proofpoint.

ANNUAL REPORT

2020 State of the Phish

An in-depth look at user awareness, vulnerability and resilience

proofpoint.com

INTRODUCTION

Do you have a good sense of how well users understand cybersecurity terms and best practices? Do you know the top issues infosec teams are dealing with as a result of phishing attacks? How about the ways organisations are fighting phishing attacks and the successes (and struggles) they're experiencing?

Our sixth annual *State of the Phish* report again brings you critical, actionable insights into the current state of the phishing threat. **You'll learn about:**

- The end-user awareness and knowledge gaps that could be hurting your cybersecurity defences
- The impacts information security professionals are experiencing because of phishing attacks and the ways they're trying to combat these threats
- How Proofpoint customers are approaching phishing awareness training, and the ways we're helping them measure programme success

This year's report includes analysis of data from a variety of sources, including the following:

A survey of more than

3,500

working adults across seven countries

(the United States, Australia, France, Germany, Japan, Spain and the United Kingdom)

A survey of more than

600

IT security professionals across the same seven countries

Nearly

50M

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

More than

9M

suspicious emails reported by our customers' end users

"Phishing" can mean different things to different people, but we use the term in a general sense. In the context of this report, phishing encompasses all socially engineered emails, regardless of the specific malicious intent (such as directing users to dangerous websites, distributing malware, collecting credentials and so on).

Table of Contents

SECTION 1

In the Mind of the End User: Global Awareness Levels

We like to kick off *State of the Phish* with a look at cybersecurity awareness of end users around the globe. This year's survey—which we conducted via a third party—polled more than 3,500 working adults across seven countries (the United States, Australia, France, Germany, Japan, Spain and the United Kingdom).

As in years past, we assessed the following:

- Recognition of commonly used cybersecurity terms: phishing, ransomware, malware, smishing (SMS/text phishing) and vishing (voice phishing)
- Understanding of the limits of technical safeguards when it comes to identifying (and fixing) malware-related incidents
- Whether younger workers have an edge over older workers in cybersecurity knowledge

This year we added questions about a broader set of cybersecurity behaviours and beliefs. We found that many workers remain unaware of fundamental best practices. This lack of knowledge can exacerbate the phishing threat and undermine your security posture.

This section covers these topics:

- Smartphone and Wi-Fi usage
- Password management
- Virtual private network (VPN) usage
- Use of work devices for personal activities

We highlight global averages, calling attention to regional outliers and other notable findings. Country-by-country breakdowns for all questions are in the Appendix.

Common terms: do users understand what you're saying?

Those in infosec and IT must wonder: Who *doesn't* know what phishing is? The (unfortunate) answer is this: countless numbers of people.

Many users are at least vaguely aware of threats from malicious software, email, text messages and phone calls. But they may not know the more formal terms used to describe them. In other words, you and your users may not be speaking the same language when it comes to critical security issues. If you've jumped into a security education programme unaware of what your users do and do not know, you could be setting yourself up for failure.

Our survey asked users to define key cybersecurity terms, offering three multiple-choice answers and an "I don't know" option. Incorrect answers and not knowing are both important signals that organisations have not defined key cybersecurity terms for employees.

What is PHISHING?

Correct **61%**

Incorrect **24%**

I Don't Know **15%**

Only 49% of US workers answered correctly.

German workers were most likely to recognise this term (66%).

What is RANSOMWARE?

Correct **31%**

Incorrect **31%**

I Don't Know **38%**

Last year, 45% of global workers answered this question correctly. This drop in awareness could be a carryover from 2018, when ransomware attacks fell off dramatically, leaving infosec teams less likely to discuss the topic with users.

What is MALWARE?

Correct **66%**

Incorrect **17%**

I Don't Know **17%**

Nearly 80% of Spanish workers answered this question correctly.

Nearly 30% of US workers believe malware is a type of hardware that boosts Wi-Fi signals.

What is SMISHING?

Correct **30%**

Incorrect **21%**

I Don't Know **49%**

Awareness of this term is up year over year. Just 25% of respondents answered correctly in our prior survey.

French workers were top performers: 54% answered correctly.

What is VISHING?

Correct **25%**

Incorrect **22%**

I Don't Know **53%**

Last year, only 18% of global workers answered this question correctly.

At 48%, French workers were about twice as likely as their global counterparts to recognise this term.

Cybersecurity behaviours: how are workers putting organisations at risk?

Email security should be a top concern of individuals and organisations alike. But users also need to recognise that decisions they make outside of their inboxes can put them (and your organisation) at greater risk of phishing attacks and other threats.

Smartphones and Wi-Fi: potential weak links

Nearly all survey respondents—95%—said they use a smartphone, and 41% said they use their devices for both personal and work activities. Here's how carefully they protect those devices (see the Appendix for more detail):

- 42% of smartphone owners opt for a biometric lock (such as a fingerprint scan).
- 24% unlock their device using a four-digit PIN.
- 10% have no lock on their device.

Wi-Fi presents another challenge. Open-access networks are virtually everywhere, and device users readily connect (often to avoid data charges). Unfortunately, familiarity can lead to misplaced trust:

- 26% of global respondents think they can safely connect to public Wi-Fi networks in trusted locations, such as local coffee shops and international airports.
- 17% aren't sure whether they should or shouldn't trust open-access Wi-Fi networks in familiar locations.

But public hotspots aren't the only source of Wi-Fi danger. Working remotely has become more common, which means that home Wi-Fi hygiene can affect the security of your organisation's data and systems.

We found that 95% of global workers have a home Wi-Fi network. But are those networks adequately protected? You be the judge:

- 49% password-protect their network.
- 45% of respondents have personalised the name of their Wi-Fi network.
- 31% have changed the default password on their Wi-Fi router.
- 19% have checked and/or updated their Wi-Fi router's firmware.
- 14% are unsure of how to implement Wi-Fi security measures.
- 11% said they find Wi-Fi security measures too time-consuming and/or inconvenient to implement.

INTERNATIONAL

14%

of UK workers never lock their smartphones.

45%

of US workers believe that trusted locations always offer safe public Wi-Fi networks.

21%

of UK workers said they are unsure of how to fully secure their home Wi-Fi networks.

KEY FINDING

Nearly 90% of survey respondents said they back up important files using cloud storage, external drives or a combination of sources. While this is a positive ransomware preparedness measure, it's important for organisations to have visibility into where their data is being stored.

INTERNATIONAL

44%

of US respondents said they use a password manager, well above the global average.

15%

of French respondents use a password manager, the fewest of the regional workers surveyed.

US respondents take top marks with VPN usage:

51% have at least one installed.

63% of those who have a VPN always use it.

VS

French respondents are least likely to use a VPN: **35%** have a VPN installed.

Japanese workers are least familiar with VPNs: **37%** don't know what a VPN is.

Technical safeguards: more misplaced trust

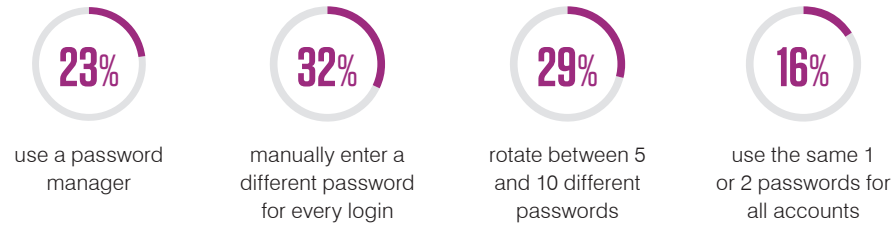
When it comes to end-user cybersecurity, misconceptions are often at the root of risky behaviours. We found that many working adults mistakenly rely on technical safeguards on home and work devices to be failsafe solutions:

- 66% of survey respondents believe that keeping anti-virus software up to date will prevent cyber attackers from accessing their devices.
- 51% think that their IT teams will be automatically notified if they accidentally install a virus or other malicious software on their work computer.

Passwords and VPNs: misused and misunderstood

Passwords are another source of frustration for infosec and IT teams. Most concerning: users' tendency to reuse passwords. Thankfully, we found that more than half of respondents are avoiding the dreaded practice—but by a slim margin.

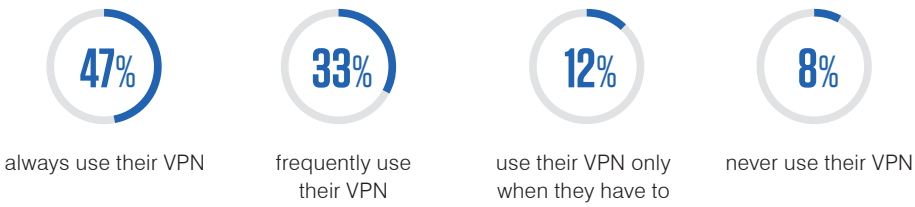
Password Habits



VPNs provide an easy way to protect sensitive data and accounts. Unfortunately, many users—and apparently, the organisations they work for—haven't received the memo.

VPN Adoption on Work and Personal Devices

VPN Usage Once Installed



KEY FINDING

~50%

of respondents said they give friends and family access to their employer-issued devices.

Corporate devices: do you know where they've been?

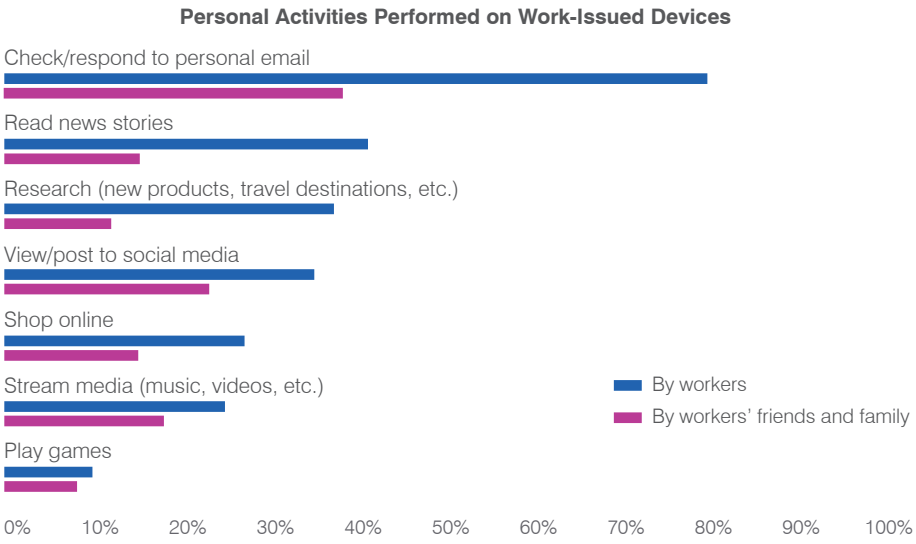
Many, if not most, organisations spell out acceptable-use policies for work-issued devices. But unless access is locked down, there's no telling whether workers are actually following those guidelines. And as the chart shows, those who have access freely use their devices for personal activities. If your employees are not well-versed in how to safely interact with email, websites and social media, their actions could lead to security risk.

Still, we're betting it's particularly worrisome to think of your employees' friends and family having access to your organisation's PCs and smartphones. Though 51% of those with work-issued devices said they deny external access, plenty of people allow their loved ones—including children—to use their devices for a range of activities.

INTERNATIONAL

61%

of US workers allow friends and family to use their work devices, making them about twice as likely as Japanese and German survey respondents to do so.



Workforce turnover: are younger workers ushering in a more cyber-secure culture?

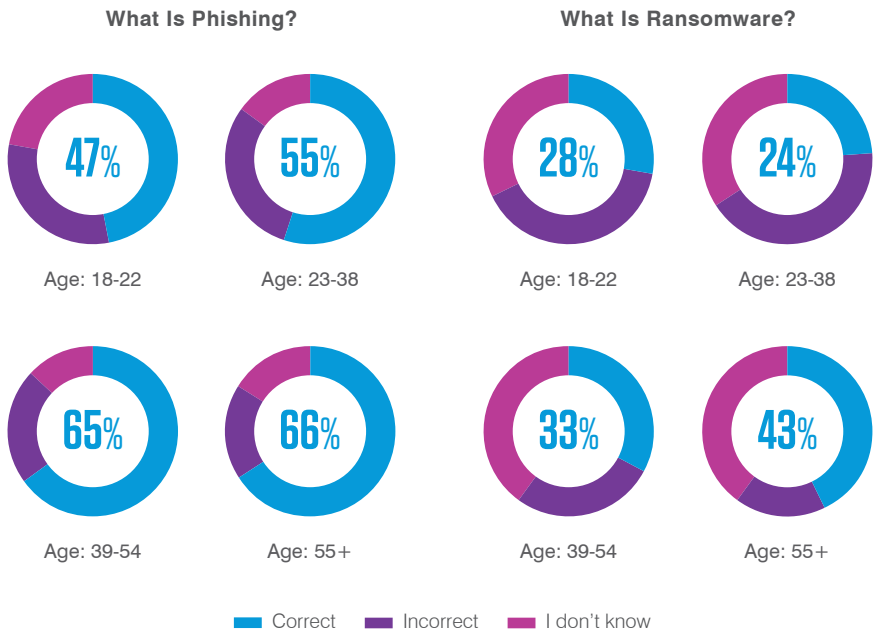
For today's younger workers, smart devices and applications are second nature. As workforces see an influx of these technology-savvy individuals, some might assume that younger workers will bring with them an innate understanding of cybersecurity best practices.

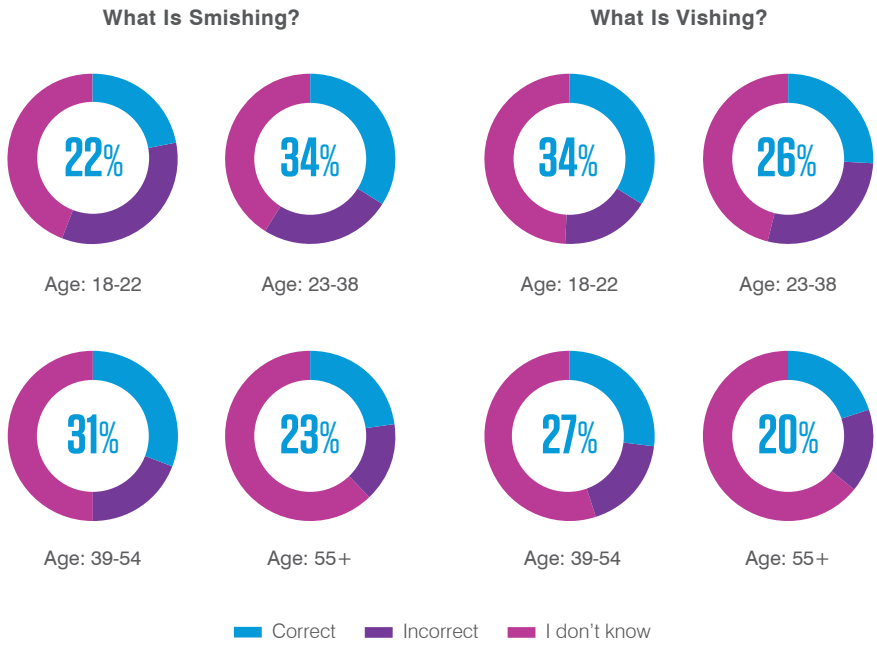
That's not always the case. Here's how younger workers and the much-discussed millennial generation compare to older employees—including baby boomers—on six key questions.[1]

[1] According to Pew Research, millennials fell into the 23-38 age bracket and baby boomers were 55 years and older in 2019, the year in which our survey was conducted.

KEY FINDING

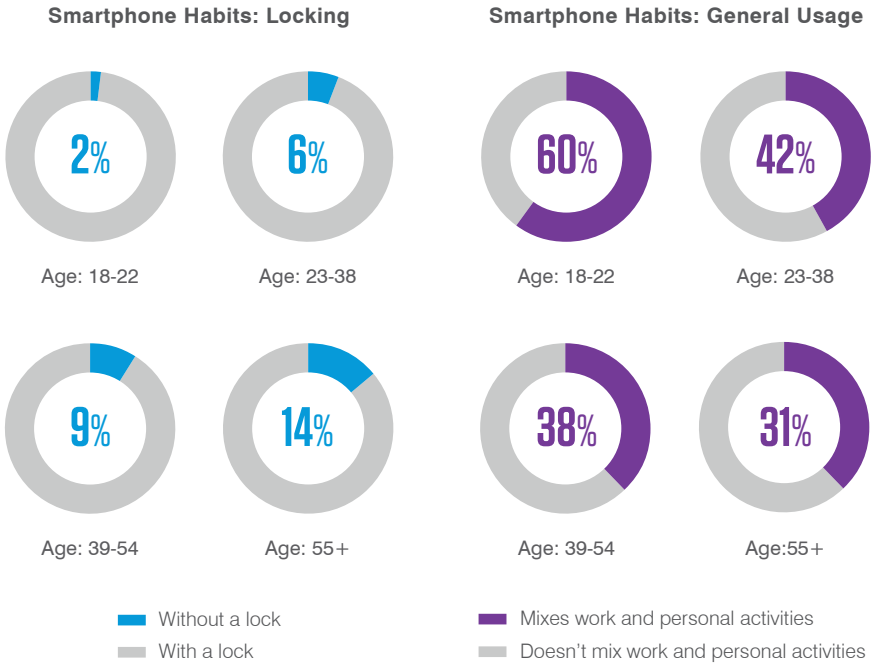
Baby boomers outperformed everyone in their recognition of phishing and ransomware terminology. Millennials had the best recognition of only one term: *smishing*.





KEY FINDING

All respondents in the 18-22 age bracket said they use a smartphone—and most of these respondents blur the lines between home life and work life on their devices. As these individuals take a more prominent role in the global workforce, mobile security practices will become more important than ever.



Key takeaway: put assumptions aside

Surveys of this nature can show results that fluctuate from year to year. The reason is simple: you're surveying a different set of respondents each year, leading to different outcomes.

The same thing happens in the workplace.

Most organisations deal with at least some employee turnover from year to year. That means they'll always have a mix of cyber-savvy and not-so-savvy employees. We can see from our survey results that younger workers don't always come armed with the cyber skills that are most important to your organisation's mission and security posture. But at the same time, you shouldn't assume *anyone* is well informed if you haven't taken the time to assess their skill sets and close any knowledge gaps.

That's why you should incorporate security awareness training into your employee onboarding sessions. This move sets the tone that cybersecurity is important at all levels of the organisation. You should also commit to ongoing cybersecurity education rather than letting employees' skills stagnate for months (or even worse, a year or more). If you de-prioritise best practices and cyber initiatives, so will your employees.

SECTION 2

Asking Around: What Infosec Pros Are Experiencing

You cannot fully understand the threat landscape without also understanding infosec professionals' phishing pain points. Actionable threat intelligence is amazing, but it doesn't exist in a vacuum. It's important to gather "people intelligence" too—and not just about end-user behaviours.

That means understanding what the people on the front lines of cybersecurity are seeing within their organisations, how they are responding to attacks, and the steps they're taking to improve security postures.

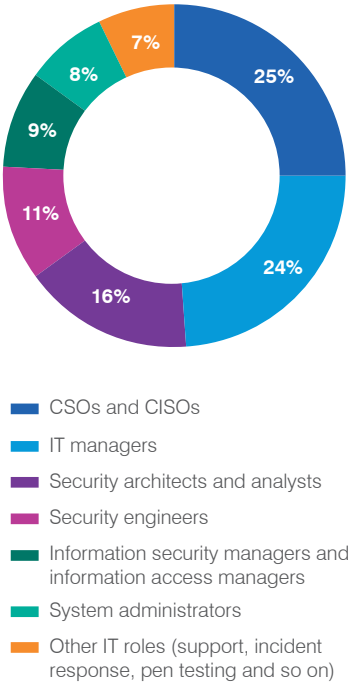
This year, we surveyed more than 600 IT security professionals across seven countries: the United States, Australia, France, Germany, Japan, Spain and the United Kingdom. We got a representative mix of infosec roles from more than 20 industries.

These different perspectives are important. Responsibilities for cybersecurity education can rest with multiple people within an organisation and span a variety of security roles. We asked all survey participants about the following phishing and social engineering issues:

- The rates of successful phishing attacks and the impacts experienced as a result
- The volume of spear phishing (attacks aimed at specific targets) and business email compromise (BEC) attacks they saw in 2019
- Whether ransomware infections happened in 2019 and if so, how they handled ransom demands
- The volume of "alternative" social engineering attempts—smishing, vishing, USB drops and social media attacks—experienced in 2019
- How they measure the cost of phishing
- Security awareness training practices
- The use of consequence models with end users who repeatedly fall for phishing attacks

As in the previous section, this one presents global averages and regional points of interest. Country-by-country breakdowns for all questions are available in the Appendix.

Survey Participants



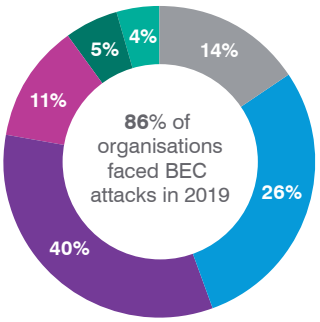
Incidents and impacts: what phishing looked like in 2019

More than half (about 60%) of global respondents said their organisation faced fewer or about the same number of phishing attacks in 2019 compared to 2018. This aligns with an attack trend we (and others) have been seeing for a while: a focus on quality over quantity.

Cyber criminals increasingly opt for more targeted, personalised attacks over bulk campaigns. This is reflected in the numbers of focused attacks respondents said their organisations faced in 2019:

Volume of Spear Phishing Attacks

Volume of BEC Attacks

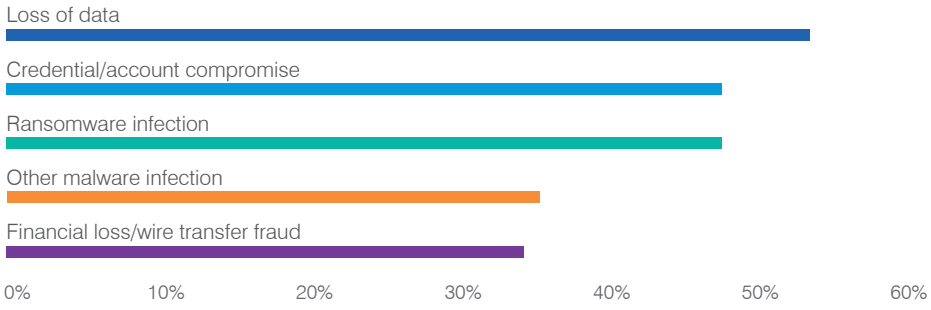


But attempts are one thing and successful attacks are another. More than half (55%) of respondents said their organisation fell victim to at least one successful phishing attack in 2019.

How organisations were affected by phishing

Phishing attacks have intent: cyber criminals want something from the organisations they target. Respondents said they experienced the following because of successful phishing attacks in 2019. (Multiple responses were allowed.)

Impacts of Successful Phishing Attacks



INTERNATIONAL

65%

of US organisations experienced a successful phishing attack last year, well above the 55% global average.

42%

of Japanese organisations experienced a successful phishing attack in 2019, the lowest incident rate across all regions surveyed.

60%

of US organisations experienced successful credential phishing attacks, higher than the 47% global average.

KEY FINDING

Japanese organisations were most likely to suffer data loss and financial loss after a successful phishing attack. This is consistent with our threat intelligence, which shows that attackers disproportionately target Japanese organisations with banking trojans that can lead to data exfiltration.

59% of Japanese organisations suffered data loss following a phishing attack.

45% suffered financial loss.

INTERNATIONAL

54%

of Australian organisations dealt with phishing-triggered ransomware infections, the highest of all regions surveyed.

55%

of Spanish organisations dealt with malware infections due to phishing attacks, well above the 35% global average.

Ransomware: grabbing headlines (and cash) in 2019

Though email-based ransomware attacks have dwindled in recent years, it's not surprising that infosec professionals reported a jump in phishing-driven infections in 2019.

GandCrab, a ransomware-as-a-service offering, plagued many organisations last year. It reportedly generated $2 billion in ransom payments before going off the market in June, when its creators claimed they were "retiring."[2]

Outside of GandCrab, many recent high-profile ransomware attacks appear to be secondary infections in organisations already compromised with other malware. So even though email-driven ransomware infections may have dropped off, the problem remains top-of-mind for many infosec professionals.

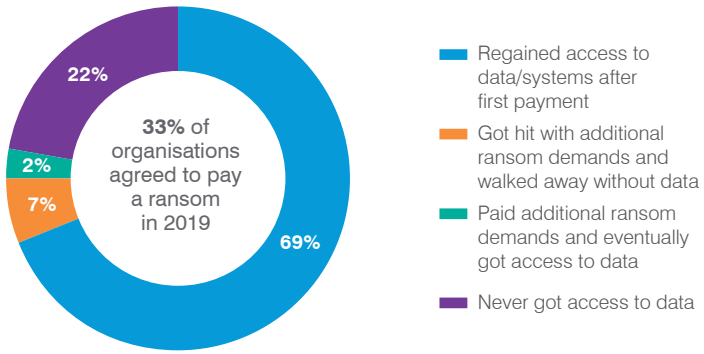
The advantage of a successful ransomware infection—from the viewpoint of the attacker—is the sense of urgency it creates. Healthcare organisations and state and local government entities were hit particularly hard in 2019. Ransomware has the power to immobilise critical infrastructure and disrupt necessary (and even life-saving) services. An organisation in this situation may conclude that paying the ransom is the most expedient—and cheapest—way to get up and running again.

We asked our survey participants about their experiences with ransomware in general in 2019. Here's what we found:

- 33% of organisations were infected with ransomware and opted to pay the ransom
- 32% were infected but did not pay the ransom

Of those who paid the ransom, many soon learned an old lesson: there is no honour among thieves.

Outcomes Following Ransom Payments



[2] Catalin Cimpanu (*ZDNet*). "GandCrab ransomware operation says it's shutting down." June 2019.

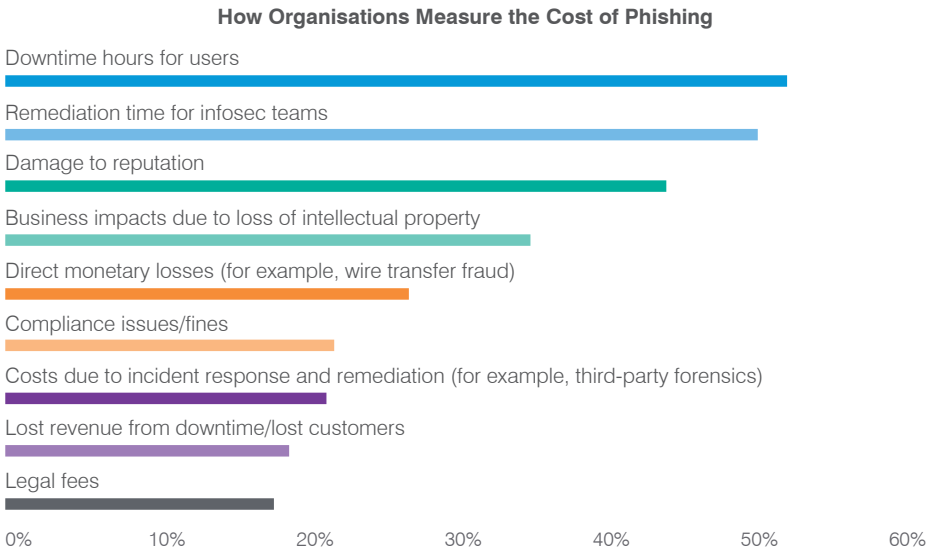
Privacy regulations may limit what organisations can measure at an individual level. But global organisations can still weigh the monetary impacts of phishing—and the value of security awareness training initiatives.

Successful phishing attacks: the cost

Along with all their immediate impacts, successful phishing attacks ultimately hit the bottom line. The vast majority (93%) of survey respondents said their organisation tracks these costs in some capacity. As you'll note in the chart, monetary damages can be tied to a number of issues, from lost productivity to unexpected (and unintended) cash outlay. (Multiple responses were allowed.)

93%

of organisations measure the cost of phishing



Social engineering beyond the inbox

Email remains the top social engineering attack vector for cyber criminals. But attackers apply similar techniques in other approaches to fool users. Many organisations saw a high volume of various social engineering attacks in 2019.

INTERNATIONAL

Spanish organisations were by far the most likely to face these "alternative" social engineering attacks in 2019:

100%
faced social and smishing attacks

99%
faced vishing attacks

98%
dealt with weaponised USB drives

VS

Australian organisations

66%
faced social attacks

62%
faced smishing attacks

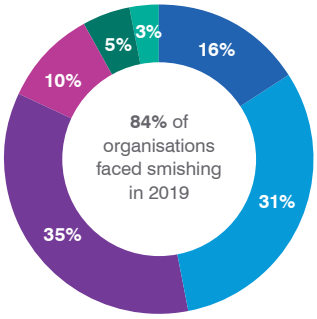
57%
faced vishing attacks

UK organisations

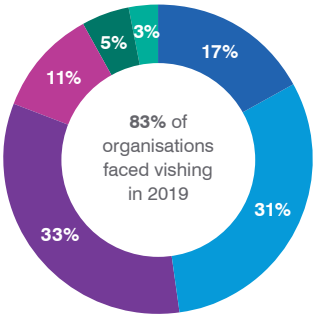
52%
dealt with weaponised USB drives

Volume of Social Media Attacks

Volume of Smishing Attacks



Volume of Vishing Attacks



Volume of Malicious USB Drops

Security awareness training: teaching users not to fall for phishing

95%
of organisations train employees to spot and avoid phishing attacks

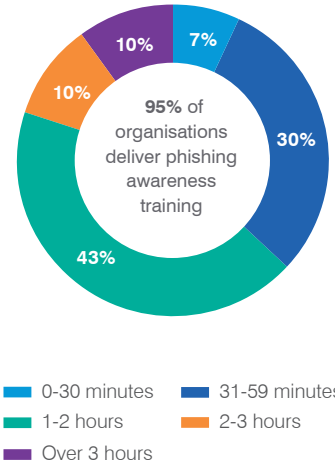
Technical tools, while a necessary part of any cyber defence, don't address the role people play. Cyber criminals seek every opportunity to infiltrate at the user level. To realise the benefits of a people-centric approach to cybersecurity, you must improve user awareness and behaviours.

The good news: 95% of survey respondents said their organisation delivers phishing awareness training. But when we dig a little deeper into the methods they're using, things get murkier.

For example, nearly 30% of organisations train just a portion of their user base. This approach puts cybersecurity on the back burner for those who aren't trained. (Targeted training is a critical part of cybersecurity education. But it works best when combined with a programme that promotes organisation-wide attention to best practices.)

Here's how organisations are deploying security awareness training programmes.

Time Allocated to Security Awareness Training Each Year



Frequency of Security Awareness Training

INTERNATIONAL

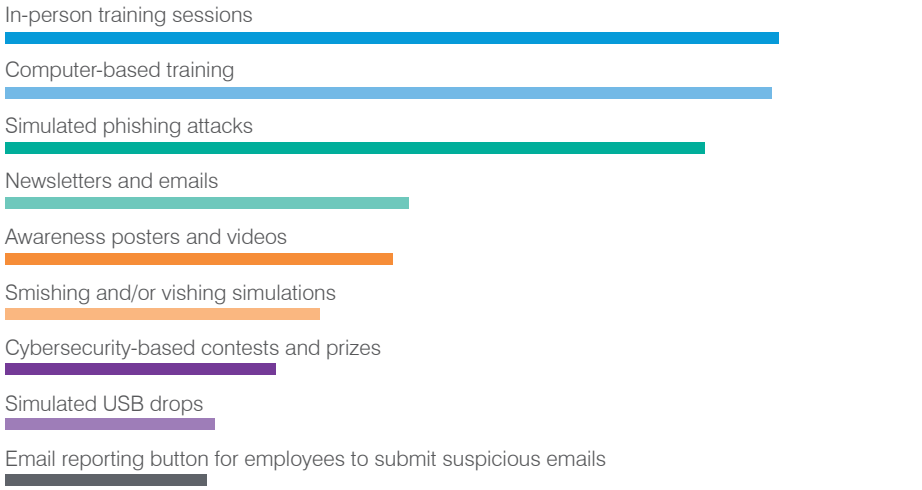
UK organisations are most likely to invest time in end-user education:

98%
allocate more than 30 minutes to training each year.

15%
dedicate 3 or more hours per year to their programmes.

11%
of Australian organisations rely on once-a-year training to improve end-user behaviours.

Tools Organisations Use in Their Programmes*



* Multiple responses were allowed.

Raising awareness and instilling good security practices are different things. "Passive" tools—such as newsletters, emails notifications and posters—can boost awareness. But they don't give employees a chance to practice cybersecurity decision-making skills.

As illustrated in the chart above, just 60% of organisations provide formal cybersecurity education to their users. That's alarmingly low. The lack of formal training, and an apparent lack of focus on end-user email reporting, undermines organisations' security postures.

Consequence models: are punishments appropriate?

KEY FINDING

63%

of organisations punish users who regularly fall for phishing attacks.

The question of "carrot vs stick" approaches to users' security mistakes elicits vehement responses from advocates on both sides—each with credible arguments. No matter where you stand, you should be informed and thoughtful about consequence models.

Our survey showed that 63% of organisations punish users who repeatedly make mistakes. We used the word "punish" intentionally in our question. Why? Because perceptions matter. We would never argue against talking to or delivering follow-up training to end users who struggle to avoid phishing attacks. But labelling these additional learning opportunities as punishments—let alone imposing harsher penalties—could lead users to equate security awareness training initiatives with distrust, fear or even anger.

Here are the punishments "repeat offenders" face within organisations that use a consequence model. (Multiple responses were allowed.)

DO PUNISHMENTS WORK?

The vast majority (84%) of organisations using them said employee awareness improved following the implementation of a consequence model.

78%

of organisations say security awareness training reduces phishing susceptibility

Key takeaway: time and effort matter

Phishing is a many-headed beast. The impacts and costs associated with successful attacks are significant and damaging. Cyber criminals are working overtime to perfect their techniques and get to your people. Are you preparing your users to defend themselves?

It's heartening to see that 78% of organisations say their security awareness training activities resulted in measurably lower phishing susceptibility. Your organisation's success depends on the time and effort you put into improving end-user knowledge.

SECTION 3

Phishing Failure Rates: A Fresh Look at Fresh Data

When we first started analysing and reporting on our customers' phishing tests, our data set was based on just over 4.5 million simulated phishing attacks.[3] At nearly 50 million phishing tests, this year's data set is an order of magnitude larger. It's an indication of just how much has changed on the phishing awareness training front during the past few years. The increase reflects both a larger customer base and more robust training by organisations.

These shifts call for a fresh look at the data we report and how we report it.

9%

average failure rate of aggregated users across all tests sent

VS

12%

average failure rate of organisations across all tests sent

Calculating failure rates: user view vs organisation view

In earlier editions of *State of the Phish*, we calculated average failure rate at the user level. That means we looked at the total number of failures compared to the total number of simulated attacks sent. And when we performed those calculations with this year's data, we found a user failure rate of 9%—the same as our two prior reports.

But there are different ways to calculate failure rates. (This is something you may have gleaned by looking at other industry studies.) When we took a different look at this year's data set, we found that user-level failure rates can be influenced, sometimes significantly, by "frequent fliers." Users who are tested more often tend to have lower failure rates. That's good news for organisations that consistently run tests. But it's not necessarily a "fair" view of how the average organisation is performing in general.

For a more balanced picture, this year's report presents user-level failure rates and organisation-level failure rates (where applicable). The latter applies equal weight to each organisation, eliminating the sway of large companies and high-volume programmes. Using this approach, we saw a 12% average failure rate among the organisations that use our phishing simulations.

You might be inclined to shrug off the 3% gap between these numbers. You shouldn't. Exploring both data sets can reveal important information about vulnerabilities at an organisational level—a message that echoes throughout this report.

[3] Wombat Security Technologies (now Proofpoint). "2016 State of the Phish." January 2016.

KEY FINDING

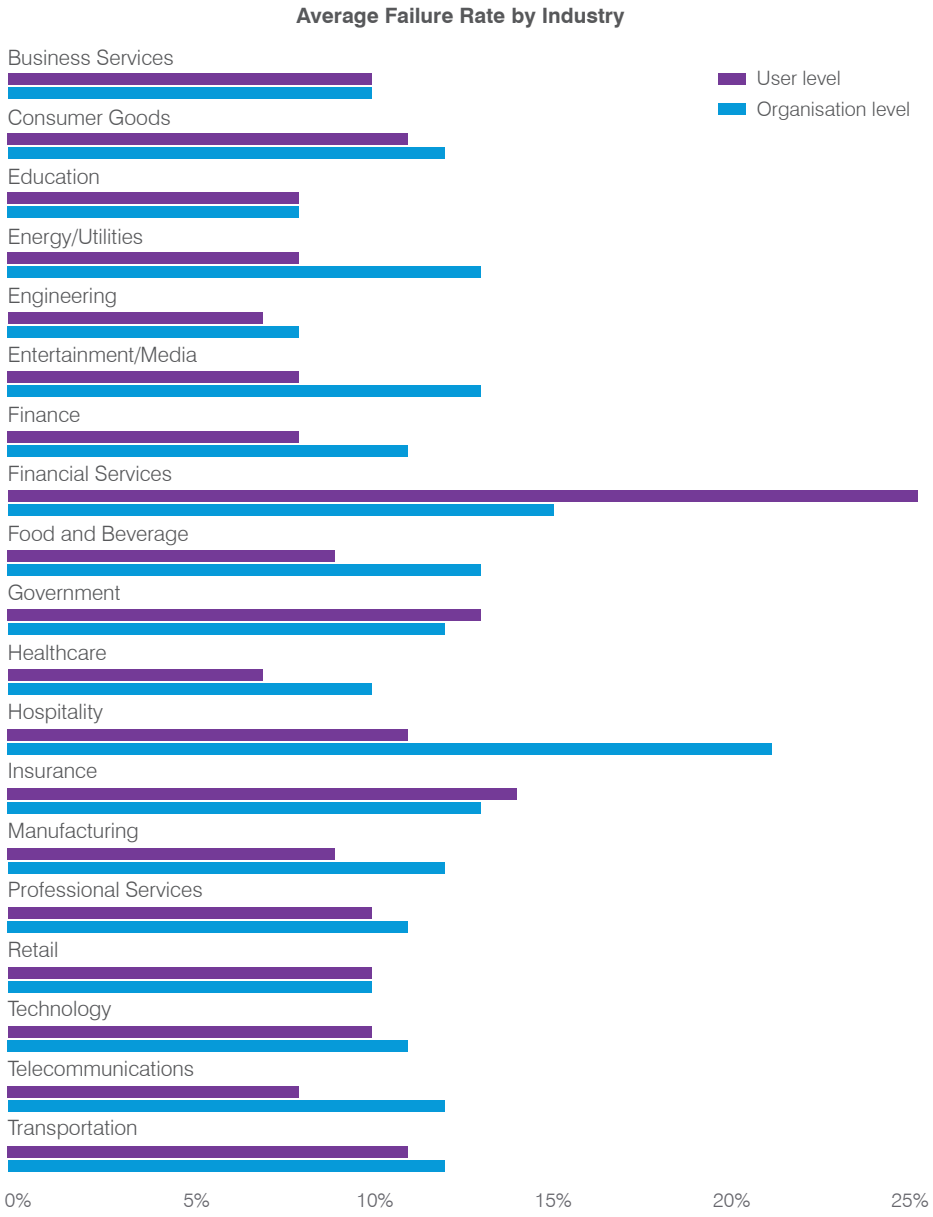
The industries that ran the most phishing tests in 2019 were healthcare, manufacturing, technology, finance and energy/utilities.

Comparing views of industry failure rates

Comparing organisation and user-level failure rates by industry reveals the influence high-volume campaigns can have on average failure rates at the user level. The user-level failure rate across all tests sent in financial services, for instance, is far higher than the organisation-level failure rate. Two advanced, high-volume simulated phishing campaigns run by one organisation caused the user failure rate for this industry to skyrocket.

But user failure rates are most often lower than organisation failure rates—in some cases markedly, as with the hospitality industry. This is because users within active organisations tend to perform better than their counterparts in organisations that send fewer phishing tests. Larger volumes of better-trained users can influence the user-level average failure rate. Equally weighting each organisation and averaging their results gives a more representative view of failure rates within each industry.

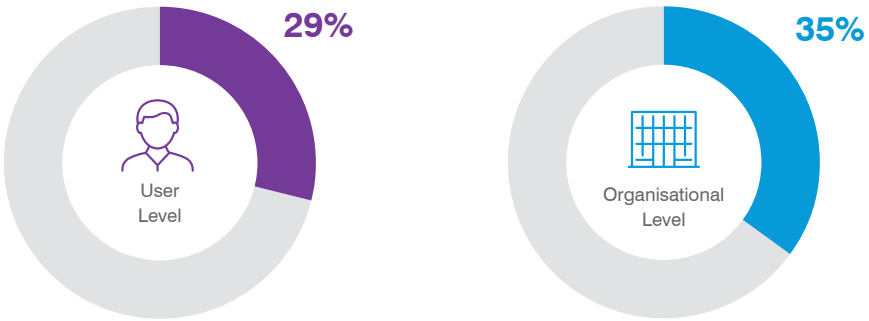
Each industry represented in our failure rate comparison includes data from at least five organisations and at least 100,000 simulated phishing attacks.



Are failure rates actually 30%?

Exploring the failure rates among the subset of phishing emails that users actually open provided additional insight. It's an interesting metric because only opened phishing emails have a chance of succeeding—the user may or may not engage.

Not every simulated phishing attack was viewed by every end user. But among messages that were opened, we found the following failure rates:



In other words, about a third of users who opened a simulated phishing email were apt to engage with it. If we think about what that could mean in the case of real-world attacks, it's a pretty sobering thought.

Arguably, calculating failure rates in this way doesn't account for people who *intentionally* didn't open emails because they knew they were dangerous. But inferring intentional actions from unintentional ones is difficult. (Unless the user reports the email—but more on that later.)

Some users might ignore emails because they think they could be dangerous. But emails are left unopened for a host of other reasons, too—reasons that have nothing to do with cybersecurity. Users might be out of the office and dismiss messages as their inbox piles up. They might be occupied with other tasks. Messages might get filed away into a subfolder and never even seen. Or perhaps an email is ignored because the subject or content just don't interest or apply to the user.

Users achieving "inbox zero" status on a daily (or even monthly) basis should be heartily (and enviously) applauded. But most people have many, many unread messages in their accounts. Unopened phishing messages aren't always a sign of user diligence.

Putting failure rates in perspective

Failure rates are interesting and provide good reference points. But they are not the ultimate gauge of a successful programme.

Avoid relying too heavily on failure rates to measure the success of your phishing awareness programme. Failure rates can—and should—fluctuate. While users should get better at identifying phishing lures over time, they should also be challenged with different, difficult-to-spot tests and lures. And that might mean spikes in failure rates from time to time—which are not a sign your users are hopeless.

Track failure rates, but keep them in perspective. Also look at open rates and compare them with failure rates. For example, if you have a low failure rate on a campaign that few users actually opened, that low rate might be an exception rather than the norm.

The best way to measure success is to take a well-rounded look at behaviour metrics. In addition to failure rates, we suggest tracking changes in the following:

- Number of successful real-world phishing attacks
- Rate of malware infections
- Quantity and quality of IT helpdesk calls
- Downtime hours for end users who fall for phishing attacks
- Remediation hours for IT staff dealing with phishing attacks
- Number of machines reimaged following attacks
- Quantity and quality of user-reported emails (more on this in Section 5)

Ultimately, your goal should not be to encourage users to blindly report or ignore emails they receive. Both practices disrupt the flow of business. Instead, aim for thoughtful treatment of incoming emails. Actionable training can empower users to be a stronger last line of defence.

Last year, we encouraged *State of the Phish* readers to use more data-entry campaigns to help counteract the growing trend of credential compromise attacks. They listened. The use of data-entry templates jumped nearly 30% year over year.

SECTION 4

Breaking It Down: Phishing Awareness Training in Practice

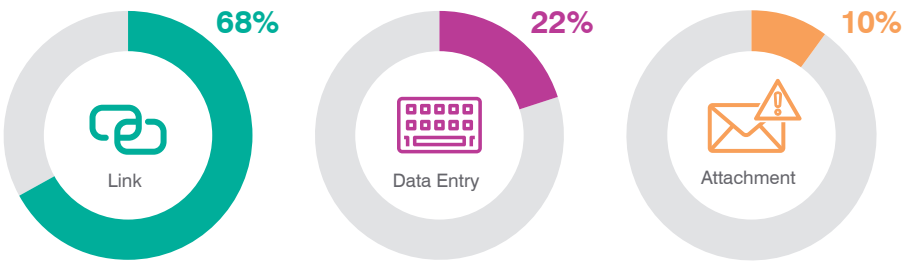
We looked at the ways our customers are using our simulated attack tools to raise phishing awareness and teach end users about best practices related to identification and avoidance. This section covers key insights and advice.

Link-based tests favoured by a large margin

Our customers can test and measure users' vulnerability to three types of phishing lures: links, attachments and data-entry requests (meaning, lures that ask for confidential data such as login credentials).

Organisations preferred link-based tests by a wide margin in 2019, just as they did in 2018.

Phishing Template Styles: Frequency of Use

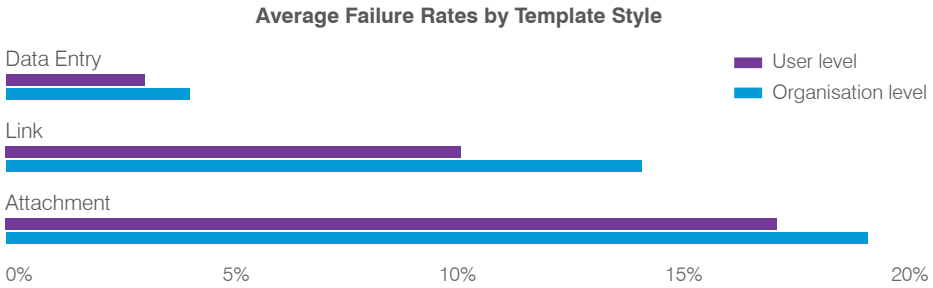


The emphasis on link-based tests is not misplaced. Our researchers found that the vast majority of payloads were delivered via URLs in 2019.

Still, it's important to consider not just frequency of attack methods, but users' vulnerability to certain lures. Email links often lead to critical secondary decision points—such as a web page that asks for users' credentials or urges them to download a file. Testing users' responses to these types of requests is critical, especially if your organisation is facing real-world attacks that leverage these techniques.

We calculated failure rates for each template style. Though attachment tests were low on organisations' priority lists during 2019, they proved the most effective in fooling users.

Users who "failed" data-entry tests submitted data after clicking a link in the simulated attack.



See the Appendix for the industry failure rates for link, data entry and attachment templates.

Personalisation: room for improvement

Cyber criminals are taking a more sophisticated, people-centric approach to attacks. That means phishing emails have become more difficult to distinguish from legitimate messages. Personalisation plays a role in this shift. Attackers do their homework, and their emails often seem personally relevant to recipients.

Unfortunately, fewer than half of our customers' 2019 simulated phishing campaigns included custom fields such as first and last names and email addresses. (It's worth noting that including the name of the recipient's organisation within a phishing test was most likely to increase failure rates.)

We recommend organisations more regularly use personalisation techniques within their tests. This step can better prepare users for targeted attacks and help them realise how sophisticated attacks can be. This understanding is especially critical in newer phishing awareness programmes. Users are less often fooled by custom fields in programmes that have been active for a year or more.

Common threads among the trickiest templates

State of the Phish readers are often curious about one topic in particular: the simulated phishing templates users struggle with the most.

This year, we looked at the phishing tests with the highest failure rates—near 100%—that included a minimum of 1,500 individual emails sent. We found some interesting common threads among these templates:

- 65% were attachment-based tests, and 35% were link-based. None were data-entry templates.
- 65% were templates based on real-world attacks identified by our threat intelligence researchers.
- Nearly 90% of tests were designed to look like they originated from a recognisable internal account or alias (such as an HR department).

Some of the more interesting subject lines in these "most successful" campaigns included the following:

- Lost Watch
- Lost Ring
- SharePoint Document
- Scanned from a Xerox Multifunction Printer
- Dealer Proposal
- Updated Building Evacuation Plan (a top failure rate for three years running)
- Confidential Document
- <First Name>, please add me to you LinkedIn network

The first two on the list are noteworthy for their simplicity—and how well they tap into curiosity and a desire to help. The last item on the list is also interesting. This invitation appeared to come from the organisation's CIO. Who turns down a connection request from a VIP? (Hardly anyone, apparently.)

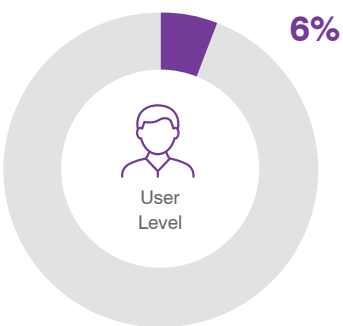
The common bonds and the subject lines in these lists all reinforce our advice to test attachment vulnerabilities more frequently and to add more personalisation to simulated phishing campaigns. Even if you see attachment-based attacks less frequently, they are going to be a problem for your organisation if almost all users fall for them.

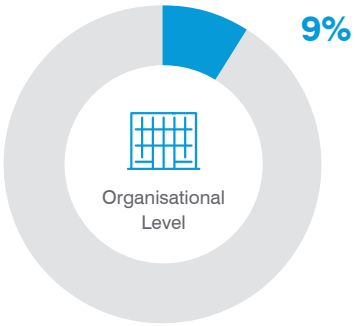
A note about smishing

Some of our customers test their users' vulnerability to smishing—SMS/text phishing—in addition to email-based phishing. The frequency of use isn't particularly high, though. Part of this is due to the rise in bring-your-own-device (BYOD) corporate cultures. Many users' only mobile devices are ones they own personally. From a legal perspective, it can be tricky to get the approvals needed to test users on their own smartphones.

That said, smishing is a global concern. As noted earlier, most organisations experienced these types of attacks in 2019. And because text messages can feel more personal than emails, users can be more vulnerable to smishing if they are not made aware of the dangers.

Here are the average failure rates we found for smishing simulations run by our customers in 2019:





KEY FINDINGS

Users reported nearly **9.2M** suspicious emails in 2019, a 67% year-over-year increase.

The median time between email receipt and reporting is **1 hour**.

On average, each PhishAlarm user reported **five emails** in 2019.

SECTION 5

End-User Reporting: Finding Nirvana

We've long advised customers to give users an easy way to report suspicious email messages and track those reports. This metric is a great way to gauge the effectiveness of phishing awareness training initiatives. Here's why:

- It extends the value of your programme by giving users a chance put their knowledge to work.
- Reported emails indicate thought and intent—signs that users are being more careful about the messages they receive. This is a more reliable reflection of awareness and understanding than "non-fails" on simulated phishing attacks, especially with messages that are left unopened.
- High-quality reports can identify active attacks that slipped past your organisation's defences.

A bird's-eye view of reporting data

We saw a continued rise in the use of our PhishAlarm® email reporting tool, an in-client button that forwards messages to designated inboxes with headers intact. In 2019, end users submitted nearly 9.2 million suspicious emails, a 67% jump over 2018.

More than half of those reported messages were flagged as potential phish and evaluated by PhishAlarm Analyzer, our real-time threat prioritisation tool. This automated analysis identified messages that were most likely to be phishing attempts so they could be quickly addressed by infosec teams.

In evaluating data about reported simulated attacks, we saw some trends. In general, users were better at reporting phishing tests with government and technical themes. They were least likely to report simulated attacks that invoked social media messages and imagery.

Reporting rates should rise over time within individual organisations as users become more confident in their ability to identify the hallmarks of suspicious messages. But organisations should keep in mind that the act of reporting, in itself, needs to be learned by users. Don't think that installing a button is enough. You also need to teach employees how (and when) to use it.

The search for nirvana

Over the past few years, several organisations have approached us with this question: what is the ideal number of emails for end users to report?

This is a tricky question, primarily because conditions fluctuate. The number of emails that "should" be reported depends first on the quantity of simulated phishing tests an organisation is sending. But it also depends on the number of phishing attacks that are getting through technical defences. Though you can easily identify the first number, the second is difficult (if not impossible) to quantify with certainty.

Each PhishAlarm user reported, on average, five emails in 2019. But we caution against targeting a specific number of reports for end users to achieve. If you tell employees they should be reporting X number of emails, they will tend to focus on quantity rather than quality. And quality of reporting is the more important metric. (See the case study at the end of this section for our analysis of all emails reported in Q3 2019.)

Clearly, the ideal would be for users to report all simulated phishing tests. But chasing a 100% reporting rate is as fruitless as chasing a 0% failure rate—it's the stuff of unicorns and pots of gold at the end of the rainbow.

Instead of chasing the unattainable, we suggest you consider this equation:

High reporting rate + low failure rate = nirvana

The 70/5 rule: your path to nirvana

You may have heard of the 80/20 rule (also known as the Pareto Principle) for business, sales and time management. We'd like to introduce the 70/5 rule for simulated phishing attacks: a greater than 70% reporting rate and a less than 5% failure rate.

Table 1 shows the top five customer campaigns that met the 70/5 rule in 2019 with 350 or more tests sent.

High Reporting Rates, Low Failure Rates

Subject Line	Template Style	Number of Messages Sent	Failure Rate	Reporting Rate
Someone has your password	Data entry	798	<1%	86%
Please DocSign this document: Contract_Change	Attachment	441	2%	85%
COMPANY CONFIDENTIAL: Upcoming public announcement	Link	442	2%	83%
Toll Violation Notice[4]	Link	676	4%	81%
Network Access Attempt	Data entry	360	1%	80%

Table 1

[4] This template had one of the highest average failure rates in 2018. Nice to see it move from that list to this list.

One smaller simulated phishing campaign (less than 100 messages) had interesting statistics: a 7% failure rate with a 100% reporting rate. Though it doesn't quite meet the 70/5 rule, it does illustrate an important point: the willingness of this organisation's users to report a message after they've made a mistake.

This is a piece of nirvana in itself. You want users to feel comfortable reporting even if—and perhaps *especially* if—they're afraid they've interacted with a malicious message. An end user's honesty could be your quickest path to remediating a successful phishing attack.

If you're in a larger organisation, you may be thinking, "That's great. But what about higher-volume campaigns?" We feel the 70/5 rule is still something to strive for. It's a stretch goal, particularly for larger organisations—but as Table 2 shows, it's within reach.

We realise that the outlier in this table, New Invoice Payments, might seem discouraging. You could be thinking that, in the case of a real-world attack, a 13% failure rate would be too high.

We would counter with this: If more than 60% of recipients reported an active attack, you'd be in a good position to get ahead of the 13% who stood to fall for the phish. This is particularly true if you automate your remediation efforts. (See the "Don't Let Reported Emails Drain You" sidebar for more advice about this.)

Top Reporting Rates of Higher-Volume Campaigns

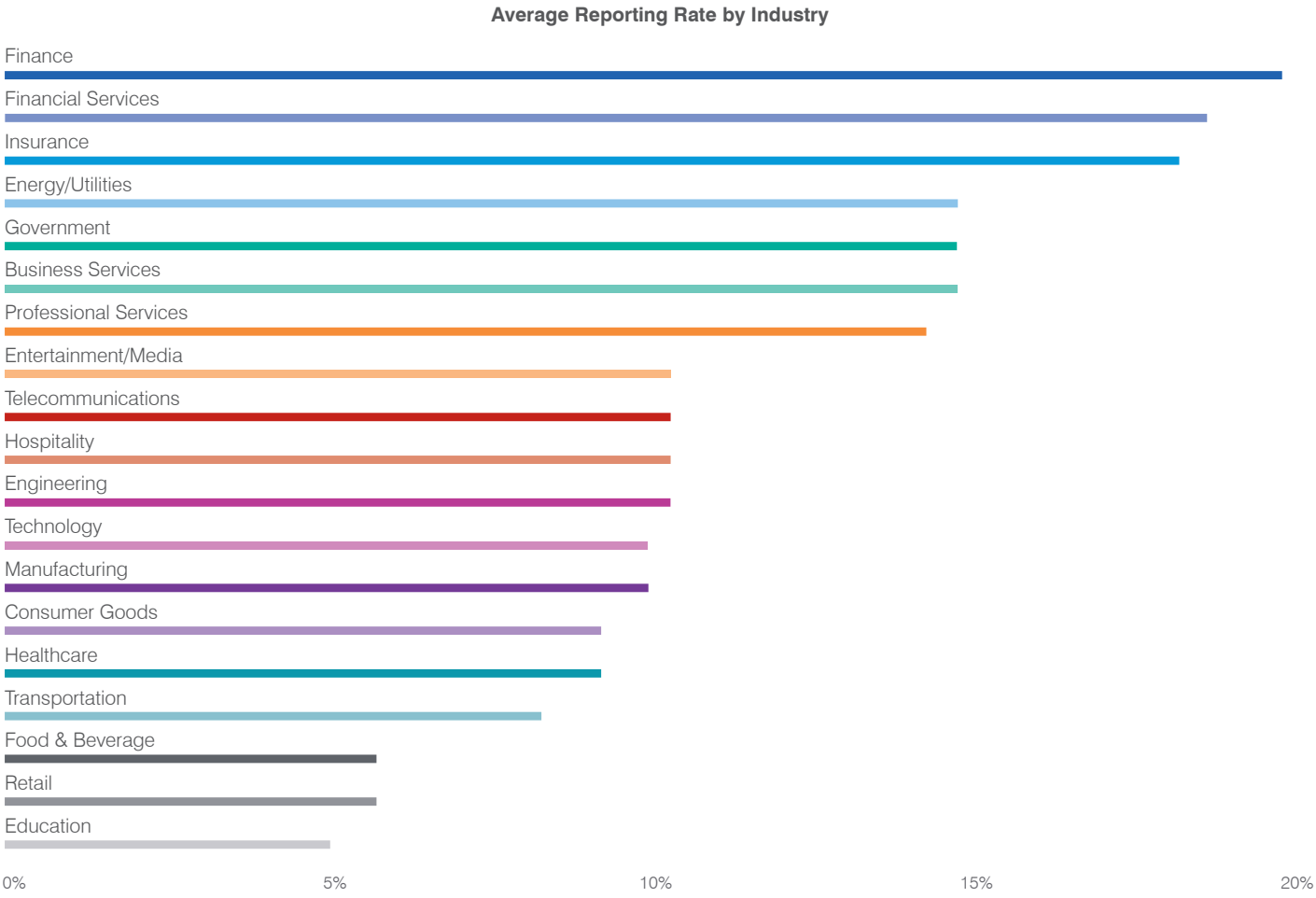
Subject Line	Template Style	Number of Messages Sent	Failure Rate	Reporting Rate
Inquiry <Company Name>	Attachment	5,689	6%	65%
New Invoice Payment	Attachment	5,704	13%	65%
Urgent Attention	Link	6,230	5%	61%
Compromised Password	Data entry	5,444	<1%	53%

Table 2

Industry reporting rates

Our analysis of industry reporting rates reveals the importance of reporting as a metric for a programme's overall success.

The finance and education sectors each had an 8% user-level failure rate in 2019—but they sit at the opposite ends of the reporting spectrum. Users in the finance industry report phishing emails at a far higher rate than those in the education sector. In real-world attacks, finance infosec teams would have a much better chance of catching attacks that slip past perimeter defences.



Don't Let Reported Emails Drain You

Engaging users and advising them to report suspicious emails is a must-do within your organisation. So is establishing a quick, simple way for users to get these messages to the right people. (We strongly encourage use of an in-client reporting button like PhishAlarm.)

But what happens once those reported emails hit your infosec team? Do you stand to become a victim of your own success? If you don't have the bandwidth to take on additional analysis and remediation, it's time to automate.

The way to do that is CLEAR—Closed-Loop Email Analysis and Response. This Proofpoint solution integrates email reporting and remediation, reducing the time it takes to neutralise an active threat from days to minutes. With CLEAR, reported emails are automatically analysed against multiple intelligence and reputation systems, and all links and attachments are sandboxed. Messages that are identified as malicious can be deleted or quarantined with a single click. In addition, the user who reported the message can be automatically notified (and thanked) for their vigilance.

CASE STUDY

Credential Phish Were Most Reported in Q3 2019

We analysed more than 600,000 reported emails during the third quarter of 2019—about 8,500 messages per business day. (User reporting drops off dramatically on weekends and holidays.) The data shows the importance of taking a people-centric approach to cybersecurity and empowering users to participate in phishing defences.

Users help catch severe security threats

With the rise in credential phishing attacks, these types of malicious emails are most frequently reported by users. However, users also identify and report malware-based attacks—some of which include extremely dangerous payloads.

In Q3 2019, nearly 20,000 end-user reported emails contained credential phishing lures. More than 4,000 reported messages had malware payloads, including keyloggers and advanced persistent threat (APT) malware.

But it's not just about quantity—quality is critical. Our systems classify threats not only by category but also by severity. End users' attentiveness helped infosec teams identify some high-severity threats, including phishing attempts with the following malware payloads:

BACKDOORS	DOWNLOADERS
STEALERS	REMOTE ACCESS TROJANS (RATS)

Reporting for all

Workers at all levels can be targeted in attacks—so all users should have the ability to report suspicious emails.

Our customers' experiences bear this out. In one recent example, two regional CFOs at a Fortune 50 organisation spotted and reported multiple, high-severity credential phishing attempts.

But at a leading insurance agency, it was two claims adjusters and a field attorney who alerted their infosec team to dangerous credential-based attacks.

These examples show that high-level executives shouldn't be the only users with access to important security awareness training tools. Everyone should have a path to improving cybersecurity behaviours and applying newfound knowledge.

SECTION 6

Digging Down: What Granular Data Can Do for You

By this point, you may have recognised a theme within our report: the need for better visibility into your users' cybersecurity behaviours. Your data will help you identify pressing vulnerabilities within your organisation and better guide your phishing prevention efforts.

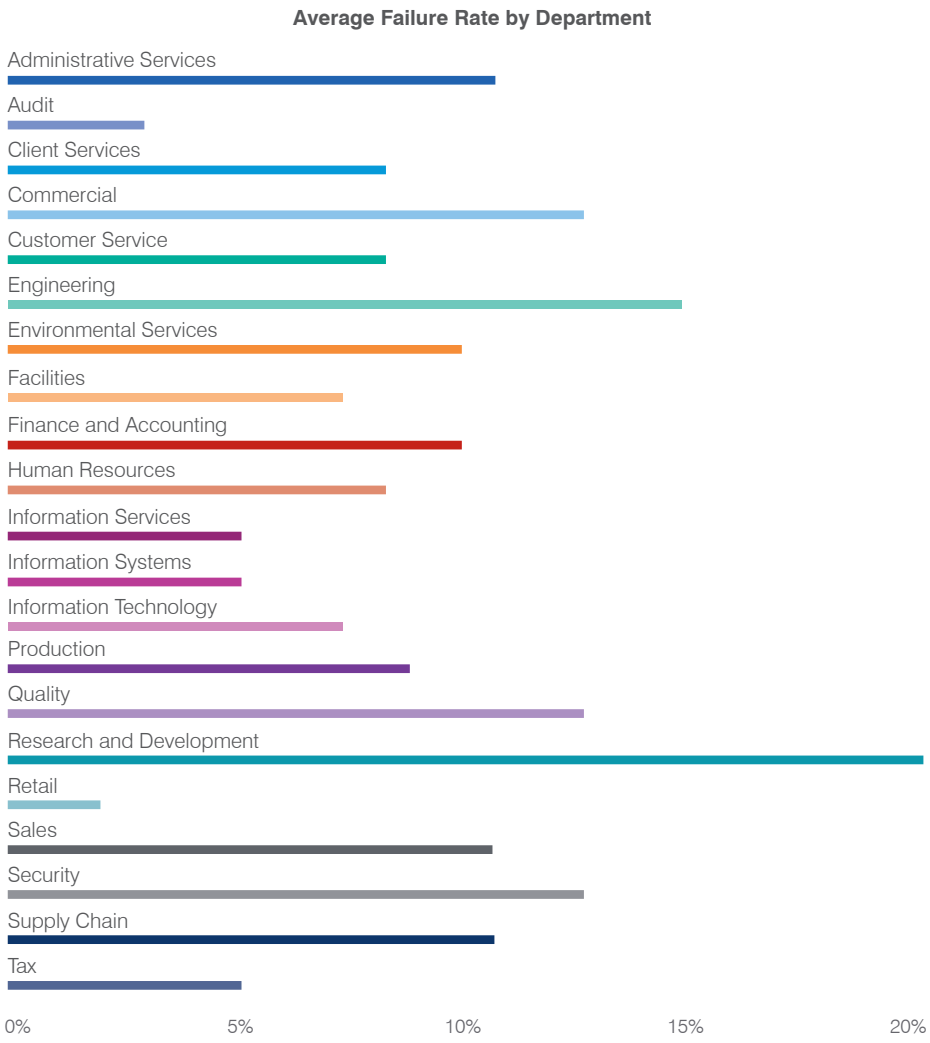
Failure rates at the department level

Many organisations are missing an important opportunity: the chance to view failure rates at a departmental level. Too few group their users by department for reporting purposes. This eliminates the ability to evaluate performance (and vulnerability) by job function.

It's an important piece of the puzzle. Attackers often target specific people—and email aliases—within organisations based on roles and responsibilities. (See the "Digging Deeper" section for more on this.)

The following chart shows the most commonly used department designations among customers using this level of data classification.[5] Departments highlighted were specified within at least 10 organisations and included at least 1,000 users.

[5] Department designations often mean different things to different organisations. They may share some terms, but the job functions they represent often vary. For example, "security" may equate to physical security within some organisations but information security in others.



Organisations that can't see this type of data are at a disadvantage. They may miss danger signs (and pleasant surprises). Take the averages from the chart, for example:

- High failure rates within R&D and engineering teams are concerning. These individuals are likely to have access to critical intellectual property and forward-looking technology.
- Low failure rates across information services, systems and technology is positive news. Because of their access, workers in these roles are likely to be targeted, so vigilance is critical (as we explain in the "Digging Down" section.)
- An 11% average failure rate for sales isn't alarmingly high—but workers in this role are likely to deal with a lot of email. Even a modestly high failure rate can be a problem for groups that receive a high volume of messages.
- Similarly, the 10% average failure rate for finance and accounting workers isn't far off the 9% average across all users. But workers in these roles can have direct access to bank accounts and key financial data. They should be among the most vigilant and prepared within your organisation (like those in audit and tax-related roles).

Digging deeper: getting to know your Very Attacked People

We use the term Very Attacked People™ (VAPs) to describe users (and email inboxes) most actively targeted by cyber attacks within an organisation. Our threat intelligence tools allow us to identify your VAPs and the ways attackers are attempting to compromise them. Time and time again, we have found that your VAPs aren't always your VIPs.

VAPs vary from industry to industry and organisation to organisation. They also vary over time. Organisations frequently experience turnover among their VAPs. The variety of roles targeted from month to month and year to year illustrates attackers' willingness to look up, down and across org charts to find inroads to data and systems they want to infiltrate.

It's important to get to know your organisation's VAPs. Here's why:

- You can quickly identify the people who are being targeted and the ways attackers are attempting to compromise them. This allows you to deliver the right training to the right people at the right time.
- You can address threats with greater certainty. You can put aside assumptions about high-value targets in favour of actionable data.
- You can identify potential attack trends. For example, commonality in attack methods and the types of roles being targeted could hint that attackers have a specific goal in mind. This type of visibility is invaluable.
- You can make more informed decisions about your training approach in general. Perhaps you struggle to get buy-in on a broad programme because decision-makers believe only a subset of employees should be trained. VAP reports can provide clarity and help you illustrate attackers' attention to a range of roles and job functions.

SECTION 7

Conclusion: Act on Your Data

The goal for your security awareness training programme should be to move the dial on behaviours that matter most to your organisation's mission. The best way to do that is to use a blend of broad and targeted education that empowers users by delivering actionable advice.

The data in this report bears that out. Attackers are focusing on people—*your* people. Ignoring that will be to your detriment. If you haven't been taking a people-centric approach to security awareness training, you should. Here are three ways to do that:

1. Commit to building a culture of security

There's a lot of shared experience across organisations and industries. Our missions, customers and data may be different, but we're facing the same battle at a fundamental level: the fight to be more secure. And if you want to truly make a change—meaning a mindset and behaviour shift that has a positive, day-to-day impact on your organisation—you must commit to bringing cybersecurity to the forefront. And that's true for everyone.

Here's why:

- Anyone in your organisation can be a target.
- At any moment, anyone in your organisation can help or hurt your security posture.

Building a security culture is critical. Everyone in your organisation should know how they can be more cyber-secure. A broad, organisation-wide security awareness training programme will help you do that.

2. Answer the three W's

Along with shared experience, we see many variations across industries, departments and user populations. Understanding what those differences mean for your organisation allows you to better combat the specific ways attackers are targeting your people.

You may be familiar with the "six W's" that guide journalists, researchers and investigators: who, what, where, when, why and how. These are all great questions to ask when trying to get to the root of an issue. At a minimum, we suggest you answer these three first:

- **Who in my organisation is being targeted by attackers?** The answer is not as simple as looking at the top tiers of your org chart.
- **What types of attacks are they facing?** Knowing the lures and traps attackers are using can help you better position your defences.
- **How can I minimise risk if these attacks get through?** The answer: use the information you've gathered to deliver the right training to the right people at the right time.

This exercise helps you defend against your most pressing and timely threats. Assessing vulnerabilities at a more granular level and matching that up against your threat intelligence allows you to pinpoint where perfect storms are brewing: the intersections of susceptibility and exposure.

3. Make time for agility

Time gets away from all of us. When we get busy, we may want to take a "set it and forget it" approach to cybersecurity. That's understandable. But it doesn't work in an era of constantly shifting attack techniques and evolving threats.

The first two actions we recommend aren't "one-and-done" activities.

Building a security culture takes ongoing effort and attention. Plan for regular training and reinforcement but be responsive to changes in the threat landscape (and your organisation).

Attackers' targets change over time. We recommend identifying your VAPs monthly, if not weekly. By pairing granular analysis with organisation-wide training, someone who becomes a VAP will have a cybersecurity foundation you can build on with additional, targeted training.

Understanding general phishing trends is important. Having benchmarks to measure your users against is valuable. But other organisations' data isn't as important as your organisation's data. You must understand your own threat climate in order to change things where you live.

APPENDIX

A. Working Adult Survey: Country-by-Country Breakdown

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
What is phishing?								
Correct answer	49%	61%	64%	66%	60%	65%	63%	61%
Incorrect answer	38%	19%	21%	15%	29%	26%	22%	24%
I don't know	13%	20%	15%	19%	11%	9%	15%	15%
What is ransomware?								
Correct answer	29%	42%	26%	23%	39%	22%	38%	31%
Incorrect answer	48%	26%	36%	22%	22%	32%	32%	31%
I don't know	23%	32%	38%	55%	39%	46%	30%	38%
What is malware?								
Correct answer	52%	70%	68%	65%	61%	79%	67%	66%
Incorrect answer	37%	12%	17%	13%	8%	11%	20%	17%
I don't know	11%	18%	15%	22%	31%	10%	13%	17%
What is smishing?								
Correct answer	36%	20%	54%	28%	17%	35%	22%	30%
Incorrect answer	26%	21%	19%	14%	24%	15%	24%	21%
I don't know	38%	59%	27%	58%	59%	50%	54%	49%
What is vishing?								
Correct answer	19%	22%	48%	17%	20%	25%	24%	25%
Incorrect answer	38%	17%	17%	26%	17%	20%	18%	22%
I don't know	43%	61%	35%	57%	63%	55%	58%	53%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
Do you use your smartphone for a mix of business and personal activities?								
Yes	46%	50%	37%	23%	43%	55%	31%	41%
No	54%	50%	63%	77%	57%	45%	69%	59%
What is the primary security lock on your smartphone?								
Biometric lock	49%	38%	34%	38%	52%	45%	40%	42%
Complex swipe pattern	11%	9%	13%	12%	9%	22%	8%	12%
Alphanumeric password	5%	6%	7%	6%	12%	7%	4%	7%
4-digit PIN	21%	26%	33%	31%	10%	19%	26%	24%
6-digit PIN	5%	9%	6%	5%	5%	2%	8%	5%
I do not use a security lock	9%	12%	7%	8%	12%	5%	14%	10%
If you are in a place you trust (for example, a local coffee shop), you can trust the location's public Wi-Fi network to keep your information secure.								
True	45%	26%	26%	20%	13%	28%	26%	26%
False	47%	59%	53%	60%	65%	60%	56%	57%
I don't know	8%	15%	21%	20%	22%	12%	18%	17%
Which of the following is true of your home Wi-Fi network? (Multiple answers allowed.)								
Network name personalised	71%	44%	40%	46%	41%	45%	31%	45%
Password required to connect	63%	61%	28%	54%	41%	34%	51%	49%
Default router password changed	40%	34%	22%	32%	29%	40%	23%	31%
Router firmware checked/updated	26%	19%	10%	17%	28%	18%	13%	19%
Some/all of these security actions not taken because they're too time-consuming and/or inconvenient	13%	8%	15%	7%	6%	15%	10%	11%
Some/all of these security actions not taken because of lack of understanding	9%	15%	18%	5%	17%	13%	21%	14%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
At home: If you use and keep anti-virus software up to date, it will prevent cyber criminals from accessing your devices.								
True	73%	69%	55%	70%	52%	76%	68%	66%
False	15%	17%	22%	15%	25%	11%	14%	17%
I don't know	12%	14%	23%	15%	23%	13%	18%	17%
At work: If you accidentally install a virus or malicious software, your IT team will be automatically notified by their monitoring tools so they can fix it.								
True	60%	54%	49%	49%	40%	63%	46%	51%
False	19%	19%	17%	19%	27%	12%	24%	20%
I don't know	21%	27%	34%	32%	33%	25%	30%	29%
How many different passwords do you use for your online accounts? (Choose the one that best applies.)								
I use a password manager for my accounts	44%	23%	15%	17%	22%	20%	22%	23%
I manually enter a different password for every account	24%	35%	34%	40%	28%	30%	35%	32%
I rotate use of about 5 to 10 passwords	20%	25%	32%	33%	29%	33%	28%	29%
I use the same 1 or 2 passwords for most/ all of my online accounts	12%	17%	19%	10%	21%	17%	15%	16%
Is a VPN installed on any of the computers or mobile devices you use?								
Yes	51%	36%	35%	37%	39%	38%	37%	39%
No, I don't feel the need to use one	25%	34%	32%	30%	24%	30%	30%	29%
No, I don't know what a VPN is	24%	30%	33%	33%	37%	32%	33%	32%
How often do you use your VPN?								
Every time security is a concern	63%	39%	50%	36%	45%	52%	44%	47%
Frequently at home or when traveling	25%	40%	31%	47%	26%	30%	35%	33%
Only when necessary (for example, to access protected corporate systems)	7%	13%	8%	6%	24%	13%	11%	12%
Rarely/never	5%	8%	11%	11%	5%	5%	10%	8%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
Which of these personal activities you do on your employer-issued laptop and/or smartphone? (Multiple answers allowed.)								
Check/respond to email	86%	78%	74%	72%	83%	83%	72%	79%
View/post to social media	44%	35%	34%	23%	38%	29%	37%	34%
Stream media (music, videos, etc.)	40%	26%	25%	18%	18%	21%	23%	25%
Shop online	41%	29%	27%	23%	15%	31%	25%	27%
Read news stories	40%	42%	41%	38%	50%	47%	29%	41%
Research (new products, travel, etc.)	38%	42%	37%	33%	39%	45%	23%	37%
Play games	20%	9%	10%	6%	6%	7%	9%	10%
None of these	5%	8%	10%	19%	7%	11%	9%	10%
Which of these activities do you allow friends/family to do on your employer-issued laptop and/or smartphone? (Multiple answers allowed.)								
Check/respond to email	59%	37%	31%	27%	28%	36%	40%	38%
View/post to social media	40%	23%	20%	16%	15%	20%	23%	23%
Stream media (music, videos, etc.)	34%	21%	14%	12%	7%	15%	20%	18%
Shop online	29%	18%	10%	12%	5%	14%	14%	15%
Read news stories	22%	15%	16%	11%	11%	18%	9%	15%
Research/complete homework	21%	11%	11%	8%	5%	15%	9%	12%
Play games	15%	10%	8%	3%	3%	7%	7%	8%
None of these	29%	49%	51%	64%	65%	54%	47%	51%

B. Infosec Survey: Country-by-Country Breakdown

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
Did your organisation experience a successful phishing attack in 2019?								
Yes	65%	54%	53%	46%	42%	56%	62%	55%
No	33%	46%	43%	49%	58%	39%	36%	42%
I don't know	2%	0%	4%	5%	0%	5%	2%	3%
Has the rate of phishing attacks on your organisation increased or decreased in 2019 compared to 2018?								
Increased	57%	43%	29%	39%	33%	33%	43%	40%
Decreased	14%	31%	35%	17%	9%	26%	19%	22%
Stayed about the same	29%	25%	31%	41%	54%	39%	37%	36%
I don't know	0%	1%	5%	3%	4%	2%	1%	2%
How many spear phishing attacks did your organisation experience in 2019?								
0	20%	25%	4%	4%	4%	1%	29%	12%
1-10	21%	37%	21%	26%	56%	28%	21%	28%
11-25	20%	15%	20%	30%	17%	43%	20%	24%
26-50	11%	9%	24%	18%	0%	13%	7%	13%
51-100	12%	8%	13%	14%	6%	6%	11%	10%
100+	10%	5%	13%	3%	11%	7%	11%	9%
I don't know	6%	1%	5%	5%	6%	2%	1%	4%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
How many BEC attacks did your organisation experience in 2019?								
0	21%	32%	3%	4%	4%	0%	35%	14%
1-10	21%	28%	21%	17%	48%	33%	25%	26%
11-25	16%	19%	26%	29%	23%	30%	12%	22%
26-50	14%	9%	23%	22%	11%	23%	14%	18%
51-100	15%	12%	16%	17%	6%	8%	4%	11%
100+	5%	0%	5%	6%	4%	5%	7%	5%
I don't know	8%	0%	6%	5%	4%	1%	3%	4%
Which of the following impacted your organisation as a result of phishing attacks in 2019? (Multiple responses allowed.)								
Loss of data	54%	51%	49%	48%	59%	45%	66%	53%
Credential/account compromise	60%	31%	49%	50%	41%	36%	47%	47%
Ransomware infection	51%	54%	42%	50%	32%	43%	48%	47%
Other malware infection	36%	26%	28%	33%	41%	55%	28%	35%
Financial loss/wire transfer fraud	37%	40%	25%	26%	45%	29%	39%	34%
Did your organisation experience a ransomware attack in 2019 and pay the ransom?								
Yes	51%	37%	32%	28%	10%	26%	35%	33%
No, we were infected but did not pay	22%	25%	44%	29%	36%	36%	32%	32%
No, we were not infected	27%	38%	24%	43%	54%	38%	33%	35%
If you paid the ransom, what was the result?								
Regained access to data/systems after first payment	80%	88%	50%	39%	100%	81%	69%	69%
Got hit with additional ransom demands, walked away without data	2%	0%	22%	15%	0%	4%	6%	7%
Paid additional ransom demands, eventually got access to data	0%	0%	0%	7%	0%	4%	25%	2%
Never got access to data	18%	12%	28%	39%	0%	11%	0%	22%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
How does your organisation measure the cost of phishing? (Multiple responses allowed.)								
Downtime hours for end users	65%	60%	51%	47%	46%	45%	50%	52%
Remediation time for infosec teams	56%	43%	54%	45%	50%	59%	39%	50%
Damage to reputation	48%	45%	41%	39%	35%	48%	48%	44%
Business impacts due to loss of IP	35%	43%	29%	36%	35%	30%	41%	35%
Direct monetary losses (like wire transfer fraud)	20%	28%	25%	29%	38%	30%	22%	27%
Compliance issues/fines	29%	18%	8%	22%	38%	21%	26%	22%
Costs due to incident response and remediation (like third-party forensics)	27%	20%	16%	19%	33%	19%	25%	22%
Legal fees	18%	14%	15%	16%	21%	17%	26%	18%
Lost revenue from downtime/lost customers	13%	29%	8%	18%	19%	23%	24%	19%
We do not measure the cost of phishing incidents	6%	8%	6%	11%	10%	1%	10%	7%
How many smishing (SMS/text phishing) attacks did your organisation experience in 2019?								
0	23%	38%	5%	4%	6%	0%	37%	16%
1-10	18%	25%	28%	36%	42%	45%	27%	31%
11-25	18%	8%	26%	39%	25%	27%	16%	23%
26-50	13%	14%	16%	10%	11%	12%	8%	12%
51-100	17%	11%	14%	8%	4%	11%	4%	10%
100+	4%	0%	10%	2%	10%	3%	6%	5%
I don't know	7%	4%	1%	1%	2%	2%	2%	3%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
How many vishing (voice phishing) attacks did your organisation experience in 2019?								
0	22%	43%	4%	5%	4%	1%	43%	17%
1-10	20%	22%	31%	39%	54%	42%	21%	31%
11-25	19%	9%	27%	31%	19%	27%	9%	21%
26-50	12%	12%	13%	10%	9%	16%	9%	12%
51-100	15%	9%	15%	11%	6%	7%	9%	11%
100+	5%	0%	8%	2%	6%	6%	6%	5%
I don't know	7%	5%	2%	2%	2%	1%	3%	3%
How many USB-based attacks did your organisation experience in 2019?								
0	27%	43%	4%	3%	4%	2%	48%	19%
1-10	17%	22%	33%	49%	50%	44%	19%	33%
11-25	16%	15%	22%	21%	25%	27%	10%	19%
26-50	13%	11%	18%	11%	2%	15%	11%	12%
51-100	17%	8%	14%	11%	6%	7%	5%	10%
100+	5%	0%	7%	3%	11%	2%	5%	4%
I don't know	5%	1%	2%	2%	2%	3%	2%	3%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
How many social media attacks (like pretexting and account takeover attempts) did your organisation experience in 2019?								
0	22%	34%	3%	4%	4%	0%	33%	14%
1-10	25%	26%	28%	37%	50%	37%	34%	33%
11-25	10%	8%	23%	24%	23%	29%	12%	19%
26-50	16%	18%	20%	18%	8%	18%	9%	16%
51-100	13%	9%	20%	10%	5%	11%	6%	11%
100+	6%	3%	4%	3%	8%	5%	3%	4%
I don't know	8%	2%	2%	4%	2%	0%	3%	3%
Does your organisation train employees to spot and avoid phishing attacks?								
Yes, we do company-wide training	86%	63%	62%	65%	86%	58%	60%	68%
Yes, we train some departments/roles	8%	32%	31%	26%	10%	38%	36%	27%
No	6%	5%	4%	6%	4%	3%	4%	4%
I don't know	0%	0%	3%	3%	0%	1%	0%	1%
How frequently does your organisation deliver cybersecurity awareness training to employees?								
Twice a month	31%	18%	25%	15%	20%	23%	25%	23%
Monthly	42%	48%	31%	31%	30%	38%	43%	38%
Quarterly	18%	16%	28%	27%	28%	21%	26%	23%
Twice a year	4%	7%	12%	18%	20%	11%	5%	10%
Yearly	5%	11%	4%	9%	2%	7%	1%	6%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
About how much time does your organisation allocate to employee cybersecurity awareness training in a calendar year?								
0-30 minutes	9%	8%	12%	3%	12%	6%	2%	7%
31-59 minutes	32%	31%	31%	31%	24%	28%	30%	30%
1-2 hours	37%	43%	37%	51%	48%	46%	40%	43%
2-3 hours	12%	8%	15%	9%	2%	7%	13%	10%
More than 3 hours	10%	10%	5%	6%	14%	13%	15%	10%
What types of security awareness training tools does your organisation use? (Multiple responses allowed.)								
Simulated phishing attacks	66%	53%	52%	49%	72%	55%	49%	56%
In-person training sessions	59%	66%	60%	56%	40%	66%	69%	61%
Computer-based training	62%	63%	48%	60%	58%	65%	64%	60%
Awareness posters and videos	32%	35%	40%	16%	26%	20%	36%	30%
Newsletters and emails	31%	32%	28%	43%	34%	20%	30%	31%
Cybersecurity-based contests/prizes	22%	27%	16%	22%	22%	20%	23%	21%
Smishing and/or vishing simulations	17%	27%	29%	23%	28%	32%	24%	25%
Simulated USB drops	16%	18%	11%	13%	28%	13%	18%	16%
Email reporting button	13%	19%	9%	15%	18%	15%	17%	15%
Has your organisation been able to quantify a reduction in phishing susceptibility due to security awareness training?								
Yes	91%	79%	71%	71%	72%	80%	78%	78%
No	7%	16%	23%	18%	18%	17%	17%	16%
I don't know	2%	5%	6%	11%	10%	3%	5%	6%
Does your organisation employ a consequence model for employees who regularly fall for phishing attacks? (Meaning, are there punishments for "repeat offenders"?)								
Yes	78%	62%	67%	53%	60%	59%	60%	63%
No	22%	32%	28%	39%	38%	39%	38%	33%
I don't know	0%	6%	5%	8%	2%	2%	2%	4%

	US	AUSTRALIA	FRANCE	GERMANY	JAPAN	SPAIN	UK	GLOBAL AVERAGE
What are the penalties that employees face as part of your organisation's consequence model? (Multiple answers permitted)								
Counselling from manager	63%	53%	25%	47%	58%	47%	45%	48%
Counselling from the infosec team	42%	55%	66%	47%	65%	47%	47%	51%
In-person follow-up training	50%	60%	49%	62%	42%	47%	68%	54%
Mandatory computer-based training	35%	38%	43%	32%	39%	44%	45%	39%
Disciplinary actions enforced by HR	25%	20%	18%	26%	35%	24%	21%	23%
Removal of access to systems	18%	28%	15%	26%	45%	17%	18%	21%
Monetary penalty	20%	8%	16%	17%	16%	15%	21%	17%
Written warning/probation	23%	15%	19%	32%	26%	19%	31%	23%
Termination	12%	10%	13%	11%	10%	10%	11%	11%
Has use of a consequence model led to an improvement in employee awareness?								
Yes, it's making a difference	92%	80%	79%	83%	84%	83%	86%	84%
No, it hasn't made a difference	6%	13%	21%	15%	10%	15%	11%	13%
Not sure, we haven't measured it	2%	2%	0%	2%	6%	2%	3%	2%
I don't know	0%	5%	0%	0%	0%	0%	0%	1%

C. Industry Failure Rates by Simulated Phishing Template Style

Different views of your data can reveal new insights. The following table shows the user-level and organisation-level failure rates of the three different phishing test styles within each industry. The differences between these two numbers is often significant.

As we cautioned earlier in the report, certain factors can unduly influence the user-level average. That is the case with failure rates for attachment-based tests. This template style was least used by our customers in 2019; just 10% of all simulated phishing emails tested users' responses to attachments. Difficult-to-detect lures—and low levels of user awareness about attachment-based phishing—may have influenced user-level failure rates in these smaller sample sets.

AVERAGE FAILURE RATE (USER LEVEL, ORGANISATION LEVEL)

INDUSTRY	LINK-BASED TESTS	ATTACHMENT-BASED TESTS	DATA ENTRY-BASED TESTS
Business Services	9%, 10%	59%, 23%	4%, 4%
Consumer Goods	12%, 13%	27%, 23%	2%, 3%
Education	10%, 10%	9%, 17%	3%, 4%
Energy/Utilities	8%, 14%	13%, 18%	2%, 3%
Engineering	7%, 10%	4%, 9%	7%, 7%
Entertainment/Media	17%, 16%	18%, 28%	3%, 3%
Finance	8%, 11%	13%, 18%	3%, 3%
Financial Services	15%, 14%	34%, 26%	5%, 3%
Food and Beverage	9%, 16%	24%, 12%	2%, 2%
Government	14%, 14%	22%, 21%	5%, 4%
Healthcare	8%, 12%	11%, 16%	4%, 4%
Hospitality	14%, 14%	17%, 51%	5%, 7%
Insurance	11%, 12%	39%, 26%	4%, 2%
Manufacturing	9%, 13%	19%, 22%	3%, 4%
Professional Services	11%, 14%	14%, 13%	3%, 4%
Retail	11%, 11%	20%, 27%	3%, 4%
Technology	10%, 13%	14%, 16%	6%, 4%
Telecommunications	8%, 11%	14%, 18%	6%, 5%
Transportation	14%, 14%	9%, 14%	6%, 5%

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' 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 organisations of all sizes, including more than half of the Fortune 1000, 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.

0400-002-01-01 12/19