SECUR-SERV

Human Risk: The Untold Story in Cybersecurity

Exclusive Benchmarks and Trends for 2025

secur-serv.com

INTRODUCTION

Imagine a cyberattack on your organization. What might it look like? You might picture a clever phishing email or a hacker using a hidden flaw to break in.

But most successful attacks don't rely on advanced tricks. They succeed because people make simple mistakes.

This eBook will show you how and why this happens — and what you can do to help your people stay alert, make safer choices, and become a stronger line of defense.

The easiest way to break through security isn't always technical — it's human. People are the strongest link in any defense, but also the weakest. They make mistakes, fall for scams, or ignore basic security habits.

According to this year's phishing report, 71% of working adults admitted they'd done something risky — reused or shared a password, clicked unknown links, or handed credentials to someone they shouldn't have. And 96% of them knew it was risky when they did it.

When forced to choose between convenience and security, most people prefer convenience. So, how can organizations turn this around?

In this report, we will examine how attitudes toward security influence everyday behavior — and how attackers capitalize on our need for speed. We'll discuss the current state of security awareness programs and assess the true resilience of individuals and organizations.

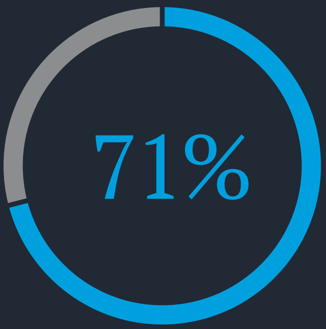
Our findings are based on a global survey of 7,500 end users and 1,050 security professionals from 15 countries. We also draw on Proofpoint's threat research, data from our products, including 183 million simulated phishing emails sent by our customers in a year, and over 24 million real emails reported by end-users in the same period.

Table of Contents

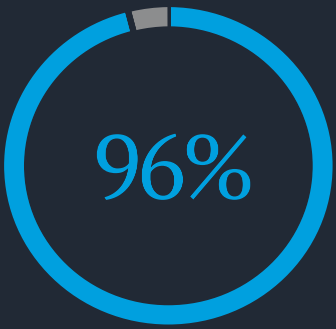
KEY FINDINGS

Over 1 million

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



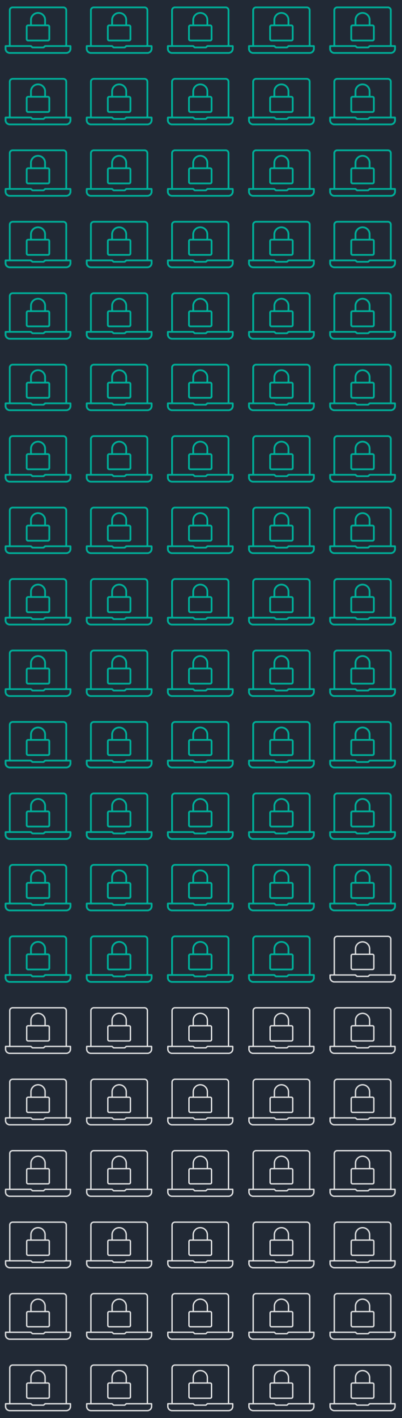
and



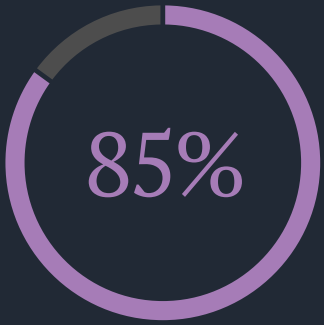
71% of users took a risky action and 96% of them knew they were doing something risky

66 million

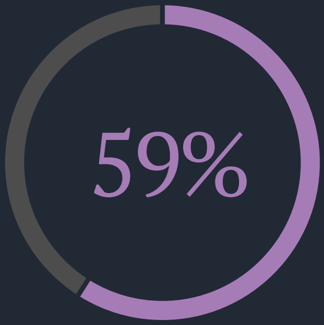
Business Email Compromise (BEC) attacks were detected and blocked on average per month by Proofpoint.



69% of organizations were infected by ransomware.



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



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.

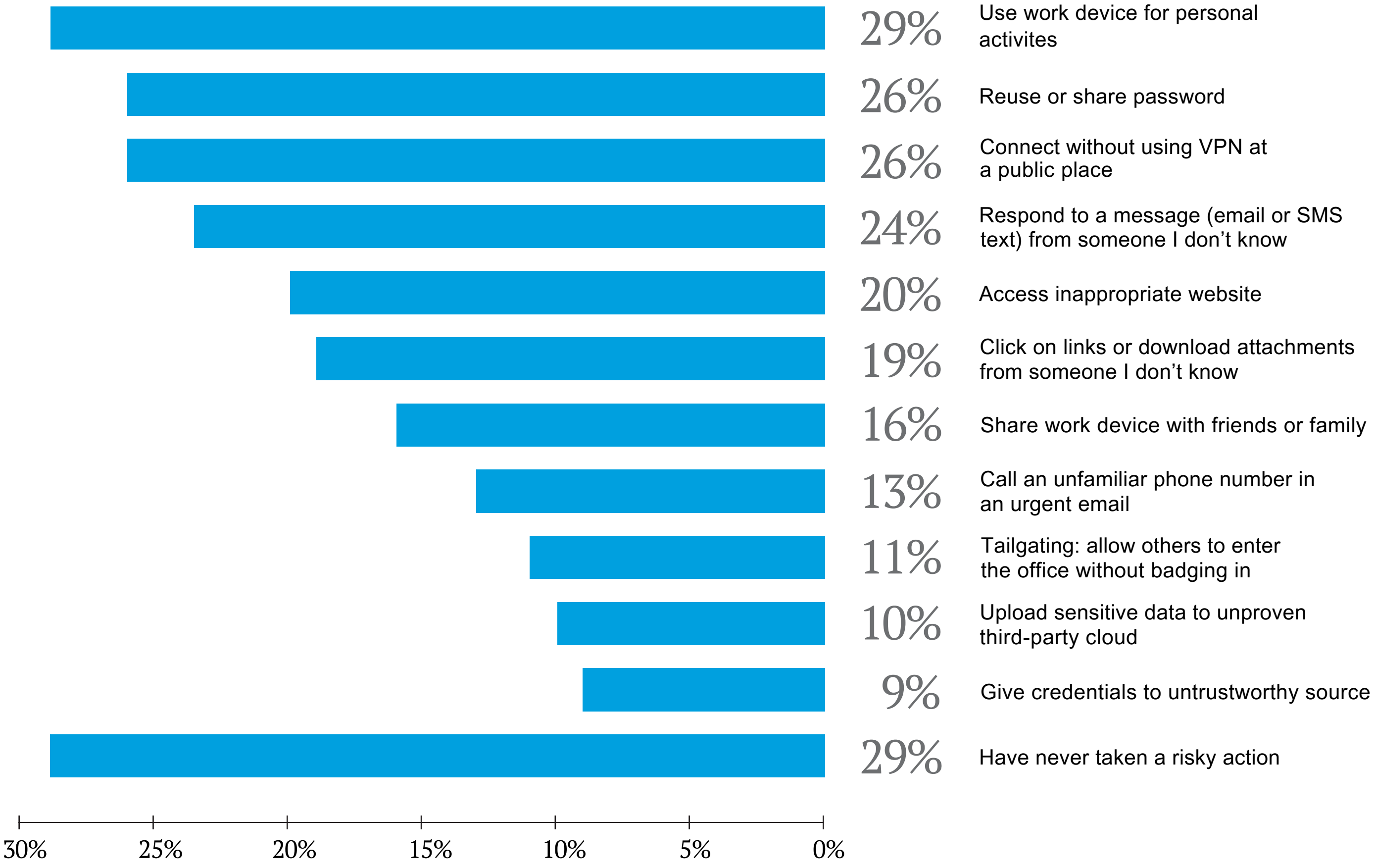
Security Behaviors and Attitudes

Even the best technical defenses can fail if people don’t follow the basics, such as avoiding suspicious links, verifying the sender’s identity, and using strong, private passwords. Yet many users skip these simple steps, putting themselves and their organizations at risk.

End-user behavior and attitudes

According to recent survey data, 71% of users admitted to taking at least one risky action, and almost all of them (96%) were aware of the risk at the time. Of those, 73% said they’d done two or more risky things. Even more concerning, more than a third of these actions were rated by the users themselves as “very risky” or “extremely risky.”

Risky Actions Taken

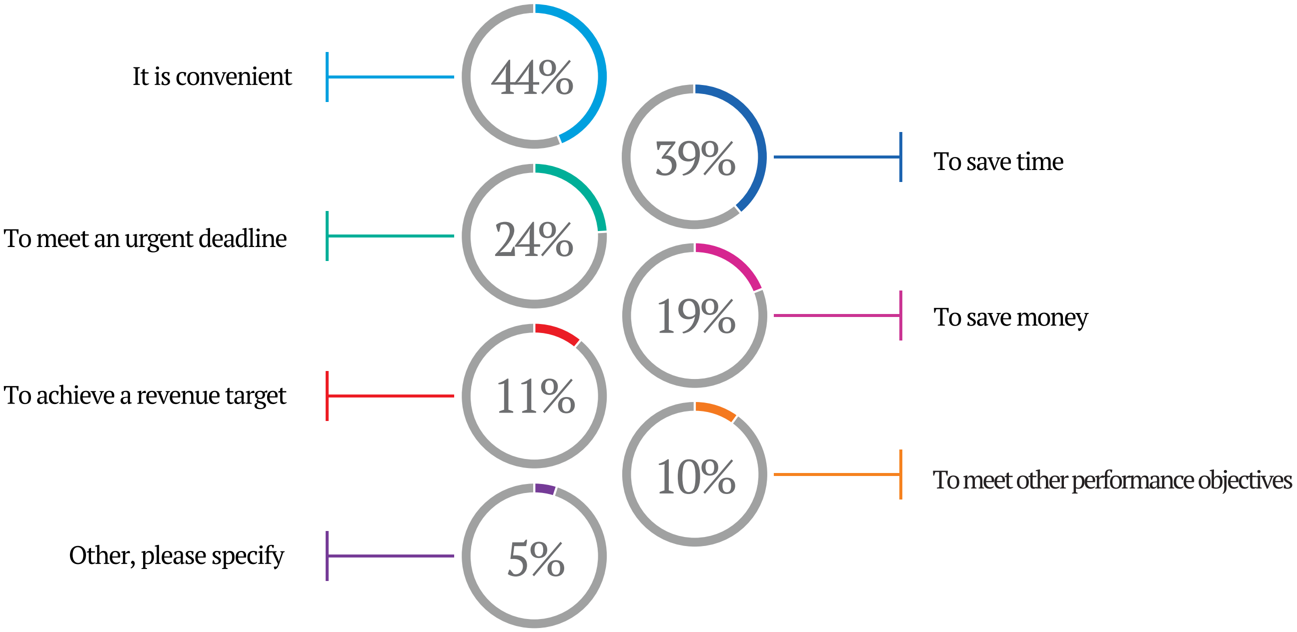


Users take risky actions for many reasons. Convenience, saving time, and reacting to urgent requests are the most common. Interestingly, a small group (2.5%) stated that they took risks solely out of curiosity.

The takeaway is clear: people do not always act carelessly because they lack security awareness. Often, they know exactly what they are doing and are willing to gamble with their organization's security.

This means organizations need to do more than train people. They must create a culture that makes safe choices the easiest choices and provide employees with the tools and support to prioritize security, even when it is inconvenient.

Why Risky Action is Taken

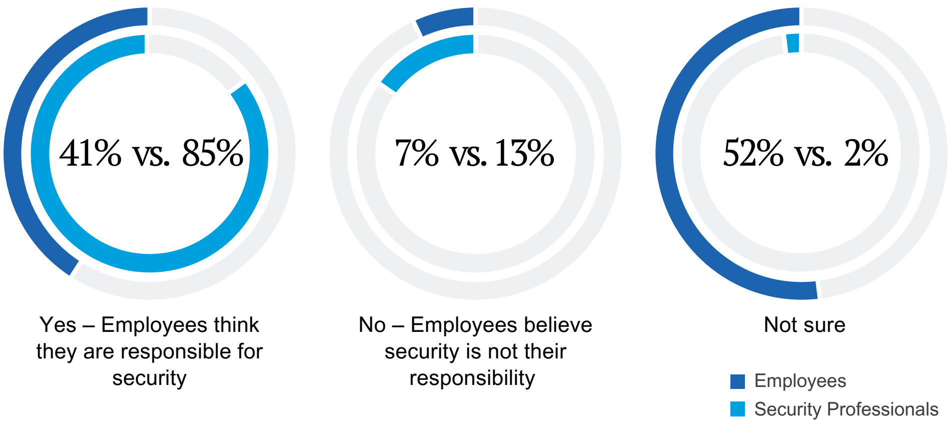


Nobody knows this better than cybercriminals. They recognize that people can be exploited through carelessness, ignorance, or even malice. Social engineering is a part of almost every email threat our researchers analyze.

Fifty-eight percent of users who took a risky action reported doing something that exposed them to basic social engineering, such as clicking on unknown links, replying to unfamiliar senders, or sharing credentials with untrustworthy sources. These actions open the door to ransomware, malware, data breaches, and financial loss.

One reason people continue to take these risks is that there is no explicit agreement on who is responsible for the consequences. Only 41% of users reported knowing they are responsible for cybersecurity at work. About 7% said they were not responsible at all, and more than half (52%) were unsure.

Perception on Security Responsibility



Eighty-five percent of security professionals say that most employees are aware of their responsibility for security. This gap between perception and reality underscores the need for organizations to have more transparent communication about shared responsibility, rather than just providing additional training on policies and best practices.

To close this gap, leaders must make accountability part of the culture. Clear roles, better messaging, and real-world examples can help people understand what is expected of them and why it matters.

The professional view

Security professionals naturally see risks differently from end users. They understand the threat landscape, the impact of a breach, and the challenges of securing complex and rapidly changing environments. They also have the tough job of balancing strong security with the need for people to work productively and without constant roadblocks.

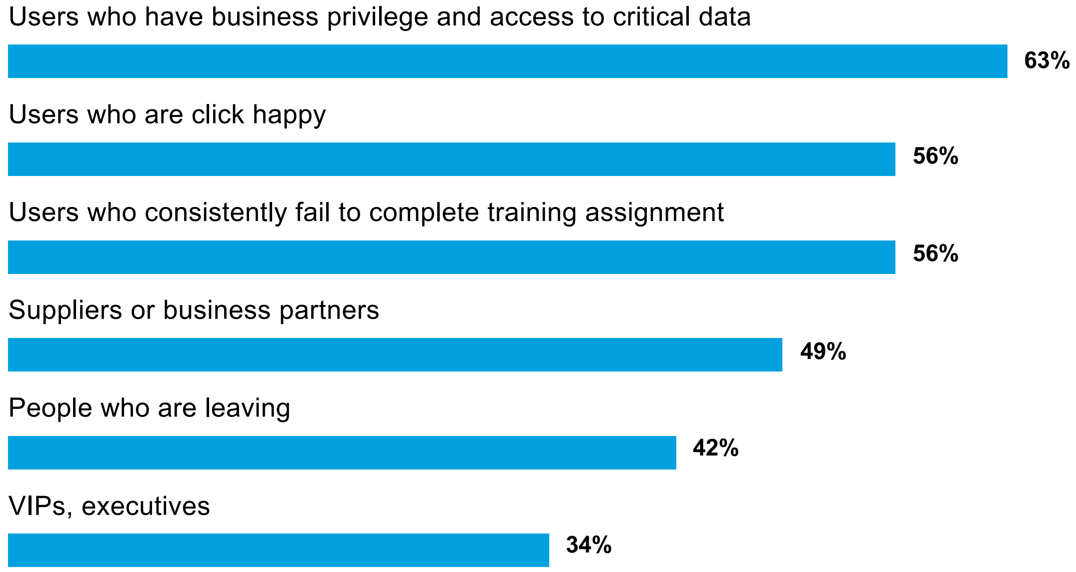
In a recent survey of security professionals, users with access to business-critical data were rated as the most significant risk (63%). This group is hard to manage because much of their access is essential for their work. Click-happy users and those who fail to complete security awareness training tied for second, at 56%.

Interestingly, these groups were seen as far riskier than executives and VPs (34%), even though executives often have wide access to valuable data.

63%

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

Users Who Represent Risk



Unfortunately, a clear overlap remains between the riskiest behaviors identified by security experts and the actions people admit to taking. Reusing passwords, using work devices for personal tasks, and visiting inappropriate websites are all considered highly unsafe practices, yet they are common everyday habits among employees.

Rank	Top Actions Considered Risky by Security Teams	Top Risky Actions Taken by End 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 shows users underestimate the real risks.

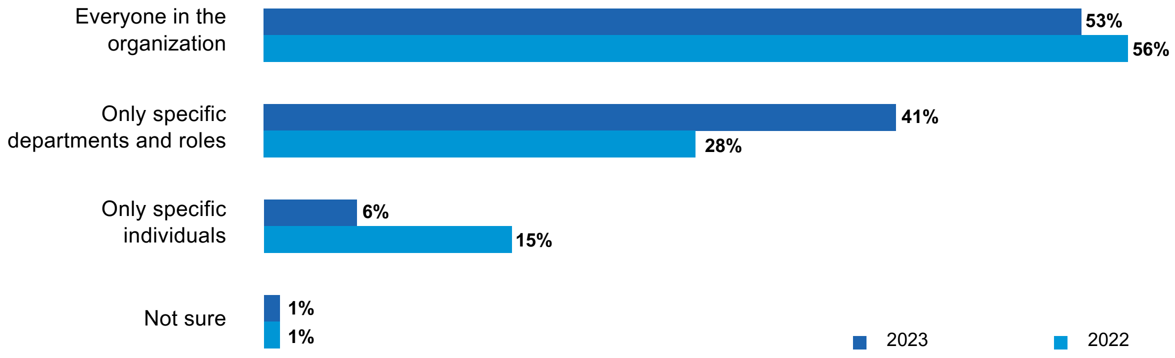
Security Awareness Trends

Training alone will not stop unsafe behavior, but teams without basic security awareness tools and knowledge are far more likely to fall victim to cybercriminals. As new social engineering tactics emerge, awareness programs must remain flexible and up-to-date to keep people prepared.

Current state of security awareness

There is some good news: 99% of organizations now have a security awareness program in place. But while the basics are covered, many still struggle to drive real behavior change. One reason could be that only 53% say they train everyone in the organization, which is down from 56% last year. This means some employees may miss out completely or get training that is outdated or incomplete.

Security Awareness Activities Assignment



Another challenge is ensuring that training topics are both broad and relevant. Security experts agree that remote work, password hygiene, and internet safety are critical areas; yet, less than a third of awareness programs cover all three.

The most common topics in current training are malware, Wi-Fi security, ransomware, and email phishing. These are important, but they do not address the full range of risks people face today.

As we will see later, cybercriminal tactics change fast. New threats can quickly become the norm, catching unprepared users off guard.

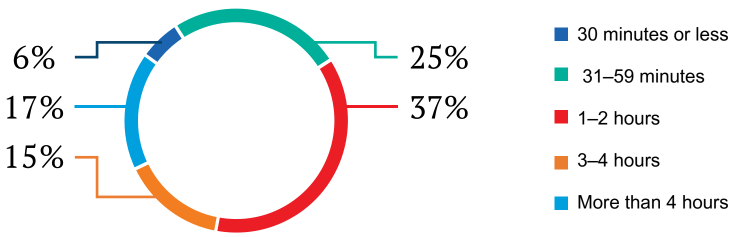
41% from 28%

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

On the positive side, recent findings show signs of progress and new approaches to security awareness. Training for specific roles and departments has increased significantly, rising from 28% to 41% in the past year. This suggests a more tailored and targeted approach.

The time allocated for user education is also increasing. More organizations now dedicate over three hours per year to awareness training, and the average time spent on training has increased for the first time in three years.

Time Allocated for Security Awareness Activities



The tactics used in training are evolving. There has been a 23% increase in the use of contests and prizes to gamify training and keep people engaged. This approach can boost motivation and create a more positive learning experience.

Computer-based training remains the most common format (45%), but other methods, such as simulated USB drops, videos, posters, and newsletters, are also gaining traction.

A mix of formats and creative tactics helps keep security awareness fresh and relevant, making it more likely that people will remember what they learn when it matters most.

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 organizations say they run simulated phishing attacks, despite the high volume of malicious email threats today. This shows there is still plenty of room to improve what goes into most security awareness training programs.

Areas for improvement

Security is not just a technical issue; it is also a cultural and organizational one. It depends on the collaboration and commitment of everyone, from security teams to everyday users. Yet there is often a gap between what security professionals believe works and what truly motivates people to make security a priority.

Recent studies indicate that increased training, tighter controls, stronger business alignment, better rewards, and visible support for security initiatives can all contribute to improved security. But fewer than a third of organizations reward positive user behaviors or promote security champions.

Recognizing and reinforcing good habits is critical. It makes people feel invested and helps build a culture where security is everyone's job. Leaders should back up policies with real incentives and recognition to make secure behavior stick.

Rank	Top Actions Requested by Security Teams	Top Actions Requested by End Users
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 they want security to be easier to use. They want processes that are more user-friendly, convenient, and transparent, along with more communication and feedback from security experts. An overwhelming 94% agree that making security more straightforward to use would motivate them to pay more attention.

These gaps between what security teams do and what users want highlight the need for open, two-way communication between security teams and end-users.

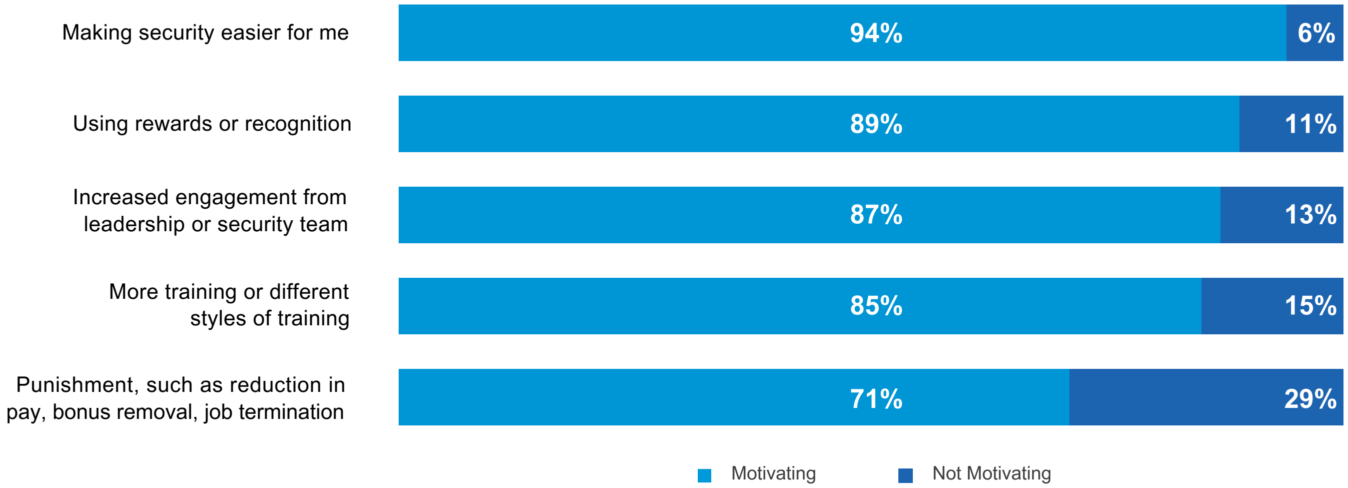
83%

of surveyed security professionals implement more training to drive behavior change

81%

implement more controls or restrictions

What Policies Motivate Users to Prioritize Cybersecurity



In line with trends from recent years, security professionals see punishment as the least effective way to address unwanted behavior, and it remains the least used approach. Punishment can backfire by creating fear, resentment, and distrust, while lowering morale and motivation. It can also discourage users from reporting incidents or asking for help, which only increases the risk of breaches.

Punishment is also the least motivating tactic for end users, though 71% still said it would push them to comply. This suggests some people may follow the rules to avoid negative consequences, but forced compliance rarely leads to lasting behavior change.

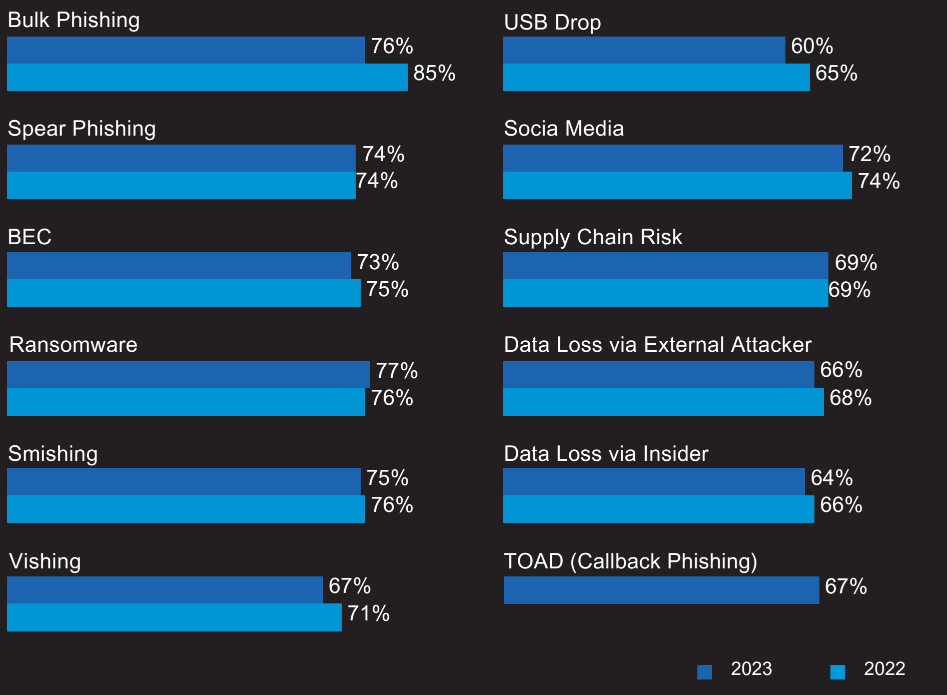
The Threat Landscape

Cybersecurity is constantly evolving as attackers devise new, more sophisticated methods to target individuals and compromise organizations. Users who take risks — such as clicking on suspicious links, opening unknown attachments, or using weak passwords — face an ever-growing range of threats.

Threat prevalence

Some of the most common attacks reported in recent studies are phishing, business email compromise (BEC), and ransomware. Each technique is different, but security teams often view them as linked together as part of a larger attack chain. For example, phishing can lead to ransomware, or a supply chain compromise can result in BEC.

Prevalence of Attacks



However, these are not the only threats that users and organizations need to watch for. Recent data shows that many new types of attacks are quickly gaining ground.

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

One emerging threat is telephone-oriented attack delivery (TOAD). In these attacks, the malicious message often appears harmless, containing only a phone number and some incorrect information. The victim calls the number for help, and that's when the attack begins. Cybercriminal call centers operate worldwide, guiding victims into giving remote access, revealing sensitive information, or installing malware themselves. Recent data shows that an average of 10 million TOAD messages are sent every month.

Another growing threat involves advanced techniques to bypass multifactor authentication (MFA), which many organizations still see as a reliable safeguard. These attacks typically use proxy servers to intercept MFA tokens, allowing attackers to bypass one-time codes and biometrics. Off-the-shelf phishing kits now often include MFA bypass tools, making it easy for even low-level attackers to succeed.

This is concerning because 89% of security professionals still view MFA as a silver bullet against account takeover, and 84% say their organizations rely on it to prevent these attacks.

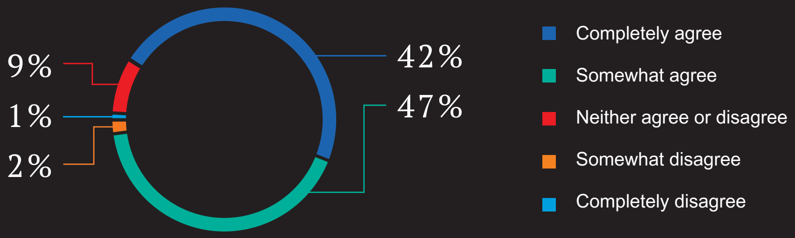
13 million

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

89%

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

Does MFA Provide Complete Protection Against Account Takeover?



Even within traditional phishing, attackers are finding new ways to slip in malicious content. One recent trend is the growing use of QR codes instead of links or attachments. This approach is especially dangerous because it can evade automated detection tools while appearing harmless and familiar to users.

The risk is simple: you cannot tell just by looking where a QR code leads. A user scanning an unfamiliar QR code might not realize they have triggered a phishing site or malware download until it is too late.

It’s also worth noting that even the least common type of attack — the classic USB drop — was still reported by 60% of respondents. This indicates that cybercriminals will employ any tactic, old or new, if they believe it might deceive an unsuspecting victim.

Despite the growing sophistication of these threats, many organizations remain unprepared. Only 23% of trained users can spot and prevent TOAD attacks, and just 23% provide any education on the safety of generative AI.

Generative AI can create realistic images, videos, or text from simple prompts, making it easier for attackers to craft convincing social engineering lures in any language. It also raises the risk of data leaks, since there is little transparency about what happens to data shared with tools like ChatGPT or Google Bard.

BEC attacks benefit from AI

Business email compromise (BEC) attacks continue to pose a serious threat, particularly in non-English-speaking countries. While fewer organizations reported BEC attempts globally, these attacks are rising fast in places like Japan (up 35% year over year), Korea (up 31%), and the UAE (up 29%).

These countries may have faced fewer BEC threats in the past due to language barriers, cultural factors, or limited visibility. But there is now a clear link between BEC and generative AI. Attackers can use AI tools to craft more convincing, personalized emails in multiple languages, making these scams more effective than ever. Recent 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. Attackers exploit the trust people have in well-known brands to trick them into clicking on or sharing sensitive information.

In 2023, more than 68 million malicious messages were linked to Microsoft products and branding, making it the most abused brand by far. Adobe and DHL were following, but each saw fewer than 10 million related messages.

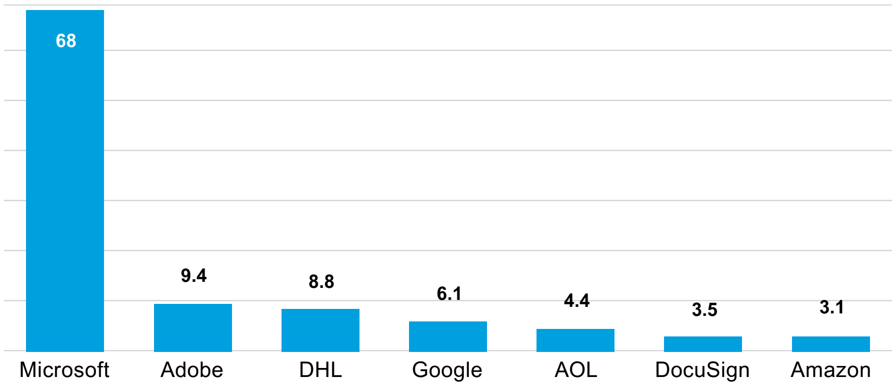
68 million

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

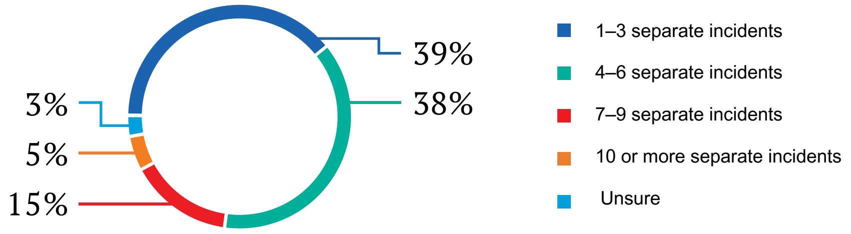
Brand Abuse Threats (Millions)



Ransomware still a major concern

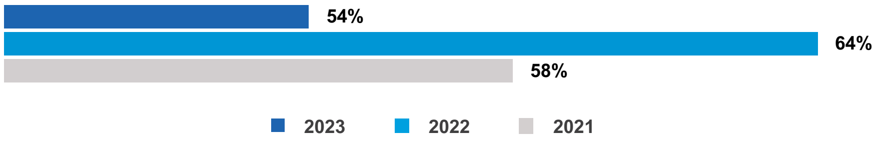
The percentage of organizations that faced a ransomware attack rose to 69%. Nearly 60% reported experiencing four or more separate ransomware incidents in a single year, showing that ransomware remains a persistent and profitable threat for attackers.

Ransomware by the Numbers



One way organizations attempt to mitigate the risk and cost of cyberattacks is by purchasing cyber insurance, which can cover expenses and damages resulting from an incident. Among organizations hit by ransomware, 96% now have cyber insurance. Most insurers (91%) helped pay ransoms, up from 82% the year before. However, the global rate of paying ransomware attackers has dropped from 64% to 54%.

Infected Organizations That Agreed to Pay Ransom

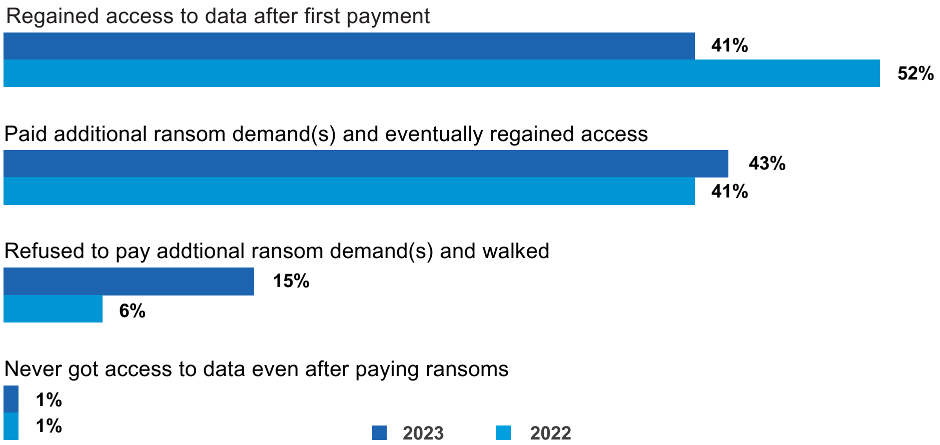


Fewer organizations are recovering their data after paying a ransom, especially after making only one payment. This helps explain why fewer are choosing to pay. Many are also realizing that paying can make things worse by funding criminals, inviting more attacks, or making it harder to recover damaged 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 can be severe, both financially and reputationally. In 2023, 71% of organizations experienced at least one successful phishing attack, down from 84% in 2022. However, while the number of successful attacks has decreased, the consequences have intensified. Reports of financial penalties, like regulatory fines, rose by 144% year over year, and reports of reputational damage increased by 50%.

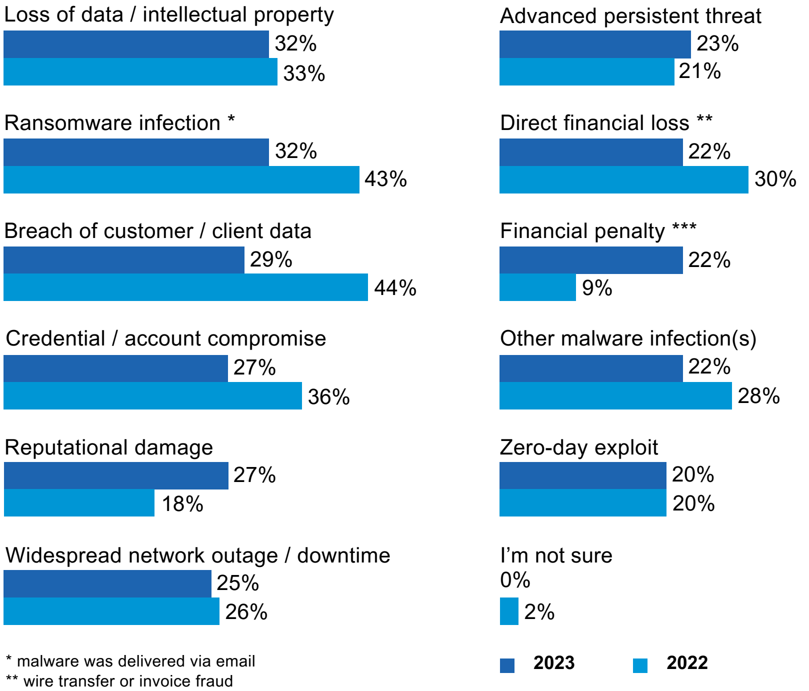
73%

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

Phishing attacks can have a significant impact, both financially and reputationally. In 2023, 71% of organizations had at least one successful phishing attack, down from 84% in 2022. But while the number dropped, the impact grew. Financial penalties increased by 144% year over year, and reports of reputational damage rose by 50%.

As attackers find new ways to gain an edge, people remain their primary target. It's vital to keep users trained to spot and resist threats. Many organizations claim to use real-world threat data to inform their training, yet significant gaps persist. For example, 73% of users faced BEC attacks, but only 29% of them train for BEC. Only 23% of TOAD attacks are covered, despite their high frequency.

The threat landscape moves fast. If you don't update your training, you leave people exposed.

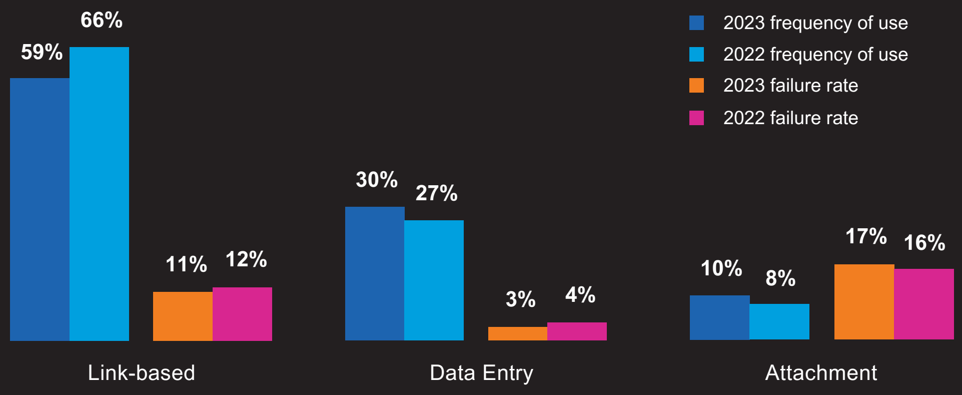
Update your awareness program often. The risks are always changing — your people should be too.

Organizational Benchmarks

One way organizations can measure and improve cybersecurity awareness is through phishing simulations—these mimic real-world scams and test users' reactions. Link-based tests are most common (59%), followed by data-entry tests (30%) and attachment-based tests (10%).

Attachment-based tests had the highest failure rate at 17%. Overall, failure rates remain consistent.

Simulation Type and Failure Rate



An analysis of failure rates by industry reveals some interesting patterns. The finance sector saw the most improvement, with failure rates dropping from 16% in 2022 to 9% in 2023. In contrast, the agriculture and construction industries experienced a three percentage point rise in failure rates. While this increase is slight, it could signal gaps in security practices within these sectors.

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 that affects phishing simulation results is the content and design of the test emails. Templates are crafted to mirror real-world threats. Microsoft appeared in 7 of the top 10 most-used templates, matching earlier data on how often its brand is abused.

The template with the highest failure rate was a fake OneDrive deactivation notice, which saw a 10% failure rate. This message claimed the user's account would be deactivated unless they clicked a link to verify their identity. Lures like this work because they tap into loss aversion and urgency, emotional triggers at the heart of successful social engineering.

18.3%

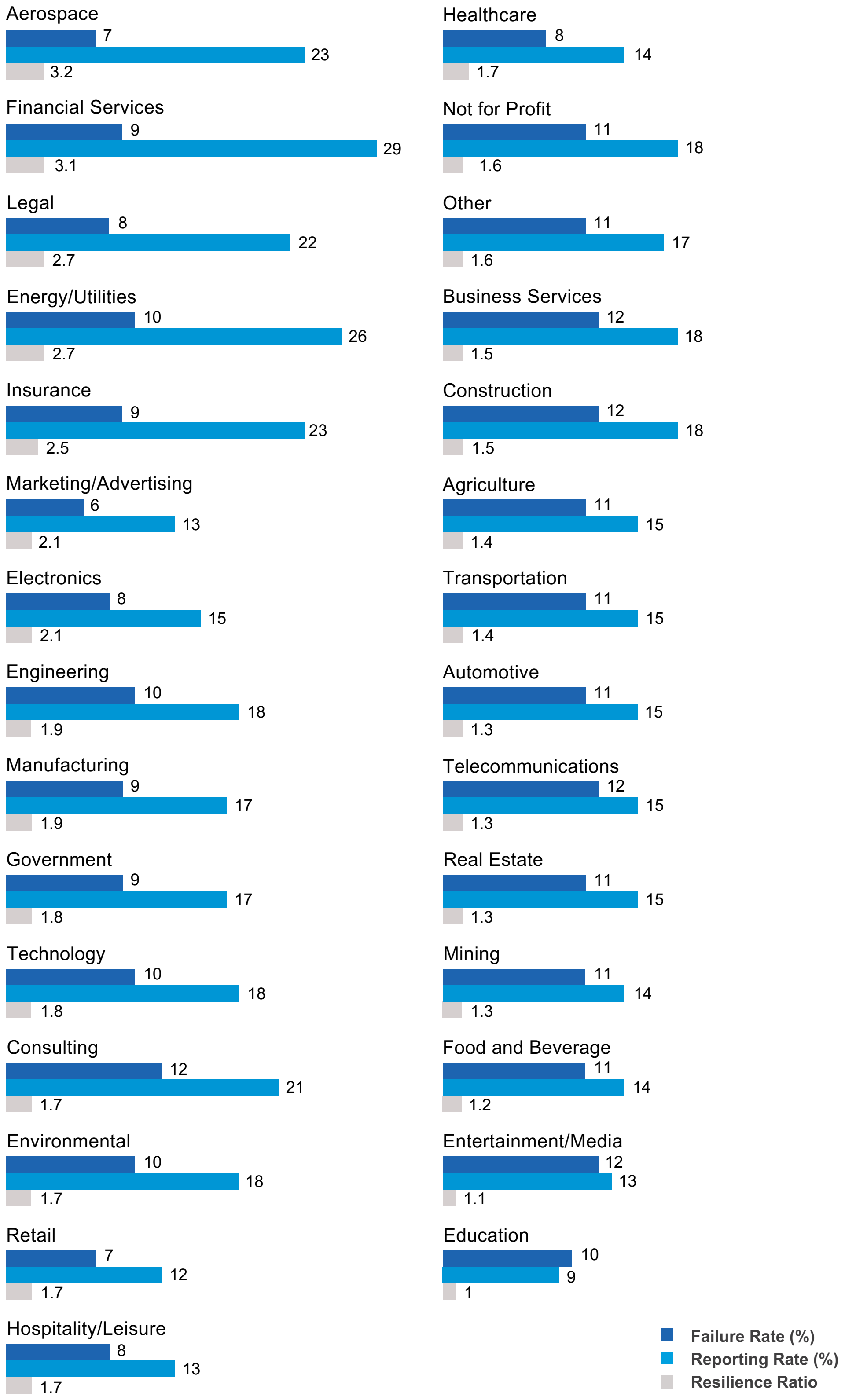
of simulated phishing emails were properly reported by users in 2023, a slight increase from 2022

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, reporting rates for simulated phishing rose slightly to 18.3%, up from 17% in 2022. This means that more users are reporting phishing emails to their IT or security teams, rather than ignoring or deleting them. Reporting rates are a key indicator of user awareness and engagement, demonstrating that people can identify and report suspicious messages.

Regular practice, feedback, and positive reinforcement can help keep reporting rates moving in the right direction.

Industry Reporting, Failure and Resilience Factor



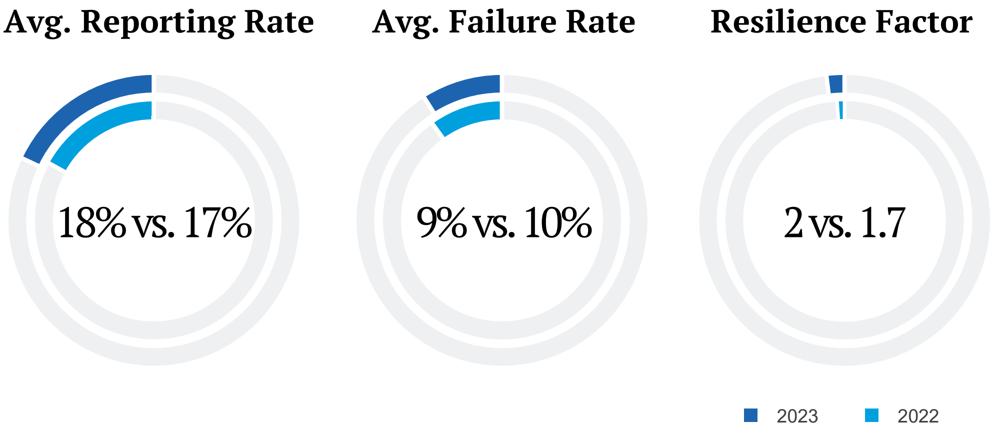
Fewer people are taking the bait. In 2023, the failure rate for simulated phishing dropped to 9.3%, down from 10% the year before. That means fewer employees clicked sketchy links, typed credentials into fake sites, or opened risky attachments. It's a good sign — every click avoided is one less chance for attackers to get in.

When people spot a phishing email and report it, that's even better. Reporting shows they're alert and ready to stop threats before they spread. Together, reporting and failure rates reveal what's called the Resilience Factor — a simple way to see if more people are catching threats than falling for them. It's calculated by dividing the reporting rate by the failure rate.

In 2023, the average Resilience Factor climbed to 2.0, up from 1.7 in 2022 and 1.5 in 2021. That steady rise means more people are catching and reporting suspicious emails than letting them slip by. It's proof that with proper training and reminders, people can genuinely be the best line of defense.

2.0

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



18% ÷ 9% = 2

reporting rate failure rate resilience factor

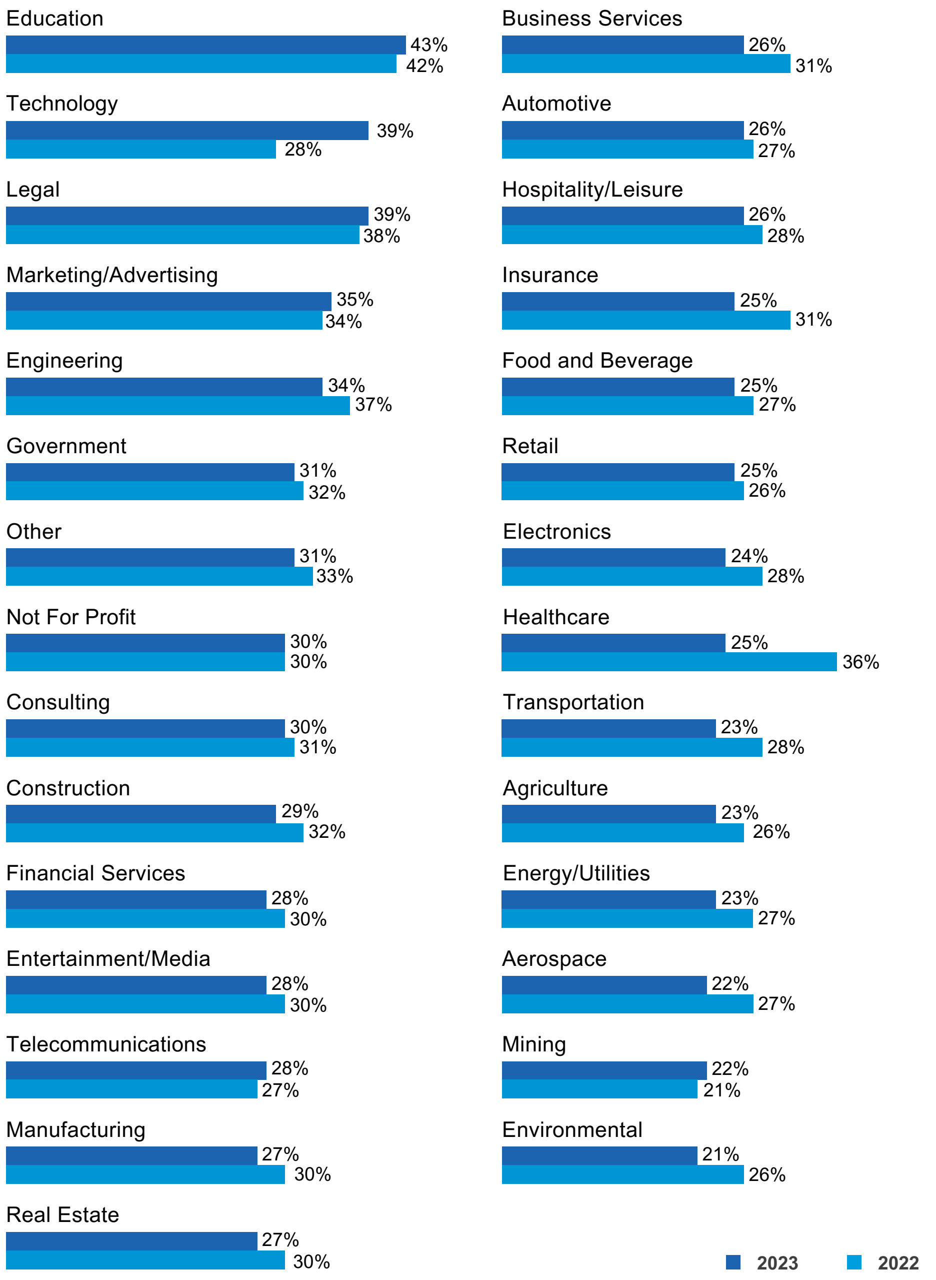
Of course, not every email people report is malicious. It is essential to examine how accurately users identify real threats. For organizations using a PhishAlarm-style reporting button, data show that the education, technology, and legal sectors had the best reporting accuracy, with technology making significant gains compared to last year.

But here's the catch: More than half of the reported emails turned out to be false alarms. In some industries, the rate of false positives was as high as 80%. Without an automated way to sort real threats from the noise, security teams can waste countless hours chasing down harmless emails instead of focusing on real risks.

9.3%

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

Accuracy Rate By Industry



Finally, examining real-world threats, end users reported approximately 24 million suspicious messages over a 12-month period, up from 18 million the previous year. Inside those reports were nearly 2 million unique threats.

~2 million

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

Threat Family	Unique Threats Reported by End Users 2023
Credential Phishing	930,707
Malware	52,646
Banking	15,700
Botnet	2,735
RAT	4, 5
Downloader	31 3,513
Stealer	2,779
MalSpam	6,161
Keylogger	2 ,17 0
Backdoor	74
Ransomware	167
TOAD	54
Payment Fraud	4
Others	876,773
Total	**1,898,650**

This shows that even as phishing and malware attacks evolve, people who have the right knowledge and skills can play a significant role in keeping their organizations safe. User-reported data is a goldmine of threat intelligence. Security teams can use it to understand what attackers are doing and to strengthen training with real-world examples.

Every report makes a difference — this data feeds back into threat detection systems, helping protect everyone.

Conclusion

A security awareness program is essential for any organization's defense, but it's not enough on its own. The data shows that 96% of people who took a risky action were aware of the risk, indicating that the information is getting through. But knowing what to do and doing it are two different things. The real challenge now is not just raising awareness, but also changing behavior.

Users want security to be easier, and they're right. However, when security can't be simplified, people must still choose between convenience and safety. In those moments, they need an apparent reason to make the safer choice.

So, how can organizations lead that change?

Drive Organizational Change

Awareness alone is not enough. To truly shift behavior, you need the right mix of threat intelligence, innovative processes, and a culture that keeps security at the forefront of mind, and easy to follow.

1. Use Threat Intelligence to Shape Your Program
Threat intelligence helps people understand the real threats they face — what they look like, how they work, and why they matter. It also provides security teams with the necessary tools to tailor training and messages that are effective.

To make threat intelligence work for you:

- Work together across the organization. Understand user, department, and business goals, then design security controls that protect without getting in the way. Security should align with how people work, rather than being an afterthought that slows them down.

- Use your data. Identify the top three risky behaviors you want to change. Pull insights from phishing tests, user feedback, or incident reports. Focus on these top risks to make your efforts targeted, trackable, and more effective.

2. Reduce Security Friction

When security feels complicated or slows people down, they become frustrated — or worse, they find ways to circumvent it.

To reduce friction:

- Spot the bottlenecks. Look for controls that negatively impact system performance or disrupt workflows. Anything that creates extra steps should be reviewed and improved.
- Use the right tools. Modern solutions, such as data loss prevention (DLP) and intelligent automation, can protect data without constant disruption. Make ease of use and automation priorities.
- Take a layered approach. Combine user-friendly processes with excellent education, threat prevention, detection, and response. The goal is to lighten the cognitive load for users, so doing the right thing is the easiest thing to do.

3. Go Beyond Training — Build a Strong Security Culture

People are more likely to make good choices when they feel that security is an integral part of their work, not just another box to check.

To build that culture:

- Run a behavior change program. Go beyond awareness. Use structured approaches to help people shift habits and reward those who make safe choices, such as reporting suspicious emails or stopping a risky action.
- Create advocates and champions. Champions help spread good habits, answer questions, and make security feel less like a rulebook and more like a shared responsibility. Peer support goes a long way toward trust and engagement.

When security feels relevant, simple, and supported by everyone, people won’t just know what to do — they’ll do it.

LEARN MORE

To learn how Secur-Serv can help you identify user-based risks and strengthen your defenses with a people-first, managed cybersecurity approach, visit secur-serv.com.

About Secur-Serv
Secur-Serv, based in Omaha, NE, is a nationwide managed services provider that puts security at the center of everything we do. We deliver comprehensive Managed IT, Cybersecurity, Managed Device, and Managed Print services to organizations of all sizes across the United States.

With a Network Operations Center in Omaha, a team of more than 2,000 field service technicians, and a full range of managed solutions, Secur-Serv helps businesses stay secure, resilient, and ready for what's next. Our people-first approach to managed cybersecurity empowers your teams to make safer choices, reduce risk, and keep your operations moving without disruption.

SECUR-SERV