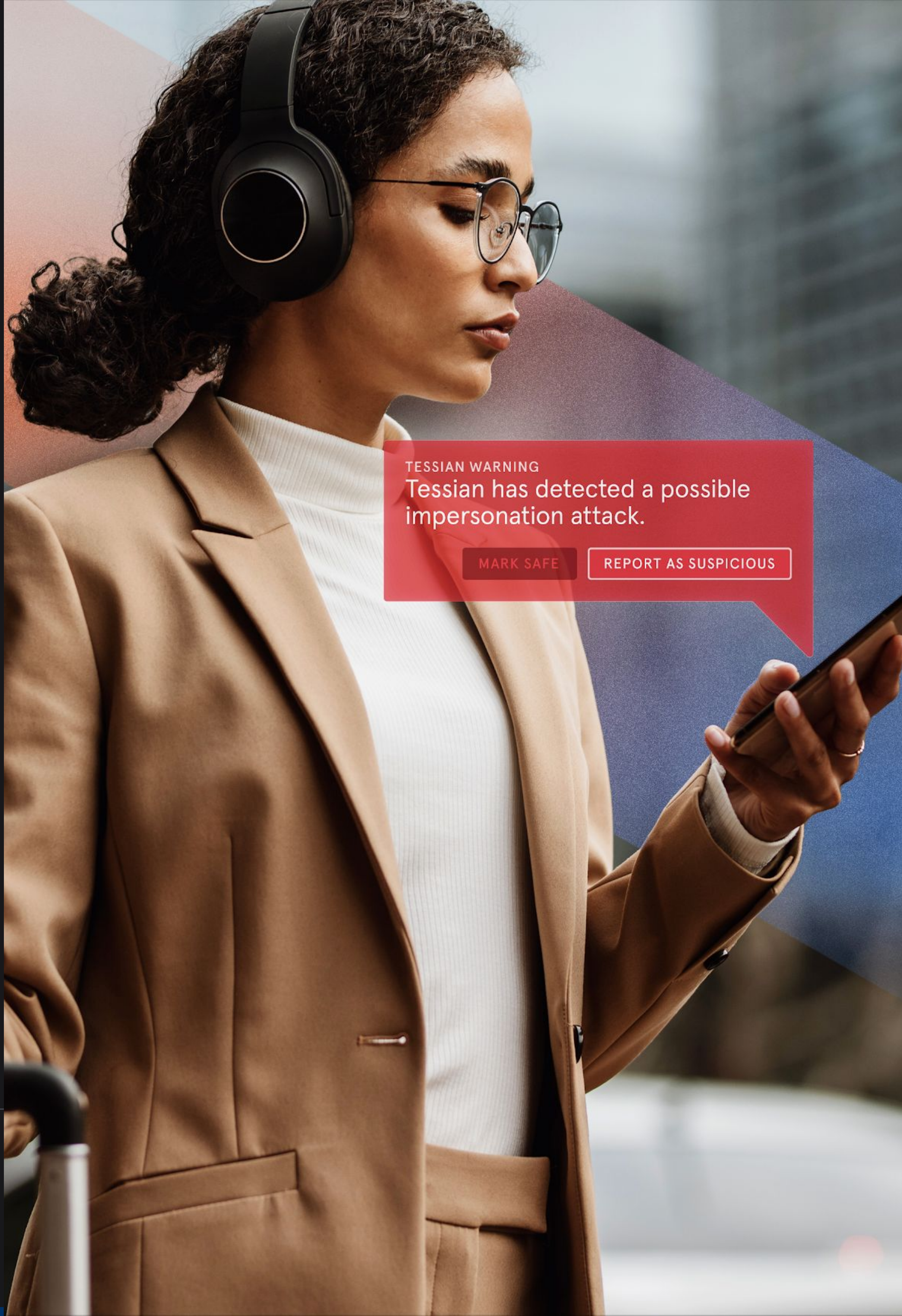
TESSIAN

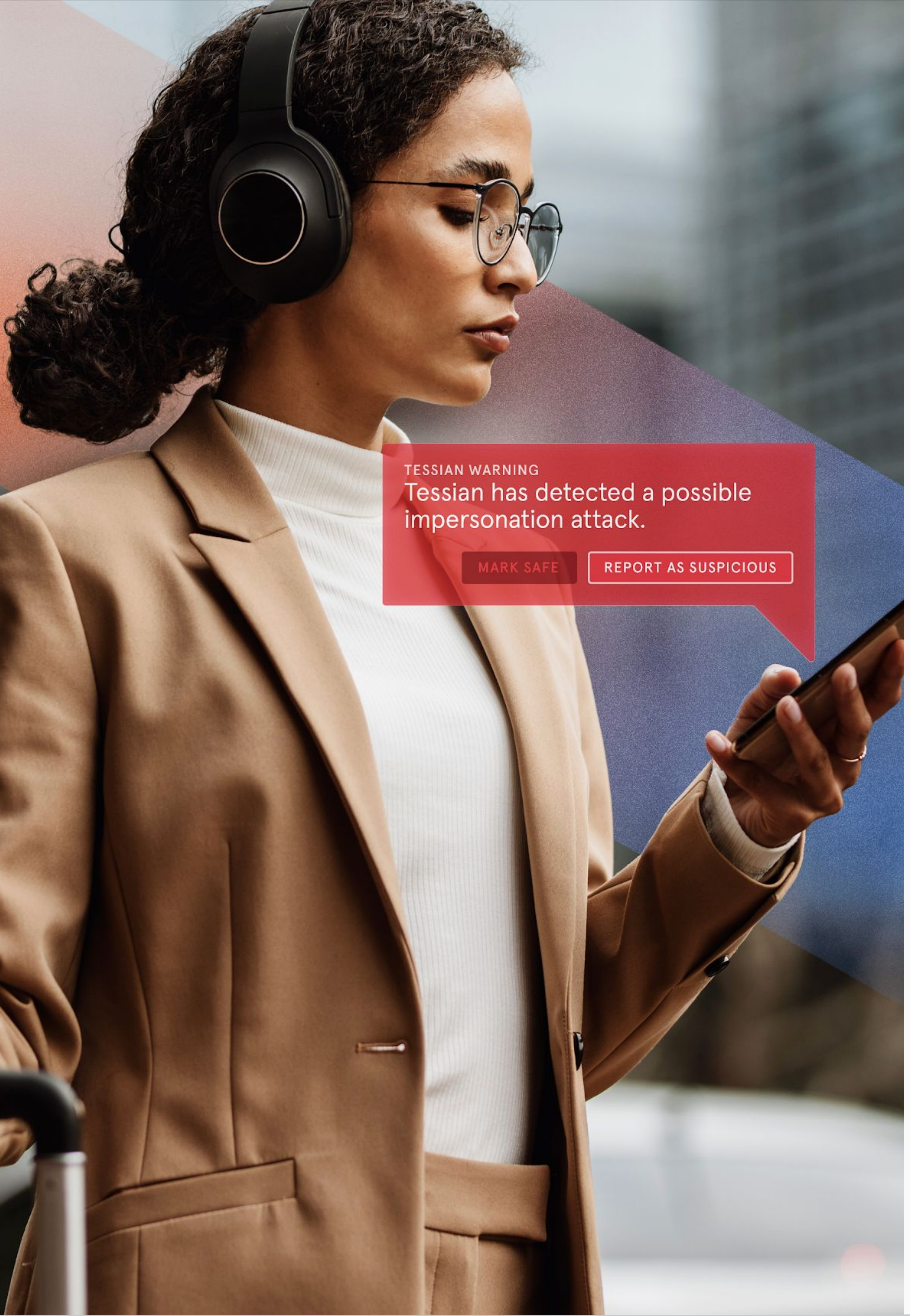
Why the Threat of Phishing Can’t Be ‘Trained Away’

One–off, tick–box training exercises are not enough to protect people from inbound and outbound threats on email, our research reveals.



TESSIAN WARNING

Tessian has detected a possible impersonation attack.



TESSIAN WARNING
Tessian has detected a possible impersonation attack.

Introduction

Today, the number one threat vector for organizations is email. With this in mind, you would assume that email security training would be high on the priority list for every business. Yet, our research reveals that just one third of organizations (**34%**) regularly provide their employees with security awareness training for email.

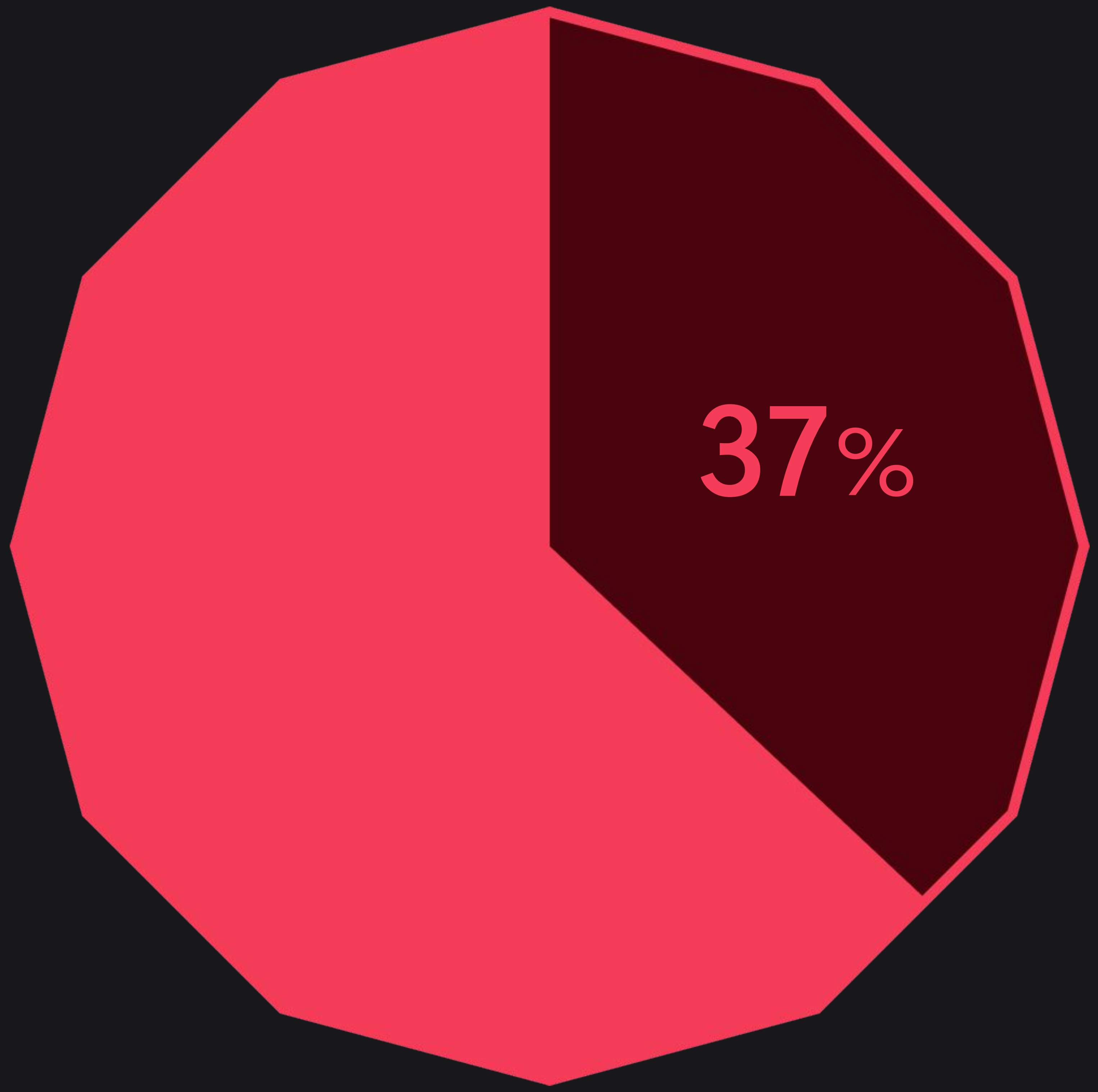
What's more, nearly a quarter (**22%**) of employees we surveyed said they do not receive any training on how to combat cyber threats on email, such as how to spot a phishing attack or what to do if they receive a suspicious email. Nearly one in five (**18%**) said they couldn't remember if this training was ever provided.

This is a cause for concern as 95% of all attacks on enterprises are the result of successful spear phishing and, last year, the number of phishing attacks reported by infosecurity professionals rose by 76%.

For those unfamiliar with the terms, phishing emails are threats in which an attacker pretends to be a trusted entity in order to trick a target into clicking a malicious link, sharing credentials or transferring money. Spear phishing is the more advanced and convincing version, targeted at specific individuals or businesses.

Without training and awareness around these threats, how can organizations expect employees to identify a malicious email and make the right cybersecurity decision 100% of the time?

Percentage in the charity sector that does not provide security awareness training:



The most vulnerable industries

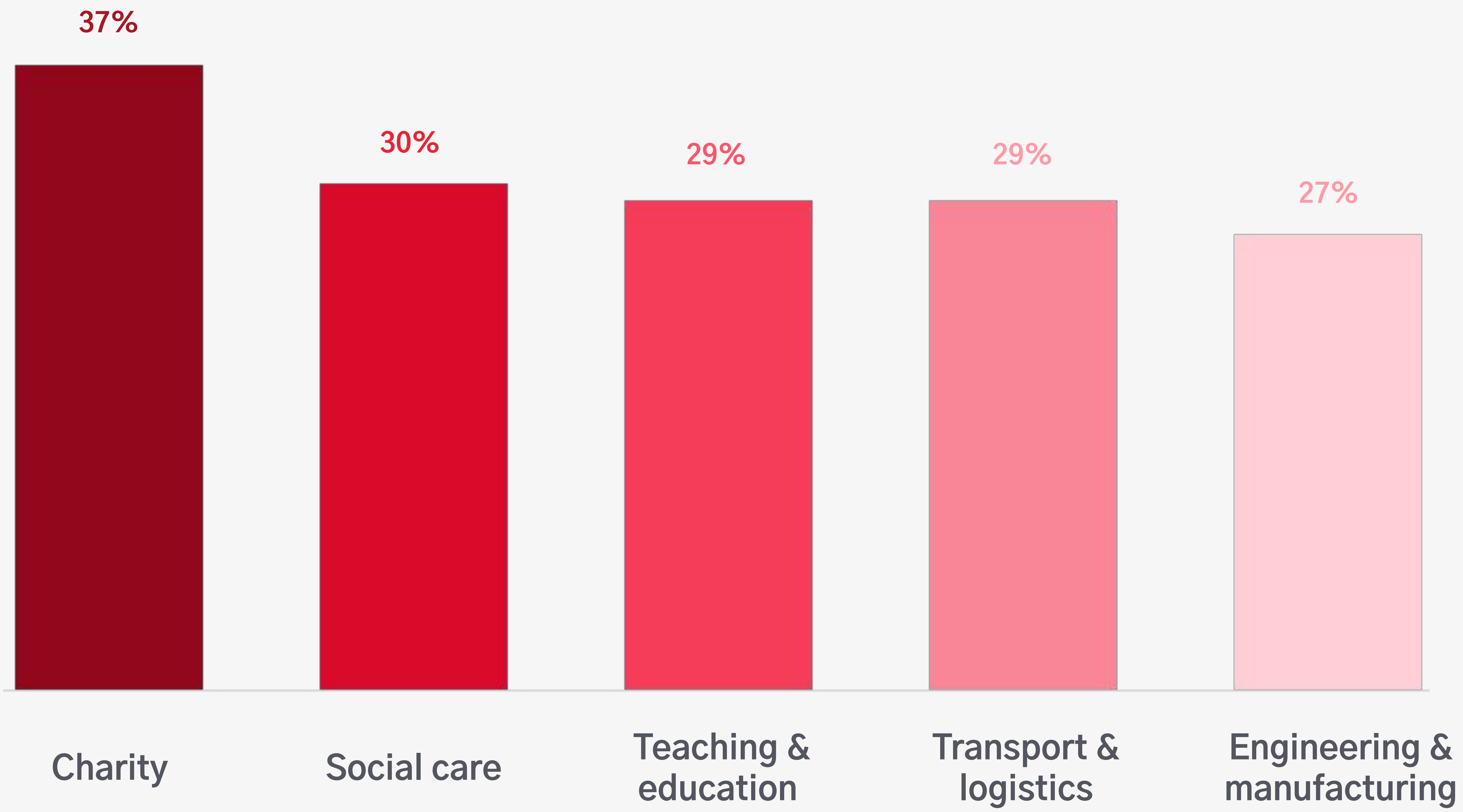
The charity sector was revealed as the industry leaving its employees most exposed to email security threats. Nearly two fifths (**37%**) of employees in the charity sector said their organization does not provide security awareness training to combat cyber threats on email, such as phishing attacks.

This is worrying; according to a 2019 report from the Department of Culture, Media and Sport, one in five charities experienced a cybersecurity breach last year and 81% of those attacks resulted from a fraudulent email.

When you consider how much valuable data charities possess, such as the personal data and financial information of donors – which could include high-net worth individuals and well-known brands – you can understand why the charity sector is a prime target for cybercriminals. In the UK, for example, £1.83bn was donated to charity in 2017, of which £1bn was donated from foundations, over £500m from companies and £313m from high net-worth individuals.

By launching a highly targeted spear phishing campaign to trick employees into sharing donor data, for example, hackers can cause significant financial and reputational damage, exploiting the private – and potentially political – interests of a donor. They can also tarnish the public image of the charity.

Percentage of employees not trained against cyber threats, by industry:



However, the charity sector is not alone in neglecting email security training. Nearly one in three (29%) respondents from the teaching and education sector say they do receive training on cyber threats on email. In fact, the UK's NCSC reported earlier this year, that universities are increasingly becoming a target for cybercriminals, which means training and other defenses are especially needed.

Companies in the engineering and manufacturing sector, too, could be putting themselves at risk as just 30% of employees in this industry report that they are regularly provided with email security training. Manufacturing is frequently reported as one of the most phished industries. Data from Symantec last year found that one in 384 emails sent to manufacturing employees contained malware, while one in every 41 manufacturing employees was on the receiving end of a phishing attack.

The goal? In addition to money and credentials, attackers are also looking to steal intellectual property. Verizon revealed that 91% of breaches in manufacturing involved the theft of trade secrets, business plans and patented designs.

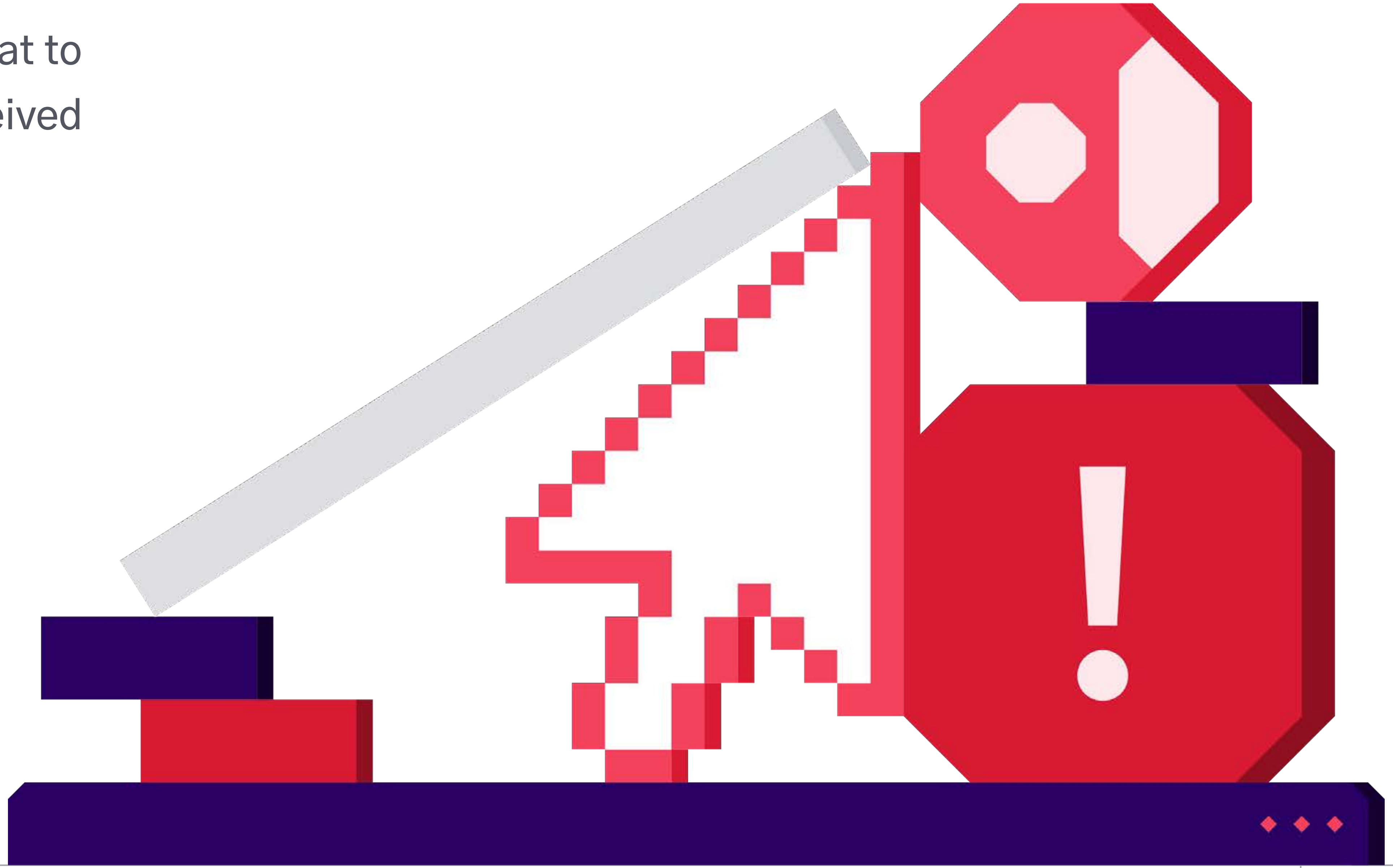
With so much at stake, and with the threat of spear phishing continually rising, email security training needs to be a foundational part of any business' cybersecurity strategy. Training programs are important in raising awareness of the threats and providing basic guidance to employees on what to do when they suspect something they've received is malicious.

SUBSCRIBE TO THE TESSIAN BLOG

Get more insights straight to your inbox.

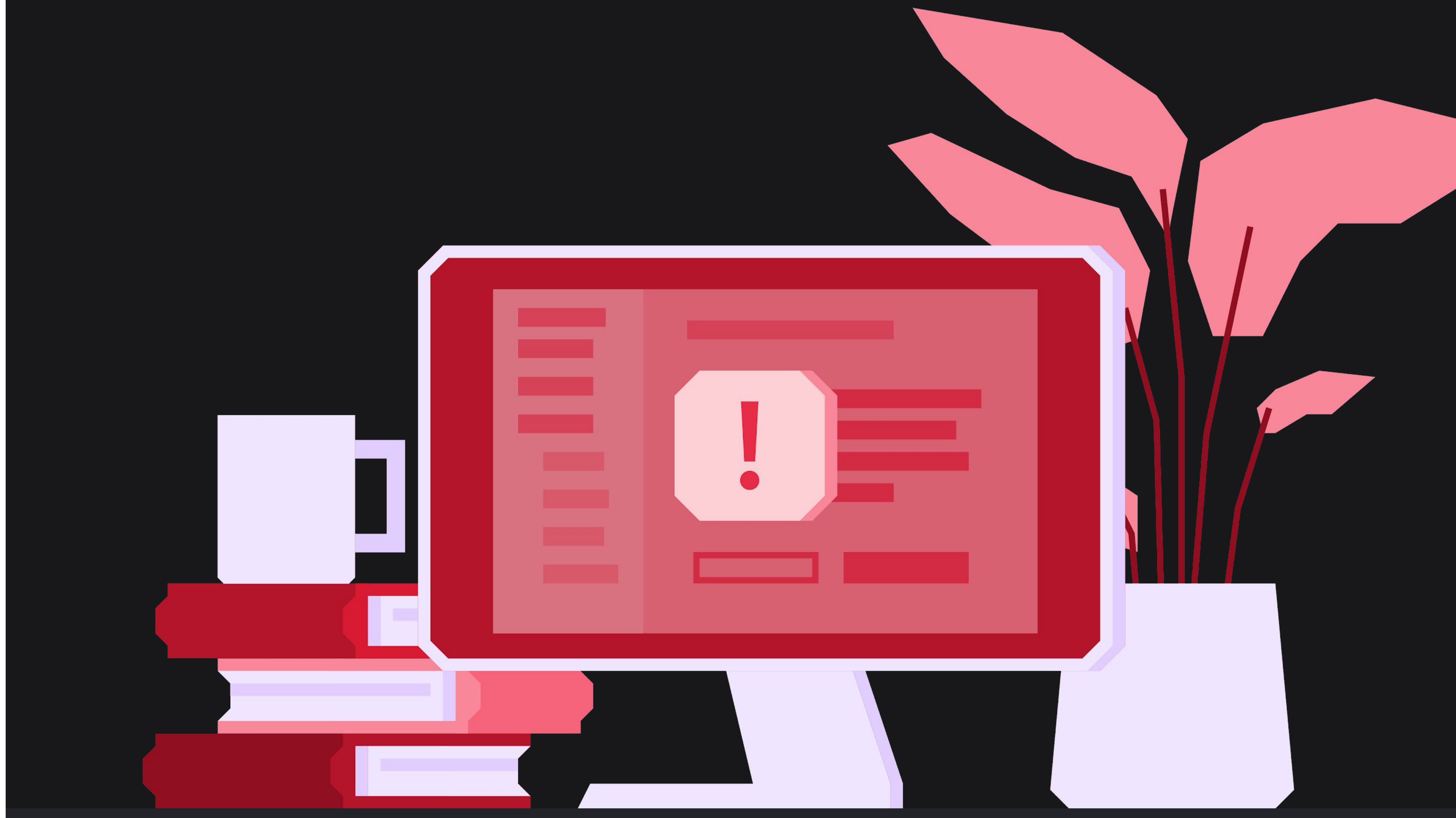
Helpful resources and shareable guides, tips for CISOs, and early access to our latest research.

SIGN ME UP →

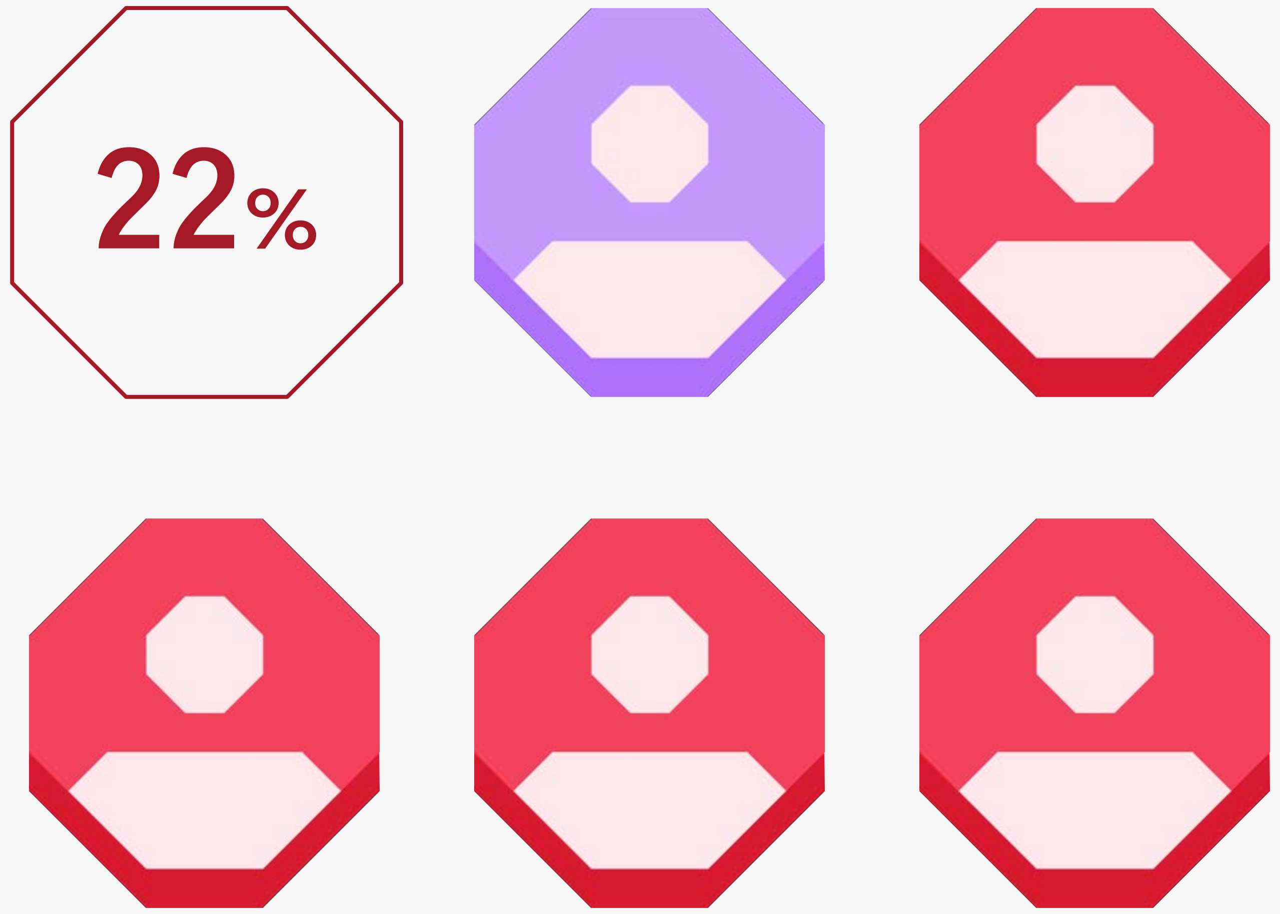


But to what extent can training *really* solve the problem?

Security training in the traditional sense is not enough. All too often training is regarded a tick–box exercise — an annual awareness session to teach employees what to look out for. But spear phishing campaigns are becoming more sophisticated and harder to detect. If we are going to stop the types of targeted attacks we see today, training needs to fundamentally change.



Percentage of employees that remember and action all training they received:



First, today's training efforts need to better resonate. Only one in five (22%) of the employees we surveyed say they remember and action all the training they received.

What's more, employees in industries that regularly provide email security training are actually the most likely to click on phishing emails. For example, despite 45% of employees in the financial services industry saying they receive regular training, one in three admitted to having clicked on a phishing email at work. Similarly in insurance and pensions, 52% of employees say they are regularly trained on email security threats, yet 22% have clicked on a phishing email at work.

TESSIAN

PSYCHOLOGY OF HUMAN ERROR

Understand the mistakes that compromise your company's cybersecurity

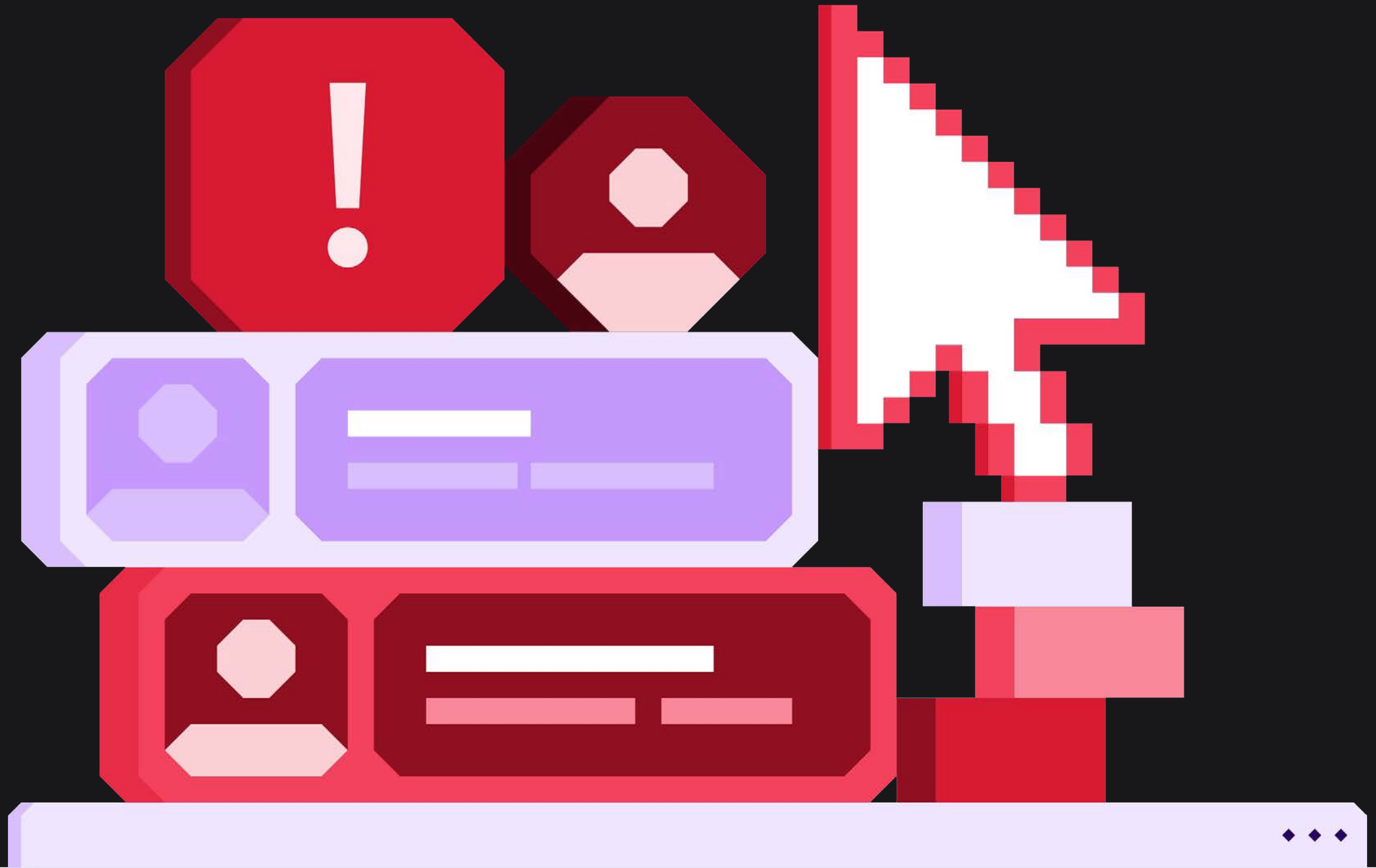
By learning the psychology behind human error, businesses can better understand how to prevent mistakes from happening before they turn into breaches.

TESSIAN

You can read more about the **Psychology of Human Error** in this research report →

Why is this? According to various academic studies, training programs in which individuals are simply made aware of threats seem to have little long–term impact in preventing social engineering attacks. In their own research, cyber psychologists Dr.Helen Jones, University of Central Lancashire and Professor John Towse, Lancaster University, found that even when people are explicitly told to be wary of malicious email messages, they remain vulnerable to making risky cyber decisions.

Jones and Towse' research suggests that although an immediate short–term improvement may follow training sessions, individuals are less able to adapt this knowledge in line with ever–changing and developing threats. "While psychological research consistently shows that regular rehearsal of information is typically associated with improved recall and retention of information, this is less effective when the associated threats are constantly shifting," says Dr Jones.



An impossible task

Training also needs to reflect the fact that cyber threats on email are constantly evolving. All too often, email security training programs advise employees to check the sender’s address or watch out for cues such as a malicious link or payload in order to spot a phishing email.

However, we regularly see new email threats as they find new ways to bypass secure email gateways. Keeping employees up to date with every new technique would require constant in-depth training. Yet, our research found that over a quarter (**26%**) of employees were given email security training when they first joined their company, but received no additional training afterward.

One particularly sophisticated and effective attack that is becoming harder to spot is advanced impersonation spear phishing.

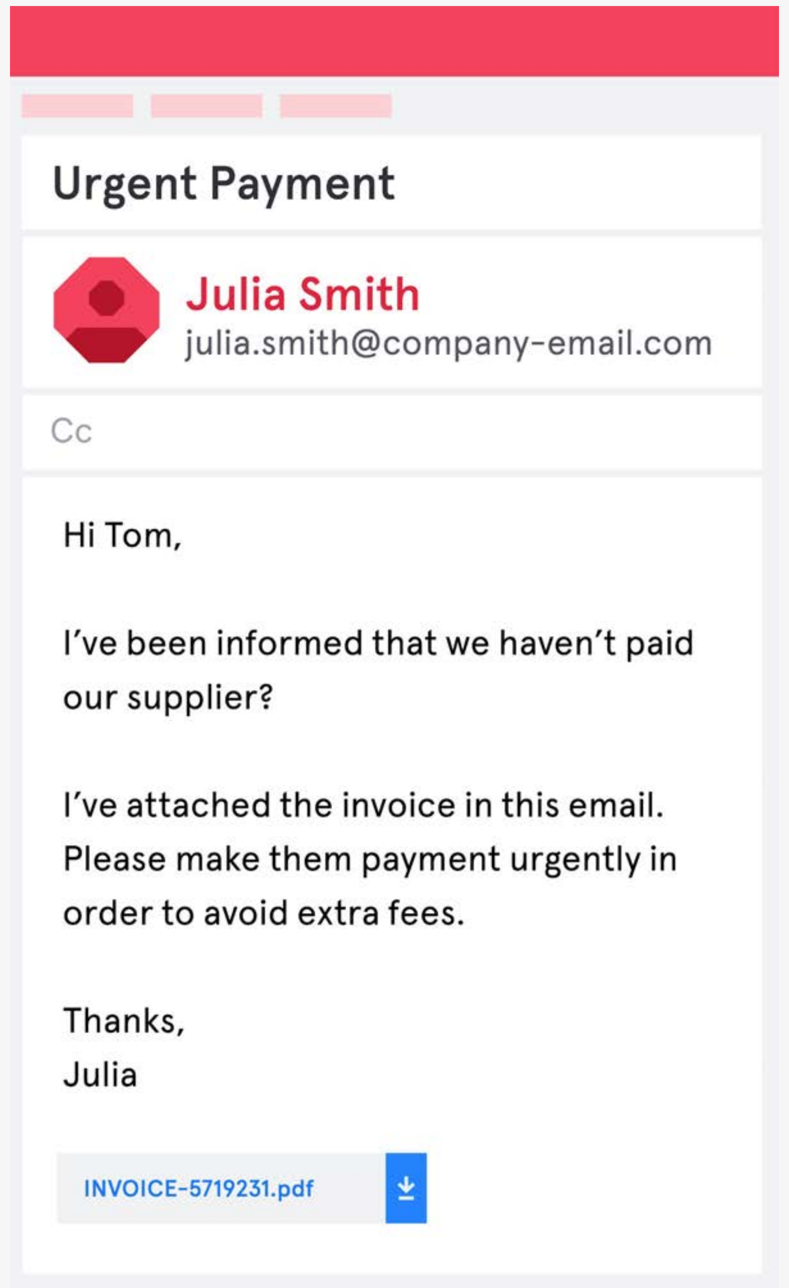
In these attacks, attackers will target an individual, impersonating a trusted contact within an employee's network, to make them comply with their requests. Broadly speaking, there are three categories of advanced impersonation spear phishing, and they can be extremely difficult for the average employee to spot:

❶ INTERNAL CONTACT:
The attacker impersonates a colleague.

❷ EXTERNAL PARTNER:
The attacker impersonates a third party, such as a supplier or customer.

❸ SERVICE PROVIDER:
The attacker impersonates an enterprise service like O365, Microsoft or Amazon.

❶ INTERNAL CONTACT



Urgent Payment

Julia Smith
julia.smith@company-email.com

Cc

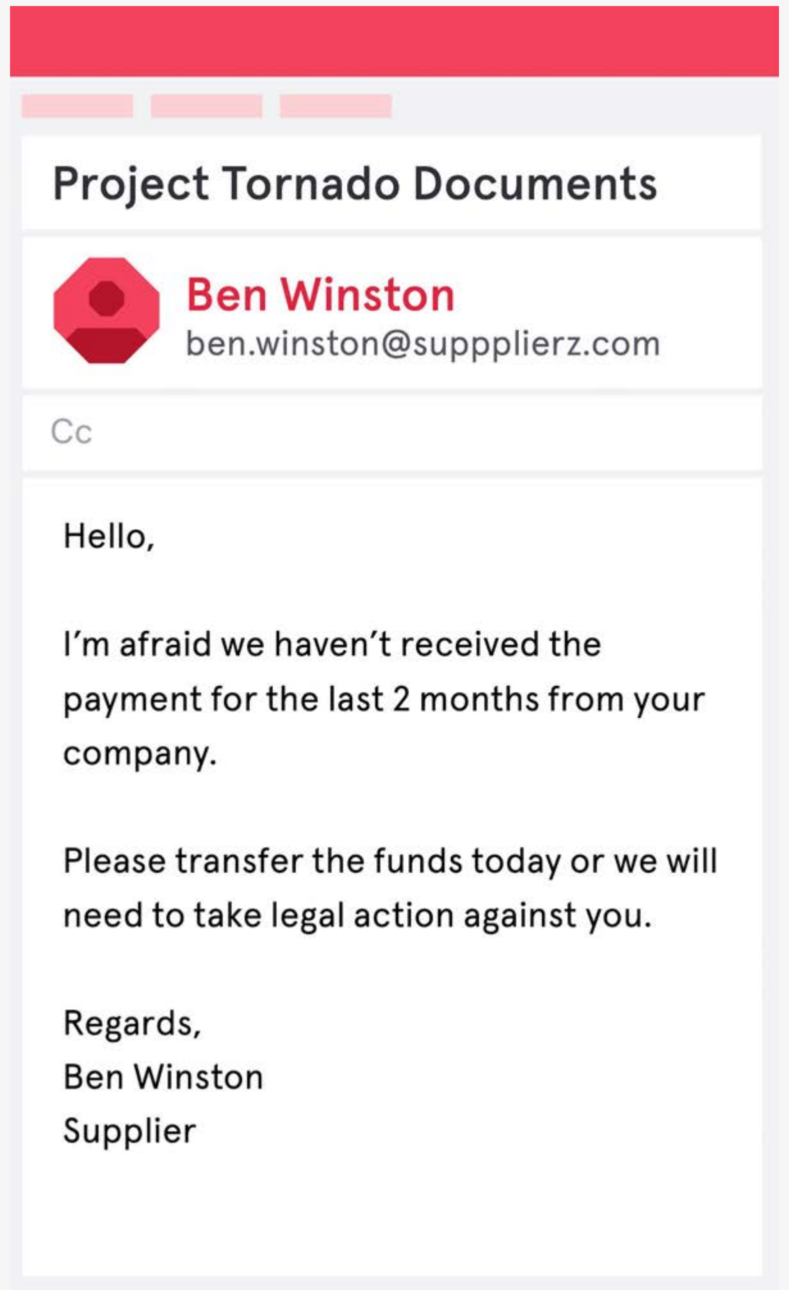
Hi Tom,

I've been informed that we haven't paid our supplier?

I've attached the invoice in this email. Please make them payment urgently in order to avoid extra fees.

Thanks,
Julia

❷ EXTERNAL PARTNER



Project Tornado Documents

Ben Winston
ben.winston@suppplierz.com

Cc

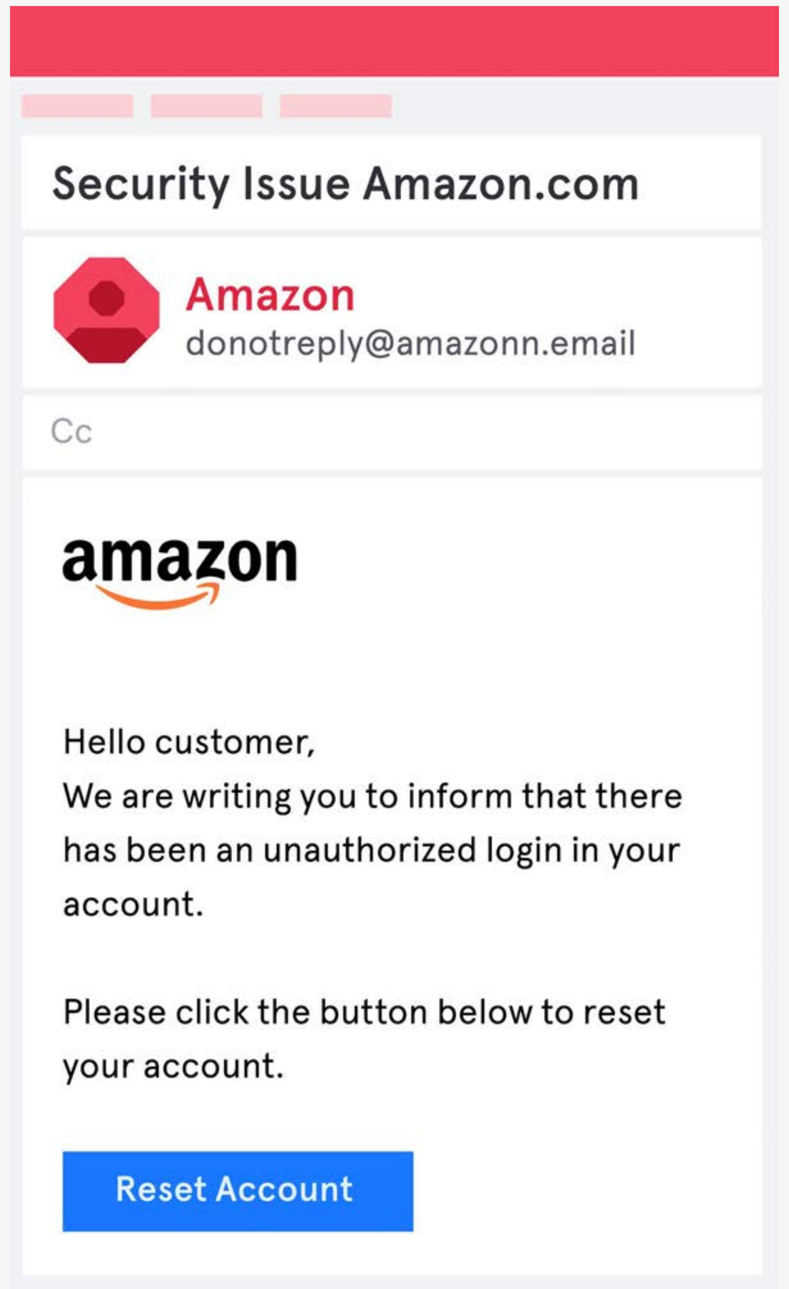
Hello,

I'm afraid we haven't received the payment for the last 2 months from your company.

Please transfer the funds today or we will need to take legal action against you.

Regards,
Ben Winston
Supplier

❸ SERVICE PROVIDER



Security Issue Amazon.com

Amazon
donotreply@amazonn.email

Cc

Hello customer,
We are writing you to inform that there has been an unauthorized login in your account.

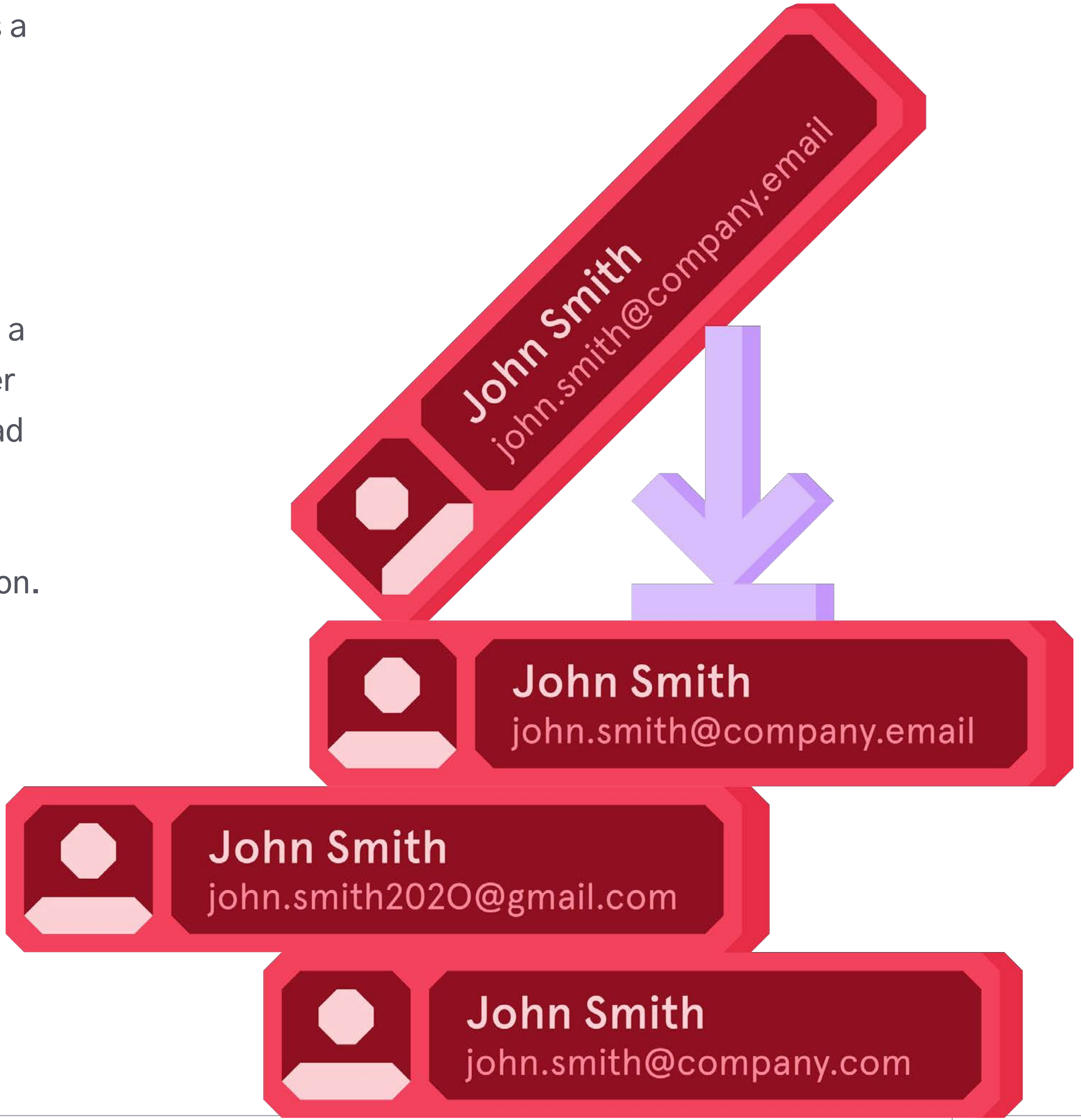
Please click the button below to reset your account.

For any category of advanced impersonation spear phishing, attackers can employ a number of technical manipulations, whether that's display name spoofing, whereby the sender's name looks legitimate but the display address is not or domain impersonation where the domain has been modified to look legitimate — such as .co. or '.email' instead of '.com'. Then there's freemail impersonation in which an attacker creates a fake personal email address while mimicking a legitimate display name.

When you consider how many variations of impersonation a cybercriminal could use to deceive his target, you can see that it becomes nearly impossible to train every employee on every potential manipulation – especially if training takes the form of one-off sessions during onboarding.

This means training guidance to look for cues such as an incorrect sender address become redundant.

Advising employees to look for other cues such as a malicious link or payload is also becoming ineffective. Hackers are increasingly moving from instant payload attacks to delayed payload or zero-payload attacks to bypass standard email defenses. In such incidents, the attacker uses impersonation via the email body copy to build up a relationship of trust with a targeted individual over time, sometimes months, before sending a payload such as "wire money here". The detection of impersonation, therefore, needs to happen much earlier to stop an employee falling for the deception.



Training for the real–world

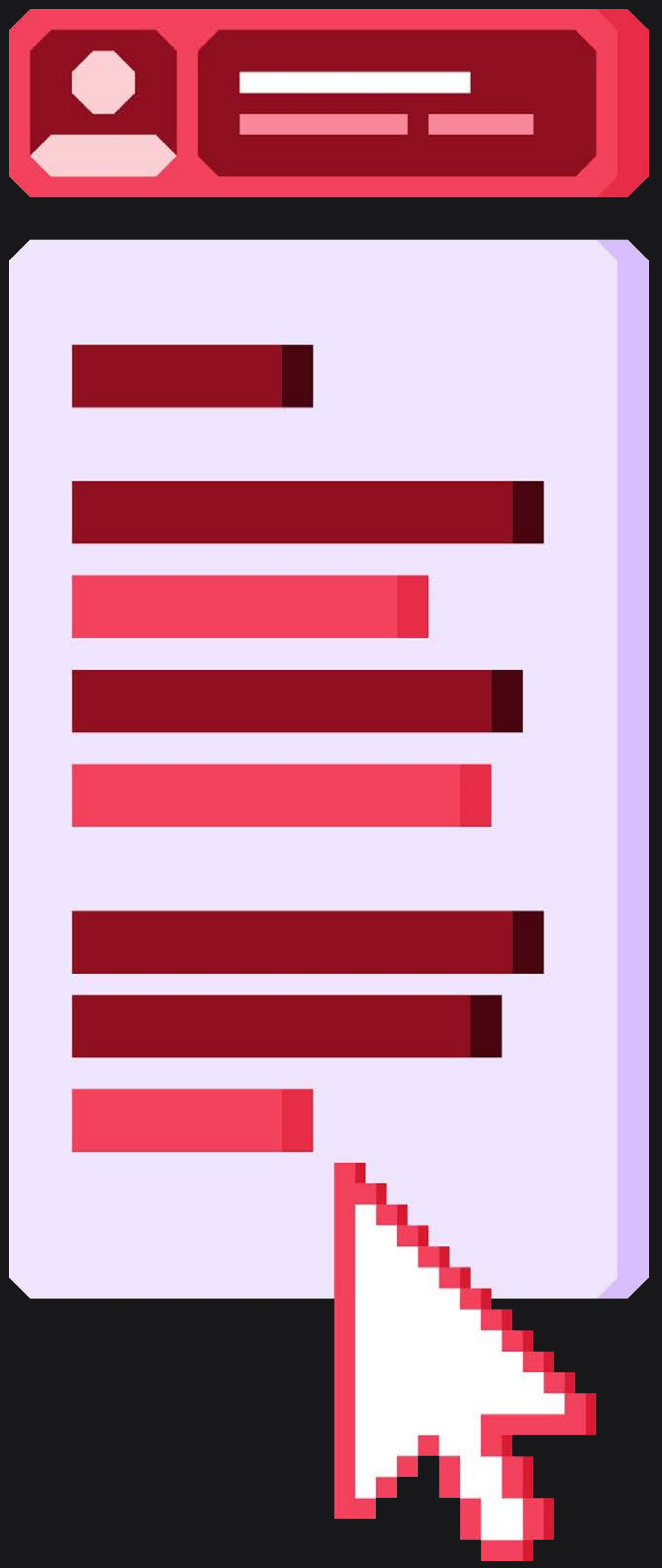
One–off, tick–box training exercises are not enough to stop people falling for increasingly advanced spear phishing attacks. In order for training to be most effective, it needs to be delivered in real–time, in–situ, and it needs to be contextual.

According to Dr. Jones, a more in–depth educational approach to help individuals understand the underlying mechanisms behind scams and attacks may be more beneficial than relying on employees looking out for cues such as poor grammar, a suspicious link and an incorrect sender address.

We can now use machine learning technology to do this. By training advanced machine learning and NLP models on historical datasets, we can look at every relationship that exists on a company’s email network, learn what that relationship looks like in a trusted state and then, in real time, detect anomalies when someone tries to impersonate it. When abnormal activity is detected, solutions like Tessian can automatically alert employees through a notification that explains why the email looks suspicious and provides guidance on what to do next.

Over time, this real–time intervention and education will reinforce secure behavior.

Simply telling your employees what to watch out for won’t work, because people make mistakes, they break the rules and they are easily deceived. As threats evolve, training cannot be your only defense; you cannot rely on your people to detect advanced impersonation attacks 100% of the time. So as spear phishing attacks become more sophisticated, so too do your businesses’ defenses and approach towards training.



TESSIAN

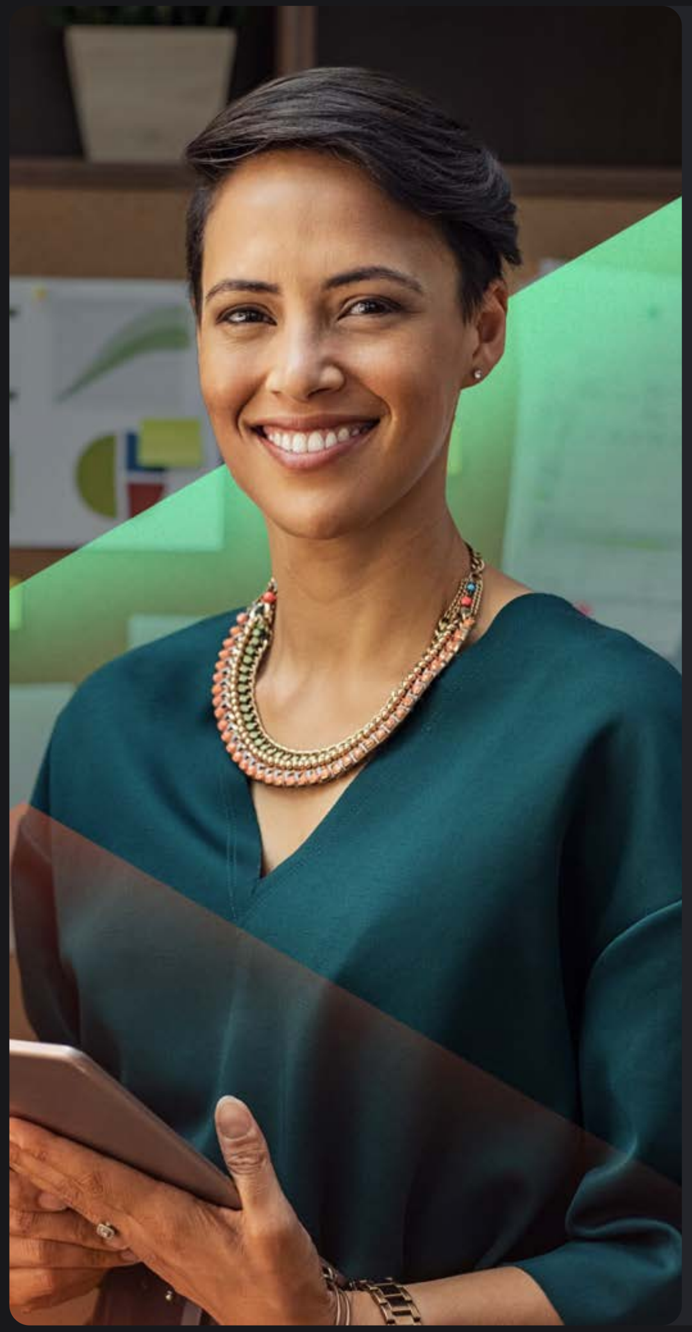
Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error – like data exfiltration, accidental data loss, business email compromise and phishing attacks – with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like March Capital, Sequoia, Accel and Balderton.

TESSIAN.COM

onepoll.

About OnePoll

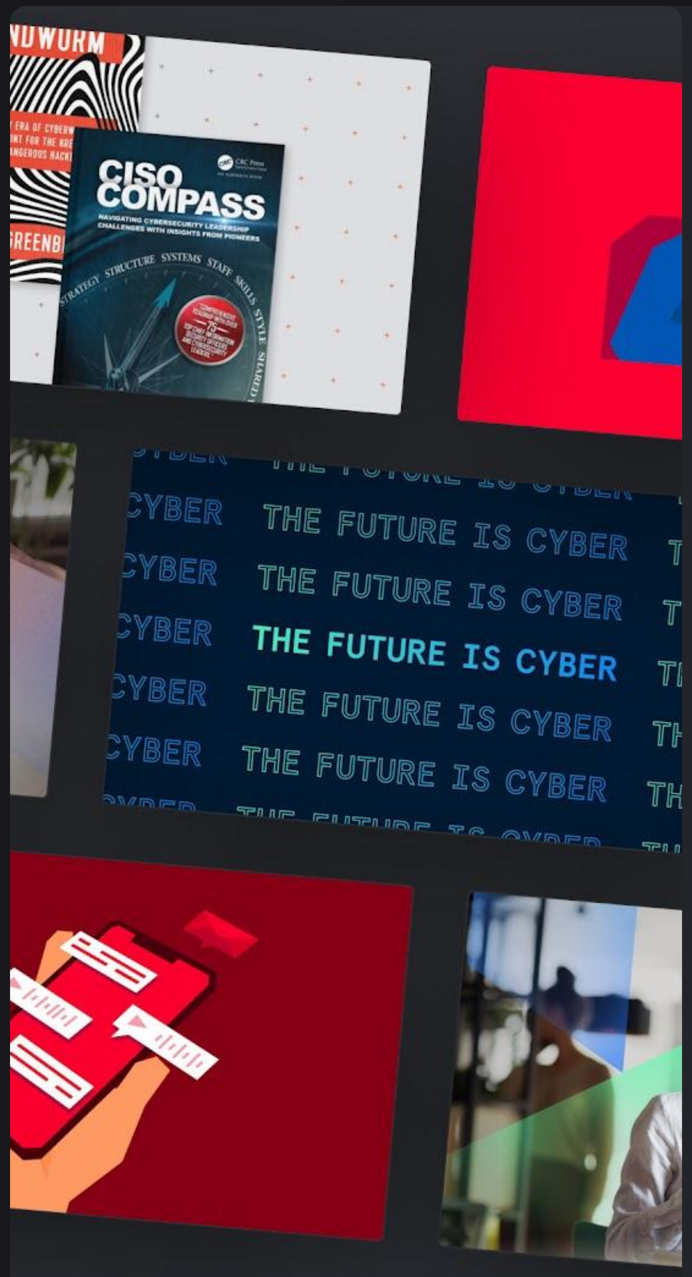
Tessian conducted a survey of 1,000 UK employees, using third-party research house OnePoll. OnePoll surveyed respondents that met the following criteria: UK employed adults who work for companies with over 100 employees, and typically work '9–5 hours'.



Learn about Human Layer Security.

Want to learn more about how Tessian prevents spear phishing, business email compromise, account takeover, and other targeted email attacks?

REQUEST A DEMO →



More Insights, Every Week.

Subscribe to our newsletter to get more insights straight to your inbox.

- Helpful resources and shareable guides
- Tips for CISOs
- Early access to our latest research

SIGN ME UP →

Share this report

TESSIAN.COM/RESEARCH →