proofpoint.

ANNUAL REPORT

2021 State of the Phish

An In-Depth Look at User Awareness, Vulnerability and Resilience

proofpoint.com

INTRODUCTION: A YEAR LIKE NO OTHER

There's no question that organisations (and individuals) faced many challenges in 2020, both new and familiar. Information security teams felt the strain, too.

On top of "ordinary" cybersecurity issues, professionals in these roles dealt with an explosion of pandemic-themed phishing scams and a continued surge in ransomware attacks—all while attempting to transition many users to work-from-home environments, effectively overnight.

Our seventh annual *State of the Phish* report explores these topics and more. We analyse survey data, simulated phishing exercises and real-world attacks to provide insights into phishing and other cyber threats—and what you can do about them.

This year's report includes data from the following:

A third-party survey of

3,500

working adults across seven countries

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

A third-party survey of

600

IT security professionals across the same seven countries

More than

60M

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

About

15M

emails reported by our customers' end users

"Phishing" can mean different things to different people. We use the term in a broad sense to encompass all socially engineered email attacks, 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

2020 Challenges: An Organisational View

57%

of respondents in a third-party survey said their organisation experienced a successful phishing attack in 2020, up from **55%** in 2019.

2020 was a banner year for phishing attacks. We saw large volumes of credential phishing emails and social engineering techniques (some more sophisticated than others). More than half of our Email Protection customers received at least 1,000 phishing attempts; for some customers, we blocked millions of messages. And while attackers targeted a wide array of industries, manufacturing companies saw the highest average volume of phishing emails.

But no technical tools are foolproof. In our global survey of infosec professionals, conducted by a third party, 57% of respondents said their organisation dealt with a successful phishing attack in 2020. That's a slight uptick over our previous survey.[1]

These attacks had serious impacts on the organisations they targeted. Compared with our previous survey, 13% more respondents said phishing attacks led to data loss. And 11% more said they led to credential compromise.

But we saw some bright spots.

Ransomware infections held steady year over year. At the same time, 17% fewer respondents reported malware infections as a result of phishing vs. our previous survey. And 47% fewer experienced direct financial loss. These results could indicate that organisations have implemented stronger preventive measures against these types of attacks.

INTERNATIONAL

74%

of US organisations experienced a successful phishing attack last year, **30%** higher than the global average and a **14%** year-over-year increase.

< 50%

of French and German organisations dealt with a successful phishing attack.

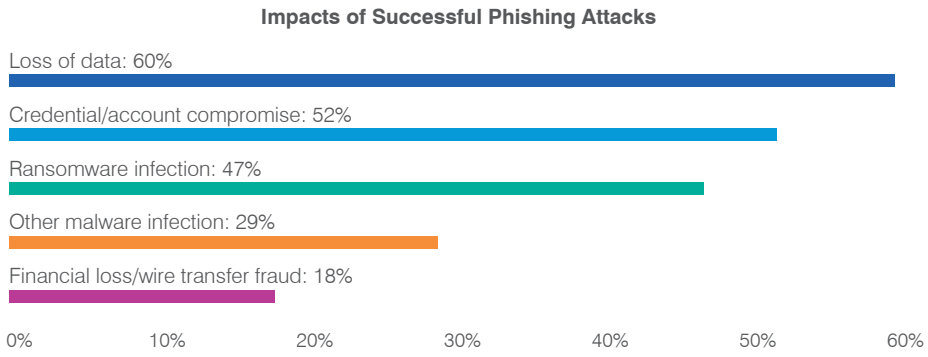

Figure 1.

[1] Unless otherwise indicated, survey results represent global averages. You can find country-by-country breakdowns of survey findings in the Appendix.

KEY FINDING

The impact of phishing attacks varied widely by region. Whether these differences stem from respondents' cultural influences or geographical diversity in attackers' methods, the contrasts are worth noting.

Take the onslaught of fraudulent Amazon messages experienced in Japan in 2020 as an example. The extreme volume of these credential phishing attacks may have contributed to that country's higher-than-average occurrence of account compromise.[2]

Some **64%** of Japanese organisations dealt with credential compromise, the most of all regions surveyed. But they were least likely to deal with direct financial losses (**11%**).

At the same time, **69%** of Spanish survey participants experienced data loss vs. just **47%** of their Australian peers.

Phishing-based ransomware affected **67%** of Australian organisations vs. just **25%** of French respondents.

In the US, **35%** of those surveyed dealt with immediate financial loss, nearly twice the global average.

The shifting nature of targeted attacks

For every successful attack, many more phishing attempts are thwarted. More than 75% of organisations said they faced broad-based phishing attacks—both successful and unsuccessful—in 2020. This wide-net approach, in which the same phishing email is sent to multiple people, was the most common across all the regions we surveyed.

But that doesn't mean spear phishing, whaling and business email compromise (BEC) should be regarded as "lesser" threats than bulk campaigns. These types of attacks reach fewer people, but their level of focus and sophistication make them more difficult for users to spot and for technical tools to block. Attackers are adept at researching and targeting specific roles and people, which means spear phishing, whaling and BEC should remain firmly on everyone's radar.

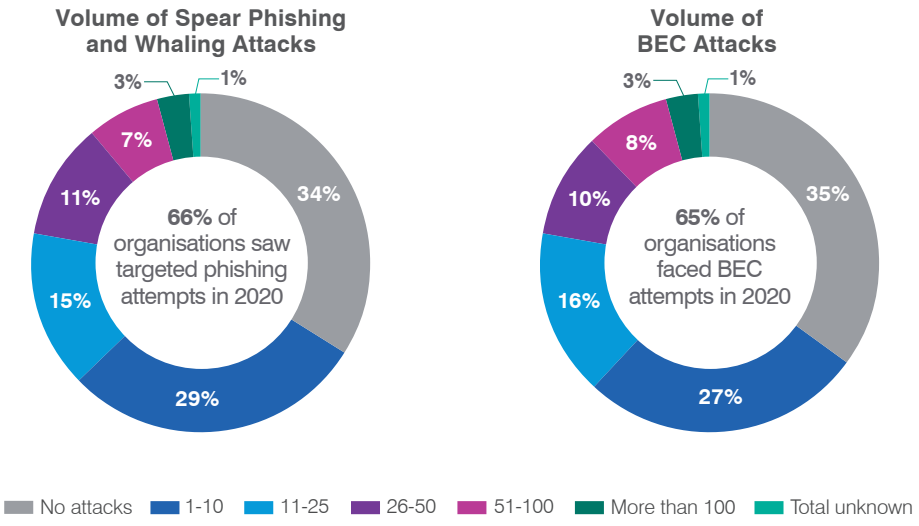

Figure 2.

[2] Proofpoint. "Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet," October 2020.

Thinking outside the inbox: social engineering attacks beyond email

Social engineering attacks come in many forms, not just email. Attackers use social media, text messages and even voicemail to trick users. Here are some of the non-email attacks (successful and unsuccessful) infosec professionals saw in 2020:

INTERNATIONAL

US and French organisations were on opposite ends of the spectrum when it came to non-email-based social engineering attacks in 2020:

US Organisations

86%
faced social attacks like pretexting and account takeover.

81%
faced SMS/text phishing (smishing) attacks.

80%
dealt with weaponised USB drives.

77%
faced voice phishing (vishing) attacks.

VS

French Organisations

48%
faced smishing attacks.

33%
faced social attacks.

31%
dealt with weaponised USB drives.

29%
faced vishing attacks.

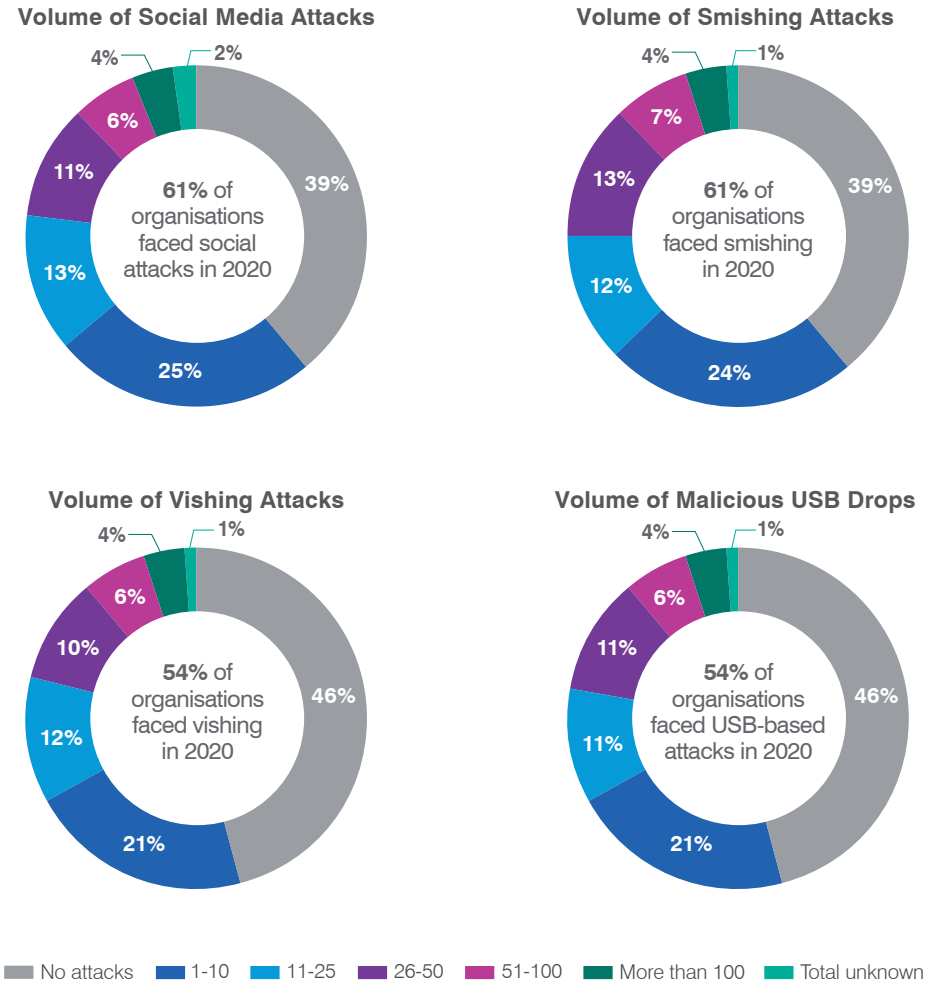

Figure 3.

Ransomware: more orgs paid up in 2020—with mixed results

KEY FINDING

French and Japanese organisations were the least likely to experience a ransomware infection (**47%** and **46%**, respectively, said they were not affected by ransomware in 2020). They were also the least likely to pay a ransom when they were infected (**18%** for both).

INTERNATIONAL

68%
of US organisations said they paid a ransom in 2020, twice the global average.

41%
of Spanish organisations refused to pay a ransom after being infected, making them the least likely to negotiate with attackers.

78%
of French organisations were lucky enough to regain access to their data and systems after paying a single ransom, the highest of any region surveyed (the US was the second highest at **76%**).

14%
of German organisations refused to pay a follow-up ransom, the highest among the regions surveyed.

We've likely all heard the old adage "There's no honour among thieves." In 2020, two-thirds of those surveyed said their organisation experienced a ransomware attack. More than half of those opted to pay attackers' ransom in an attempt to regain access to their systems and data. But our survey results show doing so often wasn't a quick fix.

We asked infosec professionals about their overall experiences with ransomware (those that resulted from phishing attacks as well as other sources). They revealed the following:

- 34% of organisations were infected and opted to pay the ransom (a slight year-over-year increase)
- 32% were infected but did not pay the ransom
- 34% said they did not experience a ransomware infection in 2020

And proving the adage out, many who risked the payment were betrayed by the outcome.

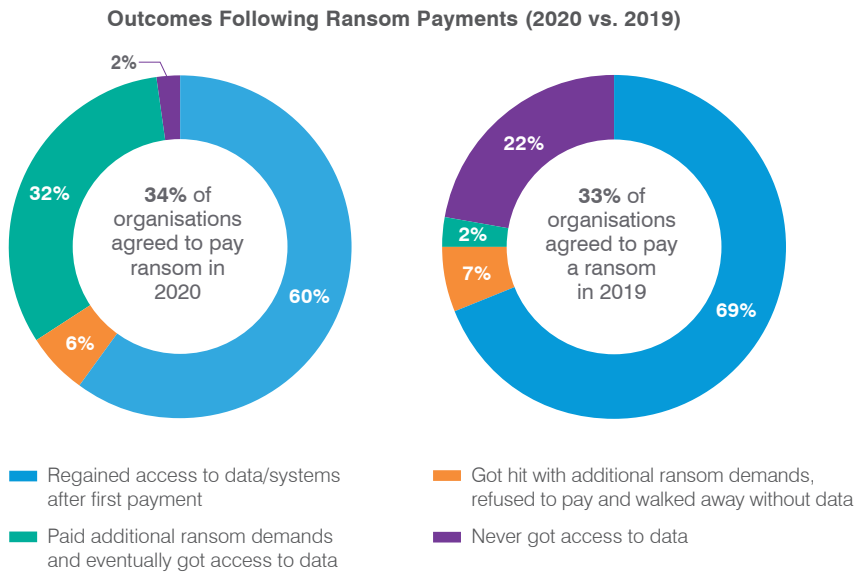

Figure 4.

As shown in the year-over-year comparison (Figure 4), paying the ransom was a far shakier bet in 2020. Victims who paid in 2020 were less likely to regain access after the first payment than they were the year before. That's alarming in itself. Even more astonishing is the increase in follow-up ransom demands and related actions:

- Requests for additional ransom demands rose by more than 320% in 2020
- 32% of 2020 respondents were willing to pay the extra ransoms, compared to just 2% in 2019—an incredible 1,500% year-over-year increase

The one bright spot: just 8% of payers ended up walking away empty-handed after negotiating with attackers, a big drop from last year's 29%.

How users fared in 2020

11%
average failure rate on phishing tests in 2020

33%
average overall view rate of simulated attacks

During our 12-month measurement period, our customers sent more than 60 million phishing tests to their users, nearly 15 million more than were sent in 2019. Given the tricky threat landscape faced by infosec teams and users alike in 2020, it is heartening to see that organisations continued to prioritise phishing awareness activities.

Another positive: the average failure rate decreased in our most recent data set. Organisations experienced an average failure rate of 11% in 2020, compared to 12% in 2019.[3]

But an overall average failure rate can only tell you so much about users' responsiveness to different types of threats. Attackers are crafty and creative. They regularly vary their lures to appeal to different people and personalities. As such, it's critical that organisations respond in kind. That means varying testing and teaching to identify and address potential areas of weakness.

Failure rates by template type

Most phishing simulation tools offer customisable email templates that let organisations test different phishing tactics. Our customers can choose a from variety of themes and lures among three primary template types: link-based, data entry-based and attachment-based. As in the prior two years, organisations heavily favoured simulated attack templates that use URL hyperlinks in 2020.

"Failed" data-entry tests refer to cases in which users submitted data after clicking a link in the simulated attack.

Phishing Template Types: Frequency of Use

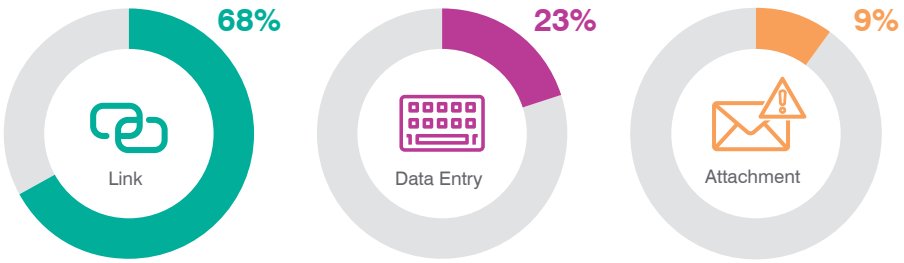

Figure 5.

Phishing Template Types: Average Failure Rates

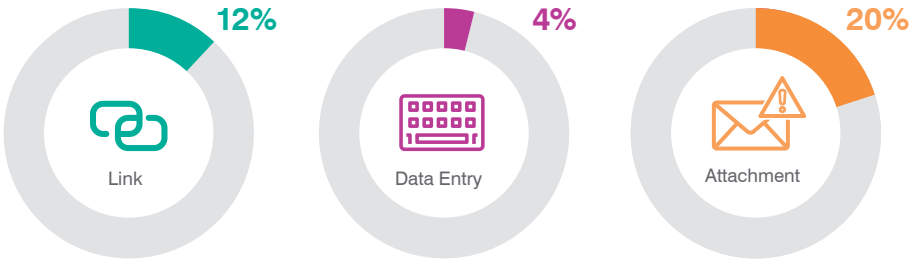

Figure 6.

[3] We calculate average failure rates at the organisational level rather than the user level, giving equal weight to each organisation's average failure rate rather than equally weighting each user's failure rate. This approach helps to eliminate the sway of large organisations and high-volume programmes, providing a more balanced view of failure data.

This lines up with what we see in real-world attacks. Link-based phishing is far more prevalent than attachment-based phishing. And attackers continue to get more creative. In 2020, we also saw a rise in the use of legitimate services such as Microsoft 365, Google Drive, Constant Contact, and SendGrid in socially engineered attacks. Many widely used, well-trusted services generate their own URLs that link to hosted content. Attackers benefit from this approach in multiple ways:

- These services have valid business uses, which makes the URLs difficult (if not impossible) to blocklist.
- URL/domain reputation-based detections cannot rule out attackers' URLs because doing so would block legitimate services.
- Workers frequently see—and use—these cloud-based services. That familiarity breeds a sense of trust that works to attackers' advantage.

But as shown in Figures 5 and 6, positive results on link-based tests don't always correlate to positive results for other types of simulations. The failure rate for attachment-based tests, for example, was far higher than for URL-based ones.

The upshot: organisations should evaluate whether they are doing enough to test how well users can recognise and avoid attachment-based phishing threats. And they should keep in mind that one phishing test is just that: one phishing test. The chameleon-like nature of phishing attacks requires a flexible and open-minded approach to testing and training users.

Your users are likely to face a wide variety of attacks and tactics. That's why a well-balanced approach to phishing simulations is best.

Campaign template themes: most used vs. most tricky

Organisations should choose simulated phishing templates that relate to the real-world threats that their users are most likely to face. But they should not ignore the elements of creativity and surprise when testing users. Often, it's "outlier" topics and themes that most keenly shed light on phishing aspects that aren't well understood by users—and lures that are too tempting to ignore.

To that end, here are the top 10 most-used themes and the top 10 most "successful" themes of 2020 phishing tests. In both categories, templates with these themes were sent to at least 2,300 users (and in some cases, many more).

Most-Used Themes

1. New Microsoft Teams request
2. Coronavirus advisory alert and health warning
3. Microsoft 365 password expiration notice
4. Deactivation of old OneDrive account
5. OneDrive shared contract notification
6. Starbucks bonus
7. World Health Organisation coronavirus safety information
8. New voicemail message alert
9. Alert about large number of files deleted from OneDrive
10. UPS shipping notice

Trickiest Themes

1. Free month of Netflix streaming for employees
2. Holiday letting agreement
3. Starbucks pumpkin spice season
4. 2020 Summer Olympics advanced ticket sales
5. Overdue invoice reminder
6. Spotify password update prompt
7. Promissory note
8. Dress code violation
9. Coronavirus mask availability and payment plans for business
10. Notice of moving violation

What of the failure rates on these sets of templates? The trickiest templates all had failure rates near 100%. And the vacation contract rental lure proved equally successful across multiple languages. In comparison, the highest failure rate among the most frequently used templates was 21%.

It's also worth noting that six of the trickiest templates were attachment-based tests. The other four were link-based tests. (No data-entry tests made the list.)

Spotlight: Coronavirus-themed phishing

No report covering the 2020 timeframe would be complete if it didn't highlight coronavirus-themed (and coronavirus-adjacent) lures. The pandemic offers a vivid case study of how attackers use timely attacks that tap into of-the-moment issues and concerns of users around the world.

We blocked millions of pandemic-related phishing emails between January and early December 2020. The combination of relevant messaging and mass distribution was unprecedented—much like 2020 itself.

Though volumes have eased since their peak in March/April 2020, attackers have continued to piggyback on people's natural interest in this topic. In late 2020, they transitioned to vaccine-related email-based lures and economic stimulus-related smishing (SMS/text phishing) attacks. As long as the coronavirus remains a global concern, we expect the topic to feature prominently in future attacks.

The initial surge of pandemic-related phishing attacks coincided with sea changes in working situations for a vast number of organisations globally. These organisations—and their users—found themselves in unfamiliar territory, striving to maintain business continuity in environments that presented many potential distractions.

At that time, some of our customers asked: do we continue security awareness training or pause for now? Our answer: attackers relish change and uncertainty. During times like this, security awareness training provides a critical line of communication to users—and a critical line of sight into user behaviours.

Fast-changing conditions at the onset of the pandemic only reinforced how important agility is. To keep up with emerging threats and unfolding events, organisations quickly began to incorporate pandemic-related testing and training activities. These included coronavirus-related phishing simulations and remote-working tips.

The failure rate for many COVID-themed tests approached 100%. The mask lure noted in the Trickiest Themes list on page 10 was just one example. Others with high failure rates used the following subjects, which reflected subjects seen on phishing attacks in the wild:

- Singapore Specialist: Coronavirus Safety Measures
- COVID-19 Hospital Visit
- FBI Warning!!! Coronavirus Scams
- COVID-19 Infected Our Staff

But overall, users performed well on coronavirus-related tests. This is impressive, given that most pandemic-themed lures heavily played on fears and issues shared across the globe. For users who were tested on the most frequently used COVID-related templates, average failure rates ranged from less than 1% to just over 20%.

SECTION 2

Benchmarking: Industry and Department Data

KEY FINDING

The industries that ran the most phishing tests in 2020 were healthcare, financial services, manufacturing, energy/utilities and technology.

Customers often ask for benchmarking data. To enable organisations to better compare themselves and their users on a more granular, peer-to-peer basis, we've gone deeper than ever this year, providing average failure rates for 20 industry and department designations.

Among our customers, manufacturing organisations faced the highest average volume of real-world phishing attacks in 2020. Other high-volume industries included technology, energy/utilities, retail and financial services. Fortunately, four of these five industries are among those that test their users the most actively. The average failure rates of each of these industries matched the overall average of 11%.

Each industry represented in our failure rate comparison includes data from at least 15 organisations and at least 150,000 simulated phishing attacks.

Industry failure rates

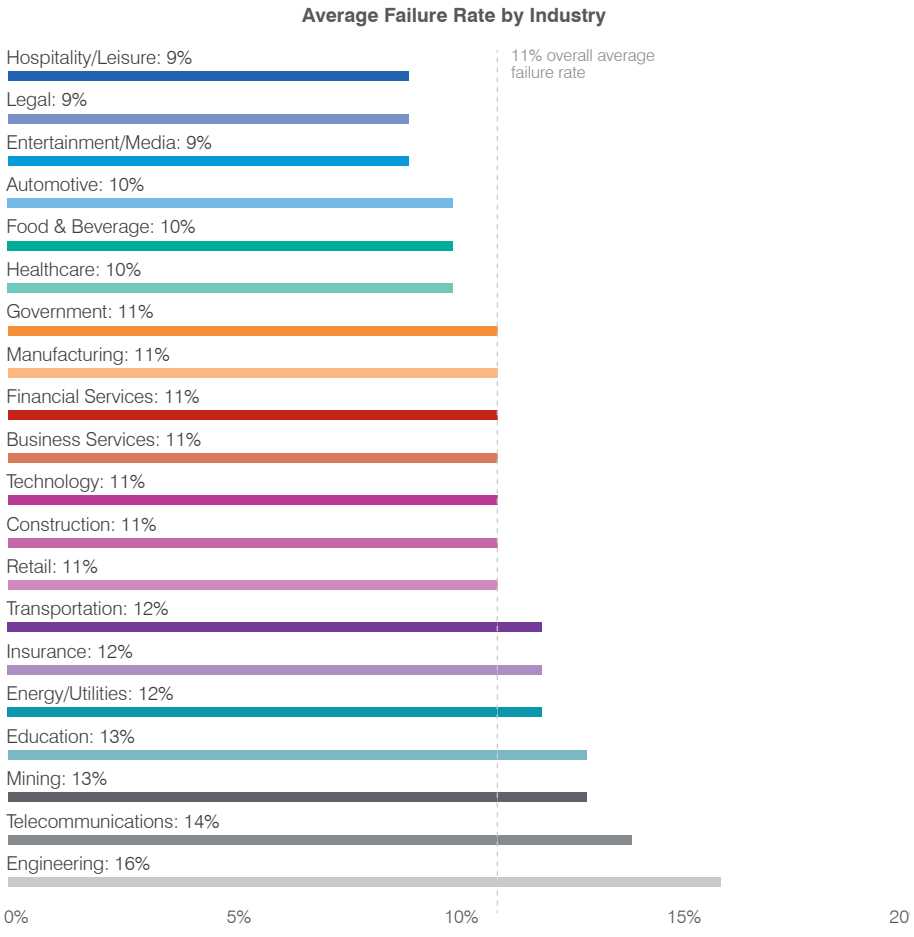

Figure 7.

Notable mentions: less active industries

The most active industries we analysed sent thousands of campaigns and millions of phishing tests to their users in 2020. Naturally, some of these higher numbers are due to the virtue of simple maths: more organisations + more users = more tests.

But that isn't always the case.

On average, each organisation in our study sent eight simulated phishing campaigns in 2020. The top five most active industries sent an average of seven to 10 campaigns.

Organisations in less active industries—such as aerospace, not-for-profit, and real estate—sent just four or five campaigns on average. These sectors each had at least 15 organisations in our sample count but did not send enough simulated phishing attacks to appear in our comparison of average failure rates.

When it comes to evaluating your users' vulnerability to phishing attacks, the number of touchpoints counts. You cannot effectively test your users using just a few simulated attacks per year. Attackers are on the hunt 24x7. We recommend testing every four to six weeks, using a variety of lures, to get the best sense of how users respond to different kinds of phishing threats.

Department failure rates

Department-level failure rates offer a finer-tuned view of potential weak spots within an organisation. Attackers often target individual inboxes and email aliases. An organisation-level failure rate alone will not reveal roles and teams that may be struggling.

Unfortunately, too few organisations group their users by department for reporting purposes. Without this insight, they cannot quickly and regularly evaluate performance (and user vulnerability) by job function.

Department designations represented in our failure rate comparison were used by at least 40 organisations and include data on a minimum of 1,500 users.

KEY FINDINGS

R&D was the worst-performing department in last year's report, clocking in with a **20%** average failure rate. This year's **8%** average failure rate represents a **60%** year-over-year improvement.

At **11%**, the average failure rate for sales held steady this year, matching our overall average failure rate. But this is a group to monitor closely. Sales email aliases are frequently targeted by attackers.

Figure 8 compares the average failure rates of 20 different departments, ranked lowest to highest.[4]

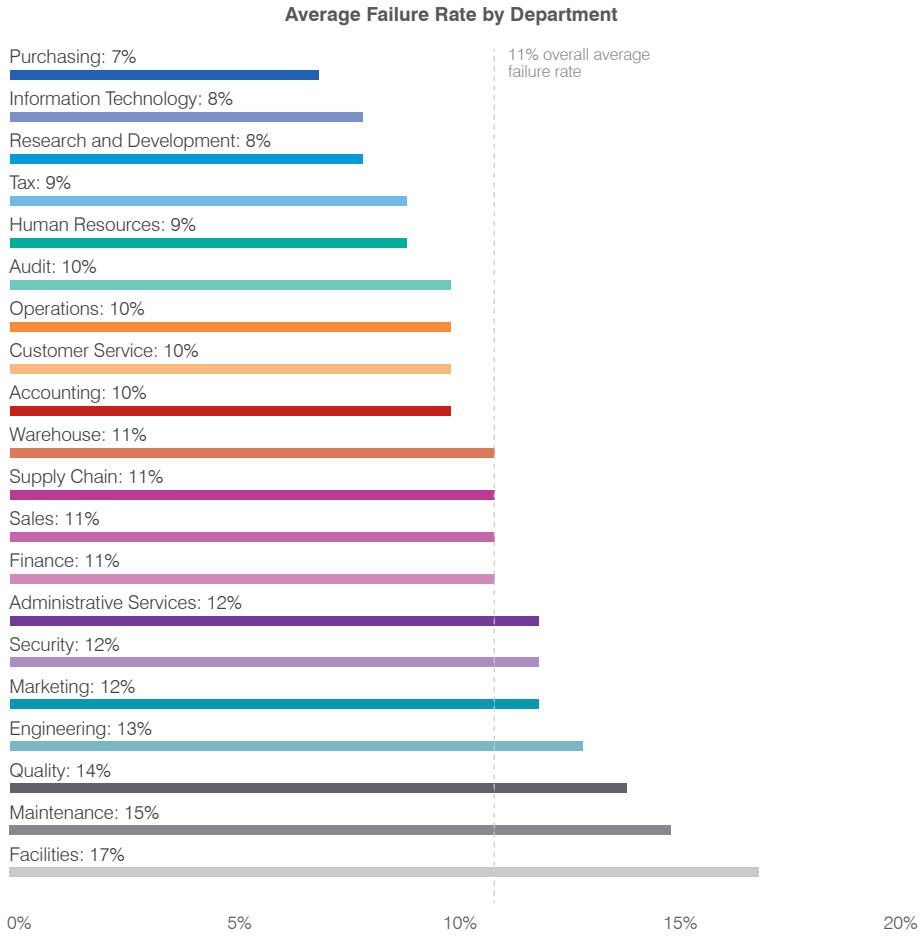

Figure 8.

It's good news to see so many departments outperforming the 11% overall average failure rate. But it's the underperforming groups that truly illustrate the value of department-level visibility into phishing test performance. Though an overall average failure rate can be a helpful metric, it is critical to understanding which roles and departments are missing that mark—especially if they are missing by a wide margin.

[4] Note that our customers self-select department designations within their data. As such, similar designations could mean different things across multiple organisations. For example, "facilities" and "maintenance" might overlap in one organisation but have different designations in another.

SECTION 3

Key Measurements: Email Reporting and Resilience Ratios

PhishAlarm customers saw a **13%** average reporting rate on phishing tests.

On average, **5** emails were reported by each PhishAlarm user.

If you've read *State of the Phish* in years past, you know we are kind of obsessed with email reporting. We strongly advise all our customers to implement our PhishAlarm® in-client reporting tool because it:

- Empowers users to apply email security behaviours and become active participants in your security efforts
- Allows users to quickly and easily alert designated infosec team members to suspicious emails
- Enhances your security culture by promoting a collaborative relationship between users and security teams
- Correlates failure rates and reporting rates so you can quantify resiliency
- Gives visibility into the types of real-world threats that are evading perimeter defences
- Provides the opportunity to integrate reporting and remediation functions to quickly identify and address active threats within the network

From a high-level perspective, our latest reporting data set is larger than ever. Over our 12-month measurement period, our customers' users reported about 15 million emails. The overall average reporting rate of simulated phishing attacks was 13%. (We explore user reporting of real threats later in this section.)

What is a resilience ratio?

PhishAlarm customers saw an average resilience factor of 1.2.

Last year, we discussed the 70:5 rule as a stretch goal for organisations that are tracking both reporting rates and failure rates on their simulated phishing campaigns. This targeted resilience ratio—an overall reporting rate of 70% or higher paired with a failure rate of 5% or lower—results in a resilience factor of 14. Organisations that achieve—and just as important, maintain—this level of resilience reach a nirvana-like state in which users are 14 times more likely to report a phishing email than engage with one.

Organisations that are using PhishAlarm have already taken the necessary first step: implementing an integrated reporting mechanism. And their average reporting rate already tops the average failure rate to deliver a positive resilience factor:

13% average reporting rate ÷ 11% average failure rate = 1.2 resilience factor

That's not the ideal resilience ratio. Still, a resilience factor greater than 1 means that more users are reporting than are failing, and that's a positive trend. Given the newness of reporting tools such as PhishAlarm, there is a lot of runway for improvement.

Benchmarking: industry resilience factors

You may wish to compare your organisation's average resilience factor to those of your industry peers. Table 1 notes the average reporting rates, average failure rates and resilience factors for the 20 industries covered in Figure 7.

The average failure rates in Table 1 are slightly different than those in Figure 7. The rates in this section are based on data related to customers that use both our simulated phishing tools and our reporting button (a subset of the data used earlier).

Average Failure Rate, Reporting Rate and Resilience Factor by Industry

Industry	Reporting Rate	Failure Rate	Resilience Factor
Financial Services			
Energy/Utilities			
Insurance			
Legal			
Engineering			
Automotive			
Business Services			
Technology			
Government			
Mining			
Food & Beverage			
Manufacturing			
Healthcare			
Entertainment/Media			
Transportation			
Telecommunications			
Construction			
Retail			
Education			
Hospitality/Leisure			

Table 1.

Several industries well outpaced the 1.2 average resilience factor. Legal and automotive lead the way, with about twice as many reports as failures.

But we also see several industries falling far behind the average, including some with negative resilience factors (more failures than reports). This could be due to a few reasons, including programme immaturity, insufficient ongoing education, or a focus on difficult/challenging phishing tests. All three of these can result in higher failure rates and lower resilience factors.

These numbers help to illustrate the advantage of pairing a strong reporting rate with a low failure rate across all manner of phishing tests. And a high resilience quotient (like the 14 we suggest striving for as a stretch goal) is not out of the question. It is more achievable on single campaigns, naturally. But we have customers who are sustaining significantly higher resilience factors—between 24 and 60—across multiple campaigns that include anywhere between 40,000 to nearly 100,000 simulated phishing emails.

If others can do it, so can you. And if you can do it once, you can do it again (and again and again…).

Spotlight: users actively reported attacks from the wild in 2020

Our PhishAlarm button works in conjunction with PhishAlarm Analyzer, which uses Proofpoint threat intelligence to identify phishing attacks in real time. The contents of emails reported via PhishAlarm are scanned by Proofpoint scoring engines, and all URLs and attachments are live-detonated in our sandbox. In this process, between 60% and 80% of reported emails are auto-assigned a definitive classification of either malicious/spam or bulk/benign.

Over our one-year measurement period, our analysis showed the following:

- Users reported more than 5 million suspicious messages from the wild
- Nearly 800,000 of the reported emails were identified as "known bad" (malicious or spam)[5]
- More than 200,00 messages were active credential phishing attacks
- More than 35,000 reported emails contained malware payloads
- Nearly 2 million reported messages were immediately auto-classified as bulk/low-risk emails, eliminating time waste for security teams

These statistics show the immense value of empowering employees to alert infosec teams to suspicious messages. Users are actively identifying and reporting credential phishing attacks and malware. Whether that malware comes in the form of an attachment or URL, payloads include remote-access Trojans (RATs), keyloggers, downloaders and even malicious code from advanced persistent threats (APTs).

Many organisations might fear the workload a reporting button might put on their infosec team. We suggest choosing a tool that integrates reporting, analysis and remediation, such as our Closed-Loop Email Analysis and Response (CLEAR) solution. With the right integrations, emails that are flagged as malicious or spam can be automatically quarantined and remediated or blocked at the email gateway. Integration also helps to cut down on noise from safe emails that users might erroneously report.

This approach allows you to take full advantage of user-based reporting without overwhelming your remediation and response teams. It also provides valuable end-user and security awareness training insights, by:

- Showing you which users are effectively putting their skills into practice by actively reporting suspicious and malicious email.
- Revealing users whose skills are not transferring. These might include users who catch simulated phishing emails but not real ones. Or they might be users who seem to be flagging safe and unsafe email indiscriminately. They may even be users who appear to be more thoughtful but submit emails that don't show warning signs of malicious intent.
- Indicating what types of active attacks are evading perimeter defences. This insight allows you to more finely tune technical safeguards, phishing testing and training plans.

[5] The percentage of "known bad" messages reported varied significantly based on the incumbent secure email gateway. On average, Proofpoint customers saw better pre-delivery block rates, leaving fewer malicious emails for end users to report.

SECTION 4

Threat-Level Intel: Identifying Very Attacked People

We measure user risk using the VAP model, which takes into account vulnerability, attacks and privilege. The VAP model assesses not just how your users are being targeted, but also how likely those users are to fall for an attack and the potential impact if they do. A VAP view of user risk can help reveal the "perfect storms" brewing underneath the surface: users with privileged access who are vulnerable to attack and being actively targeted. VAPs are risks you want to know about—and address.

Today's attacks target people, not just infrastructure. That's why we take a people-centric approach to cybersecurity, and we encourage organisations to do the same.

A people-centric approach goes beyond acknowledging the large role your users play in your security posture—a reality the cybersecurity market has widely, if belatedly, begun to embrace. It's also about knowing which users represent an elevated risk because of any combination of factors, and mitigating that risk.

We analyse incoming threats to identify what we refer to as Very Attacked People (VAPs). These are the employee and alias inboxes within your organisation that are being targeted most actively and intensely. Our analysis reveals not only which users and groups attackers are attempting to reach, but the methods, tools and tactics they're using to try to compromise them.

This kind of threat analysis provides greater context for failure and reporting rates at both a high level (organisation wide) and more granular basis (by departments and per-campaign). Correlating your testing and performance data against real-world attack data can crystallise your plan for delivering targeted training to the people attackers view as high-value targets.

But like testing and training, identifying your VAPs is not a one-time activity. VAPs change over time. And in many organisations, people drop in and out of the top-20 targets list from month to month.

You should also put aside any assumptions you have about who's likely to be a VAP. Targets vary from industry to industry, and organisation to organisation. Your high-profile VIPs are sometimes VAPs. But just as frequently—sometimes more frequently—attackers target non-VIPs and email aliases.

Organisations self-define their VIPs within our platforms. Some flag only top-tier executives as VIPs. Others take a more expansive view, accounting for factors such as visibility, privilege and responsibilities, not just job titles.

We analysed the top-20 VAPs of a large financial services organisation and a large regional healthcare system over the same three-month span. Our findings expose the challenges organisations face in attempting to stay on top of changing attack methods:

Financial Services Provider

- Only one VIP was targeted during the three-month span, but that person (the manager of the organisation's international finance group) consistently ranked among the top three VAPs.
- Only one other person—the CEO of an affiliated global payment provider—appeared in the top 20 more than once. He was a VAP for two of the three months.
- Attackers consistently attempted to deliver malicious messages to alias inboxes. A general customer service address was the top target during all three of the months observed.
- Beyond the CEO, email addresses associated with the affiliated global payment provider were frequently targeted all three months. In fact, in the second month of the observed period, 16 of the top 20 VAPs were inboxes for that affiliate. Attackers attempted to deliver phishing emails to aliases and individuals alike, including people in roles such as business development, point-of-sale (POS) management and financial crime compliance.

Healthcare System

- In the first month observed, half of the organisation's top 20 VAPs were VIPs. In month two, that decreased to seven, and in the third month, there was just one VIP in the top 20.
- Only the finance director (a VIP) remained in the top 20 all three months.
- Attackers attempted to reach VIPs through multiple email accounts during the three months observed. For example, in the first month, three addresses for the CEO were in the top 20, and attackers tried two different addresses for the SVP of operations.
- In the third month, attackers targeted multiple inboxes belonging to people no longer with the organisation. This included two previous board members and a former director of business development.
- Healthcare practitioners were not immune to appearing in the top 20. Multiple nurse practitioners, physicians, and specialty caregivers—such as an infection control nurse and a crisis worker—were targeted frequently enough to appear in the top 20 across the three-month observation period.

The comparison of VAP indicators over the same three-month span shows how the threat landscape is unique to every organisation. In addition, every organisation's users are unique, as is their value to attackers. Intensity and methodology can vary—often significantly—from month to month.

Visibility into these types of attack characteristics—and the trends and goals they may represent—can be highly beneficial. So can assessments and training tailored to address the potential risks introduced by specific VAPs.

SECTION 5

People-Centric Security: The State of Security Awareness and Training

State of the Phish would not be complete without a discussion of security awareness training. It's a critical layer of defence-in-depth cybersecurity. Organisations that are not regularly and thoughtfully factoring users into their security postures are ignoring an audience that attackers covet.

Tackling terminology

Our "what is" survey questions offered three multiple-choice answers and an "I don't know" option. Users who don't know an answer may pose as much risk as those who answer incorrectly.

Asking working adults to choose the definitions of cybersecurity terms from multiple-choice lists might seem simple. The results of this activity are anything but.

Here's a bit of good news: other than malware, awareness of all the terms highlighted on page 21 rose among working adults year over year. And awareness of malware decreased by only 1 percent, essentially remaining steady.

But this year's findings also show that you should never assume your users understand the cybersecurity terms you regularly use. Doing so can seriously hinder your security training efforts.

In some ways, the issue is like a doctor's visit. The average patient is not well-versed in medical jargon. If a doctor presents test results using language the patient doesn't understand, that patient is less likely to seek out the right treatment or make needed changes—even if the cure is simple.

Think of your users as your patients. Many of the preventative behaviours you want them to adopt are not complicated. But if you lose them at the outset by speaking in terms they don't understand, they're less likely to develop healthy habits.

What is
PHISHING?

At 52%, US workers were least likely to answer correctly (though they improved from 49% in 2019).

69% of UK workers understood this term, the highest among the regions we surveyed.

What is
RANSOMWARE?

The number of correct answers increased over last year's 31%—but so did the number of incorrect answers (also 31% in our last survey).

Just 26% of German workers answered this question correctly. In comparison, 42% of Australian respondents chose the right answer.

What is
MALWARE?

Spanish workers led their global counterparts, with 75% answering correctly. (Though that's shy of their 80% mark from last year.)

US workers underperformed the global average. Just 54% answered correctly, and nearly 40% chose incorrect answers.

What is
SMISHING?

At 60% correct, French workers were again top performers on this question, well outpacing last year's 54% mark.

Japanese workers significantly underperformed, compared to the global averages. Just 19% answered correctly, and 56% were unsure of how to answer.

What is
VISHING?

Last year, only 25% of global workers answered this question correctly. Awareness is up nearly 70% since our 2018 survey.

French workers again improved their awareness of this term. At 54%, they were three times as likely as German workers (18%) to answer this question correctly.

INTERNATIONAL

Top Performers

92%
of Japanese workers know that personal email providers cannot block all dangerous messages.

90%
of Japanese workers know that familiar logos in emails don't equate to safety.

65%
of German workers know that an email's sender details can be disguised.

64%
of Spanish respondents recognise that attachments can be infected with malware.

60%
of Spanish and Australian workers know they should be suspicious of all unsolicited email.

VS

Bottom Performers

34%
of US respondents believe emails with familiar logos are safe.

30%
of Japanese workers recognise that the origin of an email can be disguised.

22%
of Australian and Spanish workers think their organisations will automatically block all dangerous emails.

15%
of Japanese respondents were not confident enough to say whether any of the statements about email were true or false.

Let's talk about email

We explored a new line of questioning with survey participants this year: what they know about email. We aimed to find out not just whether they can define phishing, but whether they understand how email works and how it is presented by their email client. We saw some promising results.

Figure 9.

Just 8% of global respondents lacked the confidence to make at least one selection from our list. And it's excellent to see more than three quarters of respondents correctly recognising many danger signs.

Naturally, there is room for improvement—especially when it comes to recognising spoofing and how attachments and unsolicited messages should be treated. And, ultimately, you'd like 100% of users to know that technical email safeguards are not foolproof. Those who don't know that are an urgent risk to your organisation.

Who's using your org's devices?

We surveyed users about their personal habits and behaviours when it comes to the computers and smartphones issued to them by their employer. This line of questioning was timelier than ever in 2020.

More than 80% of the infosec professionals we surveyed said their organisations either requested or required at least half of their employee base to switch to a work-from-home setting last year. This transition happened abruptly for many organisations—and placed devices in a range of potentially insecure environments.

With so many workers—and their housemates—confined to their homes like never before, we wondered: would this affect the personal use and sharing of work-issued devices?

KEY FINDING

More than **50%** of those who have work-issued devices grant access to their friends and family.

INTERNATIONAL

75%

of US respondents give friends and family members access to work-issued devices. This is well more than all global counterparts and an increase from 2019 (**71%**).

For workers, the results were mixed; some behaviours (such as checking personal email, reading news stories, and researching) decreased year over year. Others (including shopping online, streaming media, and playing games) increased.

The results for device sharing were decidedly less mixed. Workers were less likely in 2020 to allow friends and family to check email on their work devices—but all other activities saw a year-over-year increase (some by as much as 50%).

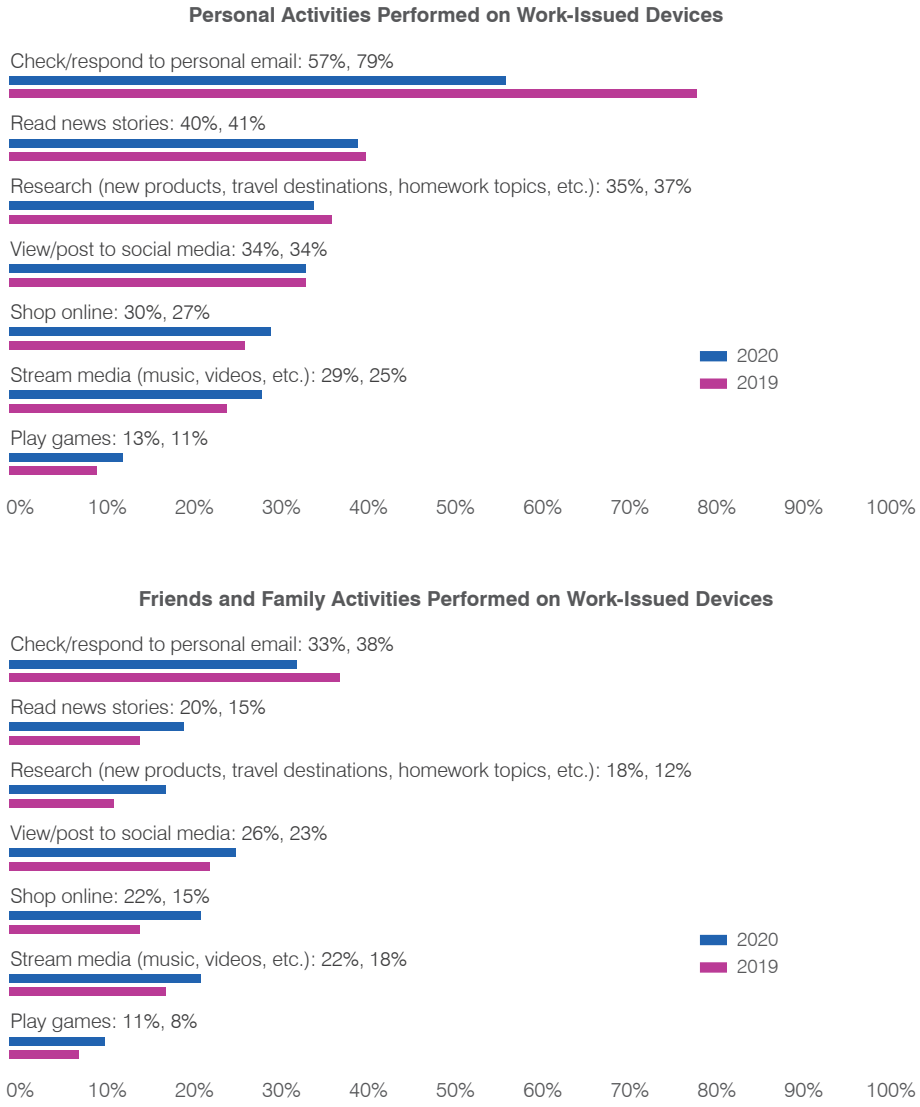

Figure 10.

98%
of organisations have a security awareness training programme.

BUT

Only **64%**
conduct formal training sessions (either in person or computer-based).

Cybersecurity training: are orgs doing enough?

No doubt about it: organisational awareness of cybersecurity education (and the need for it) has risen substantially over the past several years. And in this year's survey of infosec professionals, nearly all said their organisation has a security awareness training programme.

But having a programme is one thing. Running an effective programme is another.

Case in point: of the organisations with a programme, just over half (52%) provide company-wide training. A little more than a third (36%) train only certain departments and roles. And 11% said they are "very targeted" in their training approach, focusing on individuals rather than groups. (About 1% weren't sure how their organisation handles training.)

Even more concerning: only about 60% of respondents said their organisation delivers formal training sessions (either in person or computer-based) as part of their programme. Nearly 30% rely on simulated phishing attacks alone to teach their users.

This approach is problematic. Although simulated phishing attacks are a valuable tool, they're not enough. Phishing tests are just that: tests. They assess users' responses to a specific theme and a specific lure at a specific moment in time. They do not teach users who fail about the many and varied tactics attackers use in email-based phishing (and other social engineering scams).

In addition, phishing tests do not teach non-clickers at all—whether those users need training or not. Some, maybe even most, may recognise a simulated attack as suspicious and follow your organisation's policy for reporting and/or deleting the message. But others will ignore the same test. They might be too busy. Maybe the subject doesn't resonate with them. Or it may be some other reason. In any case, all users could benefit from formal training about this topic.

Unknowns like these show why organisations should dig beyond the surface to see what data really means. If we took the initial 98% figure at face value, it would seem that most organisations are doing the right thing when it comes to security awareness training. But when we look a little deeper, we find that the true state of security awareness training is not as clear.

When asked how frequently their organisations deliver formal training to employees, respondents indicated the following:

INTERNATIONAL

53%
of US organisations said they strictly use simulated phishing attacks to delivery security awareness training to end users, the highest of all regions surveyed.

81%
of Spanish organisations include formal training sessions in their programmes, the highest of all regions surveyed.

Frequency of Formal Training Sessions

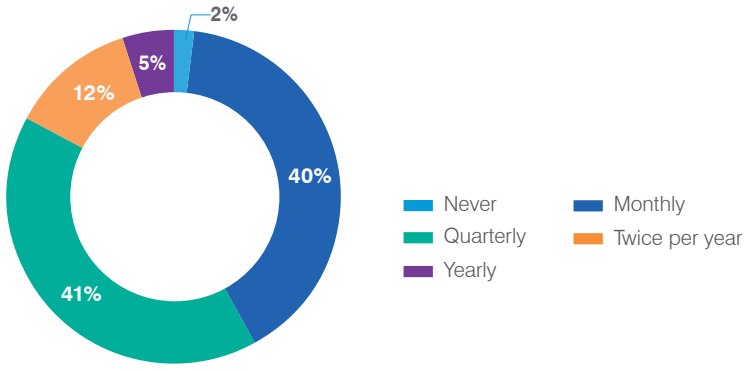

Figure 11.

INTERNATIONAL

37%

of Japanese organisations allocate less than an hour of formal training time to users in a year.

28%

of German organisations rely on once- or twice-a-year training to improve user behaviours.

Time Allocated to Formal Training Sessions Each Year

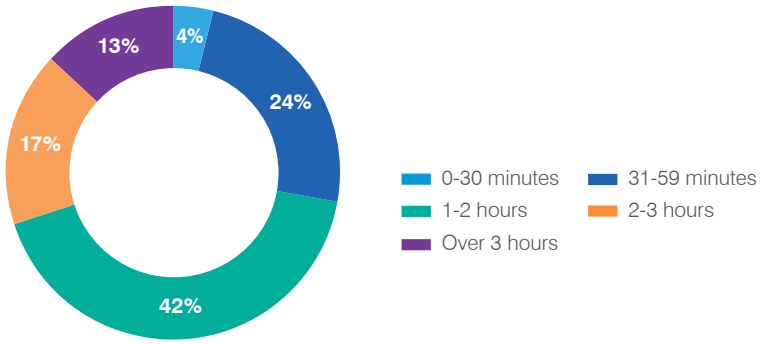

Figure 12.

As you think about how often you deliver formal training and how much time you allocate to these sessions, ask yourself this: are your people-centric defences as agile as attackers' offence? If you train only a few times a year and are not willing to devote the requisite time to your cybersecurity conversations, that answer is a clear-cut "no."

We know there are challenges to getting buy-in from your organisation and your users. You face obstacles to engagement. And you have other training considerations.

But if your interactions are infrequent and you can't identify and train users who present the most immediate risk, your organisation is doing less than attackers are. And that puts you at a major disadvantage.

Cybersecurity topics: are orgs covering enough?

We used the phrase "beyond the inbox" earlier in this report. And we'd like to introduce a similar phrase: beyond the phish. Here's a bit of the security awareness training philosophy behind these phrases:

- Don't rely on simulated phishing alone
- Don't focus strictly on email-based phishing
- Don't focus strictly on social engineering attacks

KEY FINDINGS

71% of organisations said they use an automated email reporting tool, but **only 28%** cover email reporting in their security awareness training programme.

INTERNATIONAL

Only **63%** of UK organisations train users about email-based phishing, the lowest of any region surveyed.

Just **15%** of German organisations train users about compliance-related topics, including GDPR.

90% of US organisations required or requested most of their users to work from home in 2020, but only **29%** train their employees about best practices for remote working.

Unfortunately, too many organisations have narrowed their security awareness training focus, as shown in the following chart.

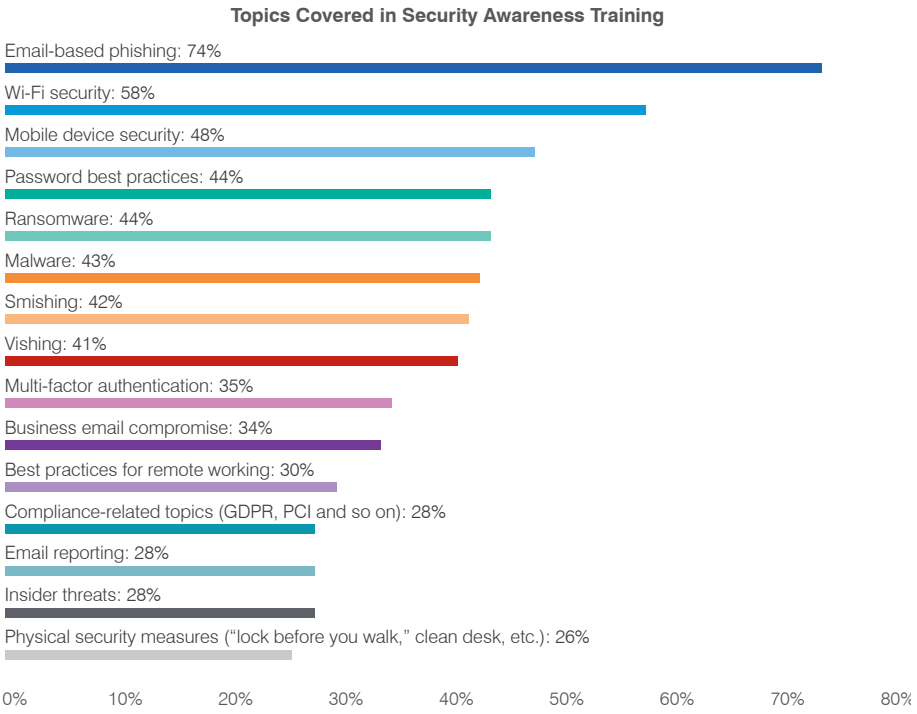

Figure 13.

Clearly, we think all users should have a strong grasp of email security. Attackers will not abandon phishing anytime soon (if ever). Given the ubiquitous nature of email in the workplace and beyond, email hygiene should be treated not as a cybersecurity skill or even a work skill, but as a life skill.

That said, organisations should consider the broader social engineering threat landscape when training users. Social engineering techniques are shared across many attack vectors beyond email. Users who can recognise and reject emotional manipulation tactics—regardless of where they appear—will work more securely across all communication channels, including email.

And organisations shouldn't stop there. Many cybersecurity behaviours affect organisational security. Simple passwords and password reuse are thorns in IT's collective side, for example. But fewer than 50% of organisations train users about password best practices, and only about a third cover multi-factor authentication in their programmes. Successful attacks often stem from a series of mistakes, committed by multiple people—inside and outside the inbox.

So many infosec professionals want users to behave differently. If you are one of them, the question to ask yourself is: am I doing all I can to bring about the changes I want to see?

KEY FINDINGS

55% of organisations punish users who regularly fall for phishing attacks (real, simulated or both).

82% of those using a consequence model said it has improved employee awareness.

INTERNATIONAL

82%
of US organisations use a consequence model, the most of all regions surveyed.

72%
of Australian organisations involve HR in disciplining repeat offenders.

35%
of Spanish organisations use a consequence model, the fewest of all regions surveyed.

32%
of UK organisations said their consequence model has not made a difference in employee awareness.

30%
of US organisations include termination as a consequence, the most of any region surveyed.

Consequence models: clarifying the conversation

There's one question our customers ask us that we don't have an answer for: how to structure a consequence model in their organisation. That's because our advice is simple: we don't recommend punishing users for honest mistakes. We feel that training should always be positioned as an opportunity, not a consequence.

But we recognise that some organisations feel the need to use a consequence model for "repeat offenders." And we wanted to know more about the escalation paths these organisations are using beyond follow-up training.

This year, we took training off the list of punishments and focused the conversation on penalties. We also asked our infosec survey respondents questions around timing and employees' responses to consequence models.

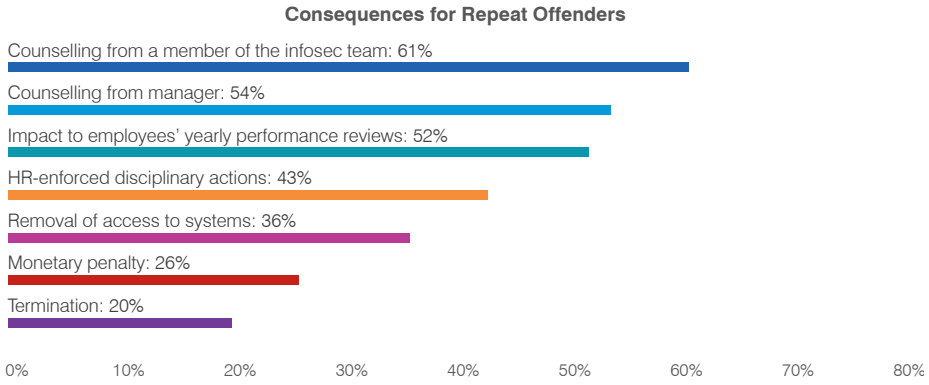

Figure 14.

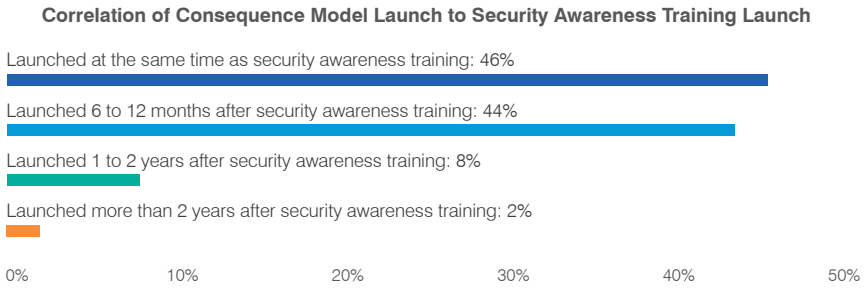

Figure 15.

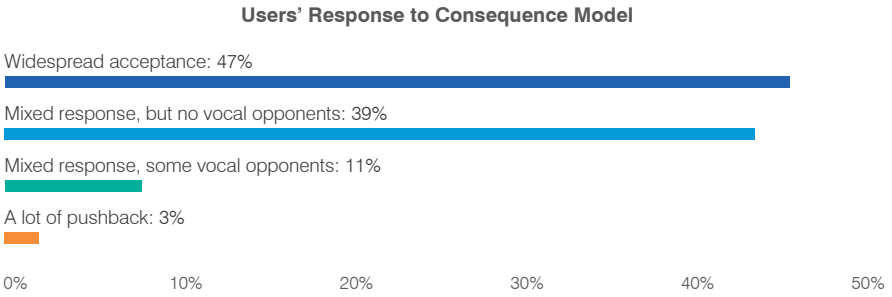

Figure 16.

Almost half of organisations said their consequence models have been widely accepted. But that still leaves more than half whose users are uncertain (or angry) about the punishments for cybersecurity mistakes.

Respondents who said their organisation is facing a lot of pushback said they are working to address their users' concerns. But user perception is an important factor to consider when introducing a consequence model. When punishments are part of the security awareness training equation, some (if not many) users could begin to view all aspects of your programme in a negative light.

SECTION 6

Conclusion: Take Notes, Take Action

80%

of organisations say security awareness training has reduced phishing susceptibility.

We know how hard organisations are working to protect their assets from cyber attackers. And we're thrilled to know that more than three quarters of infosec professionals feel that their security awareness training activities have led to measurable reductions in how vulnerable their users are to phishing.

But are organisations moving the dial as much as they could be? Are you?

We've explored a lot in this year's report, from both the infosec side and the user side of the cybersecurity awareness equation. The benchmark data, industry insights, and advice we've offered are designed to help you formulate an action plan. Here are a few key line items to consider adding to your to-do list:

Elevate users to stakeholder status

Executives and other decision-makers are important stakeholders in your organisation. But for security awareness training, users might be the most important stakeholders. A programme's success hinges on user success, but employees are often overlooked when it comes to buy-in. User engagement is critical if you want to make security a core part of your organisation's culture.

Here's how to avoid the pitfalls of a disengaged user base:

- Don't assume users understand cybersecurity lingo. If they don't recognise the terminology you use, you risk a disconnect from the start.
- Make it personal for users. Cybersecurity isn't just a "work thing," and users should understand that. Help them see the overall value of improving their security savvy—at work and at home.
- Be clear about expectations and communicate regularly with users. They should know about the goals of your programme and planned activities. (Obviously, this does not apply to the exact timing of phishing tests.)
- Make users feel empowered. They are often the only thing standing between an attacker's success or failure. Give your users the tools they need and teach them how to use them.
- Give users a safe space to learn, make mistakes, practise and learn some more. If you feel you must use a consequence model, first give employees the opportunity to learn how to avoid the behaviours they might be punished for.
- Highlight the benefits of participating in the programme and how better behaviours improve the organisation's security. In most cases, negatives are usually already crystal clear, and there's a focus on what users are doing wrong rather than what they are doing right. Flip the conversation and give users the opportunity to focus on the constructive aspects of learning about cybersecurity. They should clearly know what you are looking for from them and why you are asking them to make security a priority.

Keep benchmark data in perspective

We've hinted at this throughout the report, but it bears repeating. Benchmark datapoints like the ones we've shared about average failure and reporting rates are helpful from a comparative perspective. But if you're lagging behind the averages, that doesn't mean your organisation is "failing." And by the same token, if you're ahead, that doesn't mean you can ease off.

90%

of organisations factor threat intelligence into their security awareness training plans.

Marry threat intelligence and security awareness training

Figure 17.

It's great news that almost all organisations are using threat intelligence to inform their training decisions. But there is room for improvement. Ideally, organisations should do all three of the activities noted in Figure 17 to truly take advantage of threat intelligence.

Correlate awareness and training activities with other security functions

We often see security awareness training programmes operating independently of other security programmes. Ideally, all user-related security functions should intersect and inform. Email reporting is a great example of bridging two sides of organisational security.

But further opportunities are everywhere. For example, consider linking password training to metrics such as the number of password reset requests or the number of times it takes a user to create a new password when prompted. Another opportunity is tracking data loss prevention (DLP) violations alongside data security training activities.

Finding ways to associate training with other security initiatives offers many potential benefits:

- A more cohesive, results-oriented approach to security in general
- A clearer connection for users and better recognition of the impact their behaviours have on security
- Measurable, actionable information you can provide to your CISO and broader security team about your programme's impact on the organisation's overall security posture

APPENDIX

A. Infosec Survey: Country-by-Country Breakdown

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
Did your organisation experience a successful phishing attack in 2020?								
Yes	60%	48%	47%	56%	51%	66%	74%	57%
No	38%	49%	49%	42%	45%	29%	25%	40%
I don't know	2%	3%	4%	2%	4%	5%	1%	3%
Which impacts did your organisation experience as a result of successful phishing attacks in 2020? (Multiple responses allowed.)								
Loss of data	47%	63%	62%	61%	69%	59%	58%	60%
Credential/account compromise	47%	42%	60%	64%	37%	58%	55%	52%
Ransomware infection	67%	25%	49%	32%	49%	50%	55%	47%
Other malware infection	30%	42%	28%	25%	18%	32%	31%	29%
Financial loss/wire transfer fraud	23%	13%	13%	11%	12%	17%	35%	18%
How many of these social engineering attacks—successful or unsuccessful—did your organisation experience in 2020?								
Broad phishing attack (same email sent to multiple people)								
0	26%	34%	29%	26%	17%	18%	16%	23%
1-10	30%	33%	27%	36%	48%	38%	29%	34%
11-25	14%	16%	20%	14%	16%	22%	16%	17%
26-50	22%	8%	15%	2%	9%	5%	14%	11%
51-100	2%	6%	7%	6%	5%	6%	15%	7%
100+	6%	1%	1%	12%	5%	9%	8%	6%
I don't know	0%	2%	1%	4%	0%	2%	2%	2%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
Spear phishing/whaling (targeted attack)								
0	26%	43%	38%	46%	35%	32%	19%	34%
1-10	32%	30%	26%	20%	34%	32%	25%	29%
11-25	20%	12%	18%	12%	11%	14%	18%	15%
26-50	14%	10%	11%	8%	11%	9%	15%	11%
51-100	4%	2%	5%	12%	5%	10%	13%	7%
100+	4%	2%	1%	2%	3%	3%	8%	3%
I don't know	0%	1%	1%	0%	1%	0%	2%	1%
Business email compromise (for example, wire transfer fraud or invoice attack)								
0	34%	52%	32%	48%	22%	39%	20%	35%
1-10	30%	28%	21%	28%	37%	28%	15%	27%
11-25	16%	13%	21%	8%	17%	13%	21%	16%
26-50	10%	3%	15%	10%	7%	9%	19%	10%
51-100	8%	1%	8%	2%	12%	5%	18%	8%
100+	2%	1%	1%	4%	5%	6%	5%	3%
I don't know	0%	2%	2%	0%	0%	0%	2%	1%
Smishing (SMS/text message phishing)								
0	36%	52%	44%	42%	40%	38%	19%	39%
1-10	26%	21%	22%	26%	32%	25%	19%	24%
11-25	12%	10%	16%	8%	12%	16%	11%	12%
26-50	18%	9%	11%	14%	9%	8%	21%	13%
51-100	4%	3%	3%	6%	4%	10%	18%	7%
100+	4%	4%	2%	2%	2%	3%	9%	4%
I don't know	0%	1%	2%	2%	1%	0%	3%	1%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
Vishing (voice phishing via phone calls)								
0	32%	71%	36%	62%	54%	44%	23%	46%
1-10	28%	15%	26%	20%	22%	21%	16%	21%
11-25	14%	6%	17%	4%	12%	14%	13%	12%
26-50	18%	4%	8%	8%	7%	5%	18%	10%
51-100	6%	3%	8%	0%	2%	10%	16%	6%
100+	2%	0%	3%	6%	2%	6%	10%	4%
I don't know	0%	1%	2%	0%	1%	0%	4%	1%
USB drops (thumb drives weaponised with malicious software or code)								
0	38%	69%	37%	58%	48%	49%	20%	46%
1-10	20%	15%	28%	22%	26%	20%	16%	21%
11-25	14%	5%	15%	8%	11%	9%	16%	11%
26-50	20%	5%	9%	4%	10%	6%	21%	11%
51-100	4%	4%	5%	6%	2%	12%	14%	6%
100+	4%	1%	4%	2%	2%	3%	11%	4%
I don't know	0%	1%	2%	0%	1%	1%	2%	1%
Social media attacks (for example, pretexting or account takeover)								
0	28%	67%	38%	46%	42%	39%	14%	39%
1-10	32%	9%	21%	34%	32%	27%	21%	25%
11-25	16%	12%	20%	6%	8%	9%	18%	13%
26-50	12%	6%	7%	8%	11%	13%	18%	11%
51-100	6%	4%	8%	2%	2%	5%	18%	6%
100+	4%	0%	3%	4%	3%	7%	9%	4%
I don't know	2%	2%	3%	0%	2%	0%	2%	2%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
Did your organisation experience a ransomware attack in 2020 and pay the ransom?								
Yes	28%	18%	36%	18%	25%	44%	68%	34%
No, we were infected but did not pay	38%	35%	31%	36%	41%	31%	10%	32%
No, we were not infected	34%	47%	33%	46%	34%	25%	22%	34%
When you paid the ransom, what happened? (One answer allowed.)								
Regained access to data/systems after first payment.	50%	78%	56%	45%	56%	59%	76%	60%
Got hit with additional ransom demands. Paid again and eventually got access to data.	43%	17%	25%	44%	40%	39%	19%	32%
Got hit with additional ransom demands. Refused to pay and walked away without data.	7%	0%	14%	11%	4%	2%	3%	6%
Never got access to data, even after paying.	0%	5%	5%	0%	0%	0%	2%	2%
Does your organisation run a security awareness training programme?								
Yes	100%	95%	97%	98%	100%	96%	100%	98%
No	0%	5%	3%	2%	0%	4%	0%	2%
Which of the following topics are covered in your security awareness training programme? (Multiple responses allowed.)								
Email-based phishing	80%	75%	68%	88%	75%	63%	70%	74%
Smishing	52%	29%	32%	37%	50%	44%	47%	42%
Vishing	56%	26%	40%	37%	40%	48%	43%	41%
Wi-Fi security	58%	53%	55%	49%	64%	61%	67%	58%
Mobile device security	52%	44%	45%	49%	48%	47%	48%	48%
Password best practices	58%	51%	26%	39%	51%	43%	42%	44%
Multi-factor authentication	40%	29%	32%	33%	40%	36%	33%	35%
Insider threats	34%	32%	23%	16%	35%	22%	32%	28%
Ransomware	48%	44%	38%	39%	52%	47%	39%	44%
Malware	50%	46%	34%	41%	57%	41%	35%	43%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
Business email compromise	46%	25%	31%	39%	39%	28%	27%	34%
Email reporting	36%	22%	29%	24%	25%	31%	28%	28%
Compliance-related topics (like GDPR and PCI)	36%	23%	15%	27%	38%	31%	26%	28%
Best practices for remote working	32%	38%	14%	22%	36%	36%	29%	30%
Physical security measures (like “lock before you walk”)	32%	28%	19%	27%	23%	31%	25%	26%
Who participates in your organisation’s security awareness training programme?								
Everyone/company-wide training	48%	49%	52%	59%	42%	56%	63%	52%
Select departments/roles	38%	37%	34%	35%	49%	36%	22%	36%
Select individuals	12%	12%	14%	4%	9%	8%	15%	11%
I don’t know	2%	2%	0%	2%	0%	0%	0%	1%
What is your approach to security awareness training?								
Strictly use simulated phishing tests	26%	24%	30%	26%	11%	28%	53%	29%
Strictly use formal training sessions (in-person or computer-based)	42%	46%	39%	33%	44%	52%	30%	41%
Strictly use informational content (like emails and newsletters)	6%	8%	7%	10%	8%	7%	6%	7%
Use a mix of content types	26%	22%	24%	31%	37%	13%	11%	23%
How frequently does your organisation deliver or assign formal training (in-person or computer-based)?								
Never	3%	5%	0%	3%	0%	0%	0%	2%
Monthly	53%	29%	36%	42%	40%	29%	56%	40%
Quarterly	41%	49%	36%	32%	44%	52%	34%	41%
Twice a year	3%	14%	21%	16%	9%	14%	5%	12%
Yearly	0%	3%	7%	7%	7%	5%	5%	5%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
About how much time does your organisation allocate to formal training (in-person or computer-based) in a calendar year?								
0-30 minutes	6%	2%	8%	10%	3%	0%	2%	4%
31-59 minutes	27%	19%	21%	27%	16%	29%	24%	24%
1-2 hours	46%	34%	36%	40%	44%	48%	44%	42%
2-3 hours	6%	34%	25%	10%	17%	15%	15%	17%
More than 3 hours	15%	11%	10%	13%	20%	8%	15%	13%
Has your organisation been able to quantify a reduction in phishing susceptibility due to security awareness training?								
Yes	86%	79%	70%	72%	80%	83%	90%	80%
No	9%	15%	28%	19%	19%	11%	5%	15%
I don't know	5%	6%	2%	9%	1%	6%	5%	5%
Does your organisation use an automated email reporting tool?								
Yes	74%	62%	61%	80%	63%	71%	89%	71%
No	16%	25%	30%	14%	17%	19%	9%	19%
Not yet, but we're planning to implement one	10%	13%	9%	6%	20%	10%	2%	10%
Does your organisation's threat intelligence influence your security awareness training decisions? (Multiple answers allowed.)								
Yes, we use phishing tests that mimic trending threats	52%	45%	38%	56%	40%	33%	67%	47%
Yes, we train on specific topics that relate to attacks we are facing	50%	39%	62%	52%	55%	65%	47%	53%
Yes, we train specific individuals we know are being targeted	64%	35%	40%	38%	35%	33%	41%	41%
No, we do not adjust our training according to threat intelligence	6%	4%	7%	14%	13%	7%	5%	8%
N/A (I don't have access to my organisation's threat intelligence)	2%	3%	1%	0%	1%	3%	2%	2%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
At any point during 2020, did your organisation request or require more than 50% of your employee base to switch to a remote working model?								
Yes, we requested it	48%	46%	43%	64%	54%	47%	69%	53%
Yes, we required it	32%	31%	25%	20%	33%	45%	21%	29%
No	20%	21%	28%	14%	12%	7%	8%	16%
N/A (more than 50% of our employees always work remotely)	0%	2%	4%	2%	1%	1%	2%	2%
Does your organisation punish employees who regularly fall for phishing attacks (simulated or real)? Meaning, are there consequences (other than additional training) for "repeat offenders"?								
Yes	50%	43%	46%	66%	35%	60%	82%	55%
No	50%	47%	49%	30%	62%	36%	16%	41%
I don't know	0%	10%	5%	4%	3%	4%	2%	4%
What are the penalties (other than additional training) that employees face? (Multiple answers allowed.)								
Counselling from manager	52%	65%	52%	64%	37%	35%	71%	54%
Counselling from the infosec team	76%	60%	57%	58%	60%	63%	56%	61%
Impact to yearly performance reviews	64%	42%	54%	58%	37%	48%	61%	52%
Disciplinary actions (like a written warning) enforced by HR	72%	30%	30%	33%	51%	40%	45%	43%
Removal of access to systems	36%	30%	30%	45%	43%	33%	34%	36%
Monetary penalty	24%	16%	22%	36%	34%	18%	34%	26%
Termination	12%	26%	15%	15%	14%	27%	30%	20%
I don't know	0%	0%	0%	3%	0%	0%	0%	<1%
How did the implementation of a consequence module correlate to the launch of your security awareness training programme?								
Launched at the same time as security awareness training	44%	44%	50%	49%	34%	35%	67%	46%
Launched 6 to 12 months after security awareness training	40%	44%	43%	39%	63%	50%	29%	44%
Launched 1 to 2 years after security awareness training	12%	5%	7%	12%	3%	15%	4%	8%
Launched more than 2 years after security awareness training	4%	7%	0%	0%	0%	0%	0%	2%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
Has use of a consequence model led to an improvement in employee awareness?								
Yes, it's making a difference	88%	84%	72%	85%	80%	68%	95%	82%
No, it hasn't made a difference	12%	14%	22%	9%	20%	32%	4%	16%
Not sure, we haven't measured it	0%	0%	6%	6%	0%	0%	1%	2%
I don't know	0%	2%	0%	0%	0%	0%	0%	0%
How have employees responded to the implementation of your consequence model?								
For the most part, people seem to understand and accept the approach	48%	42%	48%	42%	46%	40%	60%	47%
A mixed response, but no overly critical opponents	44%	35%	28%	55%	43%	39%	27%	39%
A mixed response, with some fairly vocal opponents	8%	19%	20%	0%	8%	18%	7%	11%
A lot of pushback from employees	0%	2%	4%	3%	3%	3%	6%	3%
I don't know	0%	2%	0%	0%	0%	0%	0%	0%

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

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
What is phishing?								
Correct answer	66%	63%	64%	66%	63%	69%	52%	63%
Incorrect answer	17%	20%	23%	21%	17%	20%	37%	22%
I don't know	17%	17%	13%	13%	20%	11%	11%	15%
What is ransomware?								
Correct answer	42%	30%	26%	40%	28%	37%	29%	33%
Incorrect answer	35%	36%	31%	27%	30%	38%	55%	36%
I don't know	23%	34%	43%	33%	42%	25%	16%	31%
What is malware?								
Correct answer	72%	72%	58%	60%	75%	66%	54%	65%
Incorrect answer	17%	16%	24%	12%	13%	24%	38%	21%
I don't know	11%	12%	18%	28%	12%	10%	8%	14%
What is smishing?								
Correct answer	25%	60%	21%	19%	29%	27%	35%	31%
Incorrect answer	24%	16%	27%	25%	20%	32%	36%	25%
I don't know	51%	24%	52%	56%	51%	41%	29%	44%
What is vishing?								
Correct answer	22%	54%	18%	20%	26%	30%	35%	30%
Incorrect answer	18%	19%	28%	20%	18%	21%	32%	22%
I don't know	60%	27%	54%	60%	56%	49%	33%	48%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
I know the following to be true of emails (select all that apply):								
An email can appear to come from someone other than the person or company who sent it.	62%	55%	65%	30%	55%	58%	57%	55%
If an email includes logos and contact information from a company I know, it is safe.	22%	17%	17%	10%	20%	22%	34%	20%
If I click a link in an email, I will be taken to the website that matches the URL in the email.	21%	21%	21%	21%	23%	24%	30%	23%
Email attachments can be infected with dangerous software that can damage my computer.	63%	54%	63%	51%	64%	58%	52%	58%
All internal emails (like those from coworkers) are safe.	19%	22%	14%	6%	18%	15%	23%	17%
If a link in an email takes me to a file that's stored in a reputable cloud service (like Microsoft 365, Google Drive, or Dropbox), I know that file is safe.	11%	10%	8%	7%	13%	9%	15%	11%
If I have exchanged emails with someone multiple times, I know that is a safe contact.	21%	13%	16%	8%	19%	16%	21%	16%
I should be immediately cautious of any unsolicited email message.	59%	47%	53%	47%	60%	47%	41%	51%
At work, my organisation's security tools will stop all dangerous emails from reaching my inbox.	22%	15%	20%	19%	22%	20%	18%	19%
At home, my email provider will block dangerous messages so they don't reach my inbox.	16%	13%	20%	8%	15%	17%	16%	15%
I am not able to confidently choose any of these options.	7%	10%	7%	15%	5%	5%	4%	8%

	Australia	France	Germany	Japan	Spain	UK	US	Global Average
Which of these personal activities you do on your employer-issued laptop and/or smartphone? (Multiple answers allowed.)								
Check/respond to personal email	61%	59%	50%	53%	54%	51%	70%	57%
View/post to social media	33%	28%	29%	29%	30%	42%	45%	34%
Stream media (music, videos)	27%	20%	26%	19%	29%	35%	47%	29%
Shop online	36%	19%	31%	15%	28%	37%	46%	30%
Read news stories	47%	29%	35%	53%	42%	35%	42%	40%
Research (new products, travel)	38%	24%	29%	52%	36%	28%	38%	35%
Play games	13%	9%	10%	8%	11%	15%	27%	13%
None of these	18%	19%	26%	15%	23%	23%	11%	19%
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	27%	32%	31%	37%	27%	27%	52%	33%
View/post to social media	23%	19%	28%	21%	24%	29%	39%	26%
Stream media (music, videos)	17%	16%	24%	14%	20%	24%	40%	22%
Shop online	19%	18%	19%	16%	19%	23%	38%	22%
Read news stories	18%	12%	23%	24%	19%	16%	28%	20%
Research/complete homework	16%	12%	15%	26%	17%	14%	24%	18%
Play games	6%	9%	11%	8%	9%	10%	23%	11%
None of these	58%	51%	48%	49%	55%	48%	25%	48%

C. Industry Failure Rates by Simulated Phishing Template Style

Different views of data can reveal new insights. This more granular look at industry failure rates—by template style, matched up against overall failure rates—shows the widespread struggle for users to identify and avoid attachment-based phishing tests. But these very high average failure rates—including those as high as 26% to 32%—don't generally influence overall failure rates. And that tells us something else as well: that attachment-based tests are not frequently used in many organisations.

As we cautioned in the main report, an overall average failure rate can mask potential areas of risk. Our data shows that susceptibility to attachment-based phishing attacks could be a hidden issue for many organisations. Regular testing and training about these types of threats could prove very beneficial.

	Average Failure Rate			
Industry	**Link-Based Tests**	**Attachment-Based Tests**	**Data Entry-Based Tests**	**Overall**
Automotive	11%	14%	4%	10%
Business Services	12%	21%	3%	11%
Construction	13%	20%	6%	11%
Education	13%	32%	4%	13%
Energy/Utilities	11%	22%	4%	12%
Engineering	20%	24%	2%	16%
Entertainment/Media	11%	16%	3%	9%
Financial Services	12%	17%	3%	11%
Food & Beverage	11%	17%	4%	10%
Government	11%	15%	3%	11%
Healthcare	11%	19%	4%	10%
Hospitality/Leisure	11%	10%	4%	9%
Insurance	14%	23%	3%	12%
Legal	11%	10%	2%	9%
Manufacturing	12%	24%	4%	11%
Mining	18%	22%	5%	13%
Retail	12%	26%	4%	11%
Technology	13%	22%	4%	11%
Telecommunications	16%	21%	5%	14%
Transportation	11%	28%	4%	12%

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance 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.

0400-004-01-01 1/21