6-Step Anti-Phishing Action Plan for Organizations

How to build an empowering security culture and reduce phishing attacks

DASHLANE

Scare tactics are common in cybersecurity. After all, emotions are a powerful motivator, and a little tale about a big phish can resonate. But at the end of the day, negative emotions won't help you build a positive culture of cybersecurity awareness.

Embracing a blame-free security culture

When it comes to phishing initiatives, creating awareness with fear tactics often makes employees annoyed at your IT team—or worse, resentful. They may even feel so anxious about phishing that they won't open any links or attachments, even important ones. And if they do open a malicious link, they may be too afraid to inform IT about it.

Fortunately, there are more inspiring and effective ways to promote positive cybersecurity awareness than shaming and scare tactics.

What can you do instead? Nurturing a blame-free, empowering security culture takes consistent effort. We've created a 6-step action plan that guides you through the elements of a successful education and training program to prevent phishing and inspire your employees.

"I always shock people when I tell them the best tool you can have is a human-first mindset: Treating your employees with respect and providing them with the right knowledge and software. [...] It is important to view employees as internal customers."

—Naya Moss, Founder, Frauvis

Read the full interview with information security pro Naya Moss here

Why and how organizations get hooked

Cybercriminals are strong storytellers, psychologists, and marketers rolled into one. But it's not those diverse talents that make phishing their favorite hobby—it's the promise of a big catch.

If simulated phishing tests are any indication, a third of employees, on average, will click on a phishing link or open an infected attachment.[1] Phishing works because it takes advantage of some of the most basic human traits—curiosity, carelessness, urgency, fear of missing out—and scammers know how to use these factors to their advantage.

1. KnowBe4, "Phishing by Industry Benchmarking Report," 2023.

"A cybersecurity strategy is always strongest when people and technology work together."

—Hugo Rettien, Head of Technology, Non-stop dogwear

Learn how Non-stop dogwear securely shares information across five countries.

Phishing has dominated as one of the most common attack vectors for many years, and the attacks continue to escalate. Researchers observed a 1,265% increase in phishing attacks between the fourth quarter of 2022 and the third quarter of 2023—with an equivalent of 31,000 daily phishing attacks on average.[2]

While scammers have used the same core techniques over the past two decades, their tools have improved. With the rise of generative artificial intelligence (AI), the risk for organizations will grow exponentially. For example, scammers can use tools like ChatGPT to:

- Easily craft grammatically correct, error-free messages (one of the common "tells" of phishing) that are more convincing—making phishing more difficult to identify
- Translate phishing messages into languages that were less accessible previously, expanding their geographic reach
- Create AI-generated phishing websites at scale to deliver malicious code
- Build their own generative AI tools and bots, such as WormGPT, FraudGPT, and DarkBERT, to aid other cybercriminals in various malicious activities

2. SlashNext, "The State of Phishing 2023," October 2023.

53%

of IT decision-makers surveyed globally said they're concerned about ChatGPT's ability to help hackers craft more believable and legitimate-sounding phishing emails.[3]

In 2023, 62% of U.S. organizations said they experienced a phishing attack—by far the most common identity-related incident.[4] Brands providing business-related apps and services are among the most frequently impersonated (also known as brandjacking). Security researchers found that seven major companies used by employees at work—including Zoom, WeTransfer, and Microsoft—represented 72% of spoofed brands.[5]

These trends sound unsettling, but by educating and training your employees, you'll empower them with the knowledge to avoid taking the bait.

3. Blackberry, "ChatGPT May Already Be Used in Nation State Cyberattacks, Say IT Decision Makers in BlackBerry Global Research," February 2023.
4. Identity Defined Security Alliance, "Trends in Identity Security," 2023.
5. GreatHorn, "2023 State of Email Security," 2023.

Top consequences of a successful phishing attack[6]

Percentages indicate the ratio of surveyed organizations that experienced each situation.

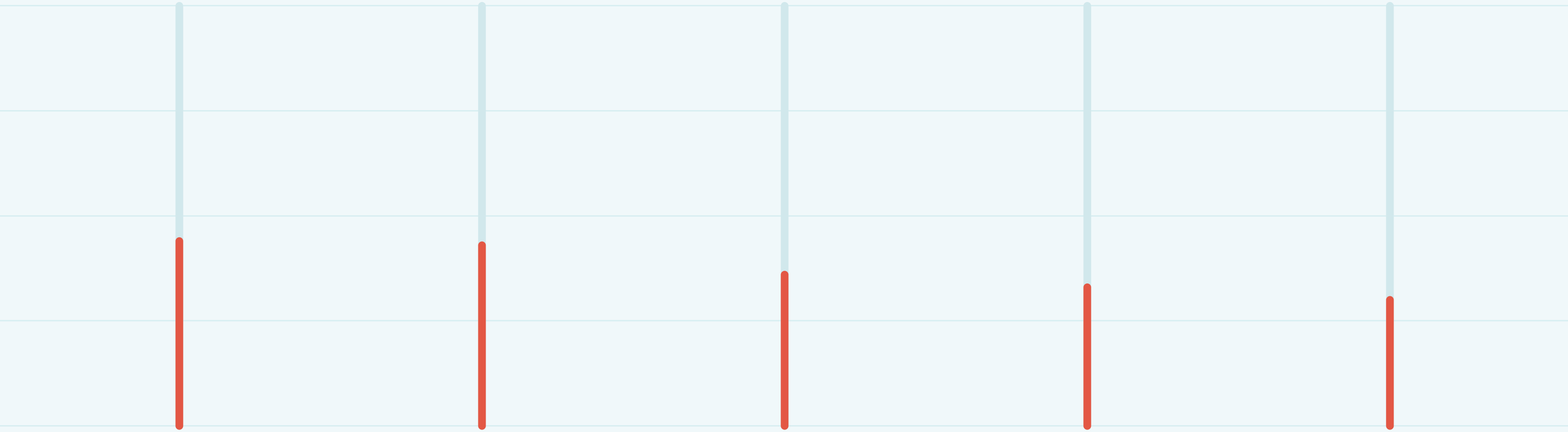
44%
breach of customer/ client data

43%
ransomware infection

36%
credential/account compromise

33%
loss of data/ intellectual property

30%
direct financial loss



6. Proofpoint, "State of the Phish," 2023.

A deeper dive into phishing attacks

Social engineering—the overarching category that includes phishing—dates back thousands of years. The digital era, however, has opened the door to numerous new tactics limited only by scammers' imaginations. As digital technology became widespread, so did phishing.

Common types of phishing and why they work

While phishing is commonly used as an umbrella term for several varieties of attacks, the types of attacks run deep.

Phishing
fraudulent emails sent to a large number of people

Attackers can cast a wide net with simple bait—generic messages—by using easy-to-find, off-the-shelf phishing kits that come complete with all the tools they need. They can spoof email addresses, impersonate brands, and use homograph attacks or typosquatting (lookalike web addresses and commonly mistyped URLs) as well as other methods to create authentic-looking emails. This tactic is effective by hooking recipients with urgent, confusing, or intriguing messaging.

Spear phishing
personalized, bespoke emails aimed at specific individuals or companies

The attackers typically look for relevant information on social media and other channels to create a more believable message. Often, they impersonate a trusted colleague or business to steal sensitive information. Because the experience is tailored to the targeted individual or business, the recipient is more likely to open the link or attachment. Threat research data from Barracuda found that 50% of organizations were victims of spear-phishing emails in the past 12 months.[8]

Whale phishing
spear-phishing targeting a high-value member of a company, such as a C-suite executive

These well-planned, advanced attacks start with gathering details about the target's personal and work lives, habits, and patterns. Scammers communicate through email, text, or phone and rely on gaining the target's trust, potentially over a longer period. They use a variety of techniques, from spying on conversations to hijacking email or text messaging accounts (known as thread hijacking), to send more authentic messages.

Smishing
phishing attacks sent through text messaging or SMS

Using fake phone numbers and often impersonating a legitimate company, attackers message links to authentic-looking sites that request sensitive information or prompt a malicious download. Since many people trust a text message more than an email—and since smishing is less common than email phishing—it's easier to catch someone off-guard. Attackers are also increasingly using conversational scams, interacting with potential victims over multiple messages to gain trust. Cybersecurity company Proofpoint found that conversational scams increased 12-fold in 2022, becoming the fastest-growing mobile threat.[7]

Vishing
phishing or spear-phishing carried out with a live voice call or robocall

A vishing call, which may come from a spoofed number, typically has a sense of urgency and often impersonates a government authority or financial institution. Caught off-guard, the targets react in the moment and don't have time to assess the situation—or they become too confused or flustered to spot a red flag. As with other types of phishing, generative AI is helping make vishing attacks much more effective. Cybercriminals can use these tools to collect social engineering data nearly instantly, as well as clone a trusted associate's or executive's voice.

Clone phishing
replicating an email and resending it with malicious content

Difficult to detect, this attack clones an existing email message to trick the recipient into opening a malicious link or attachment. The replicated message comes either from a spoofed email address or one that's nearly identical, and the body of the message is identical to the original. The scammer swaps the legitimate link or attachment with a malicious one and tells the recipient there was an error in the original message, increasing the likelihood of a click.

7. Proofpoint, "Trash Talk: Pig Butchering and Conversational Attacks Were the Fastest Growing Mobile Threats of 2022," April 2023.
8. Barracuda, "2023 spear-phishing trends," 2023.

New types of bait to watch out for

As people get better at spotting phishing attacks, scammers find new ways to entice clicks. Here are just a few of the latest varieties of phishing bait.

The QR phish

Phishing with QR codes (known as quishing) saw a resurgence due to the pandemic and has been growing rapidly. It's easy to camouflage malicious links in QR codes, and since these codes are ubiquitous both online and in the real world, they don't typically raise red flags. Quishing is difficult to spot since you can't hover over an email link to check the web address. In one recent attack, threat actors sent an employee an email that claimed to contain full documentation about the person's wages and directed the target to scan the embedded QR code with a mobile phone. The link opened to a fake SharePoint page asking the employee to input login credentials.

The Word/reCAPTCHA mashup phish

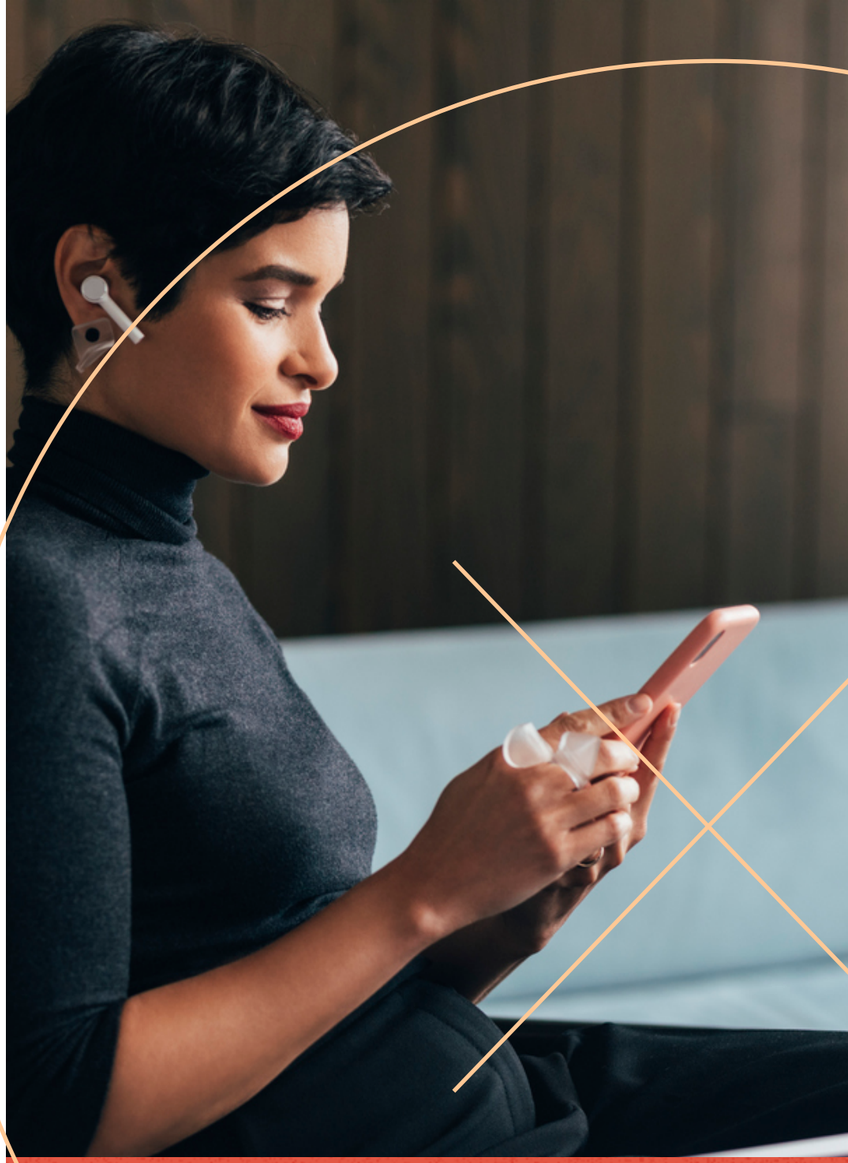
A sophisticated phishing campaign that emerged in the second half of 2023 aimed to steal credit card information from hotel guests. The attackers first targeted hotel employees with information-stealing malware (called infostealers) by reserving a room through a booking site and choosing the "pay at hotel" option. They then emailed earnest messages to the targeted employees with the infostealer masquerading as links to photos. Once the attackers gained access to the hotel system, they contacted legitimate guests with urgent requests to update their credit card information. The messages looked authentic since scammers sent them through the booking platform, but the links directed the guests to a fake website.

The Teams phish

Since collaboration tools like Microsoft Teams are common in hybrid workplaces, they're used more frequently in phishing attacks. One of the campaigns observed by security researchers in September 2023 distributed malware through attachments sent through Teams messaging. In one example, the bad actors sent a message about vacation changes with an embedded link hosted on the sender's SharePoint site and masquerading as a .zip or .pdf file. Selecting the link activated a malware download.

The SSO phish

A new "browser-within-browser" technique that emerged in 2022 takes advantage of third-party SSO options (such as "sign in with" Google, Apple, or Facebook) that are used by many legitimate websites. The attacker could email the target a phishing link to a malicious website and replicate the SSO process using HTML or CSS code, which would generate a fake pop-up login window that spoofs a legitimate domain. The technique, demonstrated by a penetration tester, has been observed in the wild at least once in the previous year.



How big companies found themselves in deep water

Okta

In October 2023, the popular identity and access provider was hacked through its ticketing support system, impacting as many as 18,000 business customers, including other identity management vendors. The company blamed the incident on an employee storing the credentials for an Okta service account in a personal Google account. The attackers stole some of the customers' authentication tokens, which could be used to hijack those customers' sessions and gain access to their networks. The hackers also ran reports that revealed data for all Okta customers, including their names, emails, companies, and roles. According to media reports, a large number of the exposed accounts belonged to IT admins.

MailChimp

The popular email marketing company was hacked in January 2023, exposing the data of more than 130 customers, including e-commerce giant WooCommerce. MailChimp said the hackers targeted employees and contractors with a social engineering attack to steal login credentials, then used those credentials to gain access to customer account data. This was the second successful social engineering attack on the company in six months. In the earlier attack, hackers used the stolen credentials of MailChimp's customer support staff to access internal tools.

MGM Resorts International

An attack by the notorious cybercriminal gang Scattered Spider caused chaos at MGM's Las Vegas casinos in September 2023 after the company discovered a cybersecurity breach and tried to contain it. The attack also exposed customer data and cost the casino operator an estimated $100 million. Scattered Spider gained access to the company by stealing or extorting help desk employees' credentials through vishing. The criminal group used similar tactics—as well as impersonating people by getting information about them from social media—to target dozens of Western companies.

Colonial Pipeline

In the spring of 2021, a major U.S. oil pipeline was taken offline for over a week due to a cyberattack. The attack caused shortages across the country and was caused by one stolen employee password. While we may never know exactly how the hacker obtained the password, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) suspects the cyberattackers gained entry through ransomware sent in phishing emails. Part of the reason CISA suspects this is because email-based attacks have been behind other high-profile infrastructure attacks in the recent past.

Norton LifeLock

Nearly 6,500 customers of the identity theft prevention company had their accounts compromised in January 2023, exposing personal data that potentially included access to their LifeLock password manager. Norton's parent company, Gen Digital, said a credential stuffing attack was likely to blame, with hackers using customers' logins that were previously breached or exposed on other websites.

6 steps to keep your employees off the hook

Phishing is no laughing matter, but humor is a more powerful (and positive) motivator than fear. As you start working on your action plan, we recommend adding some bites of humor to your awareness program.

At the very least, consider leaving out penalties. More than half of organizations have consequences such as counseling and lower performance reviews for employees who chronically fail simulated phishing attacks.[9] However, 50% of surveyed employees complain about these types of consequences. When employees are uncertain, unhappy, or angry about an idea, they're less likely to be team players when it comes to good security habits.

When you use scare tactics for cybersecurity awareness, your people won't feel invested in long-term security. Trust and creativity are much better tactics. And they're the perfect components of a strong security culture—which takes us to the first step of our action plan.

9. Proofpoint, "State of the Phish," 2023.

"One of our biggest concerns is phishing emails."

—Ben Leibert, Technical Manager, VillageReach

Learn how VillageReach minimized the risk of cyberattacks, including phishing.

STEP 1

Create a culture of security

A culture of security shouldn't require sacrificing productivity. In a security-first culture, employees:

- Understand their roles in protecting your company's data and IT resources
- Are active participants in ongoing security conversations
- Have the tools they need to maintain good security habits without impeding their work

A blame-free culture doesn't mean a lack of accountability. Instead of using a punitive model, find other ways to motivate employees to follow policies and good security habits. Use a human-centric approach to building a strong security culture—implement policies, processes, procedures, and practices based on an empathetic understanding of your employees.

A Dashlane and Harris Poll survey found that 79% of employees take at least some personal responsibility for their company's overall security.[10] Employees want to be part of the solution, and you have the opportunity to show them how they can do that.

10. Dashlane, "New Research Uncovers the State of Security in the Workplace," December 2020.

Do this, not that

Quick tips for successfully building a security culture

Fail: Instill fear in employees by fining them with salary deductions or firing them for repeatedly falling for simulated phishing. Or embarrass them by posting their photos in a shared space for public shaming. (*Yes*—these are real examples.)

Success: Implement a security champion program where peers are appointed as each team's cybersecurity expert. Provide additional training to these champions so they can answer questions about threats and help employees when they experience issues like a potential phishing attack. A peer is less intimidating to approach than a team manager or IT admin.

Fail: Require employees to use strong passwords they can't reuse or write down—without giving them a way to securely manage these credentials. This is a recipe for employee anxiety, policy circumvention, or both.

Success: Provide appropriate resources, such as a credential manager, so that employees can use and manage strong passwords. Implement a non-email-based messaging system that immediately alerts the IT team when an employee spots a phishing attempt. And instead of banning the tools that employees love, find ways to allow the secure use of those tools.

STEP 2

Implement a cybersecurity awareness, training, and education program

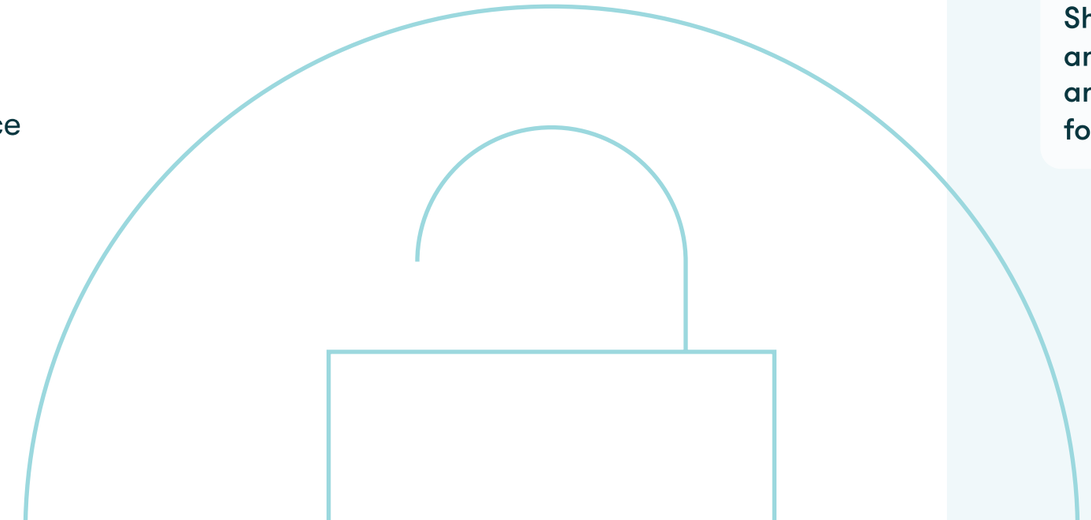
Phishing and other social engineering attacks aim to circumvent human defenses rather than security technology. That's why it's essential to go beyond implementing security tools by boosting your people's security knowledge.

A successful cybersecurity awareness, training, and education program needs to answer these five core questions:

1. Why does security matter to your organization?
2. Why should your employees care about security?
3. How do cybercriminals target and attack organizations like yours?
4. How can your employees help prevent these attacks?
5. What actions can employees take to enhance security in their daily work?

Breaking old habits takes some time, which is why security awareness and training need to be an ongoing effort. Consistent security messages also help employees retain information longer.

And remember: No one loves sitting through endless presentations, no matter how much you entice them with free pizza. Employees likely won't read long documents about security either. To engage them, use a combination of training modules with a focus on interactive sessions—and consider adding an element of entertainment.



Keep security top of mind for employees by:

REMINDER 2m ago

Integrating education and awareness into new hire onboarding

REMINDER 2m ago

Providing refresher training at a regular cadence

REMINDER 2m ago

Sending quick tips and reminders through internal communication channels

REMINDER 2m ago

Sharing relevant news about data breaches and hacks that involve social engineering and including tips for how to avoid falling for those tactics

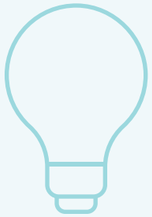
Adapted from Karen Renaud, University of Abertay, Dundee, U.K. researcher, as published in the Wall Street Journal, "Why Companies Should Stop Scaring Employees About Cybersecurity," December 7, 2020

STEP 3

Conduct simulated phishing campaigns

To help employees recognize phishing and risky actions through first-hand experiences, use a “show, don’t tell” approach with simulated phishing tests. By conducting regular mock phishing campaigns, you can turn employees from weak links in company security to points of strength.

In addition to serving as practice for spotting potentially malicious emails, phishing tests measure how many people open the emails, links, and attachments. These tests also measure how many people complete the final action (such as entering their login credentials). You can use these metrics to track your program’s effectiveness over time and identify areas that need additional education and awareness.



Organizations that have a mature employee awareness program see dramatic improvements in simulated phishing tests after 12 months, with click rates decreasing from an average of 33% to 5%, according to researchers at security awareness company KnowBe4.[11]

11. KnowBe4, “Phishing by Industry Benchmarking Report,” 2023.

Here are a few tips for conducting simulated phishing tests:

- Don’t limit the phishing test to just an email. Include vishing, smishing, and other methods that can reel people in.
- Be creative with your themes. Attackers constantly change their messages, taking advantage of seasons, trends, popular culture, and more—and so should you.
- Resist a “gotcha!” approach. Use these tests as an opportunity to educate and reward secure behavior. One way to do this is by having a department contest with a reward—and offering extra points for something besides the usual free lunch.
- Ensure employees know what to do if they spot a phishing email, whether simulated or real. For example, share the IT email address where you want them to send suspicious emails.

An insider's tip to prevent phishing

Dashlane hosted a Q&A with Rachel Tobac of SocialProof Security, an ethical hacker who uses social engineering techniques to infiltrate companies and help them strengthen their people defenses.

"One of my biggest jobs is helping people become politely paranoid, so figuring out, according to their threat model, how much polite paranoia they need to incorporate into their work and their personal life. For a person who isn't in the public eye, posting a picture of yourself drinking a mojito on the beach is completely fine but I would say, how about we don't tag the hotel, so that I don't know who to call to get information about you. If you don't tag the hotel, then I don't know who to place the call to, pretend to be you, and gain access to where you're staying and what room number you're in."

—Rachel Tobac, CEO, SocialProof Security

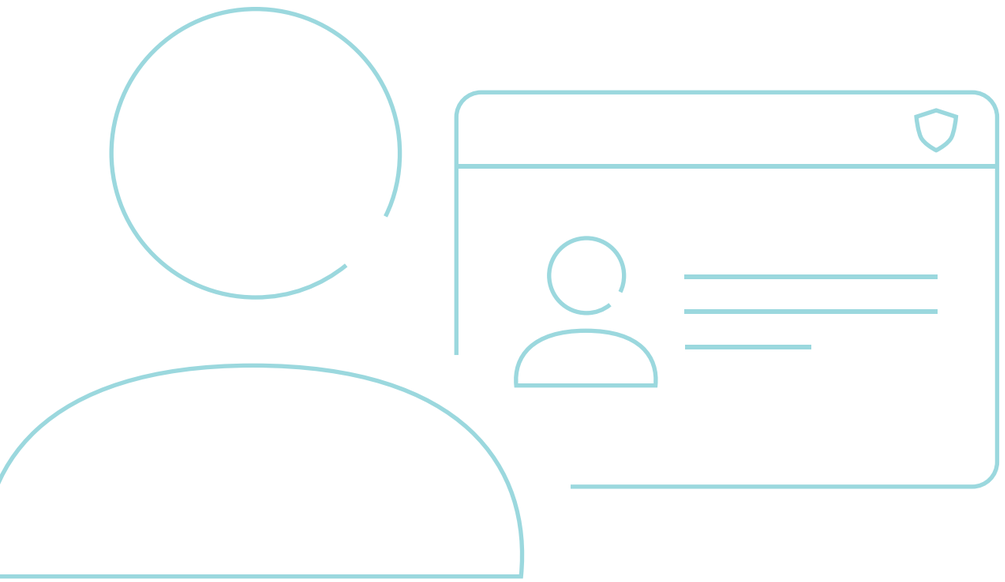
Want more tips like this? Grab a drink, a snack, and maybe a hack during our on-demand webinar with Rachel Tobac.

STEP 4

Tailor your programs to different job functions

Phishers may not always have perfect spelling, but they shine in psychology and human behavior. And they're meticulous researchers. That's why they won't send a spear-phishing email with a fake resume to Jordan in accounting or an invoice to Sam in marketing. And neither should you when you're conducting simulated phishing tests.

In addition to educating employees on universal security topics that apply to everyone, provide custom training to different teams and departments based on their roles and job functions. And don't forget your "whales," those high-value targets who need to be extra vigilant.



Here are two examples of how to customize training for different groups:

1. Accounts payable, payroll, and other financial and human resources functions:

Educate these teams on targeted attacks such as:

- Payroll diversion, where a cybercriminal redirects a paycheck or another payment to a different account
- Business email compromise, where scammers impersonate a company executive to request wire payments, bulk purchases of electronic gift cards, or sensitive employee information

These employees are also more likely to receive attachments routinely, such as PDF resumes and Excel spreadsheets. Train them on being extra vigilant and implement enhanced processes to minimize the likelihood of a successful attack.

2. Sales, marketing, and communications teams:

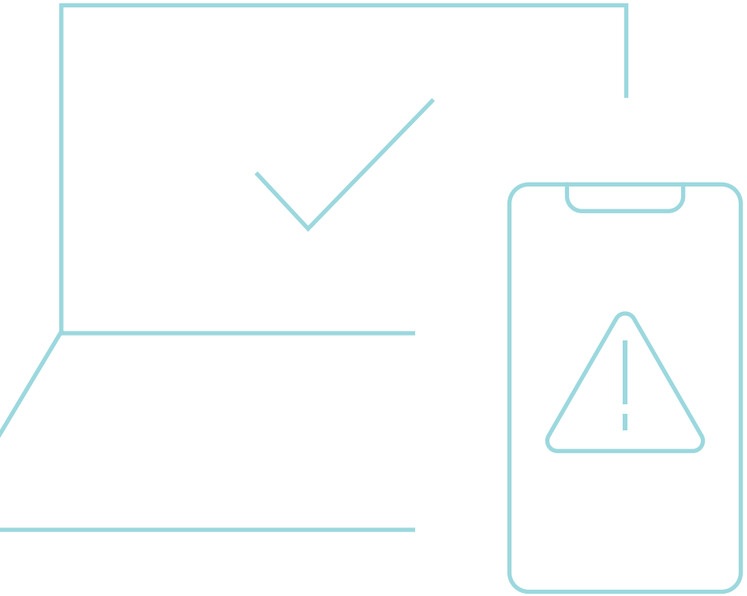
These teams are more likely to be publicly visible due to the nature of their role and being more active on social media. They need to understand how the personal information they share on social media —including their professional and career information—can be used by scammers for social engineering.

As these teams are more likely to interact with the public, educate them about social media tactics, such as phishing through spoofed profiles and fake accounts. Additionally, these teams are more likely to share accounts and have access to customer data, so their training should emphasize best practices such as secure sharing.

STEP 5

Boost phishing defenses with additional tools and processes

Education and awareness are empowering. But at the end of the day, you still need to provide tools and implement processes that support and promote secure practices.



There's no perfect recipe for this step, but there are a few simple tips recommended by the NIST Cybersecurity Framework that you can use to create a plan tailored to your environment and objectives:

- Adopt tools that provide endpoint security, credential management, and email security. These tools, among others, will minimize the impact and damage from phishing attacks.
- Many successful phishing attacks end with malware installed on a victim's device. Maintain a regular patching schedule for all apps, devices, and other systems to eliminate vulnerabilities that malware can exploit.
- Train employees on how to identify and report suspected security incidents and threats, including suspected phishing attacks. Consider creating a special email or channel for them to reach out to.

Don't get hooked

Take advantage of tools like phishing alerts, which are offered on the Dashlane Business plan.

These alerts give your employees a real-time warning before they copy and paste their credentials on a website that looks suspicious or doesn't match our records, so you can ensure they're only logging in to sites they trust. The alerts don't require any additional setup steps for your employees, and they work in the background to help reduce phishing risks and provide a secure web browsing experience.

Learn more

STEP 6

Measure effectiveness and iterate

A cybersecurity awareness program without metrics is like catch-and-release fishing—without evidence, you can't really prove anything. To see how well your efforts are working, you need a baseline at the beginning of implementation and periodic measurements afterward.

Quantifying cybersecurity posture isn't always easy, so you may need to think out of the box. Don't use the simulated phishing click rates as the only metrics because they don't provide a holistic picture. Besides, some employees are just too busy to read emails, so you may have outliers who will skew your results.

Your tools may also provide ways to creatively measure your program's effectiveness. For example, some credential managers include a password health feature that tracks your company-wide password security scores over time.

Security education and awareness building isn't a "one-and-done" endeavor. To achieve your desired outcomes, measure impact—ideally using concrete numbers and informal feedback—and regularly adjust your strategy based on results.

Final thoughts

Many organizations are improving their security technologies and processes to make it harder for phishers to hook their employees. But phishers will continue to find novel, unexpected ways to lure people with social engineering.

Your best defense is planning for the unexpected and empowering employees with up-to-date knowledge, appropriate tools, and ongoing awareness.

Want to learn how to strengthen your security and protect your business when phishing compromises employee passwords? Download our e-book, **“A Practical Guide to Cybersecurity with a Password Manager.”**

Ready to test out a credential manager? Get a free trial on Dashlane.

DASHLANE

About Dashlane

Dashlane offers businesses a password management solution that is as easy to use as it is secure. Admins can easily onboard, offboard, and manage their employees with the assurance that company data is safe. And employees can enjoy a way to manage their work and personal accounts that's already loved by millions. Our team in Paris, New York, and Lisbon is united by our passion for improving the digital experience and the belief that with the right tools, we can help everyone realize the promise of the internet. Dashlane has empowered over 18 million users and over 20,000 organizations in 180 countries to dash across the internet without compromising on security.

dashlane.com

Contact us

LinkedIn

Reddit

X

Instagram

Facebook

Blog