TESSIAN | uclan University of Central Lancashire

TESSIAN REPORT

Why Do People Make Mistakes?

Changing the Narrative Around Human Errors Over Email

OVERVIEW

With human error accounting for the majority of all data breaches, people are considered the weakest link when it comes to security. But beyond dismissing errors as human nature, have you ever wondered why people make these mistakes in the first place?

The so-called weakest link

We often hear how humans are the weakest link when it comes to security. Headlines reporting that 88% of data breaches are the result of human error[1], and that incidents of phishing scams continue to rise, serve as a constant reminder for IT security teams that people pose a huge risk to the safety and privacy of an organization’s data and systems.

People make mistakes; it’s human nature. And the consequences of these mistakes can be devastating for any business. All it takes is one person to accidentally send an email containing sensitive information to the wrong person or an individual to respond to an impersonation scam for data or systems to be compromised.

But is it entirely fair to put all the blame on employees? Are we, actually, placing too much pressure on people to act, and act perfectly, as a company’s first line of defense?

In this report, we don’t look at how people make mistakes, but instead, we examine *why*. With insight and research from academics Dr Helen Jones (University of Central Lancashire) and Professor John Towse (Lancaster University), we take a look at what happens when people make decisions and reveal how modern-day work environments and practices can actually impair a person’s ability to make the right decision 100% of the time, when faced with a cyber threat. This, we argue, can lead to dangerous cyber security behavior over email, and consequently puts data and systems at risk.

By doing so, we hope to change the narrative around humans being the weakest link in security and instead highlight the need for businesses to find ways to protect their people, reinforce safe email practices and empower employees use email securely.

[1] *88% of UK data breaches caused by human error, not cyberattacks* | **Verdict.** Verdict.co.uk. https://www.verdict.co.uk/uk-data-breaches-human-error/

Why do mistakes happen?

Generally speaking, a mistake is a decision or action that produces an unwanted or unintentional result. As emotional beings, humans make mistakes because we cannot always make objective decisions in the same way technical systems can. Because of this, we sometimes make decisions that are suboptimal, and this can lead to risky cybersecurity behavior - particularly on email.

Today, the average worker spends nearly a third of their working week on email[2], sending and receiving around 124 emails every day. Given our reliance on email, it's no wonder why email is the number one threat vector in organizations and the cause of nearly all data breaches. In fact, 94% of malware is delivered by email and it is where 96% of social attacks occur[3], with hackers crafting targeted and sophisticated phishing emails to trick unwitting employees.

Interestingly, cyber-psychologists Helen Jones and John Towse argue that in the majority of situations, we will actually make the 'right' cybersecurity decision. In their recent work, they asked individuals to identify legitimate and phishing emails and found that on average, people correctly judged two-thirds of the emails[4].

Yet one-third of the time, judgement calls failed.

According to Jones and Towse, this is because the accuracy of decision-making may, in part, be influenced by an individual's ability to engage in more analytical thinking.

It is useful, here, for us to provide a very brief overview of what happens when people make a decision. The Dual Systems Theory of Reasoning is one of a number of explanatory models popular among psychologists, and proposes two psychological systems for generating behavioral responses:

SYSTEM 1

Our emotional and intuitive response. It is automatic, fast and low effort. It allows for rapid decision making, with individuals dedicating less time to information processing. This is, usually, the dominant system in decision-making processes.

SYSTEM 2

Our analytical response. It is controlled, slow and high effort. Decisions are made using knowledge and processing necessary information coming in from the situation, allowing for rational, considered responses. It overrides System 1 in the decision-making process.

The deployment of systems depends on the nature of the individual and the nature of a specific situation. Jones and Towse believe there are situations - particularly when we are online - where the accuracy of decisions can be compromised and our judgement impaired.

[2] *The social economy: Unlocking value and productivity through social technologies* | **McKinsey and Company.** Mckinsey.com. https://www.mckinsey.com/industries/high-tech/our-insights/the-social-economy

[3] *2019 Data Breach Investigations Report* | **Verizon.** Verizon.com. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[4] *Email fraud: The search for psychological predictors of susceptibility* | **Lancaster University.** Research.lancs.ac.uk. http://www.research.lancs.ac.uk/portal/en/publications/email-fraud(d8a5407f-2782-4f75-bbb6-00e0ca243db2).html

Drawing on a long history of research into decision-making offline and online, they outline a number of elements that can lead to an individual making a mistake or falling victim to a cyber threat over email:

PERSUASION

The threat may be sophisticated and subtle. Persuasive techniques embedded in the messaging of socially-engineered spear phishing attacks - such as urgency cues, appeals to authority - can increase believability by appealing to an individual's emotional thinking, making it more difficult to detect a threat.

OUR PSYCHOLOGICAL MAKEUP

Some people may be predisposed to less analytical thinking styles and could overlook cues that would otherwise indicate the presence of a cyber threat.

TIME PRESSURES

Detection of threats may be impaired when an individual is under time pressure or when distracted or fatigued.

HIGHER FREQUENCY

Every quarter, incidence of phishing continue to rise. Simply, the more cyber decisions or threats we face, the more likely it is that we will make a mistake.

Alongside Jones and Towse's research, Tessian also conducted its own research in which we surveyed 1,000 UK employees about their working environments and practices. It was clear from both sets of data that there are factors in people's working lives that can significantly impact the ability to make the 'right' decision when it comes to email security.

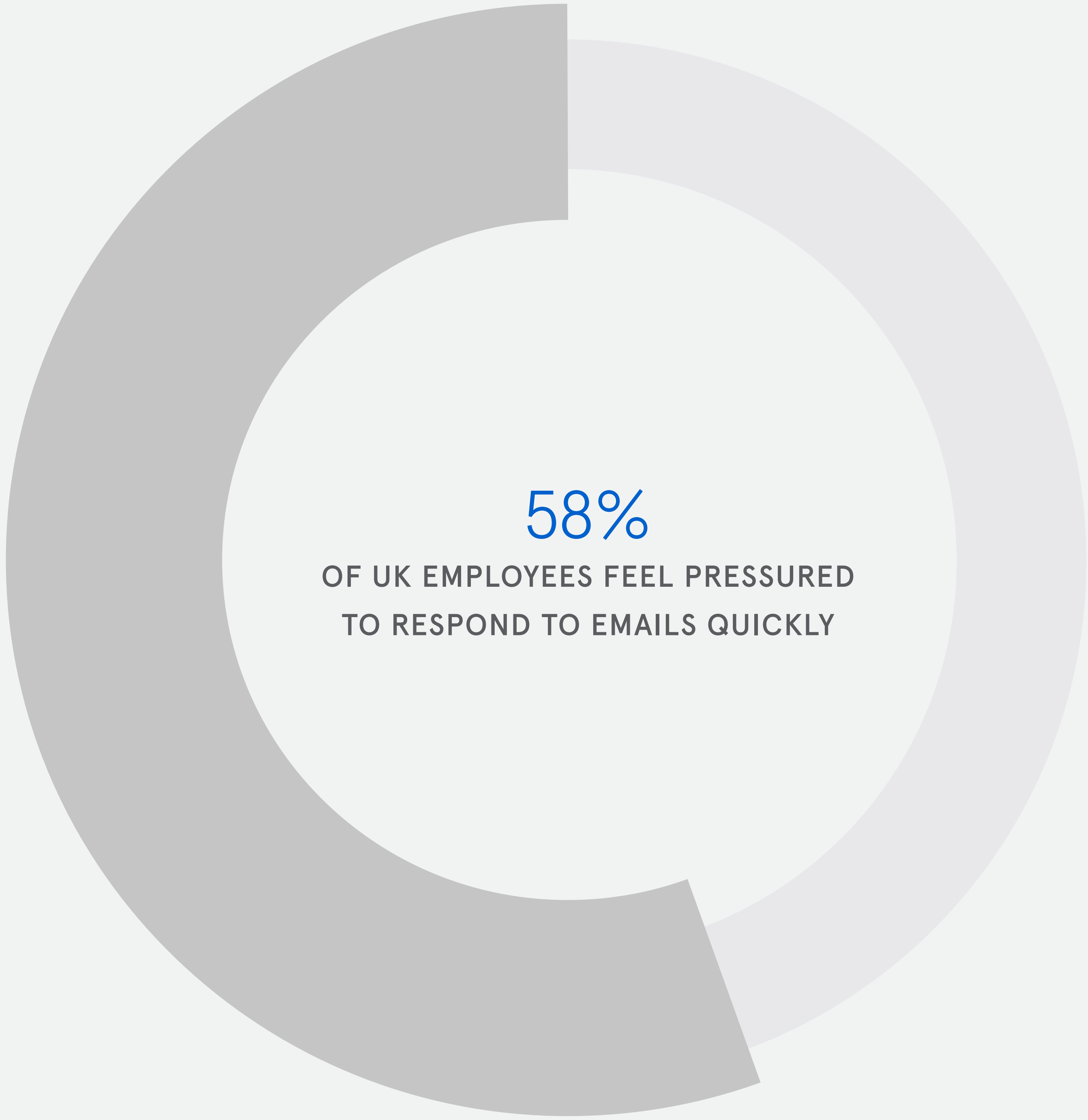
From tiredness and stress to demanding workloads, daily pressures at work can mean that employees rely on automatic, habitual responses, instead of the more effortful thinking style which allows for evaluation of available information to make an informed decision. Over the next few chapters, we take a look at each of these factors in detail.

Quick-to-click culture

The majority of UK employees (58%) say there is pressure or expectation within their organization to respond to emails quickly. Those working in the financial services industry were the most likely to say there is a 'quick to click' culture, with 70% of respondents saying they feel pressured to respond to emails quickly.

Academic reports have repeatedly shown that time pressure impacts decision accuracy[5]. In their study, Jones and Towse split participants into two groups; one group were told they had five minutes to identify phishing from legitimate emails, the other had as much as they needed. The results showed that participants under time pressure made fewer correct decisions. Although the effect of time pressure was modest in this research, even a small effect could lead to a slip-up that endangers the individual or their organization.

This, they argue, demonstrated a reliance on 'System 1' thinking when under pressure. Those with no time pressures may have been more likely to employ rational decision-making mechanisms - to think to themselves, "does this email seem right?". A 'quick-to-click' culture, then, can potentially have a significant impact on employees' ability to assess the situation in front of them.



[5] *The effect of time pressure on decision-making behaviour in a dynamic task environment* **| Science Direct.** Sciencedirect.com. https://www.sciencedirect.com/science/article/pii/0001691894900132

"The increased pressure upon employees to be constantly connected and on-the-go means that there is a higher likelihood of distraction when completing tasks," comments Jones. "Additional time pressure on tasks and the need to engage in multitasking means we dedicate less attention to each task. As such our decision-making can become suboptimal."

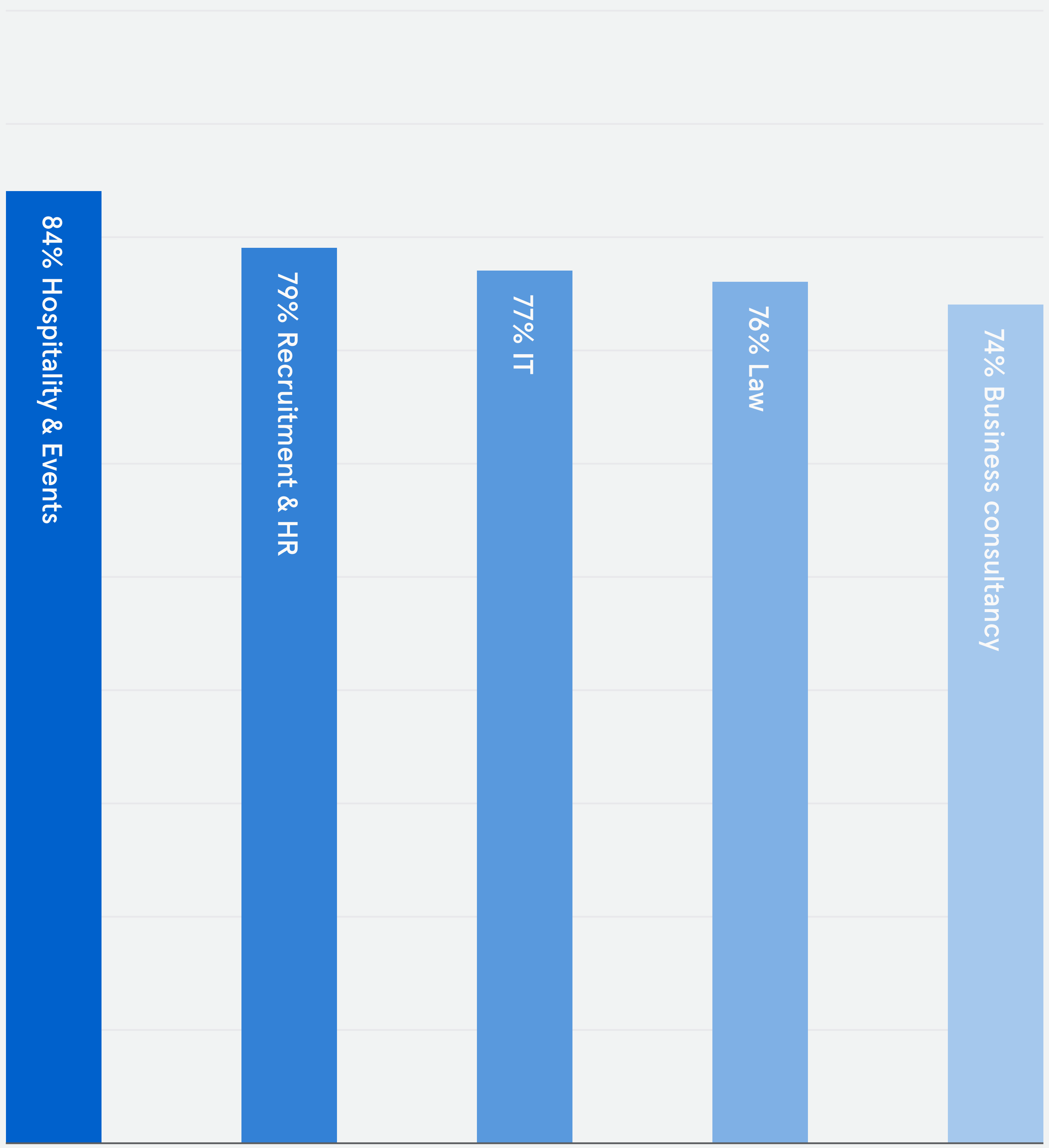
"What's more, increased engagement with multiple points of contact means that it may be difficult for an employee to keep track of everyone they receive emails from, and their reasons for getting in touch. Employees are placed in the position of having to make regular trust decisions, which will only increase the likelihood of a mistake being made."

A shift towards becoming a mobile workforce hasn't helped the situation either. 59% of UK employees told us they use their mobile phones to send work emails out of office hours, with nearly a third doing so at least 2-3 times a week.

Those in the hospitality industry were the least likely to 'switch off', with 84% of respondents saying they use their phone to send out-of-hours emails every week. The scenario was similar in recruitment/HR (79%), IT (77%), law (76%) and business consulting (74%).

This is a cause for concern; Verizon research has shown that people are significantly more susceptible to social attacks they receive on mobile devices, due to a confluence of design and the way people interact with mobile devices while simultaneously doing other activities[5]. In fact, two in five respondents (39%) surveyed by Tessian admitted that they respond to emails much more quickly on their phones.

INDUSTRIES MOST LIKELY TO HAVE EMPLOYEES SENDING OUT-OF-OFFICE EMAILS ON THEIR PHONES



‘Can I borrow you for a sec?’

Workers are busier than ever before. In fact, 44% of UK employees would describe their current workload as either ‘overwhelming’ or ‘heavy’. Those working in hospitality felt they had the heaviest workloads, followed by those in insurance and pensions, financial services, law and IT.

On top of a never-ending to-do list, employees are faced with numerous distractions at work, with the top five coming in as:

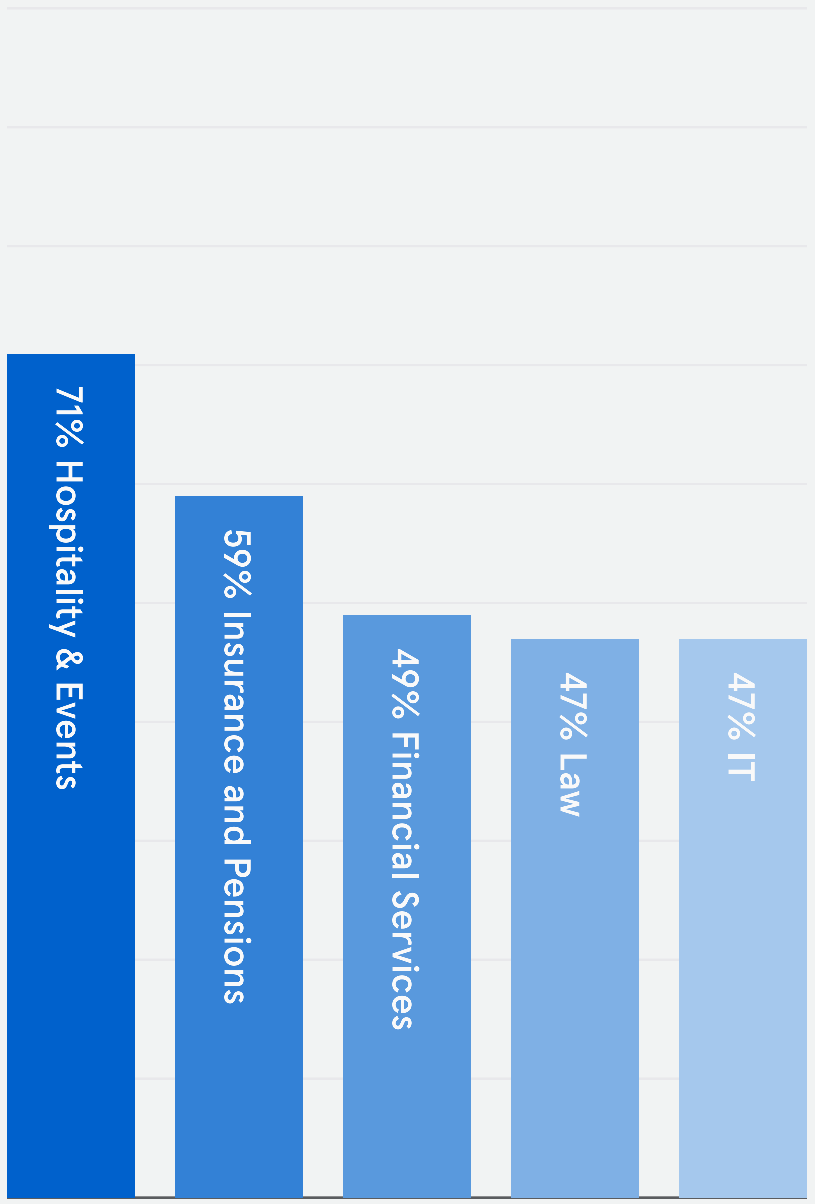
- Office noise (37%)
- Colleagues ‘dropping by’ (34%)
- Email notifications (30%)
- Meetings (26%)
- Notifications on their personal phones (20%)

Completing a primary task, whilst simultaneously engaging in a secondary task simply adds more to your cognitive load. Numerous studies have shown that, in situations where cognitive load is high, people tend to fall back on impulsive, System 1 decision-making strategies.

“When multitasking, our cognitive capacity is divided across multiple tasks and, when our cognitive capacity is compromised, we are less likely to make informed and optimal decisions, ” says Towse. “With less attention focused on the task of recognizing cybersecurity threats, we are more likely to rely on a less effortful, impulsive response.”

With so much going on, employees will likely rely more on habitual behaviors, rather than engaging in rational, analytical thinking. This can, ultimately, increase vulnerabilities to threats given that a person’s ability to spot anomalies in a phishing email, check they’ve entered the right recipient, or confirm auto-fill has generated the intended recipient becomes influenced by other tasks requiring their attention at the same time.

INDUSTRIES WITH HEAVIEST WORKLOADS, ACCORDING TO TESSIAN RESEARCH



Exhausted employees

The majority of UK employees (92%) say they feel tired at work, with one in five (20%) admitting they feel tired every day of the working week.

What's more, 91% say they feel stressed at work, with UK workers feeling stressed half of the working week (2.4 days). Women, our research shows, are more likely to be stressed than men; with 14% of men telling us they are never stressed compared to just 5% of female respondents.

WEARY WORKERS ARE MOST TIRED ON WEDNESDAY AFTERNOON

Tired and stressed employees pose a threat to the processing and handling of data over email or in the identification of malicious emails.

"When we are tired and stressed, we are less likely to question the legitimacy of messages and more likely to miss the cues that signal a threat because we have less cognitive capacity available to dedicate to evaluating new information" explains Jones. "As such, cues present in a cyber threat may be overlooked in favour of a less cognitively effortful response."

Tired employees also pose another risk; fatigue can make it harder for people to resist an impulsive desire to respond to a tempting request or persuasive suggestion in an email. A study by Washington State University found that sleep deprivation not only increased the likelihood of someone making risky decisions but also decreased their awareness about why they were taking risks[6].

Essentially, we become more impulsive when fatigued. With email being so quick and easy to use, tired employees may not even register the risk their inbox could pose. What's more, a smart hacker could even begin assessing which of your employees are the most overworked and exhausted, and target them.

> "When we are tired and stressed, we are less likely to question the legitimacy of messages and miss the cues that signal a threat."

[6] *Research shows sleep loss impedes decision making in crisis* | **Washigton State University.** Wsu.edu. https://news.wsu.edu/2015/05/07/research-shows-sleep-loss-impedes-decision-making-in-crisis/

Trust and trickery

Attackers are becoming smarter in their approaches to legacy Secure Email Gateways and becoming more convincing in their use of messaging. Often, hackers will impersonate well-known brands or senior executives within an organization, exploiting the level of trust a person will have for that sender.

The problem is that, with the continued development and ubiquitous deployment of new technologies, we are seeing a shift in the way in which trust develops online. Without the typical behavioral cues available to us when we interact with someone in person, it could be easier to manipulate trust via technology in order to increase the believability of a message or online persona.

It appears to be working; one in 10 UK employees we surveyed admits to clicking on a phishing email at work. In the financial services sector, this number rose to a worrying 29%. Furthermore, Jones and Towse found that participants in their study sometimes struggled to correctly identify phishing emails that impersonated well-known brands such as Amazon or PayPal. Alarmingly, despite recruiting over 200 participants, none judged every email correctly.

As spear-phishing attacks only grow in severity and become more targeted, the need for people to pay greater attention and spot the cues that signal a potential threat has never been higher. Yet, as we've revealed in this report, we question whether people have the time, access to the right information or the right tools to do this.

91% OF DATA BREACHES START WITH A PHISHING EMAIL[7]

[7] *Enterprise Phishing Susceptibility and Resiliency Report* | **Cofense.** Cofense.com. https://cofense.com/enterprise-phishing-susceptibility-report/

Changing the narrative

While it's been repeatedly demonstrated that the majority of data breaches result from human error, we believe it's time to change the narrative. People will inevitably make mistakes; our research found that over half of UK employees (52%) have sent an email to the wrong person while a significant percentage have clicked on a malicious link in phishing email.

"People make mistakes. But it's time to change the narrative."

But we have to remember that humans are emotional and fallible beings; they cannot make objective decisions in the same way a technical system can. There are a number of factors in people's everyday lives that impair their ability to make sound and rational decisions 100% of the time. Demanding workloads, distracting environments and sleep deprived minds mean that people do not necessarily have the cognitive capacity to process new information in their inboxes, identify the cues of a potential threat, and make an informed decision - on top of their day-to-day tasks.

Businesses, therefore, need to consider how best to limit the number of mistakes made, protect their employees and encourage them to think before they click.

By alerting users when something looks unusual before they make a mistake - via a notification detailing why an email could be a potential threat - you can provide individuals with the information they need to advise them on what they do next. Such measures can help override an employee's impulsive 'System 1 approach' to decision making, nudging them towards engaging their 'System 2'. As a result, they'll gather information and apply conscious reasoning to their actions over email.

For the first time, we can use machine learning to do this. By understanding people's email communications patterns and the relationships they have with internal and external contacts, we can build a picture of what 'normal' behavior looks like. Algorithms can, then, automatically detect when something looks unusual and alert the user. These real-time notifications reinforce safe email practices and, over time, can change user behaviour - encouraging employees to think proactively about email security.

Not every employee was hired as a security professional; they don't want to think about being the company's first line of defense nor can we expect them to spot threats in the same way technology can. For as long as people continue to communicate and collaborate over email, businesses need to find ways to prevent mistakes occurring and encourage employees to interact with email securely, in order to keep company data and systems safe and secure.

About

TESSIAN

Tessian is building the world's first Human Layer Security platform. Using stateful machine learning, we predict and stop email security threats in real time in order to protect organizations' most sensitive assets: their data, their systems, and their people. Tessian protects leading enterprises across the financial, legal and technology sectors from being compromised by spear phishing, misdirected emails, unauthorized emails and other threats caused by humans.

ABOUT DR HELEN JONES, UNIVERSITY OF CENTRAL LANCASHIRE

Helen joined the University of Central Lancashire as a lecturer in 2018. Prior to this, she worked at the University of Dundee, investigating the social psychological mechanisms underpinning the development of trust when interacting with strangers online. Helen completed her PhD at Lancaster University in 2016. This research examined potential psychological predictors of susceptibility to phishing emails. In particular, this work considered cognitive and situational influences on email response behaviour.

ABOUT PROFESSOR JOHN TOWSE, LANCASTER UNIVERSITY

John joined the Department of Psychology at Lancaster University in 2001, as a senior researcher. His work spans a number of research topics including cybercognition and the human dimensions of cybersecurity, seeking to understand how cognitive decisions interact with computer systems, devices and expectations. His work also examines how people interact with complex systems involving many consequences, and how we are required to trust individuals and systems.

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'.