proofpoint.

REPORT

# 2023 State of the Phish

An in-depth exploration of user awareness, vulnerability and resilience

proofpoint.com

## A COMMISSIONED SURVEY OF:

**7,500**

working adults across 15 countries

**1,050**

IT security professionals across those countries

## AND:

**135 million**

simulated phishing attacks sent by our customers over a 12-month period

**18 million**

emails reported by our customers' end users over a 12-month period

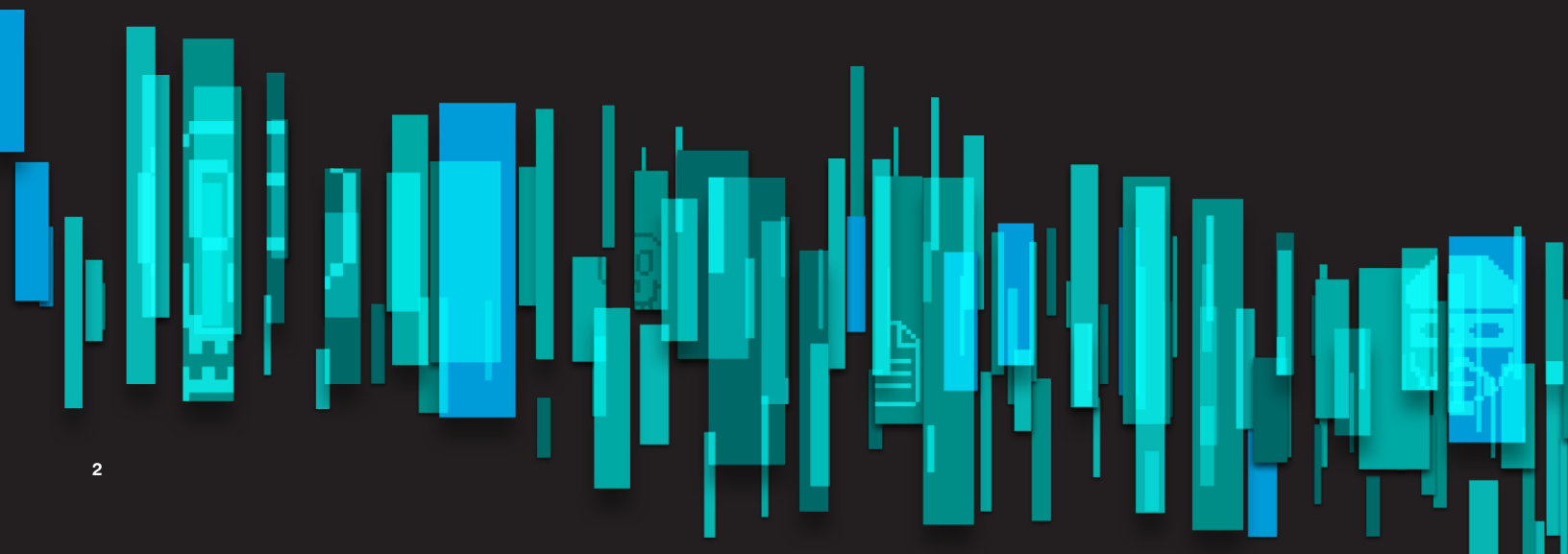
# 2022: Cyber Criminals Get Even More Creative

Every year, threat actors look for new ways to outwit victims and bypass defenses. And 2022 was no different. As businesses rolled out new security controls, cyber criminals responded.

They scaled-up complex techniques like telephone-oriented attack delivery (TOAD) and multi-factor authentication (MFA) bypass. Unknown to most users, these techniques gave cyber attackers a new advantage. At their peak, TOAD and MFA bypass saw hundreds of thousands of attacks sent per day—ubiquitous enough to threaten most organizations. And at the same time, proven tactics like brand abuse, business email compromise (BEC) and ransomware remained as popular as ever. With threat actors constantly upping their game, CISOs and Infosec teams had their work cut out.

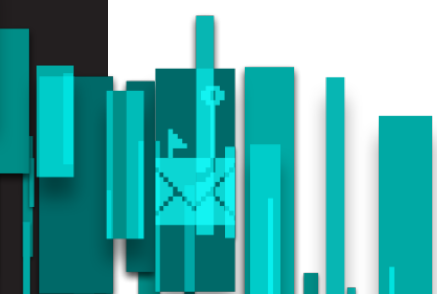
Now in its ninth year, our annual *State of the Phish* report explores end-user security awareness, resilience and risk across 15 countries (eight more than in previous years). The report benchmarks understanding of common cyber threats and defensive tactics and reveals how potential gaps in knowledge and cyber hygiene enable the real-world attack landscape. Most attacks target people before they target systems. That's why helping users build sustainable security habits is crucial. So, the last section of the report examines security awareness practices and outlines opportunities to build and reinforce a security-aware culture at every level of an organization.

The report draws on surveys of 7,500 working adults and 1,050 IT security professionals across 15 countries. It also includes findings sourced from 135 million simulated phishing attacks sent by our customers over a 12-month period and more than 18 million emails reported by our customers' end users over that same time period.



# TABLE OF CONTENTS





# Key Findings

44%

of people think an email is safe when it contains familiar branding

600K
per day

300-400K

telephone-oriented attack delivery attempts daily, with a peak of 600k per day in August 2022

1/3

of people took a risky action (such as clicking links or downloading malware) when faced with an attack

76%

Increase in direct financial loss from successful phishing

30 Million

malicious messages sent in 2022 involved Microsoft branding or products

> 1 in 10

threats were blocked as a result of user reporting





1/3+

can't define "malware," "phishing" and "ransomware"

Even basic concepts are misunderstood

ONLY 35%

of organizations conduct phishing simulations

64% of organizations infected with ransomware paid a ransom

90% of organizations affected by ransomware held a cyber insurance policy

65% of organizations reported at least one incident of insider data loss

ONLY 56%

of organizations with a security awareness program train all their employees

90%

of security professionals consider security a top priority at their company

VS.

33%

of employees say cybersecurity is not a top priority of theirs at work

## COMING TO TERMS:

Even basic concepts are still not fully understood—more than a third can't define "malware," "phishing" and "ransomware"

**40%**

of users know what ransomware is, a 9-point jump from 2019—the biggest increase among the terms we asked about

**29% and 30%**

of users knew the relatively new terms smishing and vishing, respectively

**58%**

of users knew what phishing is, a 5-point increase from last year but 3 points below 2019

# Security Habits and Knowledge Gaps

Last year's *State of the Phish* described 2021 as "the year of the new normal." The pandemic started to recede, and many workplaces permanently adopted a hybrid model. Those macro trends have continued in 2022, cementing an expanded attack surface that cyber criminals can target both in and out of the office.

The increased risks of a hybrid workplace are well understood by CISOs, and many told us in our *2022 Voice of the CISO* report that they planned to take steps to enhance security awareness programs to meet this challenge.

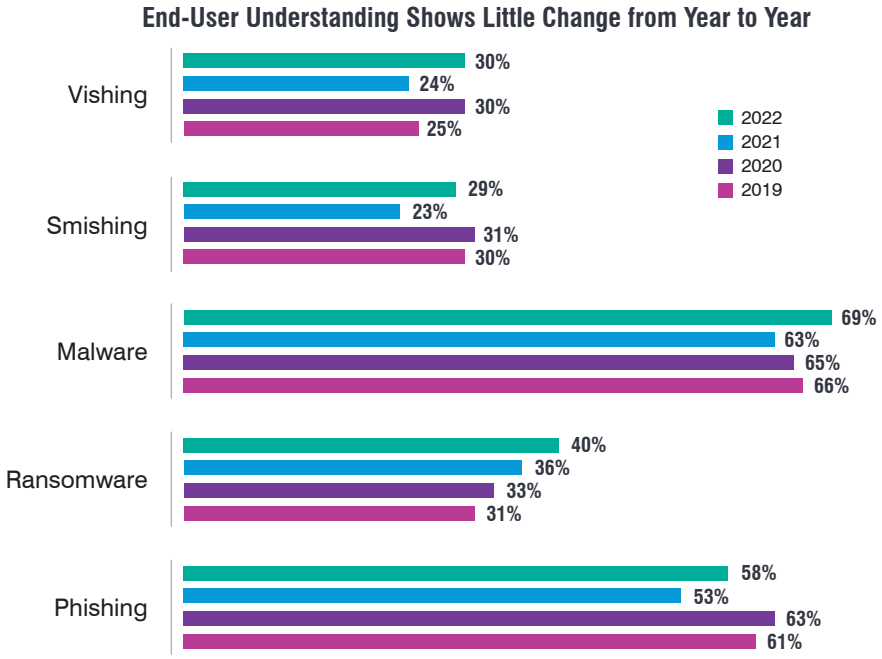
All of which begs the question: has the basic level of security awareness and understanding increased since last year?

Unfortunately, the short answer is "no."

## Terms and concepts: the same gaps remain

Common threats are still not well understood across organizations. Nearly a third of survey participants were unable to correctly define terms like "phishing" and "malware." For more advanced attacks like "ransomware," "smishing" (SMS phishing) and "vishing" (voice phishing) around two-thirds answered incorrectly.

Data from the past four years shows only modest gains or no gains at all.



# IMPOSTER SYNDROME:

21%

of users don't know that an email can appear to be from someone other than the sender

44%

of users don't know that a familiar brand doesn't make the email safe

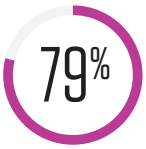
63%

of users don't know that an email link text might not match the website it goes to

Moving on from terminology to security fundamentals, the story is more encouraging. Some 80% to 90% of respondents said they understood basic email security concepts. Numbers here have increased by 2 to 3 percentage points year over year.


know to be cautious of unexpected emails


know email attachments can have damaging software

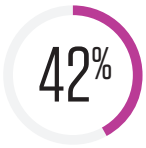



know an email can appear to come from someone other than the sender

We saw a similar degree of improvement for more advanced email security concepts, though overall understanding was lower at just 40% to 50%. Notably, people have become more aware that cyber criminals can send multiple emails to build trust. This evolution of this tactic has been a point of focus for our threat researchers this year, particularly with state-sponsored attacks.


know a familiar company brand doesn't make an email safe


know a link or attachment can affect computers beyond theirs

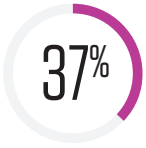



know their email provider can't automatically block all malicious emails


know exchanging multiple emails doesn't mean a sender is safe


know that files stored in the cloud are not always safe


know internal emails at work are not always safe




know an email link might not match the website it goes to


know their company can't automatically block all malicious emails

# THE UNCERTAINTY PRINCIPLE:

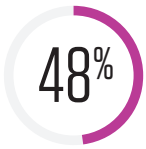
Nearly 30% of respondents said that they weren't sure if files stored in the cloud are always safe. This was by far the highest percentage of "not sure" answers; others ranged between 8% and 20%. In security terms, "not sure" and "don't know" both describe a knowledge gap. Instead of just focusing on incorrect answers, training programs should also aim to address blind spots.

## Security habits: blurred lines

In the last four years of tracking security habits both at home and at work, we've seen a noticeable shift. It's now the case that over three-quarters of people use their work devices for personal activities, with almost the same proportion using personal devices for work.


use work devices for personal activities

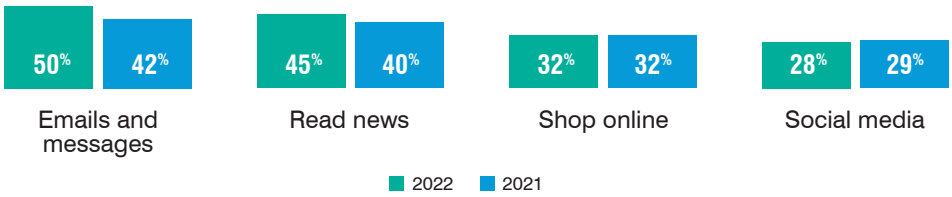

use personal devices for work devices




let family and friends use their work devices

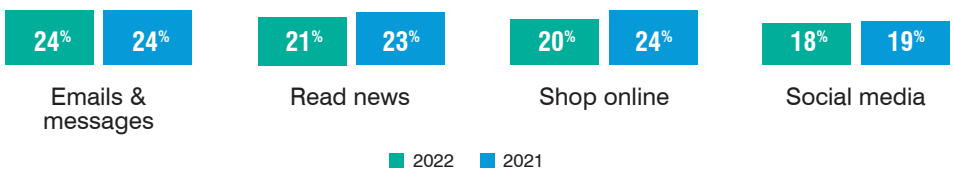
Personal use of work devices for social media and online shopping held steady from year to year. However, email, messaging and reading news all increased.

**Personal Use of Work Devices**




Nearly half of respondents said they allowed friends and family to use their work devices. This number has fallen slightly year on year (from 56% to 48%), possibly because of people returning to offices for more days during the week. Most categories of use by friends and family remained static year on year, with email and messaging the most common activities.

**Friends & Family Use of Their Work Devices**




Unfortunately, a small percentage of respondents (3%) said they didn't know what their friends or family did on their work device. This clearly represents an unacceptable level of risk.

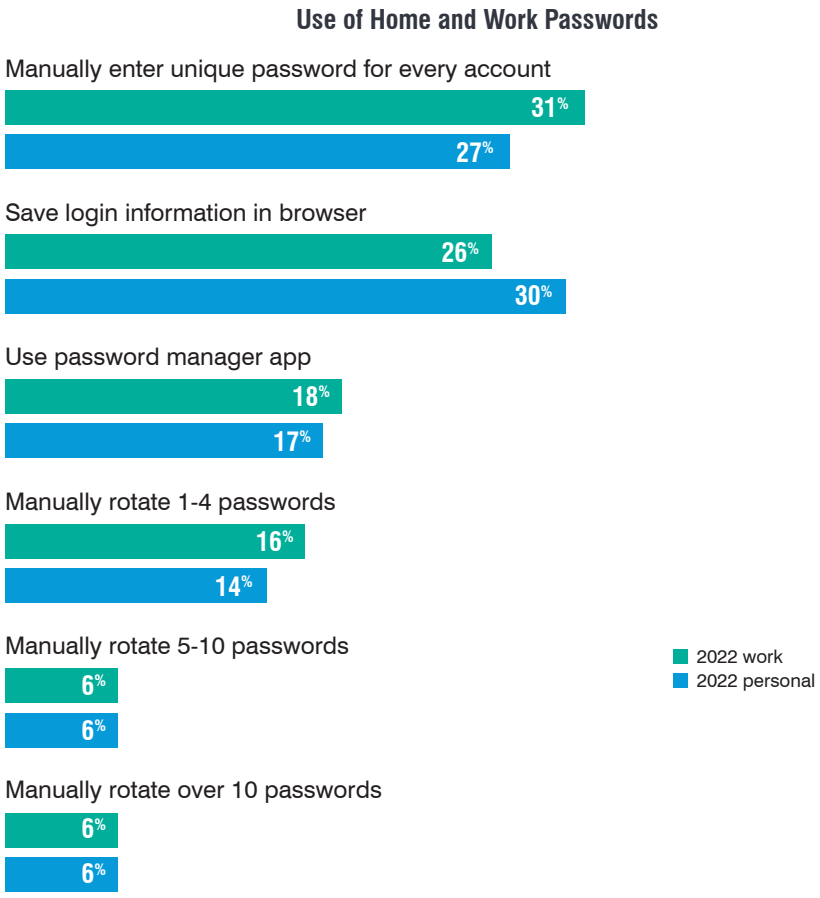
# PASSWORD UNPROTECTED:

28%

of users reuse passwords for multiple work-related accounts, jeopardizing all of them if even just one is compromised

## Security habits: password hygiene

Another area where behavior has remained disappointingly unchanged is password management.




The most common method is the most secure: using a single unique password, entered manually per account. In second and third place, less-secure browser password managers are still more popular than dedicated apps. While the least secure options are to be found in the long tail of responses, more than a quarter of respondents admitted to reusing a limited number of passwords.

# WIRELESS WEAKNESSES:

71%

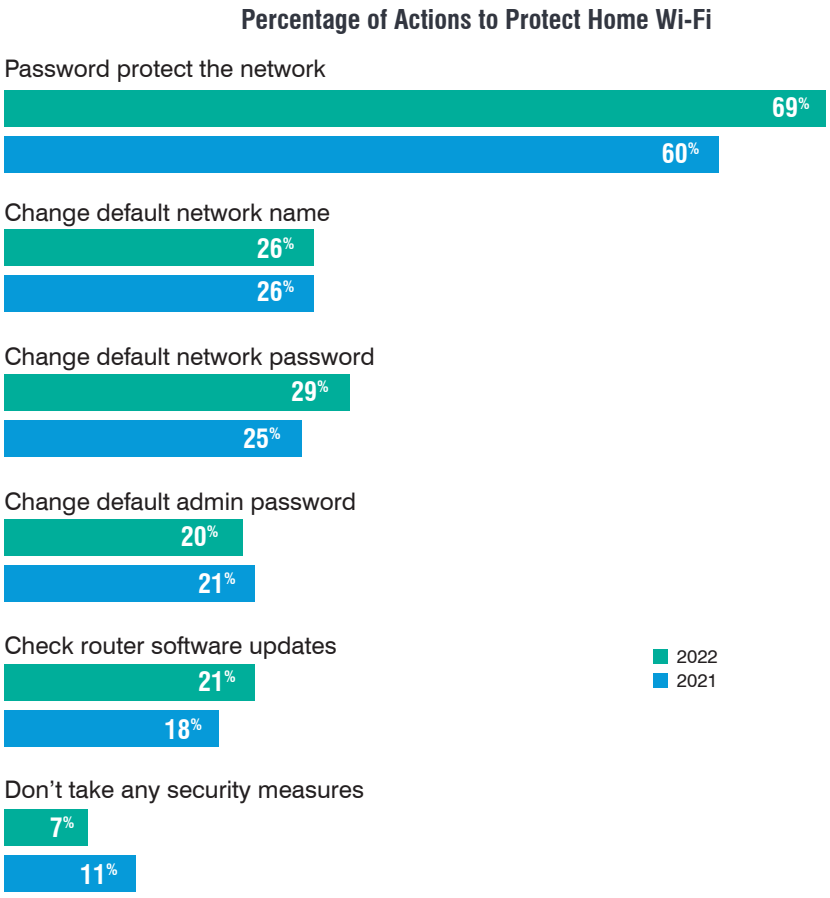
of users don't change the default network name on work WI-Fi routers

80%

of home and work Wi-Fi users didn't change the default admin password for their routers in 2022—worse than the previous year

## Security habits: Wi-Fi woes

Password problems aren't just limited to email and cloud accounts. We also found that numbers are low when it comes to Wi-Fi password best practices.




Over two-thirds of people password protect their home network. But the number of people who change default wireless and administration passwords is much lower, at less than a third each. Most alarming of all, 7% of respondents said they took no home Wi-Fi security measures at all.

## ACTIONS SPEAK VOLUMES:

34%

of users did something in 2022 that put themselves or their organizations at risk

63%

of working adults think an email link always goes to the matching website brand

11%

of recipients fell for phishing simulations mentioning "DocuSign document for review" and "FedEx delivery failure"

As part of our survey, we asked people why they don't take these necessary steps to secure their home networks. The range of answers is revealing:

**Feel security is already in place** ("That's what my network provider does.")

**Think there is built-in safety** ("(I thought it was safe enough.")

**Never think about security** ("I have never thought to change any of these things.")

**Security handled by someone they know** ("My spouse looks after this.")

**Made security changes previously** ("I made changes when it was set up.")

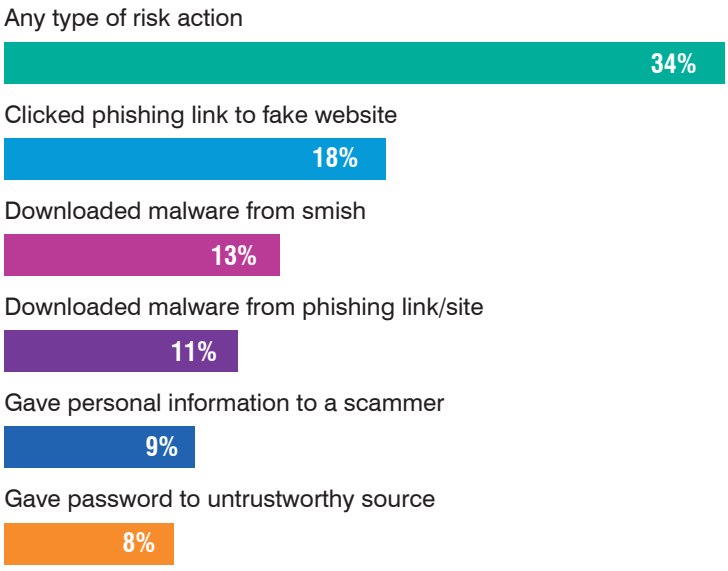
**Made some changes but not others** ("I have modified the ones I thought appropriate.")

**Don't know how to change settings** ("I was worried I would mess it up.")

## Security habits: risky business

With these gaps in knowledge and best practices, it's no surprise that many people continue to take risky actions when faced with a cyber attack. And with many risky actions not being recognized in the moment (or admitted to after the fact), these numbers are almost certainly lower than the reality.

**Risky Actions Taken by Working Adults in Threat Situations**




More than a third of respondents took at least one risky action during the year, with clicking on malicious links being the most frequent. With email overwhelmingly the most common vector for distributing phishing links and malware, training users on the correct action to take should remain a key part of ongoing security awareness initiatives.

84%

of organizations faced at least one successful phishing attack

54%

faced three or more attacks

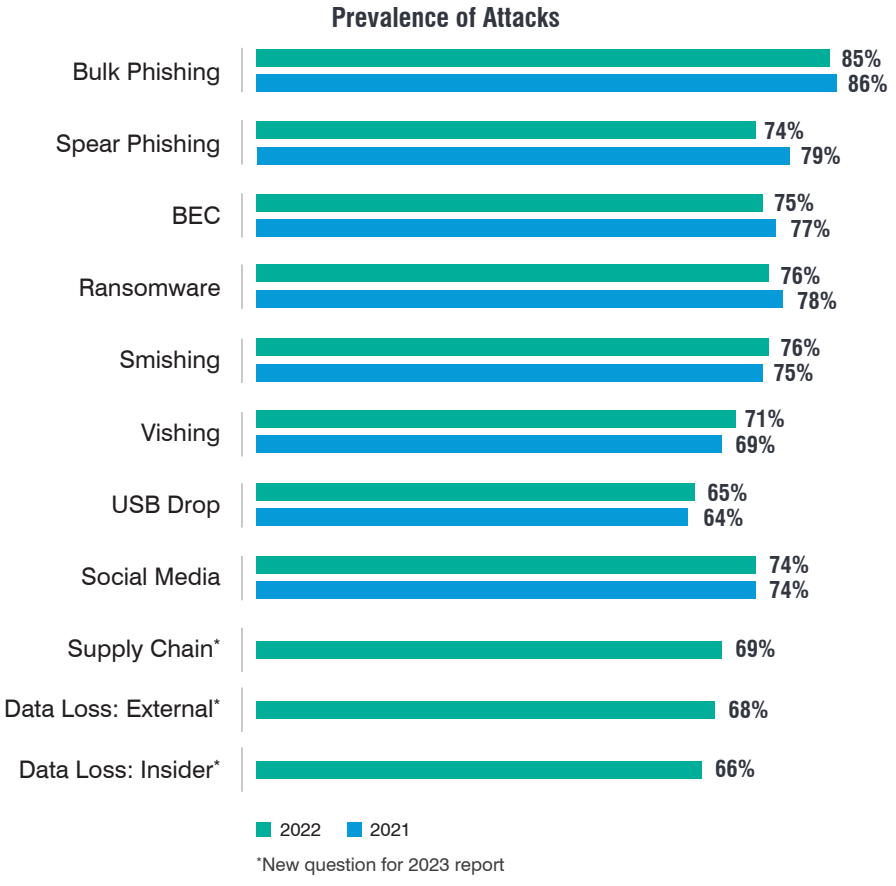
# Recognizing Risk

Cyber criminals know that most people have gaps in their security awareness. Their own campaign dashboards provide the evidence, with phishing kits, botnets and malware-as-a-service often showing click rates, downloads and other common digital "success" metrics.

Despite many techniques remaining effective, attackers aren't standing still. They have refined their social engineering tactics and introduced entirely novel attacks. When the threat landscape moves this quickly, security teams—and security awareness programs—need to be agile to keep up.

The incidence of most attack types has remained constant year on year, with high levels across the board. Threats arrive at an unrelenting pace and are almost as likely to appear from inside an organization as from an external attacker.

In total, 84% of survey respondents said that their organization had experienced at least one successful email-based phishing attack during 2022. And 54% said that they had dealt with three or more attacks.



## TOADs and MFA phishing

This year, telephone-oriented attack delivery (TOAD) and multi-factor authentication (MFA) phishing have made waves in the threat landscape. In a TOAD attack, targets receive a message, often containing a fake invoice or alert. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker. Our researchers have seen a range of next steps, including guiding victims to download malware, transfer money or enable remote access. At peak, we see over 600,000 TOAD messages sent per day, and the number has been steadily rising since the technique first appeared in 2021.

Multi-factor authentication (MFA) uses a second "factor" such as a phone or hardware key for added security when logging in to digital accounts. Enabling it is still a security best practice, but cyber attackers now have a range of methods to bypass MFA. While these are technically sophisticated attacks, some phishing-as-a-service providers already include MFA bypass in their off-the-shelf phishing kits.

## Brand abuse

Social engineering is integral to most cyber attacks. Using psychological manipulation, threat actors unsettle victims into making mistakes, ignoring warning signs or trusting malicious messages.

Social engineering's power comes from the fact that people often rely on mental shortcuts when making decisions. One of the clearest examples of social engineering is brand abuse. In these attacks, cyber criminals benefit from users' familiarity—and trust—of well-known brands. The most obvious way to take advantage of a brand is to use their logo or styling in a malicious message. But it's also worth considering that in the digital workplace, malicious links hosted on cloud storage solutions like Microsoft OneDrive, Google Drive and Dropbox are also likely to benefit from positive brand associations, as are malicious files created with familiar Microsoft 365 software.

# SIMULATING REALITY:

Microsoft was also the most common brand template used by our customers in phishing simulations. Half of the ten most-used templates were brand-abuse related. And templates featuring familiar brands tended to have high failure rates.

In 2022, we observed nearly 1,600 campaigns that involved brand abuse, and the most abused brand in our data was Microsoft. During the year, we saw over 30 million messages that used Microsoft branding or featured a Microsoft product like Office or OneDrive.

Perhaps not suprisingly, half of the 10 most-used templates by our customers in phishing simulations were brand-abuse related. Templates featuring familiar brands tended to have high failure rates.

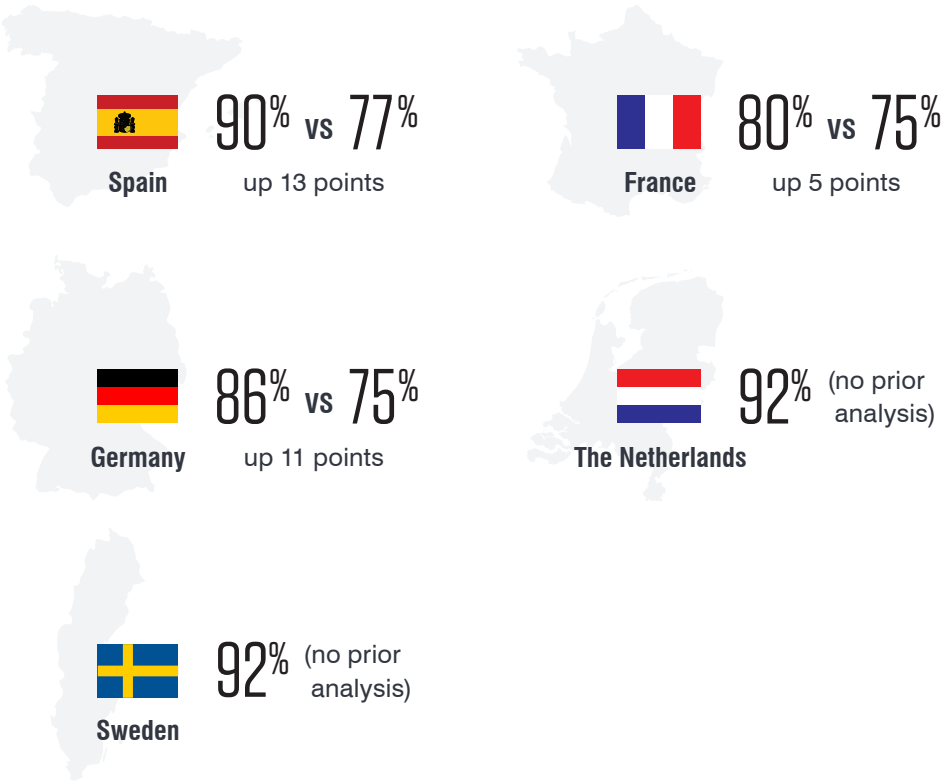
Notably, 44% of working adults in our survey said that they think an email is safe when it contains familiar branding. And Microsoft isn't the only brand experiencing regular abuse, with Amazon (6.5 million messages), DocuSign (3.6 million messages), Google (2.6 million messages), DHL (2 million messages) and Adobe (1.5 million messages) all regularly impersonated.

Board members across the globe rate BEC as their top concern (41%), followed by cloud account compromise (37%) and ransomware (32%), according to our *Cybersecurity: The 2022 Board Perspective* report.

## BEC Goes Global

In our recent *Cybersecurity: The 2022 Board Perspective* report, global board members rated business email compromise (BEC) as their top concern. English is the most common language used in BEC attacks, but some non-English-speaking countries are starting to see higher volumes of attacks in their own languages.

Year over year, we've seen growth in the following countries:




Globally, the average incidence of attempted BEC is 75%, and some countries do still fall well below this level. Japan (52%), Italy (51%), Brazil (56%), Korea (58%) and UAE (66%) all have BEC rates below that average. While the reason for these countries seeing fewer BEC attacks is unclear, there may be cultural, linguistic or logistical challenges that prevent attackers from effectively targeting and monetizing them. Or some organizations may lack visibility into the true number of attacks they're facing.

90%

of organizations that were infected by ransomware had cyber insurance

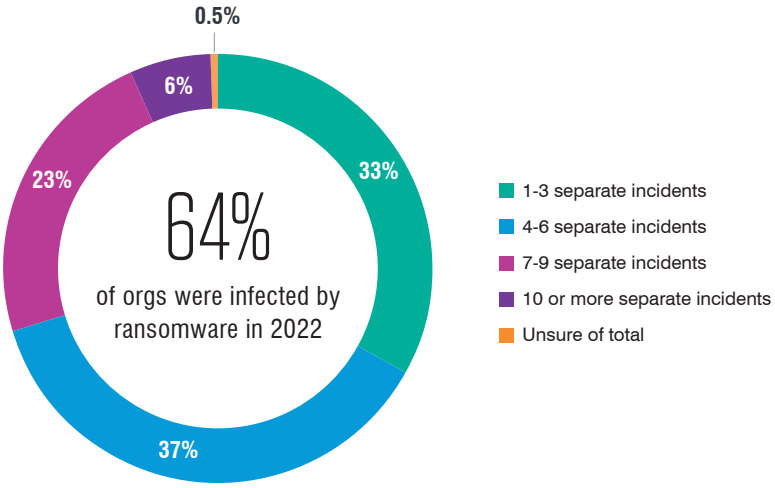
99%

of ransomware victims in the U.S. had cyber insurance, the highest percentage among countries surveyed

## Ransomware remains

BEC might be the most lucrative form of cyber attack, but ransomware can inflict massive operational, reputational and financial damage. About 76% of organizations experienced an attempted ransomware attack, with 64% experiencing a successful infection. Alarmingly, over two-thirds of respondents said their organizations experienced multiple separate incidents of infection.

**Ransomware by the Numbers**

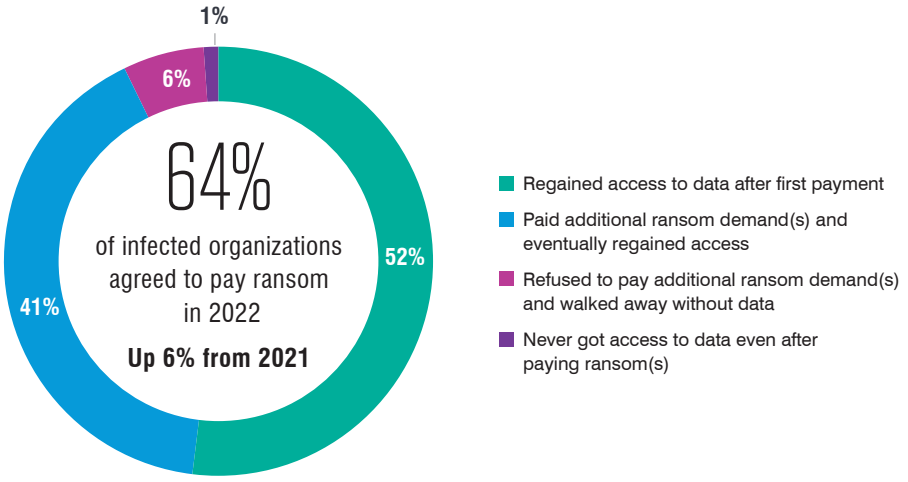



The FBI's latest Internet Crime Complaint Center (IC3) report shows that ransomware attacks have continued to rise, increasing by 51% year over year. The Bureau recommends that organizations refrain from paying, as this only contributes to the threat's growth.

There is also no guarantee that payment will result in a positive outcome. About 52% of victims—slightly better odds than a coin flip—regained access to their data after making a single ransomware payment. Nearly as many were obliged to make further payments, and some still never regained access to their data. Still, most infected organizations paid up, and many did so more than once—usually with the help of cyber insurance.

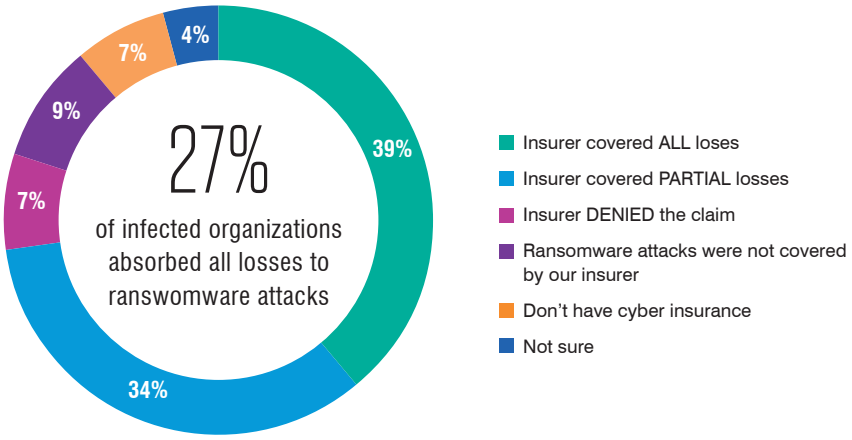
The overwhelming majority of organizations that faced a ransomware attack had cyber insurance (90%), and most of those insurers were willing to help (82%). This perhaps explains the high propensity to pay, with 64% of organizations infected with ransomware paying at least one ransom—a six-point increase from last year.

### Ransomware Infections: What Happens After Payment




Some 41% said they paid more than one ransom before regaining access to their data. The majority of companies taking out cyber insurance (73%) said that their insurer covered some or all the losses incurred.

### Cyber Insurance Role



25%

of users said they had changed jobs within the past two years

44%

of those who left a job took data with them

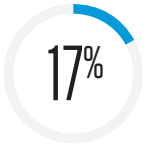
## The insider threat

According to 1,400 global CISOs surveyed in our *2022 Voice of the CISO* report, insider threats are their biggest security concern. And today's job market has made data protection an even bigger challenge. Pandemic-related job mobility coupled with post-pandemic economic uncertainty has resulted in large numbers of people changing or leaving jobs. And data shows that people often take sensitive data and credentials with them when they go.

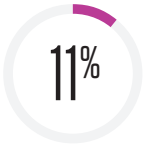
In this year's survey, we asked end users if they had changed jobs within the past two years. A quarter said that they had, and, of those who left their jobs, nearly half admitted to taking data with them when they left.

We also added questions about insider data loss to our survey of security professionals. Nearly 65% reported that their organization had experienced data loss because of an insider. The number was even higher for the U.S., the U.K. and the Netherlands at around 85%.

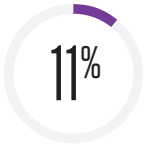

report one to 10 data loss incident(s) via insider




report 11 to 25 data loss incidents via insider




report 26 to 50 data loss incidents via insider




report over 50 data loss incidents via insider

The most common cause of data loss to insiders is the result of carelessness or negligence. But that isn't the only type of insider threat. In general, they fall into three main categories:

A **"careless user"** might cause accidental harm, such as a Japanese city contractor who lost a USB stick with the personal data of almost half a million residents.

A **"malicious user"** takes actions for deliberate harm or personal gain, such as an outgoing Pfizer employee who allegedly uploaded over 12,000 confidential files to a Google Drive account.

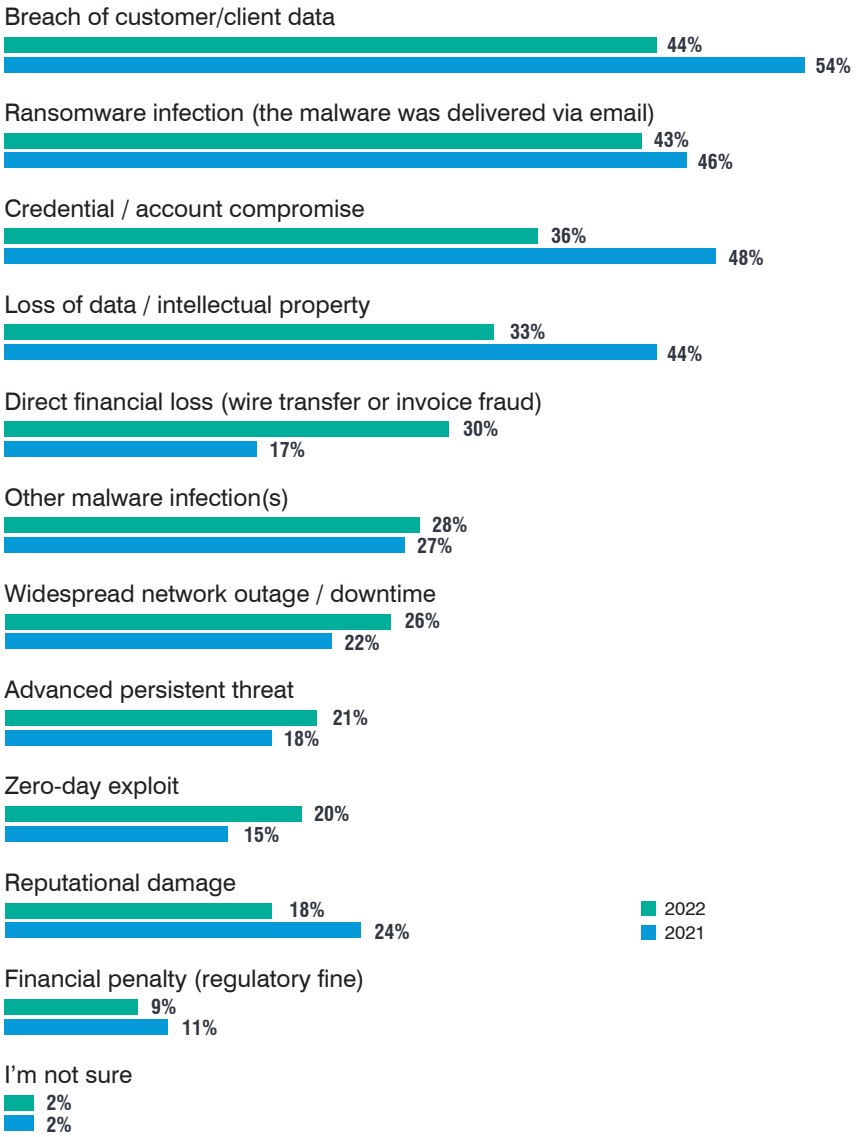
A **"compromised user"** is enticed by reward or coercion to infiltrate or exfiltrate data, such as a former SoftBank chief accepting ¥400,000 to leak confidential information to a Russian diplomat.

## Counting the cost

For most threat actors, the goal of an attack is financial. And according to our data, 30% of organizations that endured a successful attack experienced a direct monetary loss, such as a fraudulent invoice, wire transfer or payroll redirection. This is an increase of 76% year over year.

The three most common consequences of attack were data breach (44%), ransomware infection (43%) and account compromise (36%). As all three of these actions can be readily monetized by cyber criminals, the financial incentives driving attacks are clear to see.

**Results of Successful Phishing Attacks (Global Average)**



## PHISHING SIMULATION BY THE NUMBERS:

135 million+

simulated phishing attacks sent by our customers in 2022. An increase of 39 million over the 2021 number (96 million).

~410 million

simulated phishing messages have been sent since we started counting.

# Benchmarks: Failure Rates, Reporting and Resilience

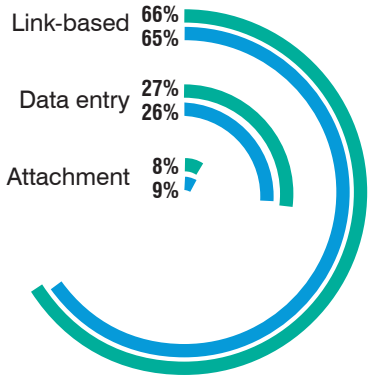
In addition to surveys and threat research, *State of the Phish* also compiles data from our phishing simulation tool to help identify areas of risk and areas for improvement.

The first headline to note is that users continue to display a major vulnerability to, well, headlines. Trending topics from news or social media are often engaging and can cause people to ignore red flags. Beyond regularly targeting seasonal events like holidays and the tax deadline, threat actors moved quickly to adopt the COVID-19 pandemic as a favored lure subject. Cyber criminals are nimble and opportunistic—so security awareness programs should use real-world threat intelligence and be modelled on real-world lures. Our researchers even saw a campaign making use of the death of Queen Elizabeth II to distribute malware.

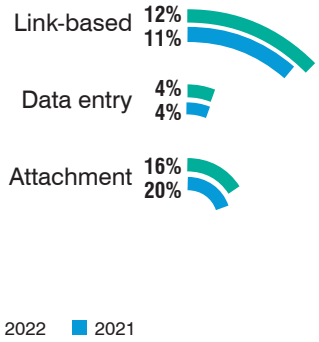
## Template failure rates

Attackers are adaptive, so phishing simulations should cover a range of templates and themes to reflect the current landscape. In real-world terms, attacks using unsafe URL links are between three to four times as common as those containing attachments. So the current ratio of link and attachment templates needs rebalancing. Especially as attachments still have an appreciably higher failure rate than links (though this has fallen by 4% since last year).

**Simulation type and frequency**




**Average failure rates**

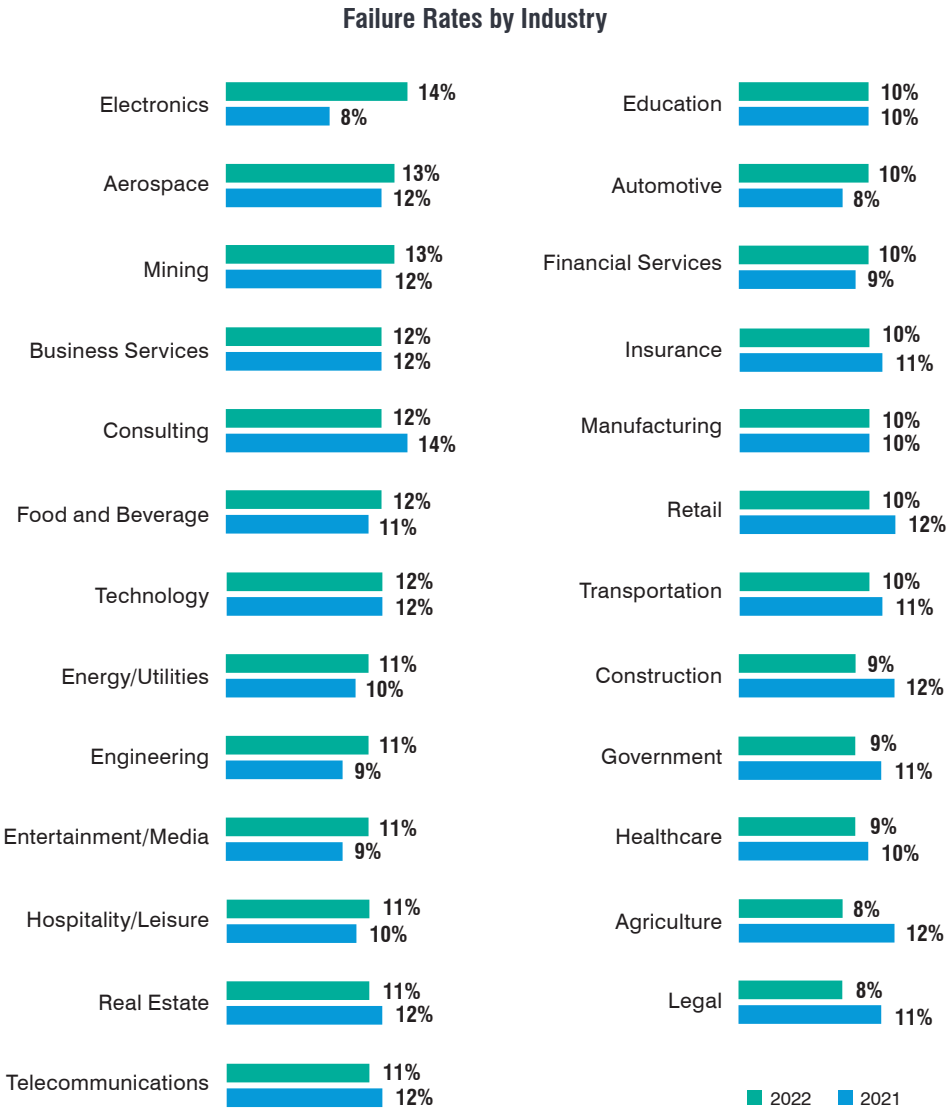


# FAILURE RATE COMPARISON:

Each industry represented in our failure rate comparison includes data from at least 20 organizations and at least 300,000 simulated phishing attacks.

## Failure rates by industry

Below are the industry average failure rates for phishing simulations. The data is in aggregate and contains all template types. Legal has the lowest overall failure rate, and electronics has the highest.



# TARGETS OF OPPORTUNITY:

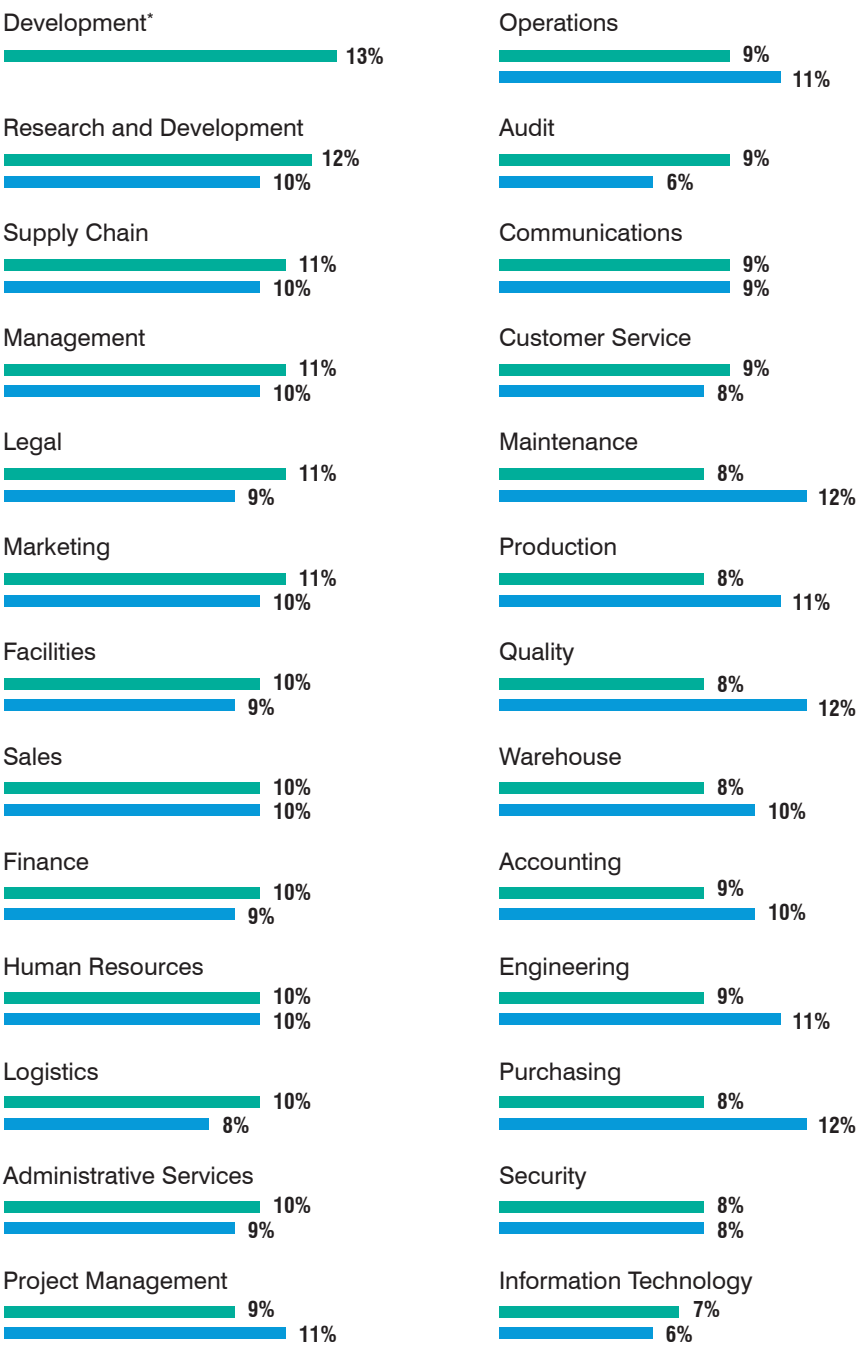
Development, R&D, supply chain, legal and managerial groups shared the highest failure rates.

## Failure rates by department

Attackers are known to comb LinkedIn and other sources to find targets in departments with access to financial information and intellectual property. So, measuring failure rates by department is crucial to identifying and mitigating that risk.

Among our customers, three-quarters of departments were involved in 474 campaigns, receiving 6,000 messages or more in 2022 with almost 800 different templates. This is a substantial increase over 2021 usage. Unfortunately, the worst-performing functions were some of the most valuable: development, R&D, supply chain, legal and managerial groups shared the highest failure rates. Between them, these groups have access to valuable IP, contracts, invoicing and high-level credentials.

## Failure Rates by Department




*New question for 2023 report

# FAMILIAR FAKES:

Microsoft was the most-used template category in phishing simulation campaigns in 2022, including subjects across Microsoft OneDrive, Teams, and O365 Auth.

## Template effectiveness

As we've seen, newsworthy topics are highly effective, both as real-world threats and simulation templates. Among the 10 most-used template themes in 2022, the failure rate for a COVID-19 lure was more than 50% higher than the next closest theme.

| Subject | Failure Rate % |
|---|---|
| Coronavirus: COVID Update | 17 |
| Cloud Services: DocuSign document for review | 11 |
| Shipping: FedEx delivery failure | 11 |
| Microsoft: OneDrive contract shared | 7 |
| Email Account Alert: Email disconnect | 7 |
| Email Account Alert: Undelivered email | 6 |
| Email Account Alert: Queued email | 4 |
| Shipping: Amazon shipment | 2 |
| E-commerce/Retail: Amazon mismatch | 1 |

COVID-19 was also represented twice in our list of "trickiest" themes—those with the highest failure rate regardless of how many times the template was used. Corporate internal communications/HR comms also appeared on the list multiple times. This suggests that employees are particularly vulnerable to messages alluding to disciplinary or other work-related issues that raise anxiety and reduce attention. Also surprising was people's tendency to fall for entertainment-themed attacks, where messages related to personal interests in sport or television landed in their corporate inbox. This perhaps reflects the reality of how often work email is used to sign up for personal accounts.

| Subject | Failure Rate % |
|---|---|
| E-commerce/Retail: E-Gift card | 27 |
| Entertainment: Squid Games next season early access | 25 |
| Banking/Financial Services: Purchase problems and funds removed | 24 |
| Coronavirus: COVID data cases report | 23 |
| Travel: Room confirmation | 23 |
| Corporate Communications: Dress code | 22 |
| HR: Code of Conduct—Reported incident | 21 |
| Coronavirus: COVID—List of infected users | 20 |
| Corporate Communications: Building evacuation plan | 20 |
| Entertainment: NBA Finals brackets | 20 |

Most of the simulated campaigns our customers ran used two or three templates, with the average being 2.4. This is slightly higher than last year. Threat actors change their email lures from day to day, so using more templates reduces the chance of a simulation becoming widely discussed and increases the accuracy of the test.

## Reporting and resilience

Reporting suspicious email is key to both defending against cyber attacks and to evaluating the effectiveness of an organization's security awareness efforts.

Overall, reporting rates for simulated phishing increased to 17% (vs. 15% in 2021). Failure rates for attacks remained at 10%. From these two numbers, we calculate a "resilience factor," which provides a quick way to gauge how resistant industries and departments are to attack. Note: the failure rates below are a subset of totals used previously, limited to customers who use our PhishAlarm in-client reporting tool.

17% average reporting rate ÷ 10% average failure rate = 1.7 resilience factor

Last year the average resilience factor was 1.5, meaning that people have become slightly better at reporting and resisting attacks. This is reflected across all three template types:

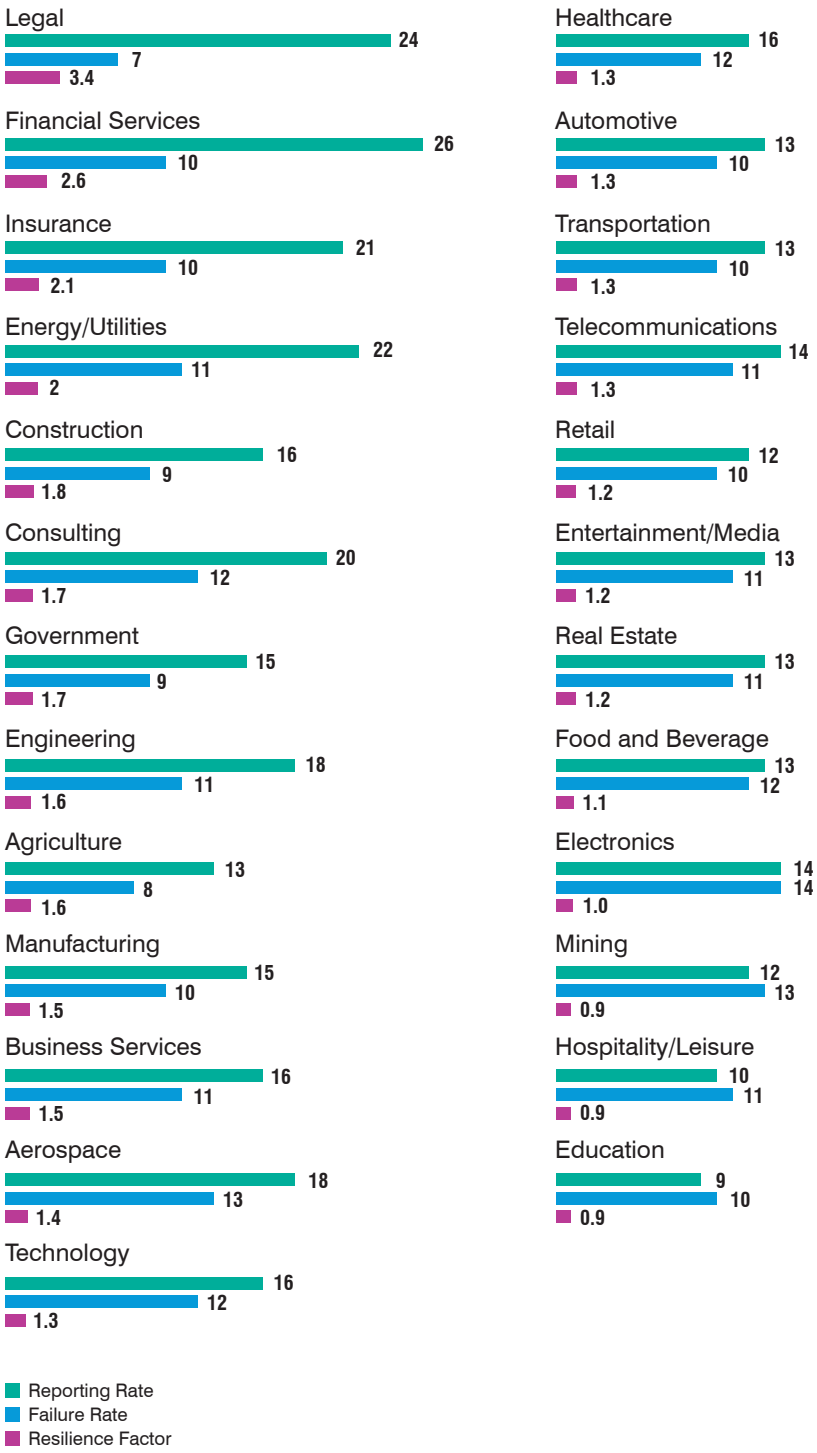
| | 2022 | 2021 |
|---|---|---|
| Link-based | 17% | 16% |
| Data entry | 19% | 17% |
| Attachment | 19% | 18% |

At industry level, there is a broad span of resilience scores, ranging from 3.4 in legal to 0.9 in education. While the relatively strong performance of high-stakes industries like financial services and energy is heartening, several critical pieces of infrastructure fall below average, including agriculture, healthcare and transportation. As ransomware attacks on healthcare services over the past few years have shown, the consequences of low cyber resilience in these organizations can be severe.

# INDUSTRY REPRESENTATION

Each industry represented in our failure rate comparison includes data from at least 20 organizations and at least 300,000 simulated phishing attacks.

## Reporting Rates by Industry



# 75 million

malicious messages were blocked by Proofpoint as a result of user-reported suspicious emails

Our PhishAlarm button is ultimately designed to let users report suspicious real-world messages, not just phishing simulations. Beyond giving security teams a way to measure user response, user-reported emails are one of the signals that power our threat detection engines. In fact, we blocked an additional 75 million malicious messages in 2022 based on intelligence from user-reported attacks.

**Between them, those malicious messages contained:**

**47 million+**
credential phishing emails

**~600,000**
downloaders

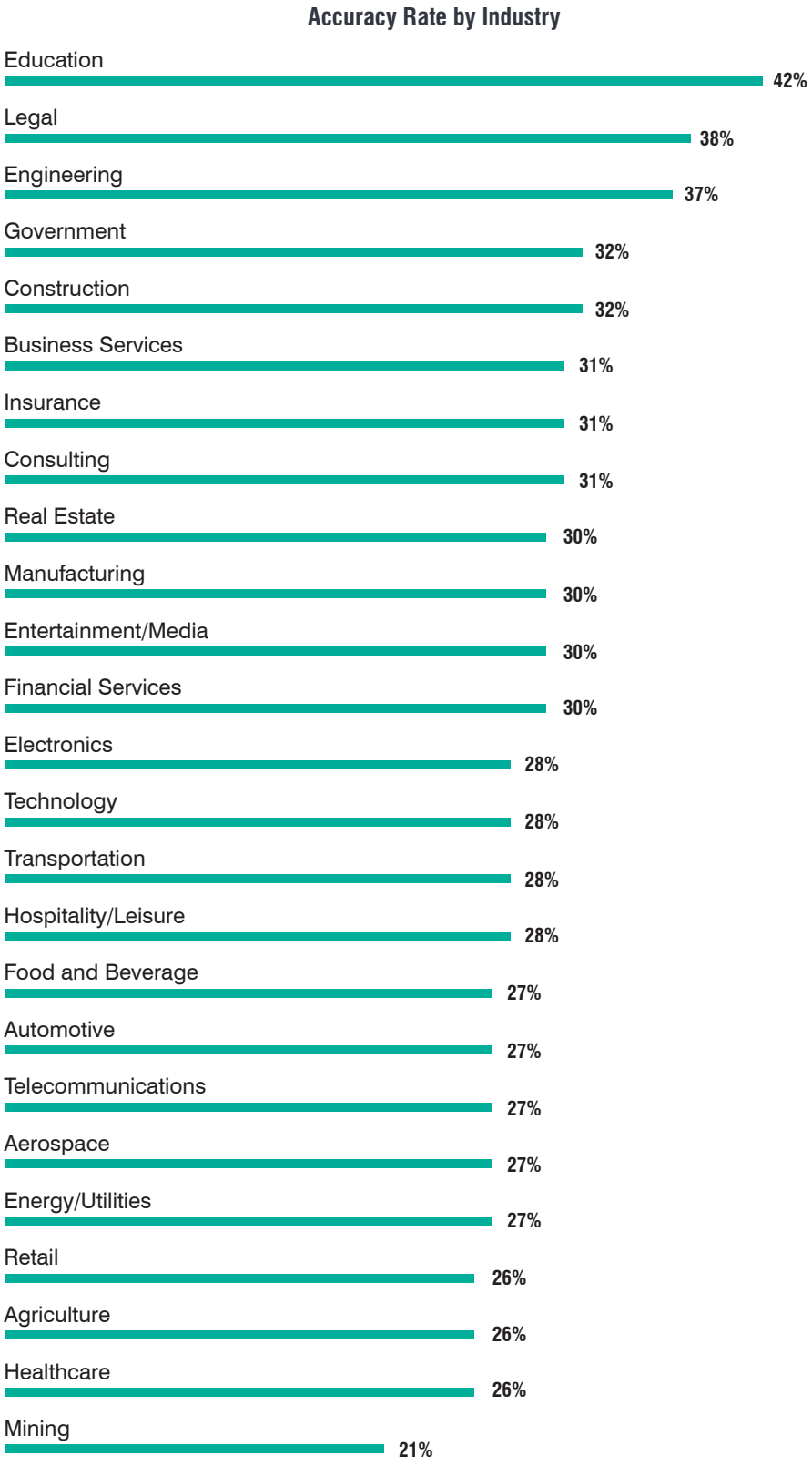
**1.5 million+**
emails containing malware

**260,000+**
keyloggers and stealers that could lead to account compromise

**1.2 million+**
banking Trojans

**680,000+**
botnet malware

Of course, not every reported email turns out to be malicious. So we also benchmark real-world reporting accuracy for customers who use our PhishAlarm report button. Notably, while education had the lowest resilience among named industries, its real-world reporting accuracy is highest.


Accuracy Rate by Industry
Education
42%
Legal
38%
Engineering
37%
Government
32%
Construction
32%
Business Services
31%
Insurance
31%
Consulting
31%
Real Estate
30%
Manufacturing
30%
Entertainment/Media
30%
Financial Services
30%
Electronics
28%
Technology
28%
Transportation
28%
Hospitality/Leisure
28%
Food and Beverage
27%
Automotive
27%
Telecommunications
27%
Aerospace
27%
Energy/Utilities
27%
Retail
26%
Agriculture
26%
Healthcare
26%
Mining
21%

98%

of organizations had a training program of some sort

but...

Only 56%

trained everyone in the organization

and...

Only 35%

ran phishing simulations

# Security Awareness: Insights and Opportunities

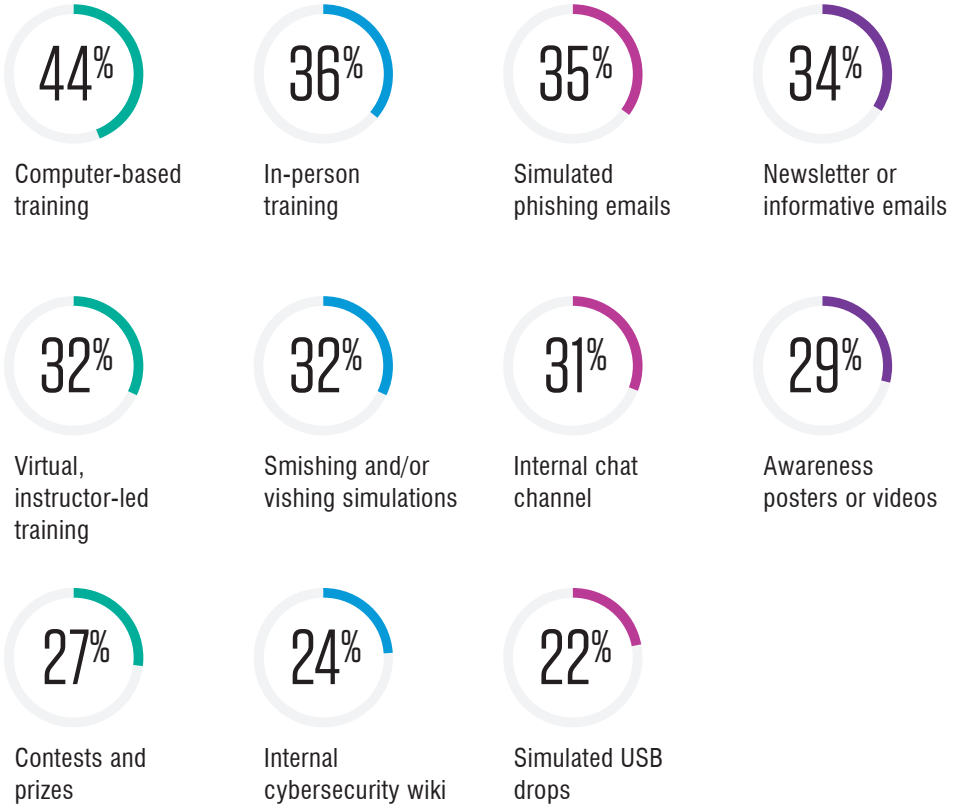
The majority of organizations covered by our surveys have security awareness programs. But most struggle to make them effective.

In fact, 27% of respondents said that failure rates had remained the same, even after introducing training. This is a big untapped opportunity. Time is already being dedicated to training, and, with a few key improvements, resilience and awareness could increase significantly.

Almost every organization offers a training program of some sort, with 74% conducting formal security awareness training. So far, so good. But only 56% train everyone in the organization—a figure which hasn't improved much since last year. And while training is the foundation of security awareness, it can only do so much.

As we've seen, the threat landscape moves fast. Threat actors are always innovating. An effective way to assess user vulnerability to new threats in a secure environment is to use phishing simulations drawn from real-world lures. But only 35% of organizations use simulations—down from 41% in 2021. Times are hard, and budgets are shrinking, but the cost of a breach makes skimping on security a risky trade.

**We asked respondents about their use of a range of training options:**




In addition to regular, formal training, 79% of organizations offered training for people who fell for real-world or simulated phishing attacks. This was a six-point drop from last year. Overall, time given to training was low, with 80% of respondents saying their organizations only offered two hours or less per year.

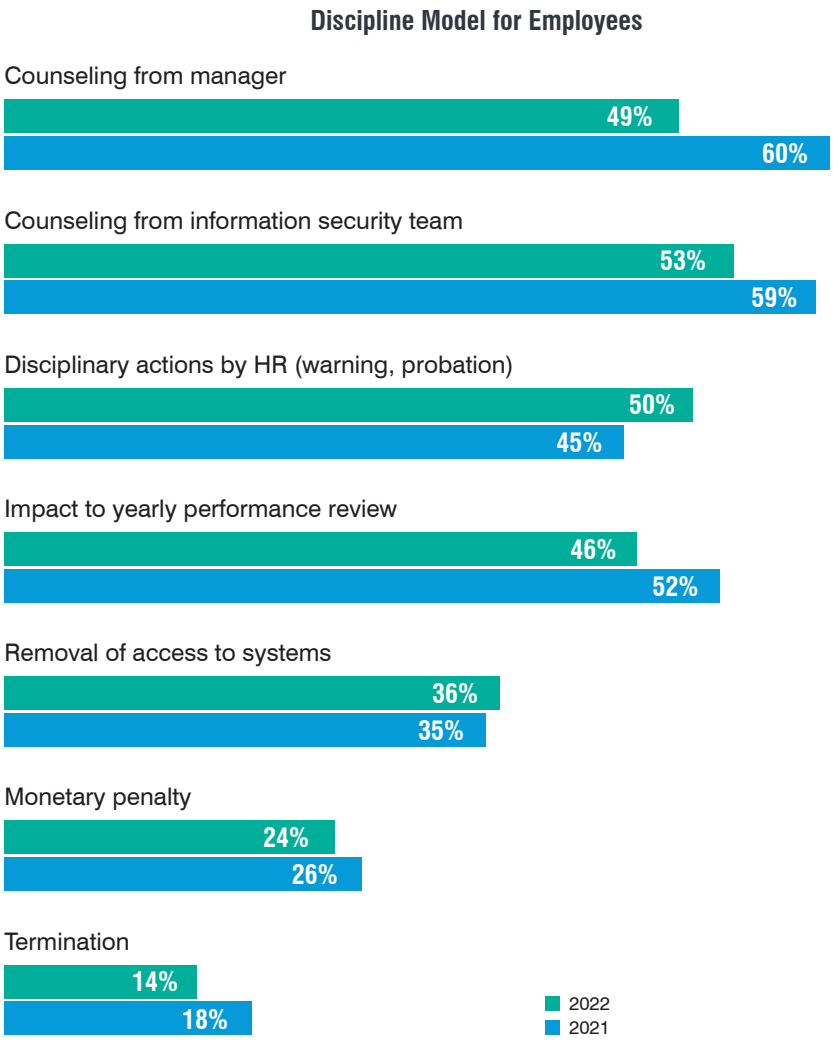
When it comes to training topics, malware, email-based phishing and Wi-Fi security were the most covered subjects, followed by ransomware. This aligns with the results of our end-user survey, which found that malware, phishing and ransomware were the terms users were most likely to correctly define.

Most organizations say that they use threat intelligence to inform their training, though this wasn't something we found reflected in more specific questioning about content. And when it comes to aligning with top CISO concerns, only 23% of programs covered supplier risk. Likewise, only 31% cover BEC, despite this being the most financially damaging form of cyber crime.

## Building a security culture

Finding the right balance between reinforcement and punishment is an perennial problem. Since last year, we've seen a few changes at both ends of the spectrum, with decreases in both the most lenient and the harshest actions for people who fail simulated or real-world attacks.

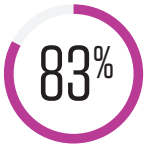
Overall, 52% of organizations have formalized consequences in place for employees who interact with real or simulated attacks (55% in 2021). And 26% of those who don't have such a model in place say they are considering it or will implement one soon. About half of organizations say they won't discipline employees until they have failed at least three phishing tests.



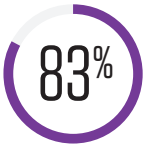
Weighing the impact of these consequence models, security professionals say they've seen good results.


said consequences had increased end users' overall phishing awareness


think security is considered a top priority for their company




feel employees think security is a top priority at work

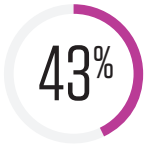



report feeling positive about the security culture at their org

On the other hand, employees take a less positive outlook:


complain about the consequence model

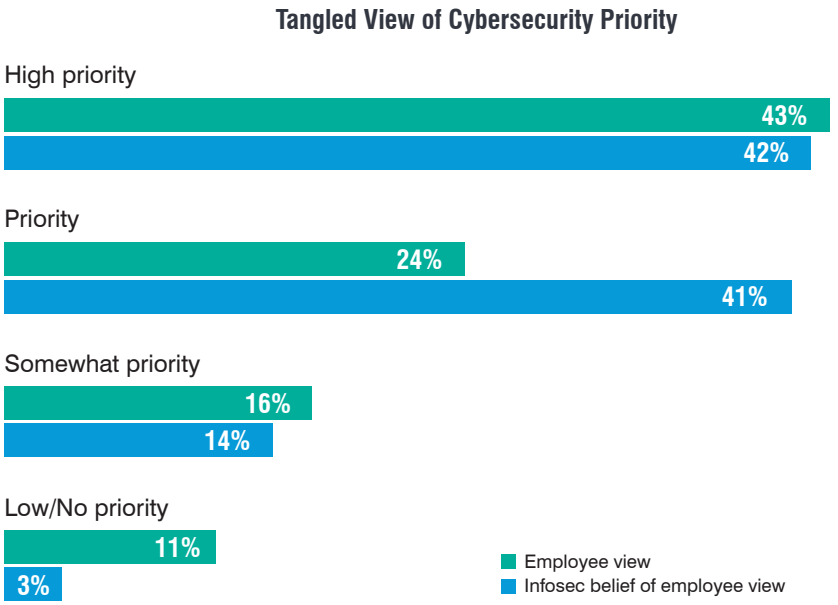

said cybersecurity is not a top priority of theirs at work




don't feel confident that their IT team will handle cybersecurity incidents


don't think company's security tools will block all dangerous emails

The data shows an obvious discrepancy in perception between security teams and end users, which possibly hints at lack of two-way communication. To build a strong, sustainable security culture, security teams need to do more than just measure how people respond to real and simulated threats. They also must understand how employees feel about the company's security culture and their place within it.




Taken together, the conflicting views of employees and security teams suggest that security culture is at a crossroads. But there is a way forward. With the right training and threat intelligence, employees can learn to understand the threat landscape and the dangers it poses. With a fair and thoughtful consequence and reward model in place, security teams can encourage and direct employees to embody the right security behaviors. And with strong executive sponsorship, company culture can reinforce the importance of protecting people and defending data.

# Conclusions

As always, there is a lot to digest in this year's *State of the Phish*. And, even as we've tried to give benchmarks and show trends, the reality is that every company faces unique risks. Building a security awareness program tailored to the specific threats faced by your organization is a big challenge.

But there's reason for optimism. 67% of security pros said that phishing failure rates have gone down since a security awareness program was implemented. And as our survey of end-user awareness shows, there is plenty of low-hanging fruit to push that number even higher.

Our analysis suggests three distinct approaches that can help you seize the opportunity.

**Reduce complexity by asking the right questions**

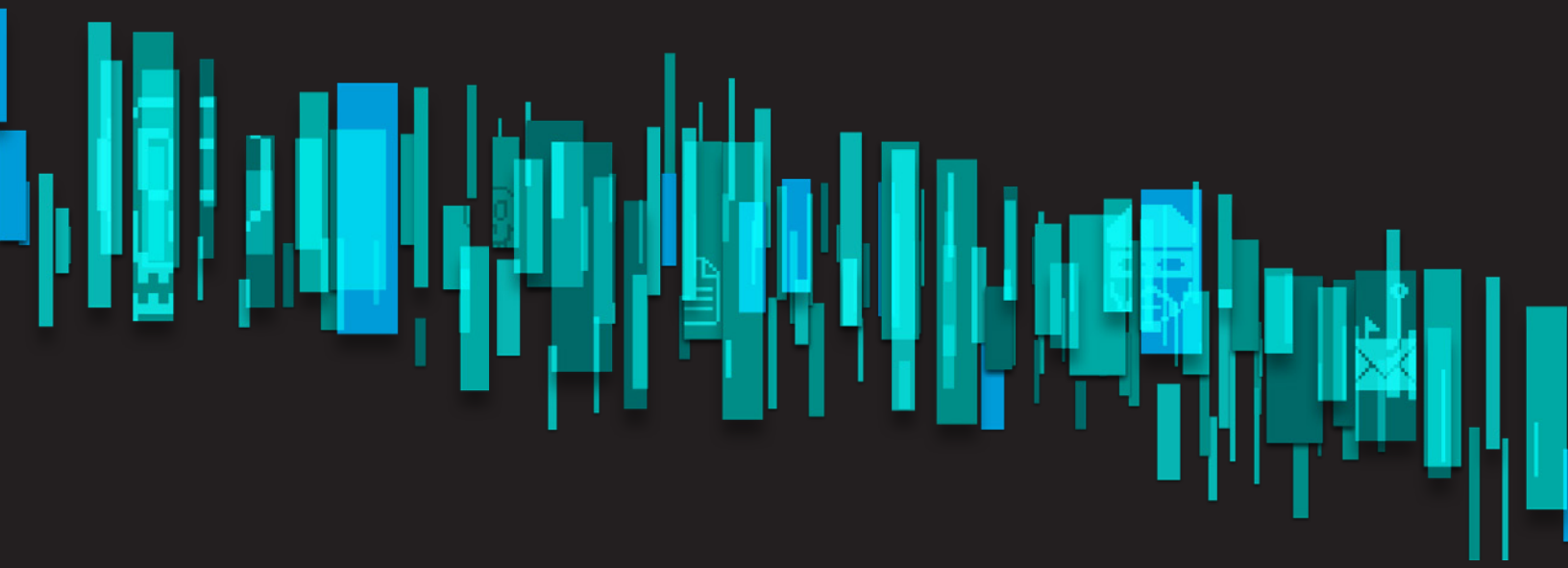
- Who in my organization is being attacked?
- Where are the current defensive gaps?
- What are my priorities to mitigate human risk?

**Pair threat intelligence with organization-wide security awareness education**

- Identify which users are most likely to be targeted and who is most likely to succumb.
- Match education, including phishing simulation and training, to threats currently circulating.
- Tailor training and assessment for most attacked users based on the threats targeting them.

**Build a security culture that goes beyond training**

- Training is crucial but not sufficient.
- A strong workplace security culture will motivate users to take security more seriously and help them build sustainable security habits that extend to their personal lives.
- Measure the behavioral metrics that matter, and respond with appropriate and fair remediation.



## LEARN MORE

To learn more about how Proofpoint provides insight into your vulnerability-, attack- and privilege-based user 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.

0400-010-01-01