2021 User Risk Report

A People-Centric View of Vulnerability

FAST FACTS

11%
average failure rate on phishing tests in 2020

33%
average overall view rate of simulated attacks

57%
percentage of workers who check personal email on work-issued devices

51%
percentage of users who know that they should treat any unsolicited email with caution

67%
percentage of users who could not identify the correct definition of ransomware

13%
The average rate at which user report simulated phishing emails as suspicious

Introduction

Behind almost every cyber attack is someone who fell victim to it. In each case, someone has clicked the wrong link, opened the wrong file or trusted the wrong email. In the 2021 Verizon Data Breach Investigations Report[1], 85% of breaches involved human error.

Despite constantly changing tactics, evolving malware and new forms of deception, people have long been the single most critical variable in cybersecurity. That's because today's attacks target people, not just technology.

While your people are your greatest asset, they're also your biggest security risk—and all too often, your last line of defense. Your Very Attacked People™ (VAPs)—those users facing the highest volume of attacks, the most advanced threats or most sophisticated tactics—aren't always the people you think they are, and they require special consideration.

For a better understanding of users' cybersecurity awareness and habits, we used our security awareness data and surveyed users around the world to gauge two key aspects of user vulnerability: what they know and what they do.

This report highlights user awareness and knowledge gaps that, if changed, could have a hugely positive impact on your cybersecurity posture. Based on those insights, we recommend tangible actions you can take to empower your people and build cyber resilience into your workforce.

What Users Are Clicking

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 organizations continued to prioritize phishing awareness activities.

Another positive: The average failure rate decreased in our most recent data set. Organizations experienced an average failure rate of 11% in 2020, compared to 12% in 2019.[2]

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. And some tactics are much harder to avoid.

[1] Verizon. "Verizon. 2021 Data Breach Investigations Report." May 2021.

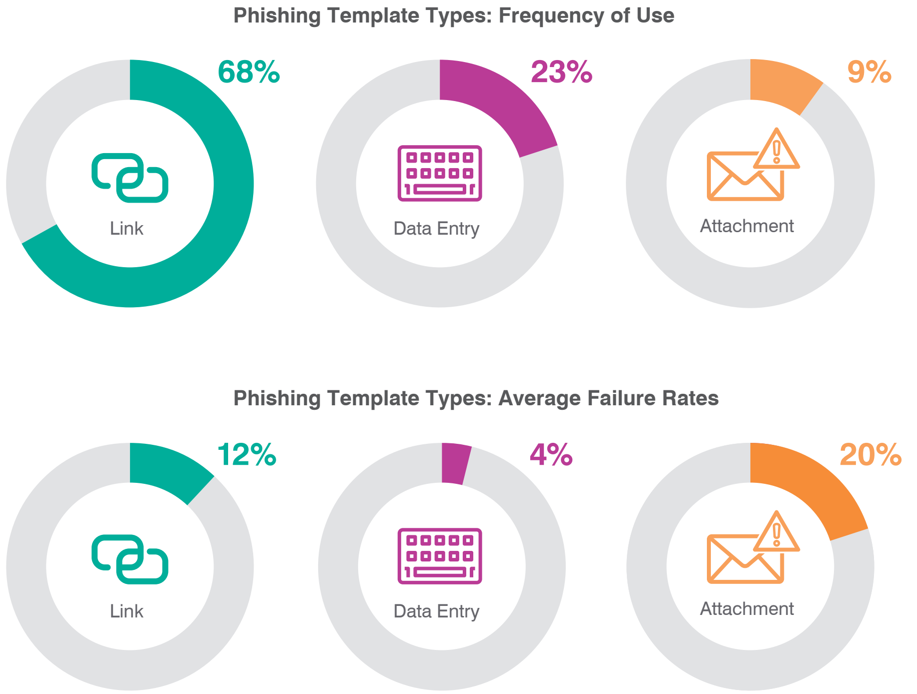
[2] We calculate average failure rates at the organizational level rather than the user level, giving equal weight to each organization's average failure rate rather than equally weighting each user's failure rate. This approach helps to eliminate the sway of large organizations and high-volume programs,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

(For a more complete view of user strengths and vulnerabilities, organizations should understand not just the threats users are clicking or avoiding, but which ones they are actively reporting as suspicious. We cover email reporting metrics in the section **What Users Are Reporting** on Page 6.)

Failure rates, by simulated phishing template type

Most phishing simulation tools offer customizable email templates that let organizations test different phishing tactics. Our customers can choose a from variety of themes and lures, including those that mimic real-world threats uncovered by our threat researchers. The templates fall into three primary types: link-based, data entry-based and attachment-based. As in the prior two years, organizations heavily favored simulated attack templates in 2020 that used URL hyperlinks.

“Failed” data-entry tests in Figure 1 refer to cases in which users submitted data after clicking a link in the simulated attack.



Phishing Template Types: Frequency of Use

Phishing Template Types: Average Failure Rates

Figure 1

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 often see—and use—these cloud-based services. That familiarity breeds a sense of trust that works to attackers’ advantage.

But as shown in Figure 1, 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: Organizations should evaluate whether they are doing enough to test how well users can recognize 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 assessing and educating 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, mixed in with other security awareness activities.

Trickiest campaign template themes

Organizations 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 "successful" themes of 2020 phishing tests. These themes were sent to at least 2,300 users (and in some cases, many more).

Themes that Tricked the Most People into Clicking

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 often-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.

Fast-changing conditions at the onset of the pandemic only reinforced how important agility is. To keep up with emerging threats and unfolding events, organizations quickly began to incorporate pandemic-related testing and education 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 section 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 often used COVID-related templates, average failure rates ranged from less than 1% to just over 20%.

Failure rates, by industry

Among our customers, manufacturing organizations 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 organizations and at least 150,000 simulated phishing attacks.

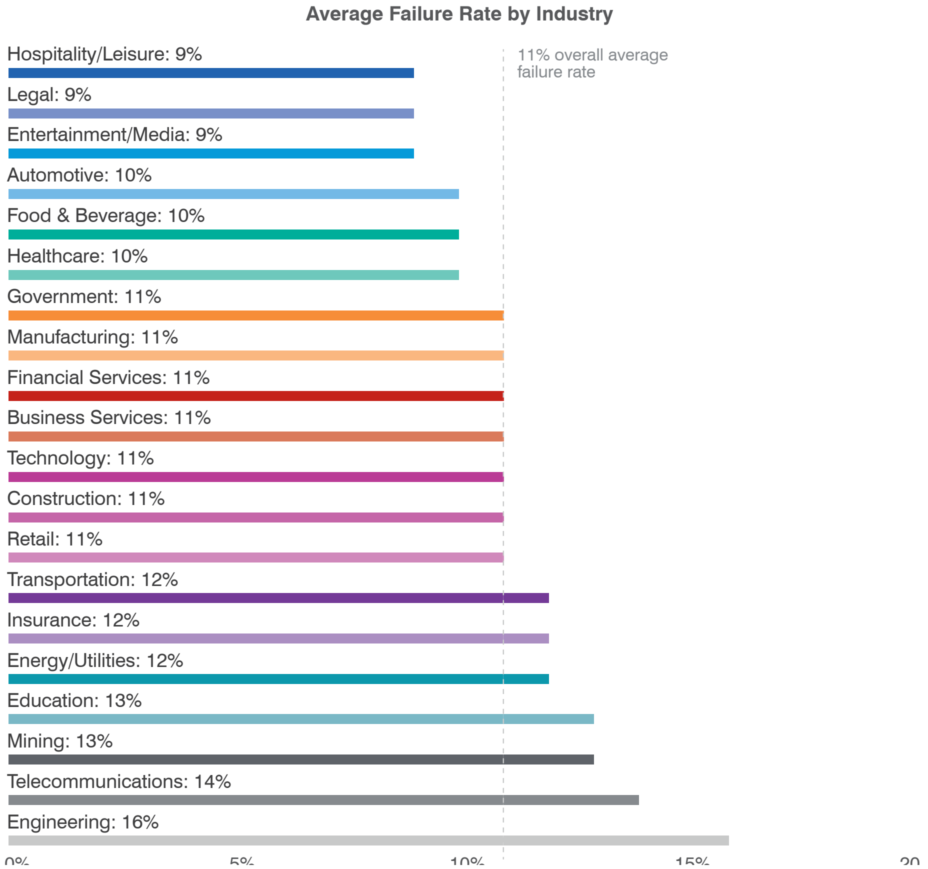

Average Failure Rate by Industry

Figure 2

Notable Mentions: Less-Active Industries

The most active industries we analyzed 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 math: more organizations + more users = more tests.

But that isn't always the case. On average, each organization in our study sent eight simulated phishing campaigns in 2020. The top five most active industries sent an average of seven to 10 campaigns.

Organizations 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 organizations 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 24/7. 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.

Failure rates, by business function

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

Department-level failure rates offer a finer-tuned view of potential weak spots within an organization. Attackers often target individual inboxes and email aliases.

An organization-level failure rate alone will not reveal roles and teams that may be struggling.

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

Figure 3 compares the average failure rates of 20 different departments, ranked lowest to highest.[3]

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.

KEY FINDINGS

R&D was the worst-performing department in last year's State of the Phish 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.

Average Failure Rate by Department

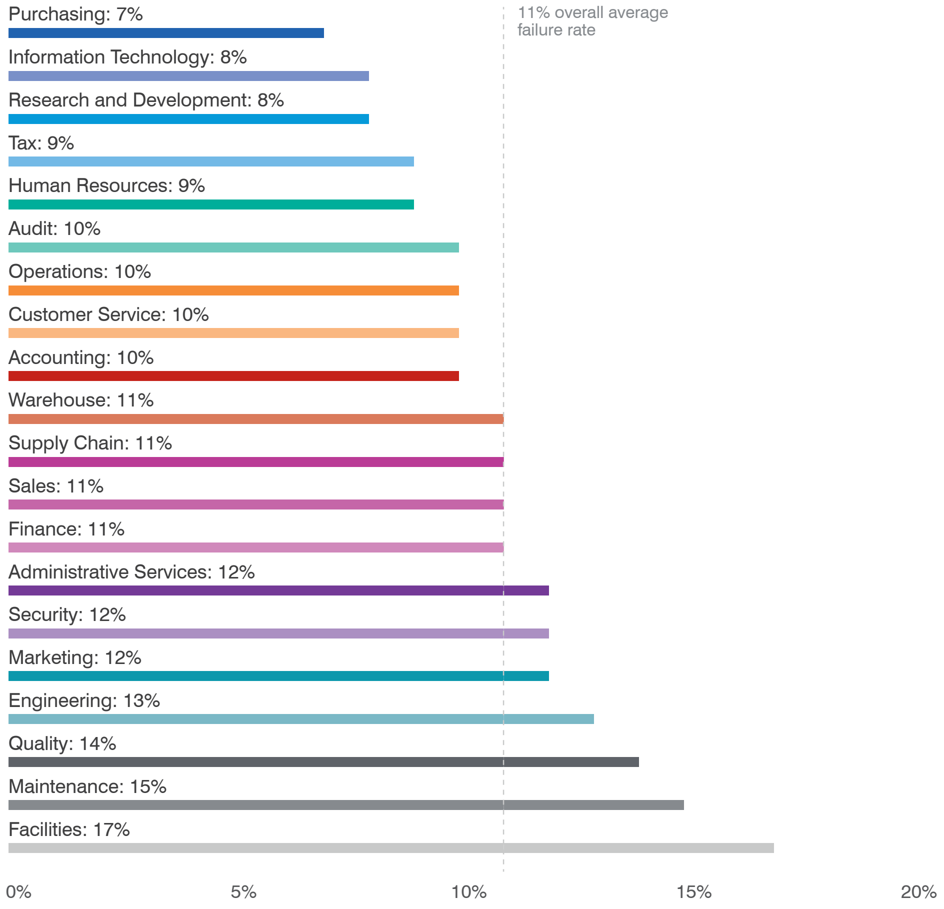


Figure 3

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

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

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

PhishAlarm customers saw an average resilience factor of 1.2

What Users Are Reporting

One-click email reporting can be a critical tool in your security arsenal, saving time and back-and-forth associated with traditional abuse mailboxes. Here are just a few of the benefits for organizations that make reporting suspicious emails easy for users:

- Empower users to apply email security behaviors and become active participants in your security efforts
- Allow users to quickly and easily alert designated infosec team members to suspicious emails
- Enhance your security culture by promoting a collaborative relationship between users and security teams
- Correlate failure rates and reporting rates of phishing simulations so you can quantify resiliency
- Get visibility into the types of real-world threats that are evading perimeter defenses
- 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.)

Calculating your "resilience factor"

Last year, we discussed the 70:5 rule as a stretch goal for organizations 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. Organizations 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.

The average reporting rate among our customers already tops the average failure rate, delivering a positive resilience factor:

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

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

Resilience factors, by industry

Table 1 notes the average reporting rates, average failure rates and resilience factors for the 20 industries covered in Figure 2.

The average failure rates in Table 1 are slightly different than those in Figure 2. 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	20%	11%	1.8
Energy/Utilities	18%	11%	1.6
Insurance	17%	10%	1.7
Legal	17%	8%	2.1
Engineering	16%	16%	1.0
Automotive	15%	8%	1.9
Business Services	14%	11%	1.3
Technology	13%	12%	1.1
Government	13%	10%	1.3
Mining	13%	13%	1.0
Food & Beverage	11%	11%	1.0
Manufacturing	10%	10%	1.0
Healthcare	10%	10%	1.0
Entertainment/Media	10%	9%	1.1
Transportation	10%	12%	–1.2
Telecommunications	9%	14%	–1.6
Construction	9%	11%	–1.2
Retail	9%	13%	–1.4
Education	6%	12%	–2.0
Hospitality/Leisure	5%	10%	–2.0

Table 1

Spotlight: Users Actively Reported Attacks from the Wild in 2020

Our PhishAlarm button works in conjunction with PhishAlarm Analyzer, which uses our threat intelligence and detection to spot phishing attacks in real time.

The contents of emails reported via PhishAlarm are scanned by Proofpoint scoring engines, and all URLs and attachments are “detonated” in our sandbox. In this process, most reported emails are automatically classified as either malicious/spam or bulk/benign. Organizations can then assign custom content rules to classify further if desired.

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)
- 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 auto-classified as bulk/low-risk emails, saving time 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).

What Users Know

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 Table 2 on page 8 rose among working adults year over year. And awareness of malware decreased by only 1%, essentially holding steady.

But this year’s findings also show that you should never assume your users understand the cybersecurity terms you regularly use. Conducting baseline education for new hires can help build that foundation for more advanced concepts.

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 behaviors 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.

Cybersecurity terms

What is PHISHING?	✓ Correct 63%	✗ Incorrect 22%	? I Don't Know 15%	At 52%, U.S. 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?	✓ Correct 33%	✗ Incorrect 36%	? I Don't Know 31%	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?	✓ Correct 65%	✗ Incorrect 21%	? I Don't Know 14%	Spanish workers led their global counterparts, with 75% answering correctly. (Though that's shy of their 80% mark from last year.) U.S. workers underperformed the global average. Just 54% answered correctly, and nearly 40% chose incorrect answers.
What is SMISHING?	✓ Correct 31%	✗ Incorrect 25%	? I Don't Know 44%	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?	✓ Correct 30%	✗ Incorrect 22%	? I Don't Know 48%	Last year, only 25% of global workers answered this question correctly. Awareness is up nearly 70% since our 2018 survey. At 54%, French workers were three times as likely as German workers (18%) to answer this question correctly.

Table 2

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 recognize 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 respondents in the U.S. believe emails with familiar logos are safe

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

22%
of Australian and Spanish workers think their organizations 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

Email concepts

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.

Email Survey Results

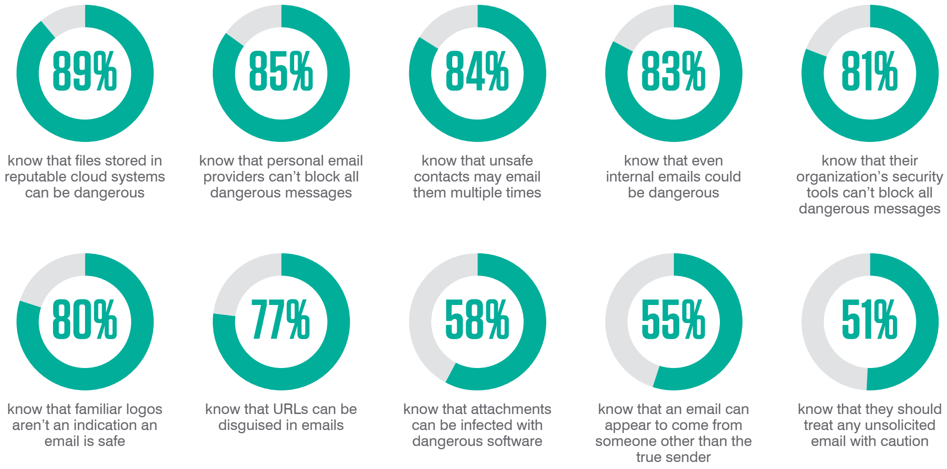


Figure 4

Just 8% of global respondents lacked the confidence to choose an answer on our list. And it's excellent to see more than three quarters of respondents correctly recognizing many danger signs.

Naturally, there is room for improvement—especially when it comes to recognizing 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 organization.

What Users Are Doing (With Work-issued Devices)

We surveyed users about their personal habits and behaviors 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 organizations 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 organizations—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.

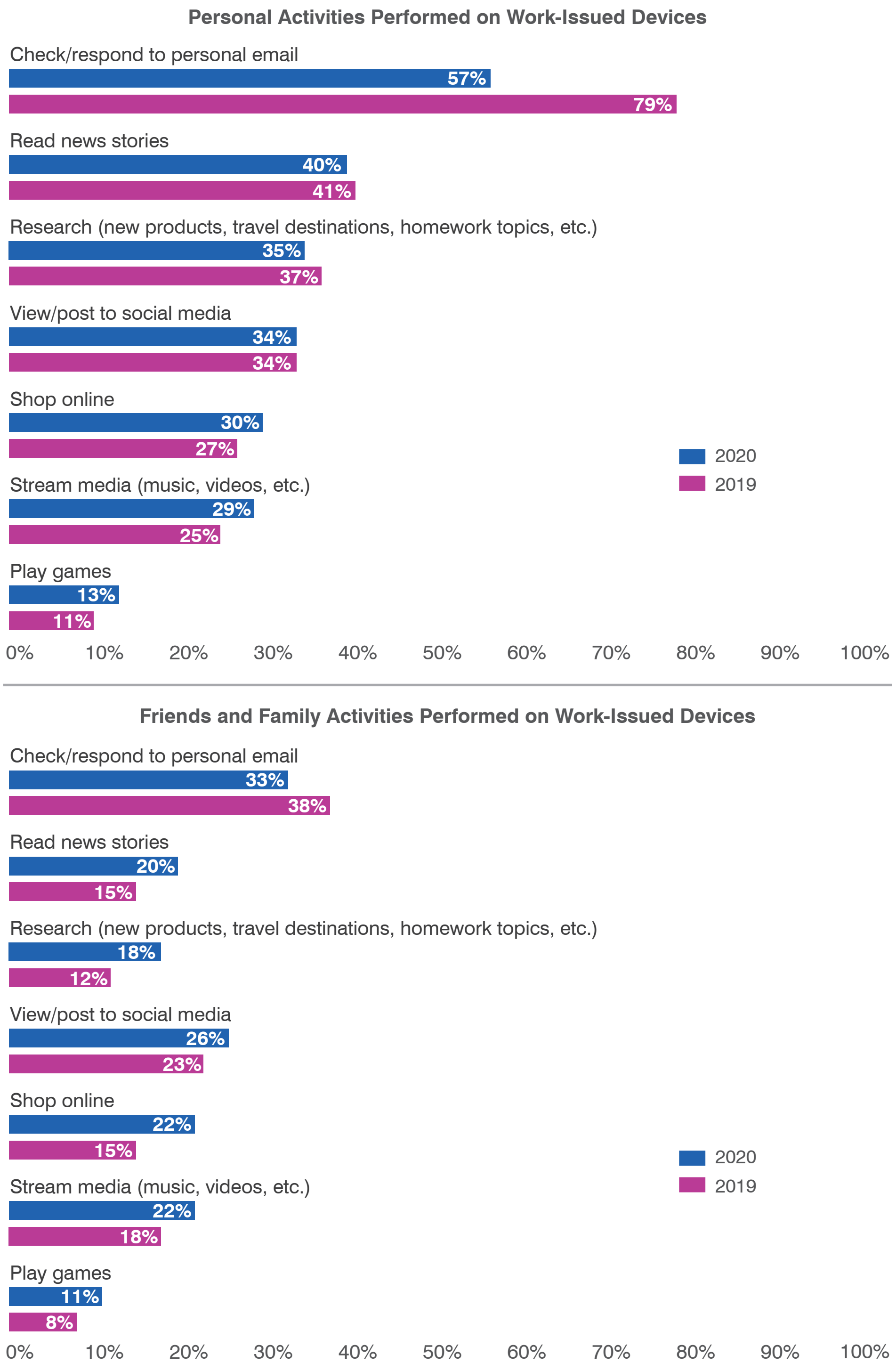
INTERNATIONAL

75%

of U.S. 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 behaviors (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%).



Personal Activities Performed on Work-Issued Devices

Friends and Family Activities Performed on Work-Issued Devices

Figure 5

Conclusion and Recommendations

Organizations need to take a more inward, people-centric view of their vulnerabilities and empower users to become a stronger line of defense.

Recognize that any user could be a target at any time. Develop a security awareness program that uses user-level visibility into your VAPs and real-life threat intelligence to provide organization wide and targeted security awareness.

To that end, here are three foundational steps you can take for a stronger last line of defense:

Commit to building a culture of security

To truly make a change—meaning a mindset and behavior shift that has a positive, day-to-day impact on your organization—you must commit to bringing cybersecurity to the forefront. Treat your users as an informed line of defense that you can activate.

At any moment, anyone in your organization can improve your security posture.

That's why building a security culture is critical. Everyone from the top down in your organization should know how they can be more cyber-aware, and how it benefits them at home. A broad, organization wide security awareness program will help you do that.

Know your users

We see many variations across industries, departments and user populations. Understanding what those differences mean for your organization allows you to better combat the specific ways attackers are targeting your people.

You should understand:

- **Who in your organization is being targeted** in higher volumes or by more advanced threats. The answer is not as simple as looking at the top tiers of your org chart.
- **What types of attacks they are facing.** Knowing the lures and traps attackers are using can help you better position your defenses.
- **What users think—and how they work.** Understanding your organization's business needs and processes is critical to building a security awareness program that works. For example, your training program may teach people to avoid so-called "shadow IT" tools. But if your internal tools don't allow them to work with outside vendors, that training may be unrealistic and demoralizing. Surveys and empathy towards users can help you better understand the real-world implications of your training program.
- **How to minimize risk if these attacks get through.** Use the information you've gathered to deliver the right education to the right people at the right time. And apply adaptive, risk-based controls to your most vulnerable users keep them protected—and safeguard the data, systems and resources they have access to.

Keep improving

Building a security culture takes ongoing effort and attention. Plan for regular education and awareness activities, and be responsive to changes in the threat landscape (and your organization).

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

Understanding general phishing trends is important. Having benchmarks to measure your users against is valuable. But other organizations' data isn't as important as your organization's data. To improve your own security posture, you must understand your own unique threat climate.

Learn more about how Proofpoint can help you change user behavior and create a strong last line of defense at **proofpoint.com/security-awareness.**

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 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**.