proofpoint.

ANNUAL REPORT

2020 User Risk Report

Exploring Vulnerability and Behavior in a People-Centric Threat Landscape

proofpoint.com

INTRODUCTION: WHY THIS REPORT MATTERS

Your cybersecurity posture is only as strong as its weakest link. And in today's people-centric threat landscape, that means your users. They are your greatest asset, your biggest risk and your last line of defense from threats.

That's because attackers have shifted their focus from infrastructure to people. No matter how well you're managing your IT infrastructure, you can't patch your way out of these people-centered attacks.

Proofpoint customers' end users reported nearly 9.2 million suspicious emails in 2019, an increase of 67% over 2018. In Q3 2019 alone, users alerted their security teams to thousands of serious threats, including:

- Nearly 20,000 credential-based phishing attacks
- More than 4,000 attacks with malware payloads, including high-severity remote access Trojans (RATs), backdoors and stealers

Attackers' targets and methods are constantly evolving. Your Very Attacked People™ (VAPs)—those users facing the highest volume of attacks, the most advanced threats or most sophisticated tactics—aren't always your VIPs.

For a better understanding of users' cybersecurity awareness and habits, we surveyed users around the world to gauge two key aspects of user vulnerability: what they know (or don't know) and what they do.

This report highlights user awareness and knowledge gaps that, if left unrectified, could hurt your cybersecurity posture. Based on those insights, we recommend specific action you can take to empower your people and build cyber resilience into your workforce.

Table of Contents

Key Findings

Here are highlights of this year's survey.

Many users are unaware of key cybersecurity concepts

- Just 61% correctly identified the definition of phishing from a multiple-choice array.
- Just 31% correctly identified the definition of ransomware.
- Millennials underperformed other age groups (including baby boomers) in identifying key terms.

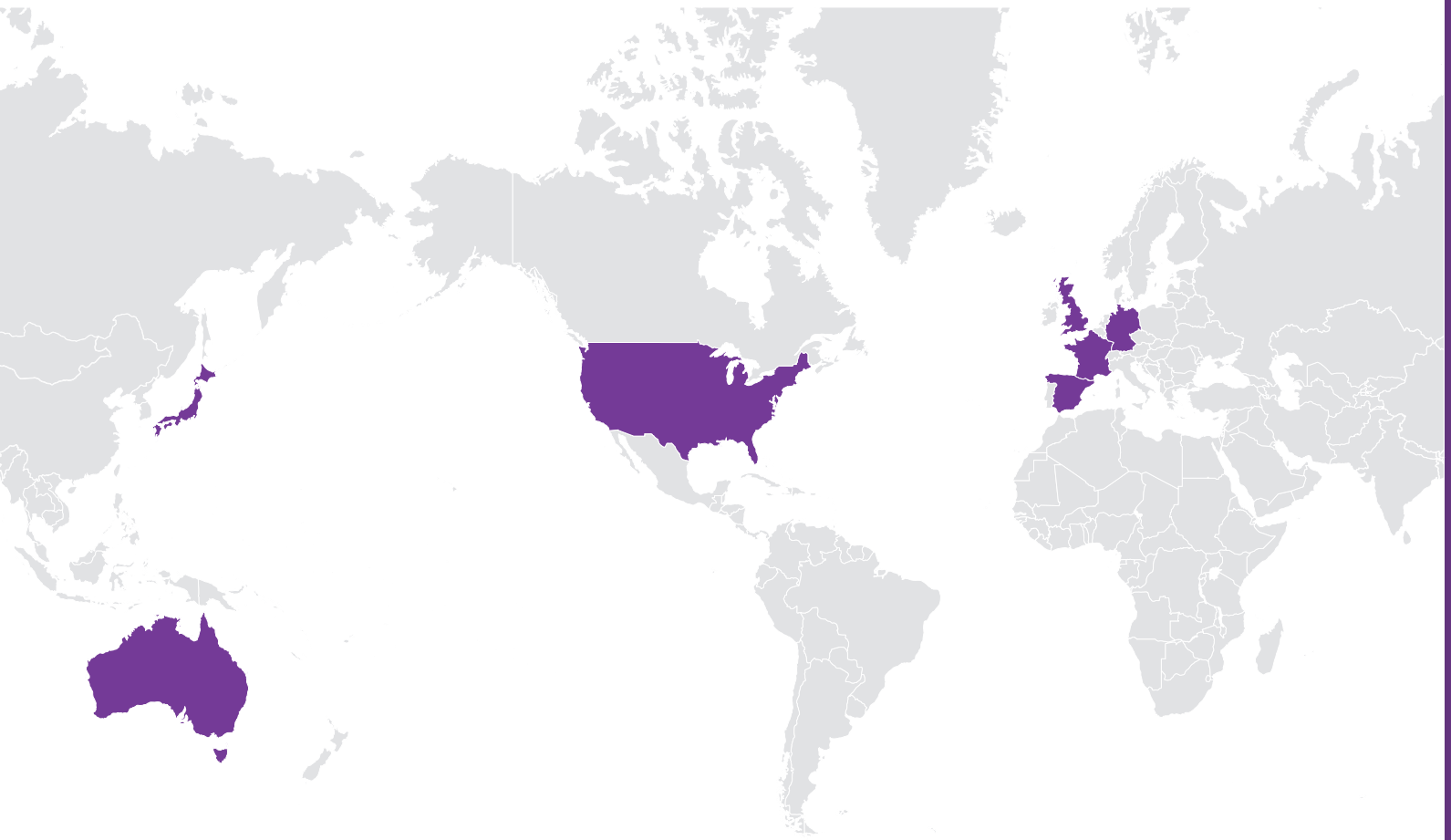
Many users do not apply key cybersecurity best practices:

- 45% admit to password reuse.
- More than 50% do not password-protect home Wi-Fi networks.
- 32% do not know what a virtual private network (VPN) is.
- 90% of working adults admit to using employer-issued devices for personal activities.
- Nearly 50% allow friends and family to access their work devices.

Methodology and Scope

Working with a third-party research firm, we polled more than 3,500 working adults across the United States, Australia, France, Germany, Japan, Spain and the United Kingdom. Our survey questions sought to assess following:

- How well users understood these commonly used cybersecurity terms: phishing, ransomware, malware, smishing (SMS/text phishing) and vishing (voice phishing)
- How well they recognized the limits of technical safeguards in identifying (and fixing) malware-related incidents
- Whether younger workers have an edge over older workers in cybersecurity knowledge



The Results

We found that many workers remain unaware of fundamental best practices. This lack of knowledge can worsen the phishing threat and undermine your security posture.

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

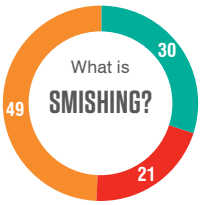
Those in security and IT must wonder: who doesn't know what phishing is? The (unfortunate) answer is this: countless numbers of people.

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

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

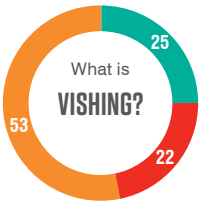
Here is a global breakdown of their answers.

- Only 49% of U.S. workers answered correctly.
- German workers were most likely to recognize this term (66%).

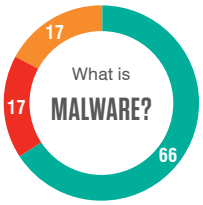


- Awareness of this term is up year over year.
- Just 25% of respondents answered correctly in our prior survey.
- French workers were top performers: 54% answered correctly.

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



- Last year, only 18% of global workers answered this question correctly.
- At 48%, French workers were about twice as likely as their global counterparts to recognize this term.



- Nearly 80% of Spanish workers answered this question correctly.
- Nearly 30% of U.S. workers believe malware is a type of hardware that boosts Wi-Fi signals.

Correct Incorrect I don't know

GLOBAL SNAPSHOT

14%

of U.K. workers never lock their smartphones.

45%

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

21%

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

Cybersecurity behaviors: how are workers putting organizations at risk?

Email security should be a top concern of individuals and organizations alike. But users also need to recognize that decisions they make outside of their inboxes can put them (and your organization) at greater risk of phishing attacks and other threats. Smartphones and Wi-Fi are potential weak links

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

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

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

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

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

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

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

Shadow Backups

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

GLOBAL SNAPSHOT

44%

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

15%

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

U.S. respondents take top marks with VPN usage:

51% have at least one installed.

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

VS

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

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

Technical safeguards: more misplaced trust

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

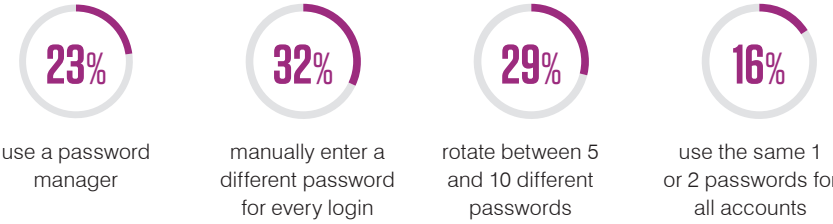
- 66% of survey respondents believe that keeping anti-virus software up to date will prevent attackers from accessing their devices.
- 51% think that their IT teams will be automatically notified if they accidentally install a virus or other malicious software on their work computer.

Passwords and VPNs: misused and misunderstood

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

Password reuse, when part of a breach replay attack, is a frequent conduit of email account compromise (EAC) and cloud account compromise. Cyber criminals often use stolen passwords from one account on others, counting on some level of password reuse.

Password Habits



No Room for Compromise

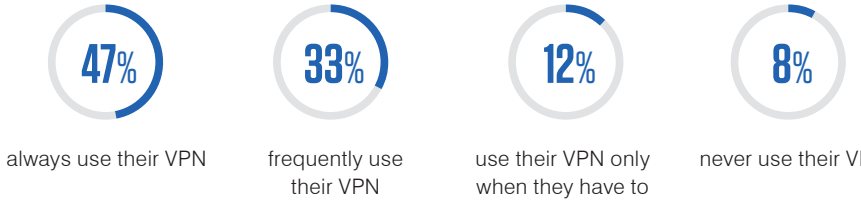
In a study of more than 1,000 cloud service tenants with more than 20 million user accounts, more than 15 million unauthorized login attempts took place in the first half of 2019 alone. More than 400,000 of these attempts resulted in successful logins. In all, about 85% of tenants were targeted by cyber attacks, and 45% had at least one compromised account in their environment.[1]

VPNs and zero-trust alternatives provide a way to protect sensitive data and accounts. Unfortunately, many users—and apparently, the organizations they work for—haven't gotten the memo.

[1] Proofpoint. "Cloud Attacks Prove Effective Across Industries in the First Half of 2019." September 2019.

VPN Adoption on Work and Personal Devices

VPN Usage Once Installed



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

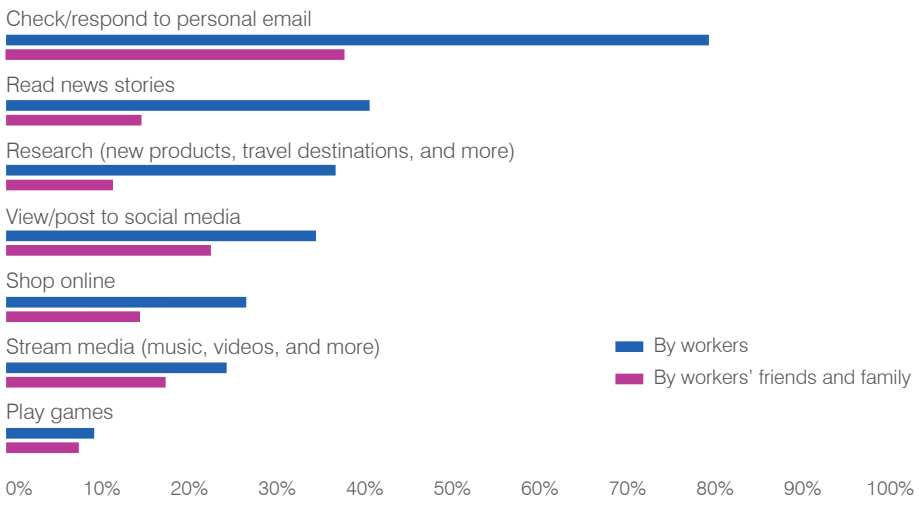
Many, if not most, organizations spell out acceptable-use policies for work-issued devices. But unless access is locked down, there's no telling whether workers are actively following those guidelines. And as the chart shows, those who have access freely use their devices for personal activities. If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

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

Sharing is Scaring

About 50% of respondent said they give friends and family access to their employer-issued devices.

Personal Activities Performed on Work-Issued Devices

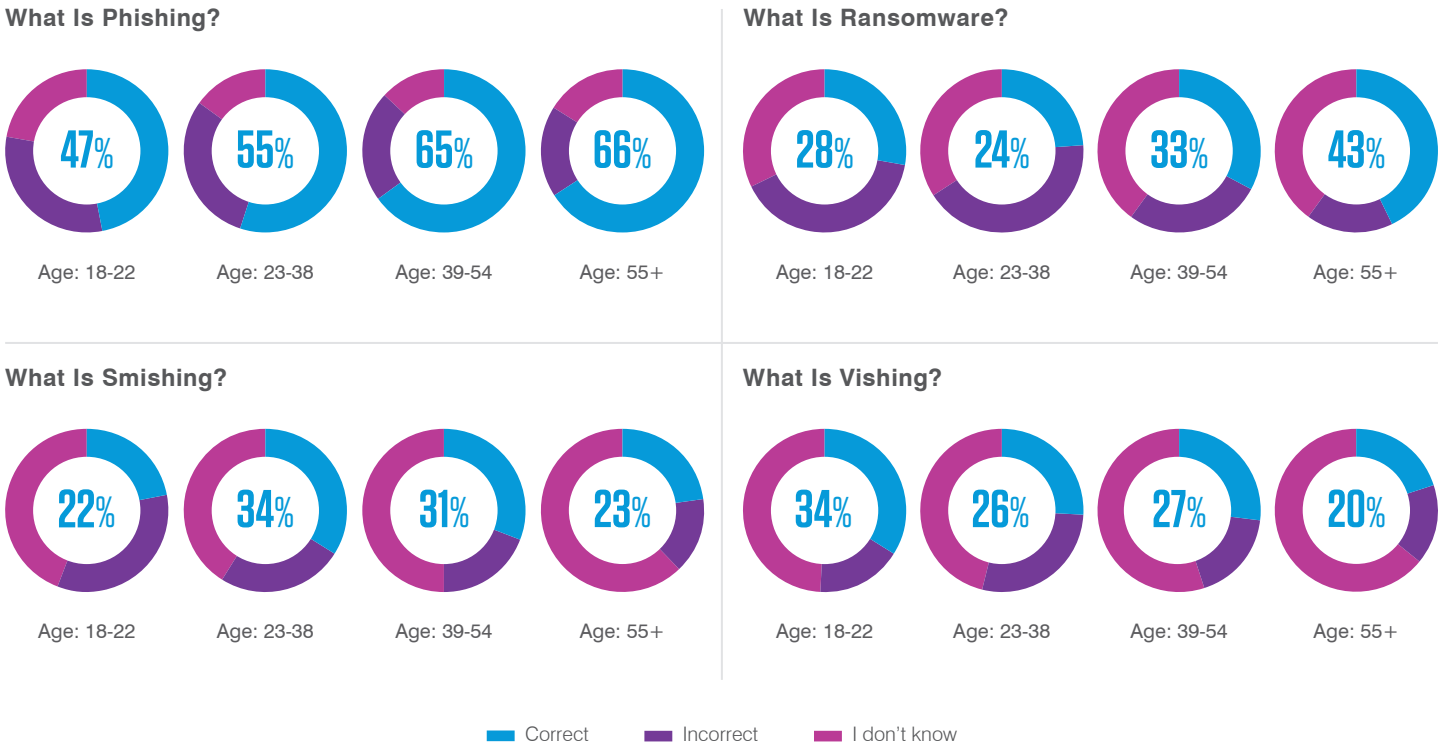


Percentage of workers who use (or permit use of) employer devices for personal tasks

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

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

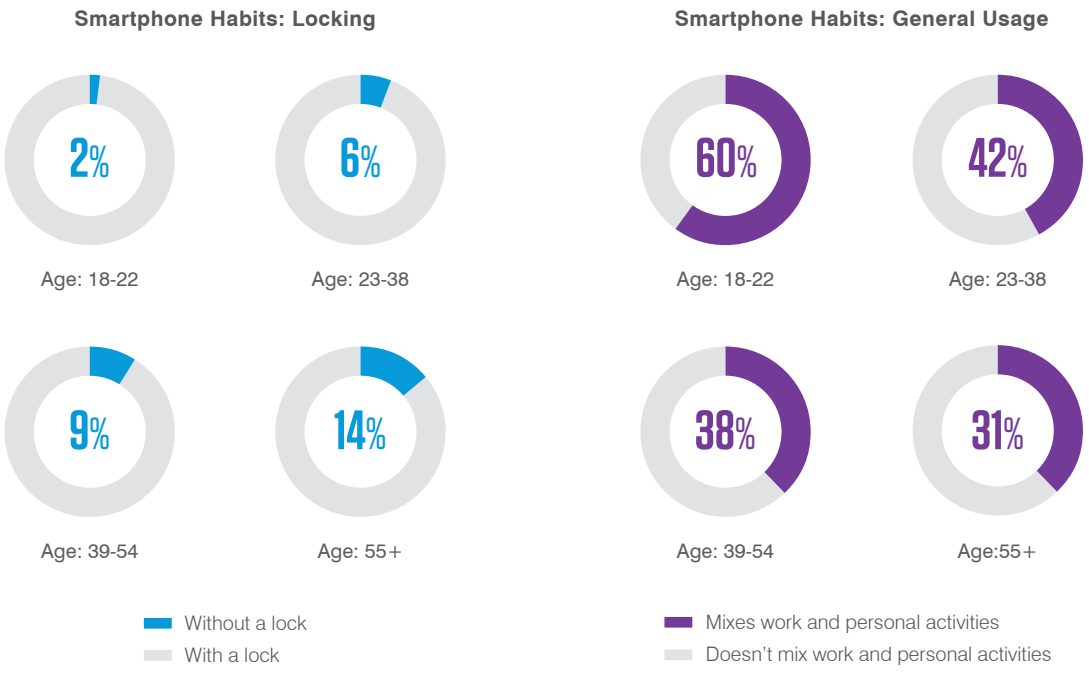
That's not always the case. Here's how younger workers and the much-discussed millennial generation compare to older employees—including baby boomers—on six key questions.[2]



OK Boomers

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

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



Blurred Lines

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

Key takeaway: put assumptions aside

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

The same thing happens in the workplace.

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

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

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 training program that uses user-level visibility into your VAPs and real-life threat intelligence to provide organization-wide and targeted security awareness training.

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

1. Commit to building a culture of security

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

Here's why:

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

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

2. Answer the three W's

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

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

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

This exercise helps you defend against your most pressing and timely threats.

Assessing vulnerabilities at a more granular level and matching that up against your threat intelligence allows you to pinpoint where perfect storms are brewing: the intersections of susceptibility and exposure.

3. Make time for agility

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

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

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

Attackers' targets change over time. We recommend identifying your VAPs monthly, if not weekly. By pairing granular analysis with organization-wide training, 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.

To learn more about how Proofpoint can help empower your people and build cyber resilience into your workforce, take our free **People Risk Assessment**. You'll learn:

- Which users have the best and worst security knowledge
- How your organization's score compares to others in your industry
- Detailed information on your people-centric risk posture broken down by department, region and more

LEARN MORE

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

ABOUT PROOFPOINT

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

proofpoint.

0404-001-01-01 04/20