, videos, posters and newsletters are also being used.

In-person training sessions	**37%**
Virtual, instructor-led training	**34%**
Computer-based training	**45%**
Simulated phishing attacks	**34%**
Awareness posters and videos	**31%**
Newsletters and emails	**38%**

Cybersecurity-based contests and prizes	**33%**
Smishing and vishing simulations	**33%**
Simulated USB drops	**23%**
Internal cybersecurity chat channel	**30%**
Internal wiki	**23%**
My company does not have a security awareness program	**1%**

However, only 34% of respondents say they perform simulated phishing attacks, despite the high volume of malicious email seen in the threat landscape. This suggests that there is still room for improvement in the composition of most security awareness training syllabuses.

Areas for improvement

Security is not only a technical issue, but also a cultural and organizational one. It requires the collaboration and commitment of all stakeholders, from security professionals to end users. However, there is often a gap between what security professionals think is effective and what end users say would motivate them to prioritize security

83%

of surveyed security professionals implement more training to drive behavior change

81%

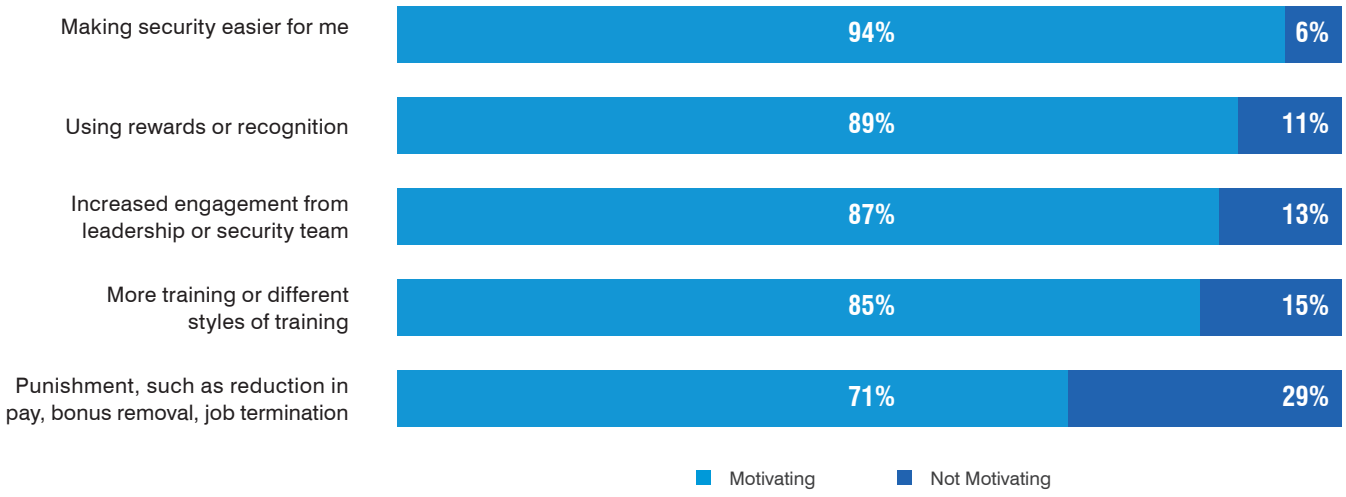
implement more controls or restrictions

According to our survey, security professionals believe that more training, tighter controls, closer business alignment, better rewards and stronger championing of security initiatives would all be effective in improving security. However, fewer than a third of organizations reward positive user behaviors or champion security initiatives. These are important ways to recognize and reinforce good security practices, and to ensure that all employees are invested in creating a security-aware culture.

Rank	Actions Taken by Security Pros	User Motivation
1	Provide more training	Making security easier for me
2	Implement more security controls or restrictions	Using rewards and recognition
3	Align security initiatives with business priorities	Increased engagement with leadership and security teams

In contrast, users overwhelmingly say that they want security to be made easier. They want processes to be more user-friendly, convenient and transparent, and they want to have more communication and feedback from security experts. Users overwhelmingly agree (94%) that improving ease of use would motivate them to be more attentive to security. These disparities between security team actions and user motivations clearly demonstrate the need for open communication between security teams and end users.

What Policies Motivate Users to Prioritize Cybersecurity



In keeping with trends we've observed over the past few years, punishing unwanted behavior was considered the least effective approach by security professionals. Fortunately, it was also the least implemented. Punishment can have negative effects, such as creating fear, resentment and distrust, and reducing motivation and morale. It can also discourage users from reporting incidents or seeking help, which can seriously increase the risk of security breaches. Punishment was also the least motivating response among end users, though 71% still agreed that this would be an incentive for them. This suggests that some users may be willing to comply with security rules to avoid negative consequences, though it is unlikely that compelled participation will lead to enduring behavior change.

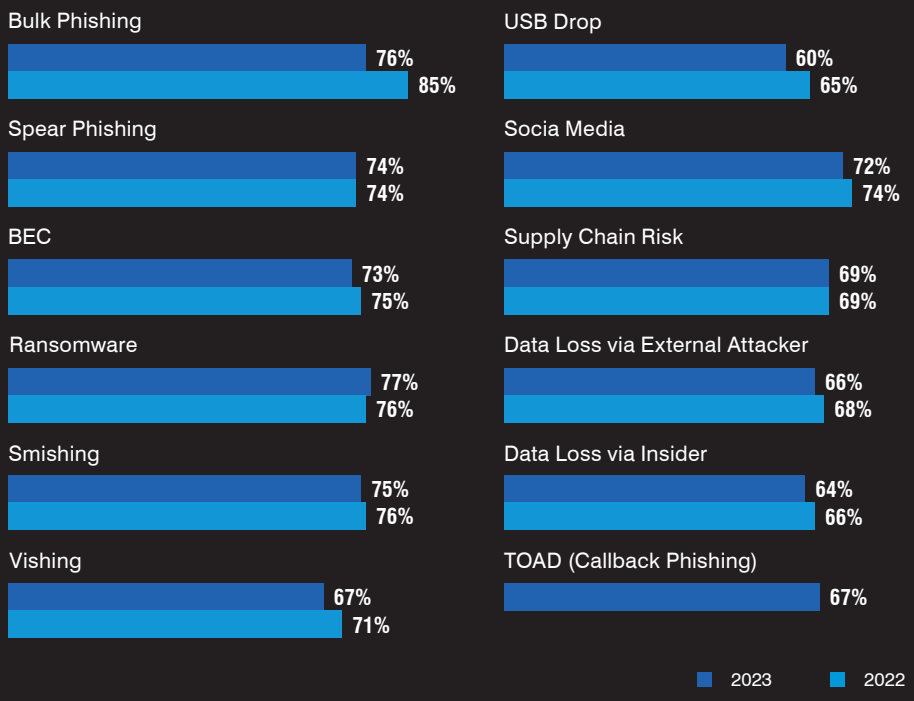
The Threat Landscape

Cybersecurity is a constantly evolving field as cybercriminals devise new and sophisticated ways to attack people and breach organizations. Users who take risks, such as clicking on suspicious links, opening unknown attachments or using weak passwords, face an increasing variety of real-world threats from attackers.

Threat prevalence

Some of the most common forms of attack reported by survey participants were phishing, business email compromise (BEC) and ransomware. While each of these techniques is distinct, security teams will often encounter them as individual components of an extended attack chain, with phishing leading to ransomware, or a supply chain attack leading to BEC.

Prevalence of Attacks



However, these aren't the only threats that users and organizations need to be aware of. According to our own data, many novel attack types are becoming increasingly prominent.

Growing threats: TOAD, MFA-Bypass, QR codes and generative AI

In telephone-oriented attack delivery (TOAD), the malicious message often appears to be completely benign, containing nothing more than a phone number and some erroneous information. It isn't until the unsuspecting victim calls the listed number for help that the attack chain is activated. Cybercriminal call centers are operating around the world, guiding victims into granting remote access, revealing sensitive information and credentials, or even infecting themselves with malware. Our data reveals that an average of 10 million TOAD messages are sent every month.

13 million

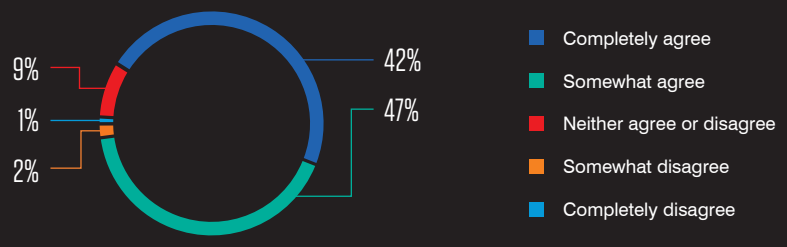
Proofpoint saw over 13M TOAD attacks at peak in August 2023

Another increasingly popular attack method involves using advanced techniques to bypass multifactor authentication (MFA), which is now a standard part of corporate cybersecurity. These attacks typically use proxy servers to intercept MFA tokens, allowing attackers to circumvent the additional layer of security provided by one-time codes and biometrics. Several off-the-shelf phish kits now include MFA bypass functionality, allowing even relatively unsophisticated attackers to benefit. We see around 1 million phishing threats using the popular EvilProxy framework every month. This is of particular concern, as 89% of security professionals still consider MFA to be a silver bullet for protection against account takeover, with 84% of respondents saying their organizations use MFA to prevent account takeover.

89%

of security pros believe that MFA can protect against account compromise completely

Does MFA Provide Complete Protection Against Account Takeover?



And within the paradigm of traditional phishing, attackers are finding new ways to embed malicious content. In recent months we've seen an increase in the use of QR codes as an alternative to links or attachments. This technique is particularly dangerous, as it both attempts to evade automated detection while presenting users with a familiar format in a context they may not have seen before. It is also impossible to tell just by looking if a QR code leads to a phishing site or malware download. Unfamiliar users scanning a QR code may not even be aware that they've engaged with a piece of malicious content until it's too late.

It's also worth noting that even the least common type of attack—USB drop—was still reported by 60% of respondents. This shows that cybercriminals are willing to try any tactic, old or new, if they think it will give them a chance to exploit an unsuspecting victim.

Despite the growing prominence and sophistication of these threats, many organizations are not adequately prepared or trained to deal with them. Only 23% of organizations train their users on how to recognize and prevent TOAD attacks, and only 23% educate their users on generative AI safety.

Generative AI is a technology that can create realistic and convincing content—such as images, videos or text—based on a given prompt or data input. This technology promises to enhance social engineering for all messaging-based attacks, as attackers can use it to improve the quality of their lure, particularly when targeting other languages. Moreover, generative AI also poses a risk of data loss, as there is currently little transparency over what happens to data that is uploaded to services such as ChatGPT and Google Bard.

BEC attacks benefit from AI

BEC attacks also continue to pose a serious threat, especially in non-English-speaking countries. Fewer organizations reported BEC attempts globally, but attacks continue to grow in prevalence among countries such as Japan (35% year-over-year increase), Korea (31% jump), and UAE (29% jump). These countries may have previously seen fewer BEC attacks due to language barriers, cultural differences or lack of visibility. But there is now a likely link between BEC and generative AI, as attackers can use the latter to create more convincing and personalized emails in multiple languages. Our own data shows an average of 66 million targeted BEC attacks every month.

Microsoft remains most-abused brand

Brand abuse is a favorite tactic for phishing and malware delivery, as attackers exploit the trust and familiarity that users have with certain brands. More than 68 million messages were associated with Microsoft products and brand in 2023, making it the most abused brand by cybercriminals. Adobe and DHL rounded out the top three, but at fewer than 10 million messages each.

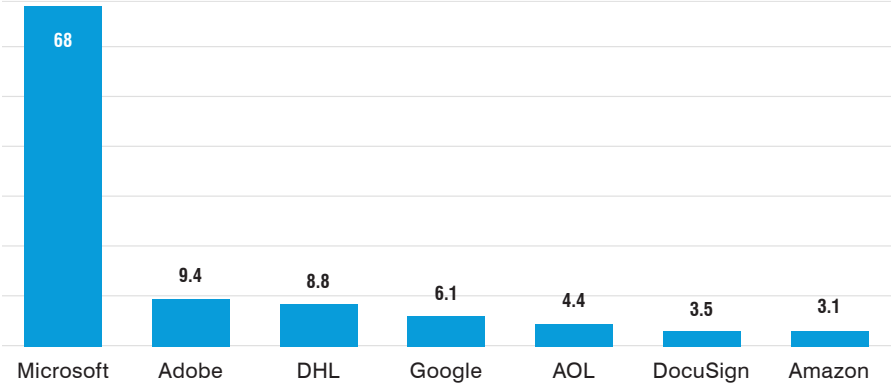
68 million

malicious messages included references to Microsoft and/or Microsoft products in 2023, making the software giant the world's most abused brand

20 million

Office 365 was the most abused Microsoft product in malicious email, with over 20 million email threats using the brand

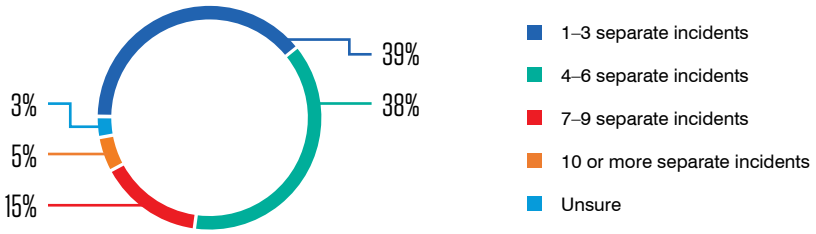
Brand Abuse Threats (Millions)



Ransomware still a major concern

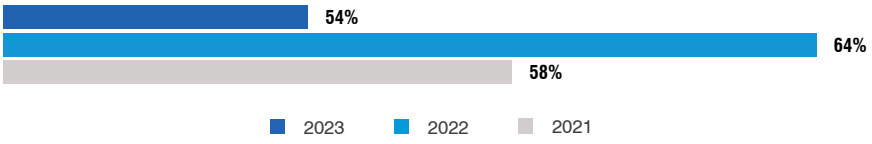
The percentage of organizations that faced a ransomware attack rose 5 percentage points to 69%. Almost 60% of organizations reported four or more separate ransomware incidents in a year, indicating that ransomware is still a persistent and lucrative form of attack.

Ransomware by the Numbers



One of the ways that organizations try to mitigate the risk and impact of cyberattacks is by purchasing cyber insurance, which covers the costs and damages associated with a cybersecurity incident. Among those that had experienced a ransomware incident, 96% now have cyber insurance. Most insurers (91%) helped with ransom payments, up from 82% the year before. However, globally, the rate of payment to ransomware attackers has declined from 64% to 54%.

Infected Organizations That Agreed to Pay Ransom

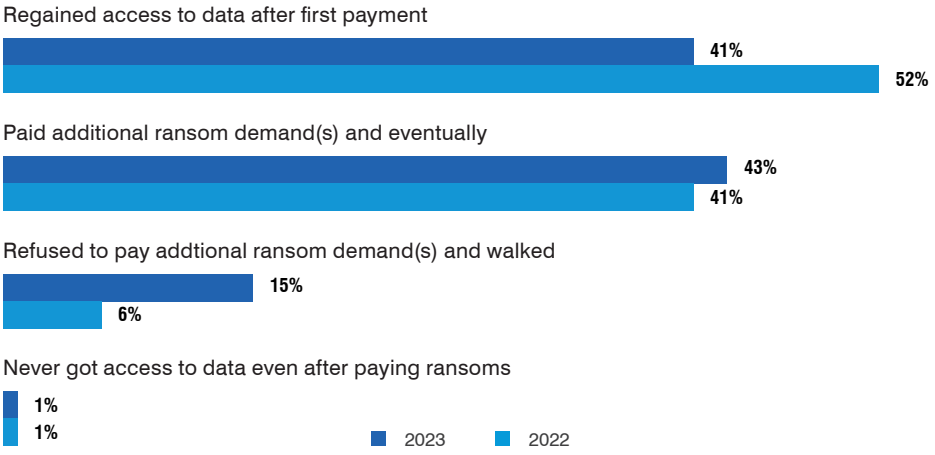


The number of respondents who regained access to their data after paying also declined, with the number who regained access after a single payment seeing the largest decline. This may be one explanation for the drop in payments. Another possible reason is that organizations are becoming more aware of the drawbacks and risks of paying ransoms, such as encouraging more attacks, funding criminal activities or receiving corrupted or incomplete data.

15%

of organizations refused to pay more than one ransom after their first payment didn't get their data back, up from just 6% in 2022

Ransomware Infections: What Happens After Payment



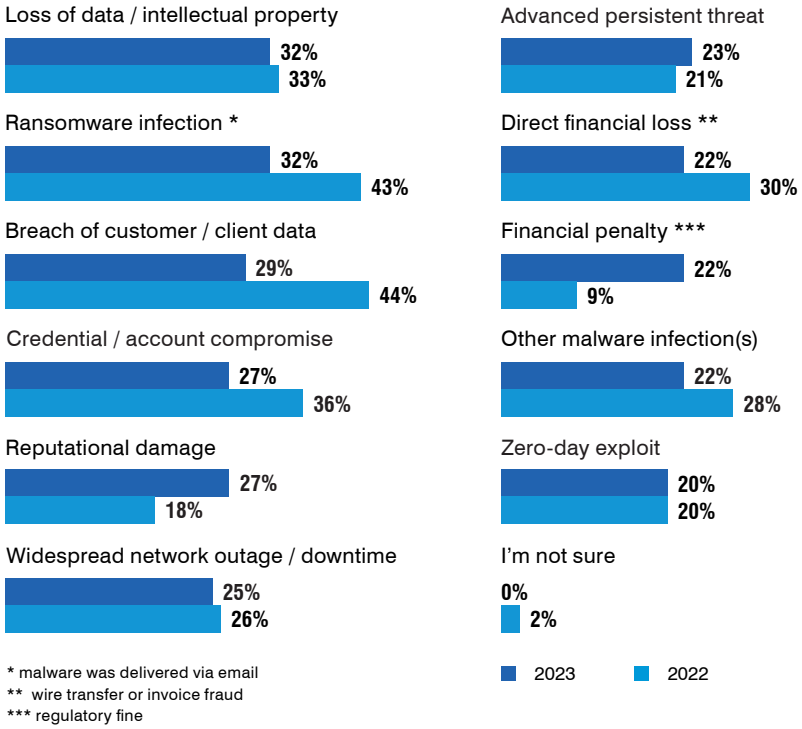
Attack consequences

The impact of phishing attacks on organizations can be devastating, both financially and reputationally. 71% of organizations experienced at least one successful phishing attack in 2023, down from 84% in 2022. However, while the incidence of successful phishing attacks has declined, some of the negative consequences have soared. Year on year, we saw a 144% increase in reports of financial penalties, such as regulatory fines, and a 50% increase in reports of reputational damage due to phishing incidents.

73%
of organizations reported a BEC attack, but only

29%
teach users about BEC attacks

Results of Successful Phishing Attacks



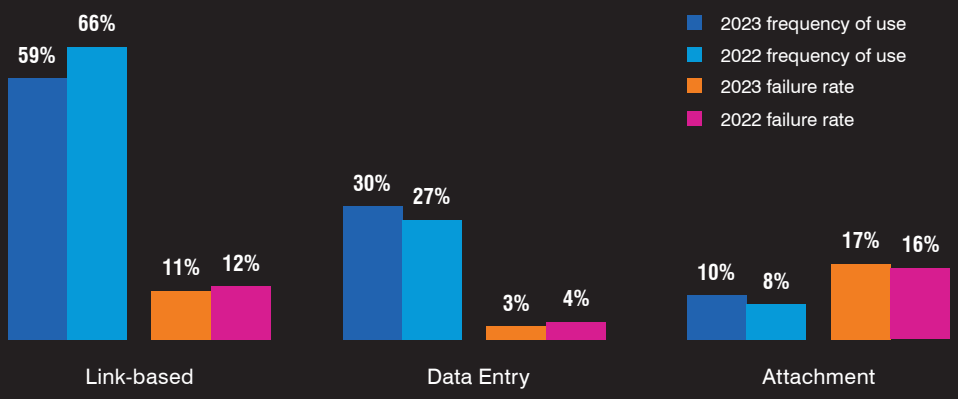
* malware was delivered via email
** wire transfer or invoice fraud
*** regulatory fine

The threat landscape is constantly evolving, as cybercriminals employ new tactics and techniques in their quest to gain an advantage. This is why it's key to equip people with the knowledge they need to identify and resist attacks; after all, as sophisticated as these techniques are becoming, people remain their primary target. Most organizations say they use real-world threat intelligence to shape their security awareness program, however there are some major disparities. For example, 73% of organizations experienced a BEC attack, but only 29% train users specifically on BEC threats. Similarly, only 23% of organizations provide training on TOAD attacks, despite their ubiquity. The threat landscape moves pretty fast; if you don't stop and update your program once in a while you could miss something.

Organizational Benchmarks

One of the ways that organizations can measure and improve their cybersecurity awareness and resilience is by conducting phishing simulations. Proofpoint phishing simulations mimic real-world phishing scenarios and assess how users respond to them. Our customers conducted 183 million phishing simulations over a 12-month period. Of these, link-based tests were the most common, accounting for 59% of all simulations, followed by data-entry tests (30%) and attachment-based tests (10%). However, attachment-based tests had the highest failure rate overall, at 17%. Failure rates for all types of simulations were within 1 percentage point of last year's results.

Simulation Type and Failure Rate



We also analyzed failure rates by industry and found some interesting patterns. The finance industry saw the most improvement, with failure rates decreasing by 7 percentage points, from 16% in 2022 to 9% in 2023. On the other hand, the agriculture and construction industries both saw their failure rates increase by 3 percentage points from last year. Although this increase is relatively small, it may point to an underlying issue with security approaches in these industries.

Current Industry Failure Rate

	Industry	2023	2022	Change (% points)
	Marketing/Advertising	6%	5%	1%
	Retail	7%	10%	-3%
	Aerospace	7%	13%	-6%
	Electronics	8%	14%	-6%
	Hospitality/Leisure	8%	11%	-3%
	Healthcare	8%	9%	-1%
	Legal	8%	8%	0%
	Manufacturing	9%	10%	-1%
	Insurance	9%	10%	-1%
Best Improvement	**Finance**	9%	16%	-7%
	Financial Services	9%	10%	-1%
	Government	9%	9%	0%
	Engineering	10%	11%	-1%
	Education	10%	10%	0%
	Energy/Utilities	10%	11%	-1%
	Environmental	10%	8%	2%
	Technology	10%	12%	-2%
	Other	11%	13%	-2%
Worst Increase (tie)	**Agriculture**	11%	8%	3%
	Mining	11%	13%	-2%
	Non-profit	11%	13%	-2%
	Transportation	11%	10%	1%
	Automotive	11%	10%	1%
	Food and Beverage	11%	12%	-1%
	Real Estate	11%	11%	0%
	Telecommunications	12%	11%	1%
	Entertainment/Media	12%	11%	1%
	Business Services	12%	12%	0%
	Consulting	12%	12%	0%
Worst Increase (tie)	**Construction**	12%	9%	3%

Another factor influencing the success or failure of phishing simulations is the content and design of the test phishing emails. Templates are designed to mimic real-world threats; accordingly, our customers featured Microsoft in 7 of the top 10 phishing simulation templates, matching the data about abuse of its brand and products shared in the previous section. The highest failure rate among these templates was for a OneDrive deactivation email, which had a failure rate of 10%. This email claimed that the user's OneDrive account would be deactivated unless they clicked on a link and verified their identity. A lure like this is designed to trigger feelings of loss aversion and urgency—provoking the strong emotional response that is often at the core of effective social engineering.

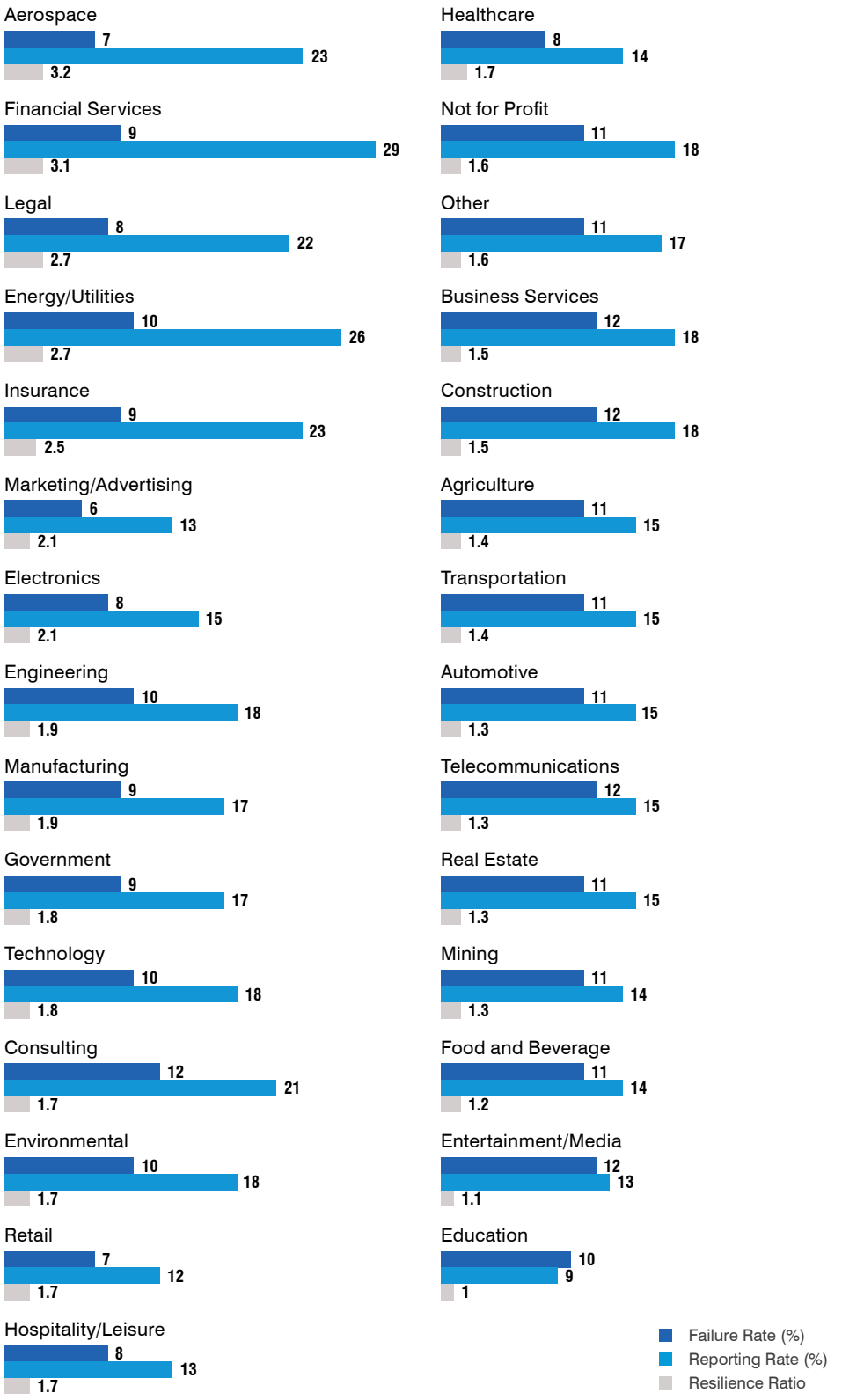
18.3%

of simulated phishing emails were properly reported by users in 2023, a slight increase from 2022

Rank	Subject	Failure Rate
1	Microsoft: Microsoft password expiration	4%
2	Microsoft: Microsoft deactivation of old OneDrive account	10%
3	IT: password expiration	8%
4	Microsoft: Teams reply (phish hook enabled)	5%
5	IT: system update	4%
6	Microsoft: Microsoft voicemail	8%
7	Social media: LinkedIn search appearance	2%
8	Microsoft: O365 re-authentication	6%
9	Email account alert: email password change	7%
10	Microsoft: your storage capacity is full	5%

Overall, the reporting rates for simulated phishing increased slightly to 18.3%, from 17% in 2022. This means that slightly more users reported the phishing emails they received to their IT or security team, rather than ignoring or deleting them. Reporting rates are an important indicator of user awareness and engagement, as they show that users can recognize and flag suspicious messages.

Industry Reporting, Failure and Resilience Factor

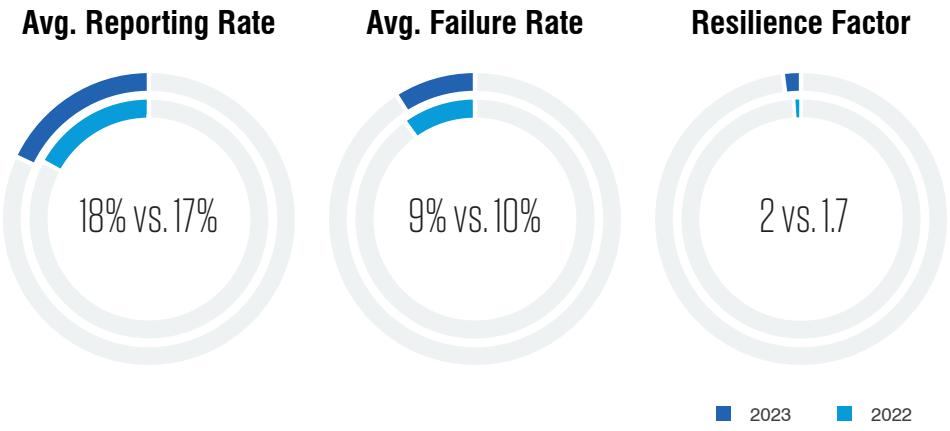


Overall failure rates for simulated phishing dropped to 9.3%, from 10% in 2022. This means that fewer users clicked on links, entered their credentials on fake websites or opened attachments. Failure rates are an important indicator of user vulnerability and risk, as they show how likely users are to fall for a real phishing attack.

Based on these reporting and failure rates, we calculate a Resilience Factor for each organization. The Resilience Factor is a metric that compares how many users reported simulated phishing emails versus how many users fell for them. (It's calculated as the average reporting rate divided by the average failure rate.) A higher Resilience Factor means that the organization has more users who report phishing emails than users who fail them, and vice versa. The average Resilience Factor increased to 2.0 in 2023, from 1.7 in 2022. This number has been creeping up over the past three years, starting at 1.5 in 2021, indicating that organizations are becoming more resilient to phishing attacks as their users become more aware and proactive.

2.0

Organizations' Resilience Factor rose to 2.0 in 2023, the third straight yearly increase



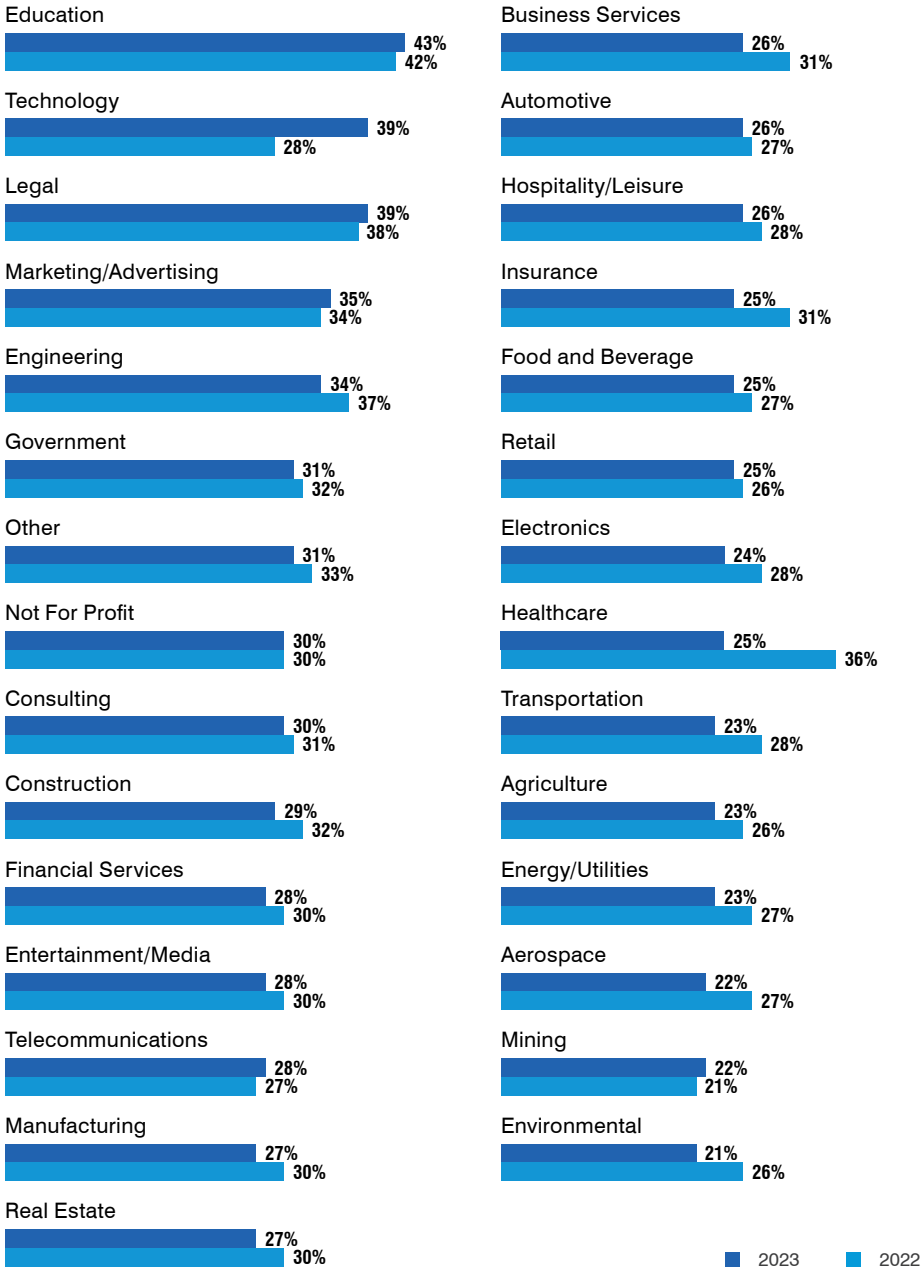
18% reporting rate ÷ 9% failure rate = 2 resilience factor

Not every reported email is, in fact, malicious. So we also benchmark real-world reporting accuracy for customers who use our PhishAlarm reporting button. By this measure, the education, technology and legal sectors ranked best, with tech improving significantly from the year before. Still, more than half of reported emails were false positives; in some sectors, than number was close to 80%. Without an automated way to verify all those reported emails as true threats, it adds up to hours upon hours of needless work by security teams.

9.3%

of simulated phishing emails got users to click in 2023, a slight decrease from 2022

Accuracy Rate By Industry



~2 million

unique threats were found in email reported by end users last year

Finally, we looked at reporting of real-world threats from our customers' end users. Some 24 million messages were reported over a 12-month period, up from 18 million in 2022. Between them, these messages contained nearly 2 million unique threats.

Threat Family	Unique Threats Reported by End Users 2023
Credential Phishing	930,707
Malware	52,646
Banking	15,700
Botnet	2,735
RAT	4,531
Downloader	3,513
Stealer	2,779
MalSpam	6,161
Keylogger	2,170
Backdoor	74
Ransomware	167
TOAD	54
Payment Fraud	4
Others	876,773
Total	**1,898,650**

This shows that while the variety of phishing and malware attacks are increasing, people empowered with the right knowledge and right skills can proactively help keep organizations safe. User-reported data is a valuable source of threat intelligence that security teams can use to better understand their adversaries, and to boost security education with real-world examples. And the data from these user reports also feeds back into our threat detections, raising the tide for all boats.

Conclusion

A security awareness program should be an essential component of any organization's security strategy, but by itself it isn't enough. Our data shows that 96% of people who took a risky action knew that what they were doing might be risky, so it seems that key information is getting through. However, knowing what to do and doing it are two different things. The challenge is now not just awareness, but behavior change.

Users say they want security to be made easier for them, and they're right to want that. But in those instances where processes can't be made any easier and a choice remains between convenience and security, users still need to be convinced to choose correctly.

So how can organizations lead this behavior change?

Use threat intelligence to inform your behavior change program

This will help users to understand the nature, scope and impact of the threats they face, and will help security teams tailor their program and messaging accordingly. To use threat intelligence effectively, organizations should:

- Work collaboratively across the organization to understand user, department and organizational goals, and then implement security controls that protect the organization without getting in the way. Security should be aligned with business objectives and user needs and should not be an afterthought or create unnecessary barriers or operational burdens.
- Use internal data to define the top three risky behaviors that you want to change. Internal data, such as simulated phishing assessment, user feedback or incident reports, can provide valuable insights into the most common mistakes and risky actions. By focusing on the top three risky behaviors, organizations can prioritize their efforts and resources, and measure their progress and impact more easily.

Reduce security friction

Complex or drawn-out security processes can lead to user frustration, dissatisfaction and even resistance, potentially undermining the security culture of the organization.

- Track where security controls create bottlenecks and work to alleviate them. Anything that slows down system performance, interrupts user workflows or requires multiple steps should be a candidate for review. These bottlenecks can reduce productivity and efficiency and make users more likely to bypass security controls altogether. Using the latest technology can help create a light-touch environment that minimizes disruption. For example, data loss prevention (DLP) solutions can help by monitoring authorized senders and recipients without getting in the way.
- Ease of use and automation should be prioritized, coupled with best-in-class security education, threat prevention, detection and response technology. By applying these principles and taking an integrated multilayered platform approach, organizations can not only better defend against the constantly changing threat landscape, but also reduce the cognitive load and effort users have to expend to follow security rules.

Go beyond training

Build a strong security culture with better communication and engagement. A strong security culture will positively influence how users approach and handle security issues and foster a sense of responsibility.

- Implement a behavior change program tailored to user and business needs. A behavior change program is a systematic and structured approach to changing user behavior and habits. Find ways to positively reward users who avoid risky actions and proactively help keep the organization safe, such as reporting suspicious email or activity.
- Advocates or champions can help reduce the number of users who don't know if security is their responsibility. By promoting best practices and providing peer support and guidance, advocates or champions can foster trust, increase engagement, and help create a positive and collaborative security culture.

LEARN MORE

To learn more about how Proofpoint provides insight into your user-based risks and helps you mitigate them with a people-centric cybersecurity strategy, visit **proofpoint.com.**

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**

proofpoint.

0400-015-01-01