TESSIAN

TESSIAN REPORT

Why the threat of phishing can’t be ‘trained away’

OVERVIEW

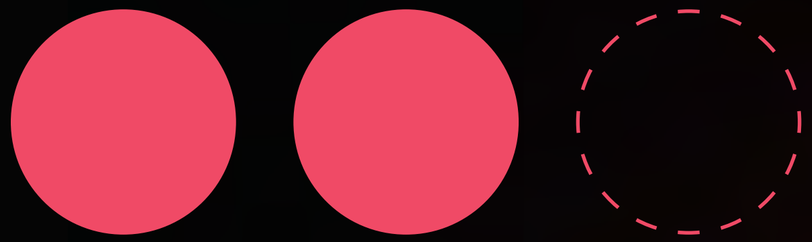
Security awareness training is important in teaching employees the basics of how to stay safe online. Yet, two thirds of employees are not regularly trained about cyber threats on email - the number one threat vector in organisation - and those that are trained do not remember what they are taught. So, to what extent can training really stop people falling for phishing attacks?

CONTENTS

Introduction

2 out of 3

employees are not regularly trained on email security.



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 because 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?

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 [1], 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 [2], of which £1bn was donated from foundations, over £500m from companies and £313m from high net-worth individuals.

Percentage of employees not trained against cyber threats, by industry

By launching highly targeted spear phishing campaigns to trick employees into sharing donor data or transferring funds to phoney accounts, hackers can cause significant financial and reputational damage. Just last year, for example, Save the Children reported that it had fallen victim to a business email compromise scam that cost the charity $1 million [3]. In the same week, the Wellcome Trust - the UK's largest charity organisation, with around £26 billion of assets - revealed that it had suffered two successful phishing attacks [4] after the email of four senior executives was compromised. This resulted in unauthorised access to systems and the loss of commercially sensitive data.

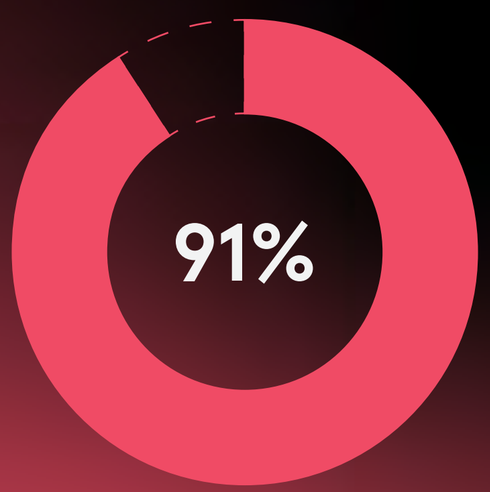
The sector must also consider that, with access to sensitive donor data, hackers could exploit the private - and potentially political - interests of a donor, further tarnishing the public image of the charity.

However, this 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 [5] 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 [6] 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 [7] 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.



of breaches in manufacturing involve the theft of trade secrets, business plans and patented designs

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.

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.

Why is this? According to various academic studies [8], 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 hackers 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:

INTERNAL CONTACT
the attacker impersonates a colleague

EXTERNAL PARTNER
the attacker impersonates a third party, such as a supplier or customer

SERVICE PROVIDER
the attacker impersonates an enterprise service like O365, Microsoft or Amazon

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 email scams we see today. Simply telling your employees what to watch out for and, consequently, how to act for will not work in the fight against advanced spear phishing attacks and other threats on email.

Training needs to fundamentally change. It needs to be provided regularly, in-situ and it needs to be contextual. According to Dr. Jones, an 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.

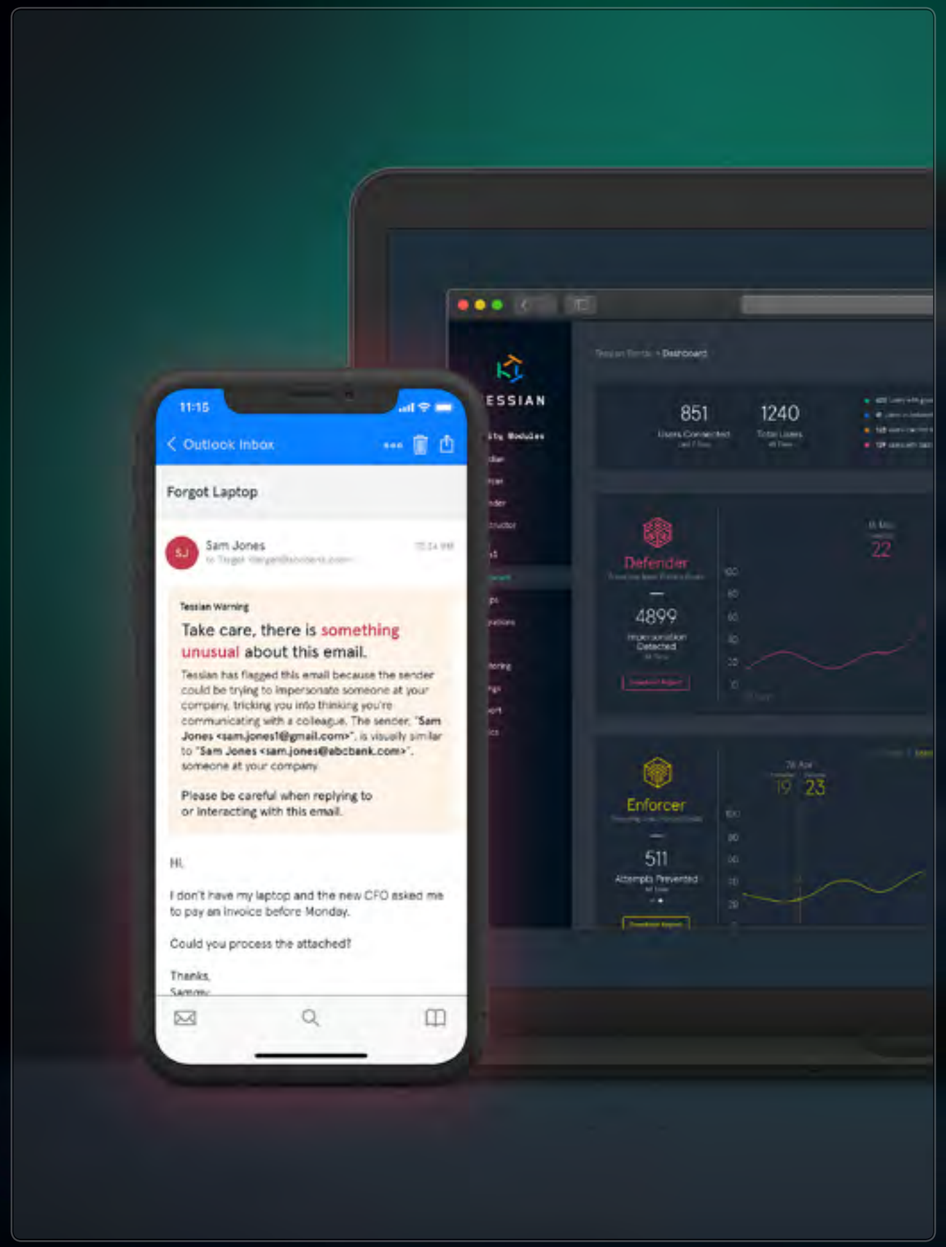
However, it's also important that training is supported by technology that can automatically detect suspicious emails and alert individuals to potential threats. Businesses that rely on training as their only defense against spear phishing attacks still ultimately relying on their people doing the right thing 100% of the time. This is unrealistic - not only because employees are faced with the impossible task of identifying every type of impersonation but also because people make mistakes, they break the rules and they are easily deceived.

For the first time, machine learning provides that extra layer of protection against human error on email. 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.

We cannot 'train away' phishing, but we can prevent people falling prey to the scams. As threats continue to evolve and as spear phishing attacks become more sophisticated, businesses' defenses and approaches towards training, too, need to transform and become more sophisticated.

About the research

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'.



References

1 Department of Culture, Media and Sport: Cyber Security Breaches Survey 2019
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

2 Coutts: Million Pound Donors Report 2017
https://www.thirdsector.co.uk/donations-1m-totalled-record-183bn-last-year-report-shows/fundraising/article/1450633

3 The Boston Globe: Hackers fooled Save the Children into sending $1 million to a phony account
https://www.bostonglobe.com/business/2018/12/12/hackers-fooled-save-children-into-sending-million-phony-account/KPnRi8xIbPGuhGZaFmIhRP/story.html

4 Wellcome Collection: Annual Report and Financial Statements 2018
https://wellcome.ac.uk/sites/default/files/wellcome-trust-annual-report-and-financial-statements-2018.pdf

5 NCSC: Active Cyber Defence - The Second Year 2019
https://www.ncsc.gov.uk/report/active-cyber-defence-report-2019

6 Symantec: 2019 Internet Security Threat Report
https://www.symantec.com/security-center/threat-report

7 Verizon: 2018 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

8 Marianne Junger, L. Montoya, F.J. Overink (2017): Priming and warnings are not effective to prevent social engineering attacks
https://research.utwente.nl/en/publications/priming-and-warnings-are-not-effective-to-prevent-social-engineer

TESSIAN

Tessian is building the world's first Human Layer Security platform to automatically secure all human-digital interactions in the enterprise. Today, our filters use stateful machine learning to protect people using email and to prevent threats like spear phishing, accidental data loss, data exfiltration and other non-compliant email activity. **tessian.com**