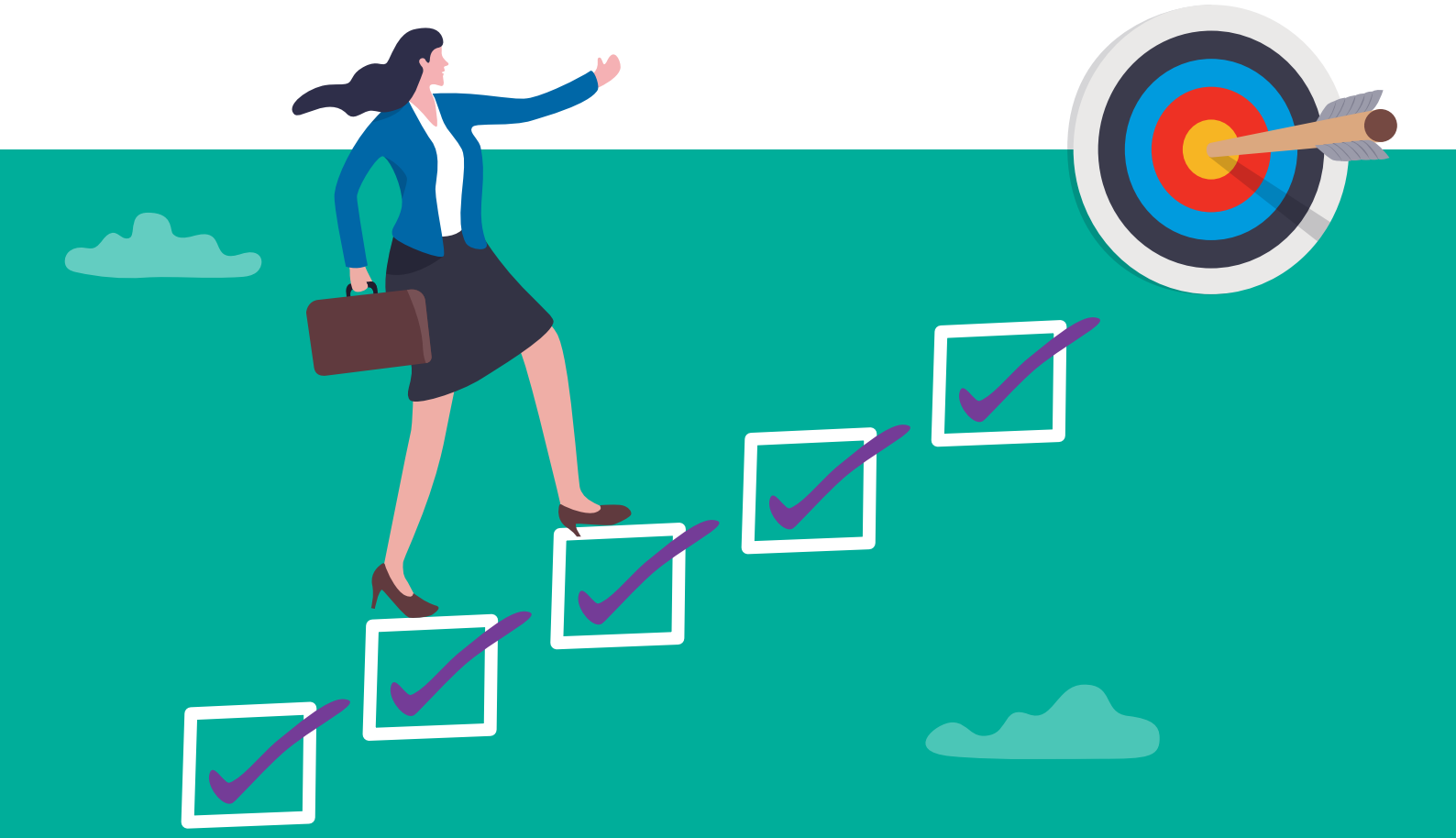
proofpoint.

EBOOK

2023 EDITION

Driving Real Behaviour Change

The Complete Guide to Building a Security Awareness Programme that Works



proofpoint.com

Putting People at the Centre of Your Cybersecurity Efforts

Today's most potent cyber threat isn't a zero-day vulnerability, new malware or the latest exploit kit. It's your own users.

That's because today's attacks target people, not IT infrastructure. No matter what form they take, most cyber attacks need a human victim to help activate them. They trick people into opening malicious attachments, clicking unsafe URLs, handing over account credentials and even taking direct action—such as wiring money or sending sensitive data.

Why user education is key

According to the "2022 Data Breach Investigations Report," 82% of breaches involved the human element. As the report puts it: "malware and stolen credentials provide a great second step after a social attack gets the actor in the door, which emphasises the importance of having a strong security awareness programme."[1]

User awareness training is one of the most important things you can do to secure your organisation. By teaching your users how to recognise, reject and report attempted phishing, you can create a strong last line of defence against today's biggest cyber threats.

What you'll get from this guide

Starting a new training programme may seem daunting. Maintaining one that keeps your users engaged, changes their behaviour and reduces your organisation s exposure to threats might be an even bigger challenge.

We're here to help.

This guide shows you how to create and sustain an efficient and effective cybersecurity education programme regardless of your programme maturity, vendor or obstacles you may face. It provides key facts, effective strategies, valuable resources and practical tips for security leaders at every stage of the security awareness journey.

Here are a just a few of the questions we ll help answer:

- How do I get buy in? Who should I work with internally?
- What should I do? How often?
- How do I engage my people?
- How do I measure and share success?

82%

of breaches involved the human element.[1]

1 Verizon. "2022 Data Breach Investigations Report." June 2022.

A people-centric model for measuring and mitigating user risk

Just as every person is unique, so is their value to cyber attackers and their risk to your organisation. At Proofpoint, we have created the Very Attacked People (VAP)™ model to measure and mitigate three distinct aspects of user risk.

Security awareness training is most directly related to user vulnerability. But your programme should also take your users' attack profile and privilege into account. This insight helps you take a people centric approach to user awareness that includes tailored, proactive and targeted follow up training.

V

Vulnerability

This sizes up how likely your user is to fall victim to an attack due to their susceptibility to attackers' tactics or risky digital habits. This can be measured by knowledge assessments, security awareness training quizzes and simulated phishing attacks.

A

Attack Profile

This quantifies the volume and sophistication of attacks and attackers targeting the user. It may also take into account related or similar users inside and outside of the organisation.

P

Privilege

This weighs the value and sensitivity of data, systems and resources the user has access to. It can also be viewed as a way of measuring how much damage a successful attack against that user could cause.

Table of Contents

SECTION 1

What to Know Before You Start

You've done it. The procurement process is finally over. Your new security awareness vendor sends you a link to your software, and the world is yours. You're ready to start launching simulated phishing attacks, gathering data, assigning training and using all the amazing features and content you've seen from your product demos.

You send out the announcement about your security awareness programme. Suddenly your inbox is flooded with replies:

- Who approved this exercise?
- I'm talking to my VP about this.
- Do I really need to do this?

These are among the first obstacles our customers typically face. But they also point the way to one early step you can take to ensure a successful security awareness programme: get user buy-in.

A common theme we hear from customers is some users just not wanting to be involved in security awareness training.

Getting users on your side

A common theme we hear from customers is that some users just do not want to be involved in security awareness training. Maybe the simulated attacks make users feel vulnerable. Others might see training as just another corporate exercise and distraction from their "real" work.

Here are some ways to overcome this common obstacle:

Communicate with user benefit in mind. When you're drafting user-facing communications, be aware of the "What's in it for me?" question users will be asking. Bring up real-world examples such as identify theft, stolen credit cards, account breaches and other stories. Show how training will help users in their personal life. This will make the programme more relatable and improve participation.

Balance assessments and training. Simulated phishing assessments are popular components of programmes. But sometimes they can be overused. Many customers have spoken to us about the need to balance assessments, training and awareness activities. As one customer told us: "When I only send out phishing simulations, users think we're trying to trick them." It's good to have a balance of both in a programme, along with awareness and other activities such as contests.

Have a friendly face at company events. Computer-based assessments and training can come off as impersonal. Having a booth at large company events or doing virtual sessions like webinars can give users a more personal connection. Start with an employee kick-off, set up learning events and provide helpful resources. Consider giving out swag or even just coffee. These steps also humanise the programme with a friendly face and name.

Overcoming resistance

Based on conversations with customers, non-engaged users typically fall into two camps:

- **Repeat offenders:** users who continuously fail phishing simulations and other assessments
- **Non-participators:** users who refuse to take part in training

You may find yourself having tried everything to address these uses—emails, in-person chats, discussions with managers or even taking away network access. If you still can't change behaviour, it is not the end of the road.

One customer's strategy was having the CISO or other leader schedule 15 minutes on these users' calendars to talk about:

- The importance of user behaviour and security awareness
- How the department is trying to help protect the company and users in personal situations
- Why employees should commit to become more vigilant or take part in training to help

This kind of interaction leaves a strong impression. It conveys the importance of good behaviours and stronger participation in more personal, tangible way.

The double-edged sword of user-reported phishing

At one of our annual conferences, a customer raised his hand after a presentation.

"My users don't report phishing emails to our abuse mailbox," he said. "It's all spam or legitimate messages. Our team can't keep up. How should we handle this?"

Abuse mailboxes are a great way to reduce risk. But they are notoriously time-consuming to manage. We have found two solutions to this common obstacle:

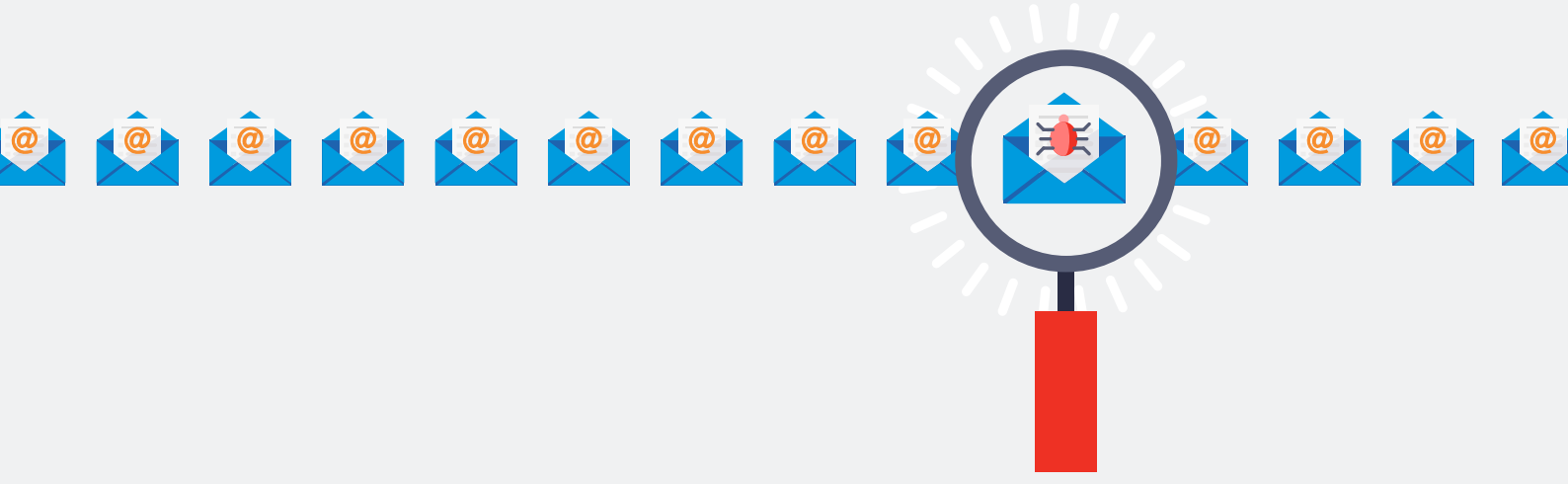
- Help users get better at spotting true phishing email
- Automate the process of analysing and responding to reported phishing email

Improved reporting will be the natural outcome of an effective security-awareness programme. Many customers see improved reporting—more true malicious messages and fewer false positives—about six to 12 months after they deploy a consistent programme that trains users to identify phishing emails.

Automating email analysis and response can ease workloads by automatically analysing and enriching through sandboxing and threat intelligence. This reduces IT overhead by automatically removing malicious content from users' inboxes or closing out false positives.

Another benefit of automated response is that users can receive customised feedback that lets them know whether the message they reported was truly malicious. This step helps educate users and improves security, reinforcing positive behaviour with a simple thanks for reporting malicious email.

Improved reporting will be the natural outcome of an effective security-awareness programme.



SECTION 2

Timing Your Programme

Timing is not an isolated detail for your security awareness training programme—it is the sum of all your efforts. It is the right training, the right people, and many other tactical, organisational and strategic components that produce the composite result of “the right time.”

Every organisation is unique, and no two training programmes will be the same. But yours should include all the following elements:

- Defining training needs
- Identifying users with specific training needs
- Mapping out activities
- Creating and managing schedules
- Communicating and testing first steps
- Determining frequency and timing of programme activities

Recommended order of activities: a checklist

The more diligence and planning you apply to your programme, the more successful your programme will be. Here are key steps that have proven helpful for our customers.

A central tenet of people-centric cybersecurity is that every user is different.

1. **Define training needs.**

   People-centric cybersecurity starts with measuring user risk. User assessments provide insight on where users might be most vulnerable—and what training assignments they need to improve their understanding of critical topics such as phishing, data protection, mobile security and more.

   Risk doesn't exist in a vacuum. A key part of identifying training needs is understanding the current threat landscape. This is where threat intelligence plays a critical role. Timely real-world threat intelligence helps you understand current and emerging threats users may face.

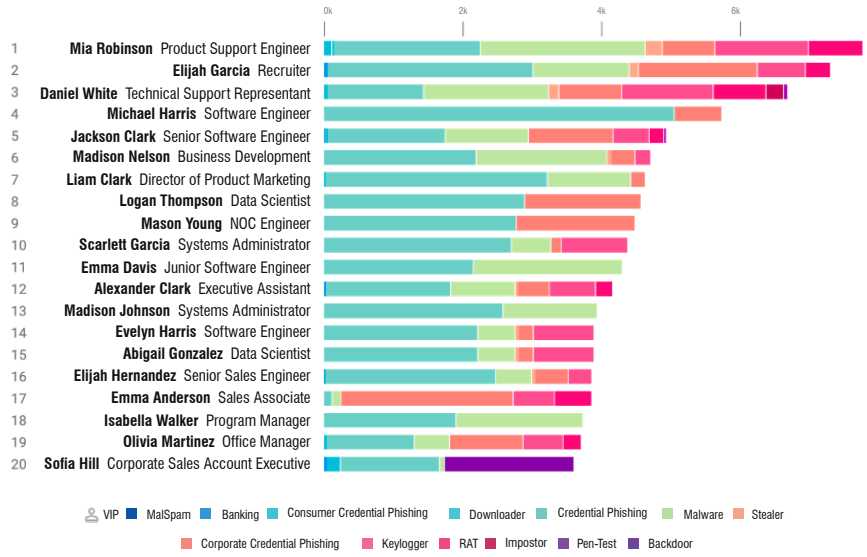
2. **Identify user and groups who may need a different curriculum or training tailored to their needs.**

   A central tenet of people-centric cybersecurity is that every user is different. A one-size-fits-all defence won't work in today's environment—and that includes security awareness programmes.

   These groups may require tailored or specialised training:

   - VAPs**:** Users who pose an elevated risk because they're especially vulnerable to cyber attackers' tactics, are more heavily targeted in attacks or have access to valuable data, systems or resources.

A VAP report from Proofpoint Targeted Attack Protection



- VIPs: C-level executives, board members and high-profile staff who may need specific training and guidance because of their importance to the organisation. Many VIPs may also be VAPs.
- Designated roles and departments: Users in human resources, finance, legal, compliance, development or other roles may need legally mandated or other specific training. Consider different knowledge assessments and simulations for these groups as your training programme matures.

3. **Mapping out key activities to include in your programme.**

   A successful training programme has the right mix of assessments, training, support materials, communications and virtual or in-person activities. Here are elements you should consider for yours:

   - User assessments to gauge knowledge and vulnerabilities. These may include knowledge assessments and simulated phishing, USB and smishing (SMS/text phishing) attacks
   - Computer-based training designed around on user needs and the current threat landscape
   - Awareness activities (posters, webinars, newsletters, videos) to introduce concepts and reinforce key messages
   - In-person and virtual activities such as lunch-and-learns or webinars. Get creative. For example, some of our customers have created cybersecurity escape rooms that have been successful.

4. **Test and communicate first steps.**

   For many organisations, a comprehensive user training programme might be a big change. Start with a small group of users to work out any kinks. Telegraph first steps early and often to everyone. Keep surprises to a minimum.

   Two months before launch

   Send a test phishing simulation to a small “in the know” group to reveal any hidden technical issues. Then send a moderately difficult baseline phishing test to all employees.

   For now, send users who fall for your phishing lure to a 404 “page not found” site. (Later, you’ll send users who click to an educational landing page.)

   One month before launch

   Announce the programme to users. If you’re deploying an email reporting add-in, explain its purpose and how to use it. And if you have access to content such as posters, images or other security awareness materials, post them around the office or on a wiki about your programme.

5. **Determine the frequency and timing of programme activities.**

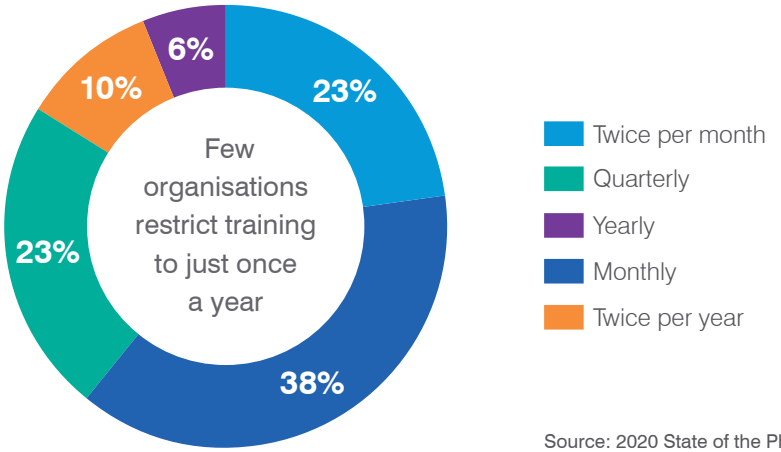
   Again, timing is everything. We recommend the following cadence for your security awareness activities:

   - Send a phishing test every four to six weeks. Mix up the types of themes and lures used.
   - Use auto-enrollment on phishing tests at least once a quarter. Use a targeted follow-up training module, depending on the type of attack sent.
   - Review VAP reports monthly or bimonthly. Depending on what it reveals, decide who should receive targeted training and which training content to use.
   - Assign organisation-wide training at least quarterly.
   - Repeat broad knowledge assessments and phishing tests at least once a year to compare to baseline assessments.
   - To reinforce learning retention, schedule at least bi-annual security awareness activities such as webinars, contests or (if possible) in-person activities.

Create a yearly framework to schedule the components and timing of training activities. Stay flexible, adjusting your schedule as the broader threat landscape changes.

Our *2020 State of the Phish* report found that security awareness training has progressed beyond yearly and quarterly activity to become a monthly or even bi-monthly event. We recommend monthly or more frequent training, including targeted training, awareness campaigns and knowledge assessments.

Frequency of Security Awareness Training



Source: 2020 State of the Phish

When to make a change

The threat landscape is constantly evolving. That's why your security awareness programme needs a continuous approach. From the initial assessment baseline, future assessments can help track user proficiency and help you plan ways to reduce risk.

Here are situations that call for changing the frequency or order of your training activities:

- **When specific user threats become more prevalent or attackers use a specific brand or lure.** Modify assessment content, such as simulated phishing campaign templates, or use threat-driven educational content to better manage the risk.
- **If your organisation experiences an event, such as a data breach.** Consider updating your planned activities and frequency of communication, assessments and training related to that event.
- **If new laws or regulations require more training.** Follow up with a customised knowledge assessment to see how users have retained that training content.
- **When your organisation releases or updates a policy or has doubts about user knowledge of an existing policy.** A customised knowledge assessment can help you find gaps in user understanding and guide training efforts.
- **If a security awareness programme stopped for more than six months.** In this case, it may make sense to relaunch the programme to ensure users understand its context and importance.

We do not recommend ramping up the training frequency too much—even with repeat offenders who struggle with assessments. Monthly phishing assessments and selectively enrolling users who "fail" into a single training is a reasonable, targeted approach. But assigning those users to four training sessions may feel like punishment and cause them to resent the programme.

Above all, don't try to do everything all at once. Start with the proper analysis up front, backed with threat intelligence and assessments. From there, work throughout your organisation to build a realistic plan that everyone can embrace.

The threat landscape is constantly evolving. That's why your security awareness programme needs a continuous approach.

SECTION 3

Why Engagement Is Critical

It might seem obvious that security awareness training is inherently a people-centric effort. It's aimed at equipping people to recognise attacks that target them and changing user behaviour.

That's why keeping users engaged is critical to a successful programme. But even the most well-intentioned programme can grow tedious when people don't have rich and meaningful experiences.

Keeping users engaged is critical to a successful programme.

The most successful programmes:

- Use branding to make their relevance clear to users
- Use scientifically proven learning principles to change behaviour
- Reinforce training with a diverse mix of content and media
- Enlist champions across the organisation for support and improvements
- Guide users with the right balance of incentives and consequences

Think of these five principles as pillars of a framework for an effective programme that your users value. Customers across a wide swath of industries have used these concepts to create security awareness training programmes that reduce risk, cut costs and support data privacy compliance.

Brand your programme

The right name can help users understand what your security awareness training programme is for and why it should matter to them.

For instance, your organisation may need users to treat European Union customer data with extreme caution to comply with General Data Protection Regulation (GDPR). A title as plain and forgettable as “GDPR training” may not spark the user engagement you need to inspire changes in behaviour.

A better theme might be “Become a Data Privacy Defender.” The title clearly highlights the programme’s purpose (data privacy) and the user’s role (an active contributor to the privacy effort).

Your organisation’s culture may call for a more direct approach, with more practical themes. Even then, naming your programmes around specific topics—such as phishing, social engineering, email, working from home—is an improvement.

Use learning science principles

Your programme should draw on decades of learning science for the most effective learning, retention and behaviour change. A well-rounded programme provides both conceptual and procedural knowledge. Give users the big picture and specific lessons. Here are some proven techniques:

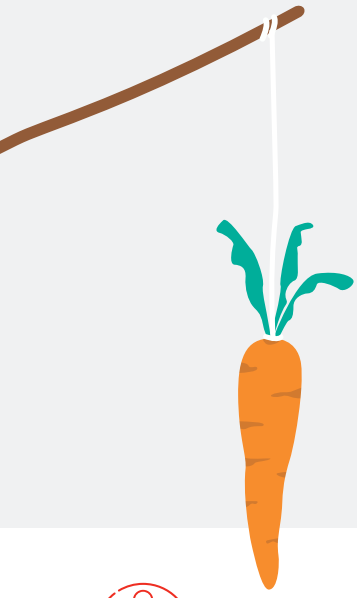
- **Serve small bites.** Keep training to minutes (rather than hours) and focus on single topics as often as possible.
- **Reinforce lessons.** Provide feedback, and keep training and awareness persistent.
- **Train in context.** Assign training relevant to roles and threats.
- **Give immediate feedback.** Give real-time results on training or phishing exercises.
- **Let users set the pace.** Everyone is unique and learns at different speeds.
- **Tell a story.** Give real-world examples.
- **Vary the message.** Ensure that topics have multiple content sets that vary in wording and phrasing.
- **Involve your students.** Interactive content and exercises improve retention.
- **Make them think.** Exercises should test how students can apply their knowledge.
- **Measure results.** Assess students up front and track progress continuously.

Keep training interesting with diverse content and media

According to the "Rule of Seven," advertisers must get their message in front of a prospect at least seven times to make it stick. The learning process is similar.

Regardless of what security awareness training solution you are using, deliver lessons through multiple channels and activities. Here are just a few examples of activities and channels you might use.

ACTIVITIES	CHANNELS
Attack simulations (phishing, USB, SMS and so on)	Security awareness training tools
Knowledge assessments	Security awareness training tool or survey tool
Identifying and monitoring VAPs	Threat intelligence/email gateway
Computer-based training	Security awareness training modules through an online platform or other learning management system (LMS)
Awareness campaigns	Posters, videos, podcasts, webinars, guest speakers, infographics
In-person or virtual awareness and training exercises	Lunch-and-learns, webinars, booths at company events, speaking slots at company events, in-person training, escape rooms
Contests/gamification	Acknowledge positive behaviour change through an existing company channel such as a newsletter or wiki
Security awareness information	Company wiki, intranet or shared company calendar
Security awareness updates	Company newsletter, chat app channel (such as Microsoft Teams and Slack) or integrated into another department's communications
User feedback about security awareness training programme	Survey tool or shared mailbox
User phishing reporting	In-client email reporting add-in solution or abuse mailbox address



When users think poorly of their organisation's security awareness training, they can be indifferent and may even resist it.

Enlist other departments and people in key roles to help

IT security, marketing, HR and key executives can play important roles in your programme. Draw on their expertise to support and improve your approach, content and delivery.

Here are a few ways other departments can help:

- **IT security** may be able recommend content to make it relevant to corporate policy (such as a password policy). It can also reveal users who might need more training because they're more heavily targeted in cyber attacks or handle sensitive data.
- **Marketing** can help design security awareness materials and other content so that they align with your organisation's brand elements.
- **HR teams** can advise on organisational dynamics and provide insight on working with executives and line of business (LOB) leaders.
- **The CISO** (or other key CXOs or business leaders) can communicate support and stress the importance of the programme.

Carrot versus stick: guiding users toward better behaviour

When users think poorly of their organisation's security awareness training, they can be indifferent and may even resist it. So far, we've outlined steps that can help set the stage for a programme that's well received and shows real value. When it comes to "carrot-versus-stick" approaches to training, most of our customers favor the carrot.

But every so often, user resistance may call for a stick. In these rare cases, a consequence model can help ensure compliance with training polices. While they should be a last resort, here are consequence models our customers have used:

- A "three strikes" programme in which users who click on three simulated phishing emails will have a consequence such a discussion with a manager or temporarily limited network access or loss of access privilege
- Consequences such as: HR writeups; cuts in pay, bonus or benefits; and, in rare cases, termination

A best practice is to focus on carrot-style incentives and use consequence models as a last resort. Our customers find that an overreliance on the latter makes users less likely to engage with the programme. But if you work in a highly regulated or especially sensitive industry, the stick may be necessary.

SECTION 4

The Essential Role of Data

After getting approval to run your security awareness programme, you're probably eager to jump right in with simulated phishing attacks and advanced user training.

But it's important to start with a strategic plan. To maximise the benefits (lower user risk) and minimise the costs (users' time), your first steps should be providing foundational knowledge, understanding users' vulnerabilities, and focusing training where it's needed most.

Building a foundation

Your first instinct as a security expert might be to simulate advanced phishing attacks or train users to identify the biggest threats facing your organisation. While it's a logical impulse, it won't have the impact you're hoping for if your users still don't know the basics.

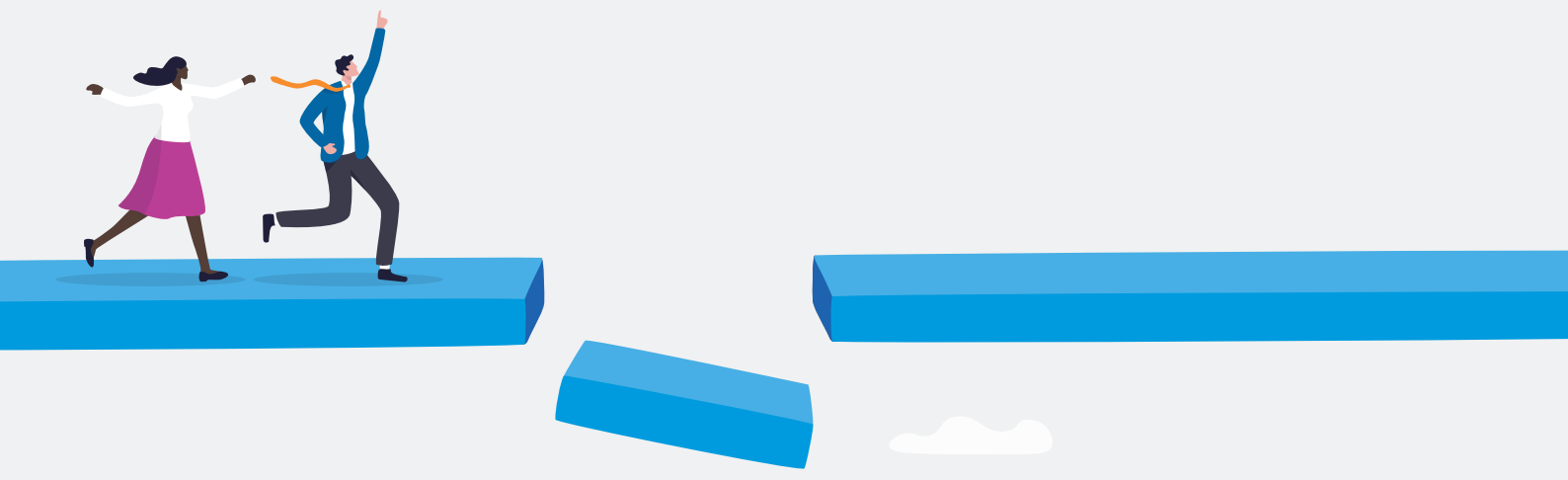
In our *2020 State of the Phish* report, we found that many working adults can't define terms such as phishing and ransomware.

	Correct	Incorrect	I Don't Know	
What is PHISHING?	61%	24%	15%	• Only 49% of U.S. workers answered correctly. • German workers were most likely to recognise this term (66%).
What is RANSOMWARE?	31%	31%	38%	• Last year, 45% of global workers answered this question correctly. This drop in awareness could be a carryover from 2018, when ransomware attacks fell off dramatically, leaving security teams less likely to discuss the topic with users.

Source: 2020 State of the Phish

These knowledge gaps are why we highly recommend foundational training in core topics such as security essentials and phishing before you assess or train on more advanced topics.

Many training solutions, including ours, allows for onboarding training assignments for new hires. We recommend that these include several fundamental training modules. That way, you're always providing foundational training for all users before they're asked to complete more advanced assessments and training.



Identify vulnerable users and VAPs

Using the VAP model we described in the introduction, your programme should give extra attention to users who pose an elevated risk because they're:

- Especially vulnerable to cyber attackers' tactics
- More heavily targeted in attacks
- Have access privileges to valuable data, systems or resources

(See "A people-centric model for measuring and mitigating user risk," on page 3.)

Measuring vulnerabilities, attacks and privilege

For vulnerabilities, simulated phishing attacks and question-based knowledge assessments are invaluable. They can help you pinpoint who might need more training, what tactics users might fall for and what areas to cover.

Quantifying user risk under the VAP model enables you to focus your training programme and reduce risk more quickly.

For attacks, knowing which users are being most heavily targeted, how and by whom requires insight from your security team's threat intelligence solution. We identify these VAPs through our Attack Index, a composite score that takes these factors into account:

- **Attacker type.** The attacker's level of sophistication and, in turn, risk to the organisation. For example, a state-sponsored attacker gets a much higher score than a small-time cyber criminal.
- **Targeting type.** A way of describing how narrowly the attack is targeted. Did the threat hit only one user or the entire planet? Was it focused on a user, company, industry or geography? Or was it a "spray-and-pray" campaign seen by half the globe? The more targeted the threat, the higher score it gets.
- **Threat type.** This component reflects the type of malware involved in the attack. In most cases, the malware used in an attack can reveal how severe the threat is or how much effort the attacker put into it. A remote access Trojan (RAT) or stealer, for example, gets a higher score than a generic consumer-focused credential phishing attempt.

For privilege, organisations can start by taking an inventory of all the potentially valuable things people have access to: data, financial authority, key relationships and more.

The user's position in the org chart is naturally a factor in scoring privilege. But it's not the only factor—and often, not even the most important one. An administrative assistant might make a more appealing target than a mid-level manager for corporate espionage because the assistant has access to the CEO's calendar. In the same way, a hospital nurse with access to patient records might be a more useful target than the CEO for identity thieves.

Password Habits

use a password manager

rotate between 5 and 10 different passwords

manually enter a different password for every login

use the same 1 or 2 passwords for all accounts

Source: 2020 State of the Phish

Using VAP data beyond training

Quantifying user risk under the VAP model enables you to focus your training programme and reduce risk more quickly. It may also provide context as to why attackers are targeting these users. With this insight, you can keep a closer eye on these users and ones with similar titles and deploy adaptive controls such as isolating browser activity or stepping up authentication requirements as needed.

Blending this information with threat intelligence—including the rich insight from a tool such as Proofpoint Targeted Attack Protection (TAP)—provides greater insight into whether users are targeted with malicious content.

Knowing whether users are clicking simulated phishing email is helpful. Knowing if they're clicking real malicious content is even more important, even if that click is blocked. This data can put potential risk and gaps in sharp relief.

Beyond phishing: addressing other hot-button topics

Phishing is the most discussed topic in security awareness training. But focusing your programme solely on email-based threats can leave major gaps in other important topical areas.

Consider using a broad-based knowledge assessment to understand users' knowledge of cybersecurity topics and your organisation's own policies or guidelines.

Our *2020 State of the Phish* report revealed several risky behaviours. Here are just a few of the findings:

- 45% of working adults admit to using the same passwords for multiple accounts.
- Only 49% password-protect their home Wi-Fi networks.
- 26% believe they can safely connect to a free Wi-Fi network in a trusted location (such as a coffee shop or airport).
- 17% aren't sure whether open-access networks in these locations are safe.

Such behaviours expose your organisation to serious risk. Diversifying you programme to address these and other potential areas of weakness can reduce your exposure.

When covering these topics, use real-life stories and vivid examples. Relevant, concrete details help users understand how attackers work—and why it matters.

Keeping your programme agile

Every organisation has a unique threat landscape, user base and security awareness culture. And as important as planning ahead is, so is agility.

An agile programme adapts to changing circumstances, targeting your training to the right people at the right time. It helps ensure that your programme is comprehensive, effective and efficient. And it helps reduce user risk by making the most of the one or two hours per year most organisations can spare for security awareness training.

The most effective programmes align training exercises to real and potential threats. Adapt your programme as circumstances dictate. Life is unpredictable, and sudden changes can create new knowledge gaps and user risks.

Here are some examples of situations where you may change your plan based on need or newly revealed vulnerabilities:

- Your phishing assessments show users understand link-based attacks, but they have trouble spotting attachment-based attacks
- Your organisation is targeted with a growing volume of business email compromise (BEC) attacks
- Your email security team notices attackers using a specific brand of phishing lure or type of attack
- In your knowledge assessments, you notice a specific department struggles with an essential topic

Automating follow-up training

Automating these efforts can make your efforts even more agile. For instance, our customers use the auto-enrollment feature of our solution to automatically assign training sessions based on how users fare in simulated attacks and knowledge assessments. The feature directs training to users who need it most but doesn't force them to complete it at that moment.

Automated follow-up is a good way to tailor training to actual vulnerabilities and gaps rather than using a one-size-fits-all approach that assigns the same training to all users. Targeted training saves users time and makes it easier for stakeholders to embrace.

Letting users test-out

Another way to tailor training is letting users "test out" by showing they understand cybersecurity concepts and are demonstrating good behaviour. If users have taken their foundational training, consistently reject (or report) simulated phishing attacks and perform well on knowledge assessments, they may need less training overall.

The promise of being able to test out may help users feel better about the training and give them an incentive for engaging more thoughtfully with assessments.

SECTION 5

Metrics that Matter: Measuring Your Success

If you run a security awareness programme, you're probably familiar with click rate, also known as failure rate. It's the first and primary statistic we hear about from customers seeking to measure how effective their programme is. And to be sure, it's important to track.

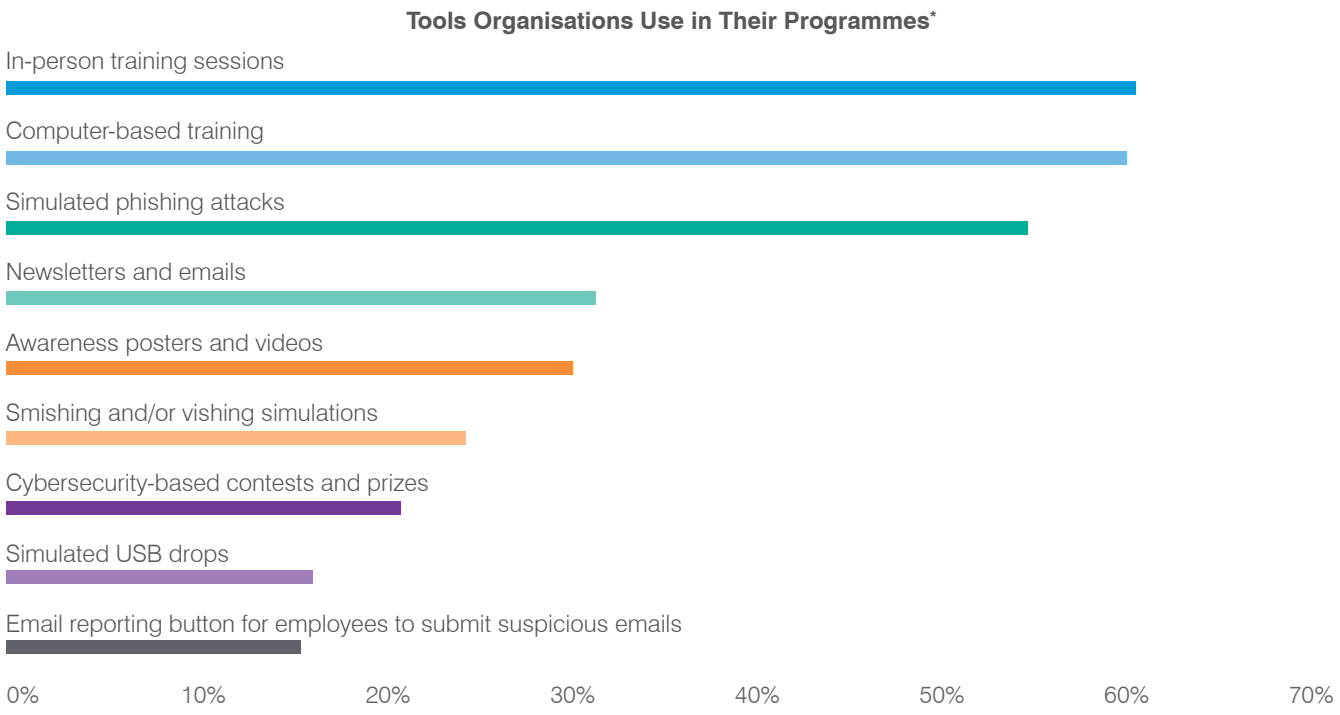
Reporting rate

But it's not the only metric that should be on your radar. Measuring the rates at which users actively report malicious email (actual and simulated) can provide key insights.

Email reporting add-ins enable users to easily alert their security team to suspicious emails. These tools can also measure how many users who receive a simulated phishing email report it, a metric known as the reporting rate.

Unfortunately, just 15% organisations are using these tools in their security awareness programme, according to our *2020 State of the Phish* survey.

Our data found more variability in the reporting rate than click rates, suggesting that the reporting rate is a better overall indicator of behaviour change.



* Multiple responses were allowed.

Source: 2020 State of the Phish

Knowledge levels

Another source of insight is knowledge levels. Click rate and reporting rate can measure user resilience to phishing attacks. But knowledge assessments measure how well they understand other topics such as data privacy, passwords and mobile security.

For instance, highly regulated organisations or departments may require specific training. Understanding users' knowledge levels—and whether they're rising or falling—is essential.

Benchmarking click and reporting rates

If you send out a simulated phishing email, what is considered a "good" click rate? The answer depends to two main factors:

- How difficult and targeted the simulated phishing email is
- How experienced your users are

As a rule, click rates (or failure rates) of under 5% are considered good.

As a rule, click rates (or failure rates) of under 5% are considered good. But a more accurate measure is how much above or below the rate is versus the average failure rate (AFR) across a broader swath of organisations.

Proofpoint, along with many other vendors, provides the AFR of different simulated phishing templates. As shown in this screenshot, a 5% failure rate reflects a poorer-than-average result for some templates.

Average failure rate comparison from our ThreatSim® product *(in green)*.

Jump in this quick meeting	Corporate	8%
FREE GDPR Readiness Tools - Targets Legal or HR	Commercial	3%
College Admissions Help	Consumer	2%
Online dating - Message waiting	Proofpoint - Consumer	5%

That's why comparing your results to these AFRs provides better insight into users' phishing awareness. AFRs can change over time as more organisations use certain templates.

For reporting rates (users who recognise a simulated phishing email as suspicious and report it), aim for 70%. Several of our customers achieved reporting rates of greater than 80%, along with a low failure rate.

Measuring your effect

Security awareness metrics are important, and they should be easy to access within your security awareness software. But the real goal of any security awareness training programme is reducing user risk.

To that end, external metrics can help evaluate and prove the value of your programme. Key measures include:

- Number of malware infections and user machine remediations
- Time and resources spent on abuse mailbox management
- Number of successful phishing attacks from the wild
- Downtime hours for users

These metrics also can help you get continued buy-in for your programme from key stakeholders. One of our customers saved $345,000 in headcount expenses by using a component of our Closed-Loop Email Analysis and Response (CLEAR) solution. (You can read more about this in the Forrester report "The Total Economic Impact Of Proofpoint Advanced Email Protection.")

One of our customers saved

$345,000

in headcount expenses by using a component of our CLEAR solution.

Using your data to change the conversation

A lot of metrics used to talk about how security awareness training—"failure rate," "click rate" and the like—can have negative connotations and emphasise mistakes rather than successes. Other metrics, such as reporting rates and knowledge levels, stress positive behaviours over negative ones. And they better show how users are performing as a line of defence against today's targeted attacks.

Use this data to tell success stories about the ways users are improving your organisation's security posture. Suppose a user reports a truly malicious message and your incident response team was able to remove it before it exposed your organisation. Stories like this can help sell your programme internally to key stakeholders and improve your company's security culture.

SECTION 6

Beyond Training: How to Build a Security Culture

About 99% of organisations say they provide phishing awareness training to their users.[2] But 43% say they train only a portion of their user base. It's no wonder that phishing is still the threat type most likely to cause a data breach.

What can we do better? The answer lies in developing a systematic, sustainable and customised security culture—one that pervades the organisation across all users and all digital activities.

This approach takes a concerted investment of time, effort, resources and companywide support. But the return can be invaluable. A robust security culture can improve your organisation's security posture, compliance and business outcomes. Done right, it can even boost employee morale and productivity.

2 Proofpoint. "2022 State of the Phish." February 2022.

What is a security culture?

According to MIT researchers Keman Huang and Keri Pearlson, a security culture is "the beliefs, values, and attitudes that drive employee behaviours to protect and defend the organisation from cyber-attacks."[3]

In other words, employees—all of them—are active agents in the defence of the organisation's data, systems and resources.

To build a security culture, you need to find ways to change how your people think about the topic. A security culture should be embedded into your core corporate culture. It must inspire—and endure.

What shapes a culture

A cybersecurity culture comprises three overlapping factors:

- **Responsibility for cybersecurity.** Employees feel that they and their coworkers are responsible for acting to prevent security incidents.
- **An understanding of why cybersecurity is important.** Employees believe cyber threats are a material risk to the organisation's success and could affect them personally.
- **The power to act.** Employees feel empowered through their cybersecurity knowledge. The must feel confident that they understand the security policy. And they must trust that the organisation will support them if they make an honest security-related mistake.

Characteristics of a strong security culture

A strong security culture:

- **Is holistic and continuous.** A security culture needs to go beyond training or sporadic phishing simulations. The goal is to raise morale and create a more engaged and secure workforce. You can achieve this in many ways. A security culture promotes learning and awareness through relevant and tailored content and updates on the evolving threat landscape. Users receive emails and other reminders that help them understand why they are taking part in the programme and how it helps them at work—and in their personal lives. And they are encouraged to confidently report suspicious digital events.
- **Has cross-functional advocates.** Support trickles down from the C-suite to management to end users. Apart from leadership, other champions may include security, information technology, HR, compliance and audit, and marketing and public relations.[4]
- **Creates and sustains expectations.** This involves devising and enforcing security policies that drive cultural norms.

3 Keman Huang and Keri Pearlson (MIT). "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture." January 2019.
4 SANS Institute. "2021 Security Awareness Report: Managing Human Cyber Risk." November 2021.

The benefits

A strong security awareness culture can advance the organisation's mission and provide meaningful, measurable benefits. Here are just a few:

Improved agility and resilience

A security culture spurs users to recognise potential threats. It also enables security teams to react to and resolve threats faster. Agility and resilience increase when people are inspired, engaged and supportive of each other to achieve a network effect. The benefits ripple throughout the organisation.

Organisational risk reduction

We live in an era of remote and hybrid workforces, the cloud and personal devices. That's usually a recipe for increased risk. A strong security culture can set leaders' minds at rest—and let them focus on other areas of the business.

Pain-free compliance

Complying with government regulations, industry standards and internal security policies will become easier. That reduces the odds of fines and other penalties.

Competitive advantage

Customers and partners will choose your company over competitors when they feel that yours is safer to do business with. Promote security as a core value.

Common obstacles

Organisations spend millions on security tools, services and staff. But even with those investments, many still overlook their biggest risk factor: people.

Tackling the human factor is the most important security measure you can take. It's also one of the trickiest. Awareness activities can seem disruptive and distracting. Some employees feel that it gets in the way of "real" work. Many resist the extra demands, such as reporting suspicious emails or sitting through training webinars. And technical staff and HR may feel timid about running a security culture because they are not equipped to build and nurture one.

Challenges include:

- Selling the idea to upper management
- Persuasively quantifying ROI
- Convincing users that security training and awareness are positives and getting them to actively take part
- Changing user behaviour

Making it real with the ACE Framework

Motivation is the key to generating a strong security culture. It involves three key ingredients. The first is autonomy. This means making learning personalised and self-directed for every user. The second is mastery. This means giving users the tools and time they need to progress and become proficient with cybersecurity knowledge and skills. And the final ingredient is purpose. This means giving users a sense that they're becoming part of a mission larger than themselves.

Using the ACE Framework

Here are three steps you can take to help you build a sustainable security culture. This is a continuous process that we call the ACE framework.

A Assessing user vulnerability

Every organisation is different, with unique risks and security priorities.

Ask yourself:

- What do your users know?
- Who among them is being targeted? With what types of attacks?
- What would these users do when faced with threats?
- What do they believe? How do they feel about cybersecurity?

By exploring these and other questions, you can determine where the vulnerabilities are.

C Changing behaviour

Building a security culture is an ongoing process, not a one-off event. Take a holistic approach.

That means reaching out to employees on a regular basis through multiple communication channels. These might include regular newsletters, internal blogs and updates on the latest threats and attack vectors.

Offer a variety of content and personalise it. Everyone is different and reacts and learns differently. Remember to continually reinforce the importance of security in a positive way.

E Evaluating progress and tracking success

Share metrics that show progress, continuous improvement and ROI. These quantifiable measures validate your investment. They show the value of a security culture to leadership and the organisation as a whole.

Never let a good crisis go to waste. After an attack, show how a stronger security culture reduced the amount of time, money and effort spent to resolve an incident—or helped the organisation avoid it altogether.

There are many ways to measure your organisation's level of security awareness so that you can evaluate how your security culture has changed user behaviour.

These include:

- Click rates for your most vulnerable users
- Reporting rate for phishing simulations
- How accurately your users can identify true threats

Why it matters

Creating a vibrant security culture benefits the entire cross-section of your users—from the C-suite to the security team to managers and end users.

But there's no one-size-fits-all template. Every organisation has a different personality and unique needs. Some of these differences are driven by the business. Others by the industry. And every culture is driven by a whole host of internal and external factors.

By building an enduring programme that gets buy-in at all levels, security awareness becomes ingrained in your organisation's core values. A true security culture is not just about a one-time security training session. It's a mindset that informs day-to-day business and personal activities.

This section is a high-level introduction to building a security culture.

For a deeper look into security cultures and the ACE Framework, download our e-book *Beyond Awareness Training: Building a sustainable security culture—and why it matters.*

SECTION 7

Conclusions and Recommendations

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

If you haven't been taking a people-centric approach to security awareness training, now is the time to start. Here are five pillars of an effective, efficient programme:

Put people at the centre

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

User awareness training is one of the most important things you can do to secure your organisation. By teaching your users how to recognise, reject and report attempted phishing, you can create a strong last line of defence against today's biggest cyber threats.

Plan your rollout

Every organisation is unique, and no two training programmes will be the same. But as described in Section 2, yours should include all the following elements:

- Defining training needs
- Identifying users with specific training needs
- Mapping out activities
- Creating and managing schedules
- Communicating and testing first steps
- Determining frequency and timing of programme activities

The more diligence and planning you apply to your programme, the more successful your programme will be.

Engage your users

Keeping users engaged is critical to a successful programme. But even the most well-intentioned programme can grow tedious when people don't have rich and meaningful experiences.

The most successful programmes:

- Use branding to make their relevance clear to users
- Use scientifically proven learning principles to change behaviour
- Reinforce training with a diverse mix of content and media
- Enlist champions across the organisation for support and improvements
- Guide users with the right balance of incentives and consequences

Use data to identify vulnerable users, focus training and stay agile

Your first steps should be providing foundational knowledge, understanding users' vulnerabilities, and focusing training where it's needed most. Here, simulated phishing attacks and question-based knowledge assessments can be invaluable insight into where to focus your training efforts. Threat intelligence that provides insight into the attacks your users are facing can also help you align training content to real-world threats. And knowing which users have access to the organisation's most sensitive data can help you tailor training and apply other security controls to high-privilege users.

Automated follow-up training and opt-out options for knowledgeable, low-risk users can help you stay agile at scale.

Measure your success with internal and external metrics

Click rates (or failure rates) for simulated phishing emails are important. But email reporting rates may be an even better measure of how resilient your users are to attacks.

Knowledge assessments can measure how well they understand other topics.

Ultimately, external metrics such as malware infections and downtime can help show the effect and value of your programme.

These metrics also can help you get continued buy-in for your programme from key stakeholders. Use this data to highlight the ways in which users are improving your organisation's security posture. These metrics not only help sell your programme internally but also bolster your company's security culture.

Learn more

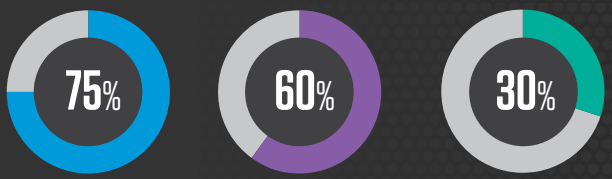
To learn more about your users' cybersecurity knowledge, strengths and weaknesses—and how you can foster behaviour change—take our free People Risk Assessment at proofpoint.com/uk/people-risk-assessment.

Why Proofpoint

Every day, we analyse more than:

2.6B EMAILS	**49B** URLS	**1.9B** ATTACHMENTS
1.7B MOBILE MESSAGES	**430M** WEB DOMAINS	**143,000** SOCIAL MEDIA ACCOUNTS

We are trusted by more than:



OF THE FORTUNE 100 | OF THE FORTUNE 1000 | OF THE FORTUNE GLOBAL 2000

8,000 ENTERPRISES

200,000 SMALL BUSINESSES

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. 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 75 percent of the Fortune 100, 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.

0504-001-02-02 10/22