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.

People make mistakes. It’s human nature.

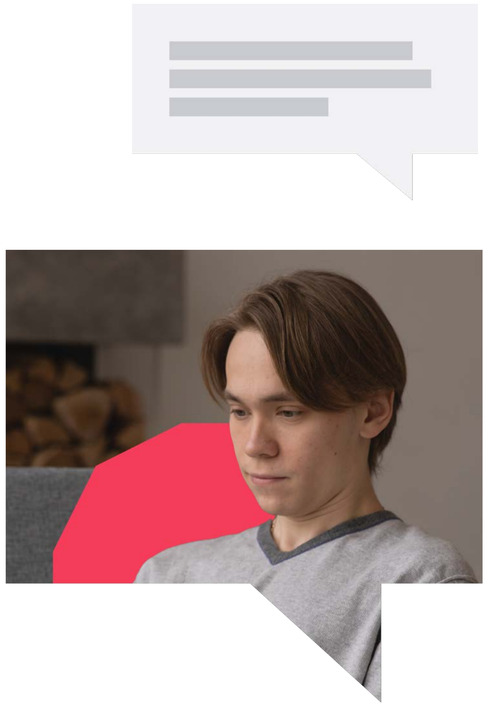
But people control more sensitive data than ever before.

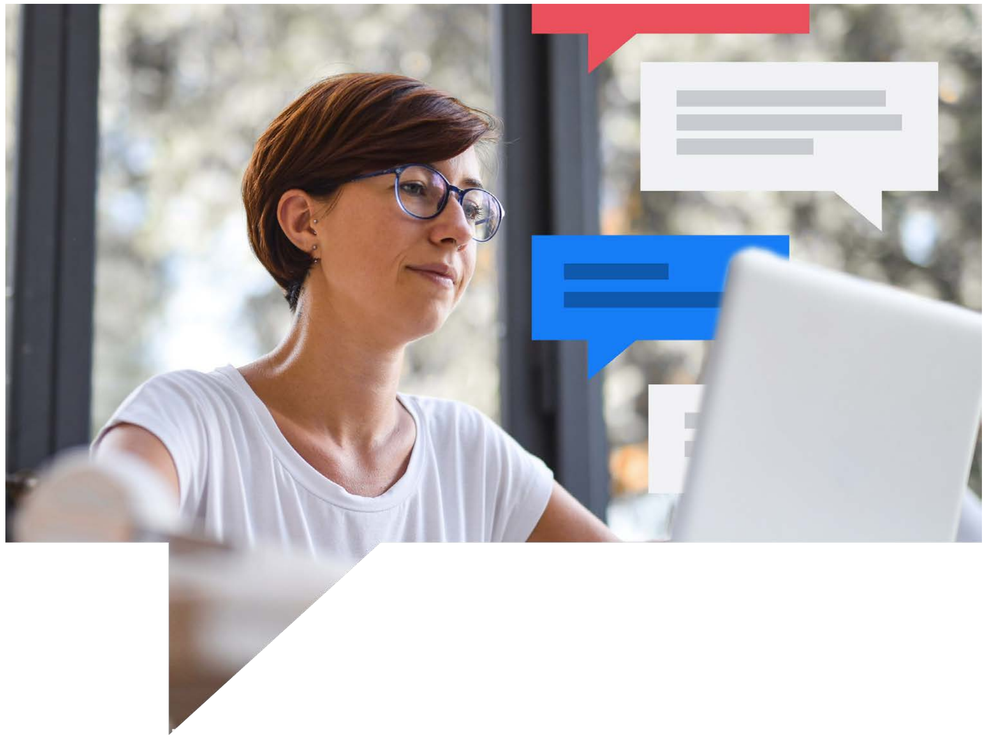
This means that mistakes can cause significant damage to a company’s reputation, bottom line, and future. In fact, 88% of today’s data breaches are caused by human error and, according to Verizon, user error is among the fastest-growing causes of breaches. This is why we often hear that humans are the “weakest link” in security.

But the narrative needs to change.

The truth is, people are every organization’s most important asset, and businesses must find ways to protect them while enabling them to work securely. But how?

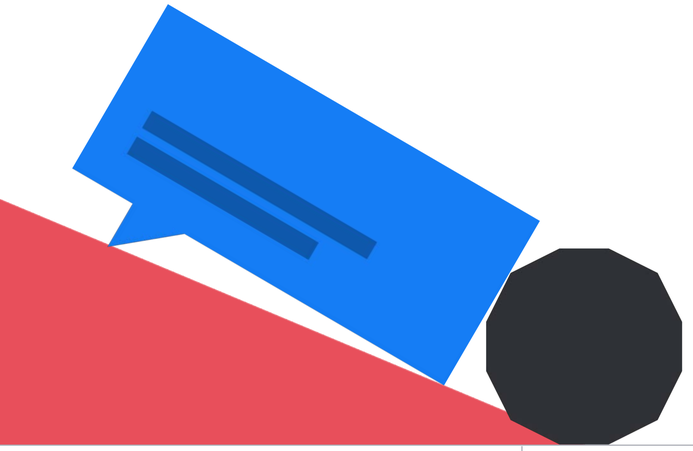
You can only find a solution once you understand the problem. That’s why we’re bringing to light the reasons why people make mistakes at work.





Executive Summary

Why Do People Make Mistakes explores why people make mistakes so that businesses can better understand how they can prevent them from happening, before they turn into data breaches.



In this report, we share findings from a survey commissioned by Tessian in which 2,000 professionals in the US and UK were asked about mistakes they've made at work. We also collaborated with Jeff Hancock, the Harry and Norman Chandler Professor of Communication at Stanford University and expert in trust and deception, to explain how certain factors impact human error.

Our research reveals how distraction, stress and fatigue influence people's ability to consistently make good cybersecurity decisions, and how the events of 2020 have highlighted why now – more than ever – businesses need to protect their employees. We also unpack why a one-size-fits-all approach to cybersecurity won't work for today's workforce. *(Hint: It's because people think and work in different ways)*.

READERS WILL:

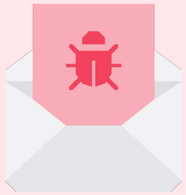
- Learn why protecting people is critical to protecting company data and systems.
- Find out why people make mistakes at work and understand how external factors affect our abilities to consistently make safe cybersecurity decisions.
- Understand how to prevent mistakes from happening before they turn into breaches.

WHY DO PEOPLE MAKE MISTAKES

Key Findings

1 in 4 workers

have clicked on a phishing email at work.



Jump to Page 8 ↗

58% of employees

have sent an email to the wrong person at work.

Jump to Page 11 ↗

57% of employees

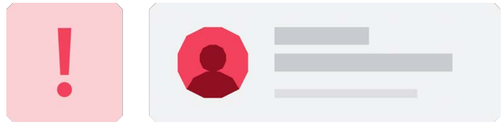
are more distracted when working from home

Jump to Page 15 ↗

1 in 5 companies

lost customers following a misdirected email.

Jump to Page 12 ↗



43% of people

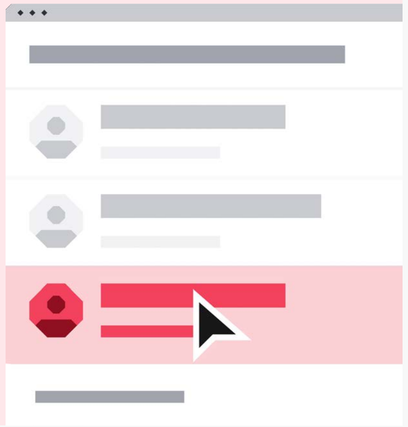
have made mistakes at work that compromised cybersecurity.

Jump to Page 7 ↗

Younger workers are

5x more likely

to make mistakes with security consequences.



Over half of employees

make more mistakes when they're stressed, while 43% are more error-prone when tired.

Jump to Page 14 ↗

A third of workers

rarely or never think about cybersecurity at work.

Jump to Page 26 ↗

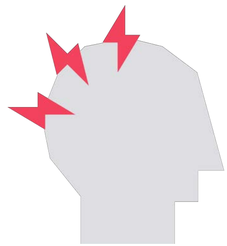
93% of staff

are tired and stressed at work.

Jump to Page 19 ↗

1 in 10

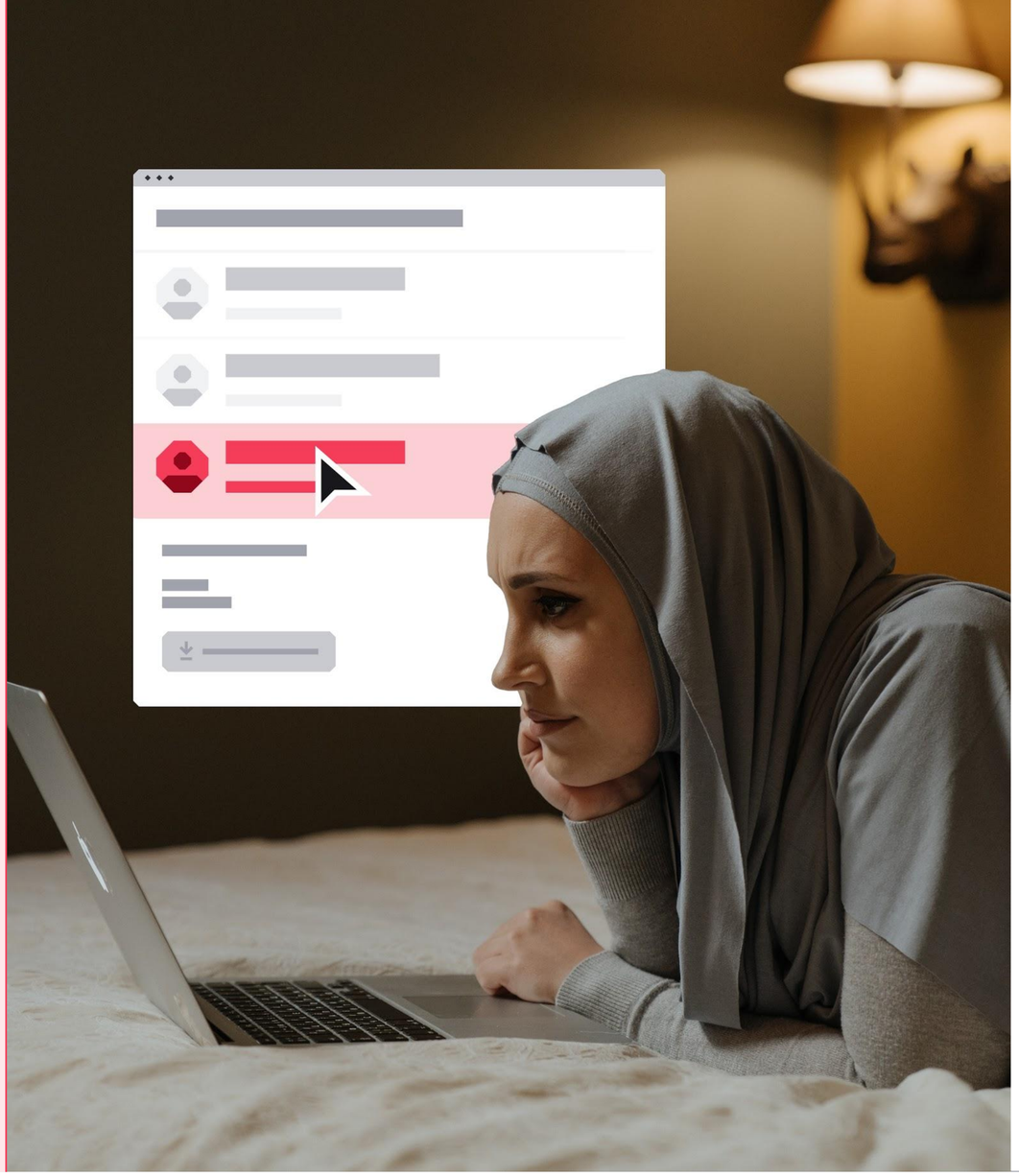
feel tired **every** day of the week.



CHAPTER 1

To err is human

06



CHAPTER 2

Why
mista
happ

CHAPTER 3

Why de
graphic
culture

13

Everyone makes mistakes.

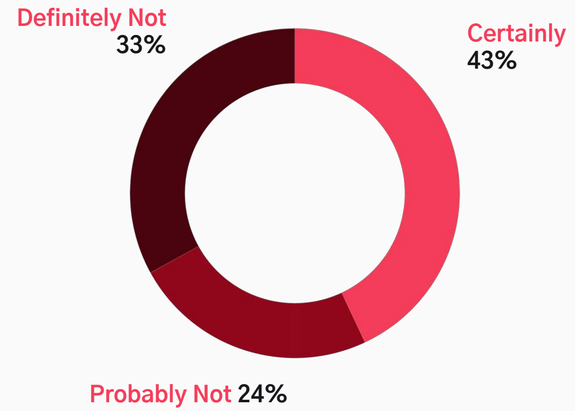
Making mistakes is how we, as humans, learn. It is through learning that we can prevent mistakes from escalating or happening again.

Sometimes, however, mistakes can have serious consequences for cybersecurity, especially when people are in control of so much sensitive data – such as customer, financial and employee information – and systems.

In fact, two-fifths of employees (43%) surveyed said they are “very” or “pretty” certain they have made a mistake at work that had security repercussions for themselves or their company.

While these figures could make us believe humans are the “weakest link” in cybersecurity, we don’t think that’s the case. That’s why we set out to understand what kind of mistakes people make and why.

”I have made a mistake at work that have had security repercussions for myself or the company”

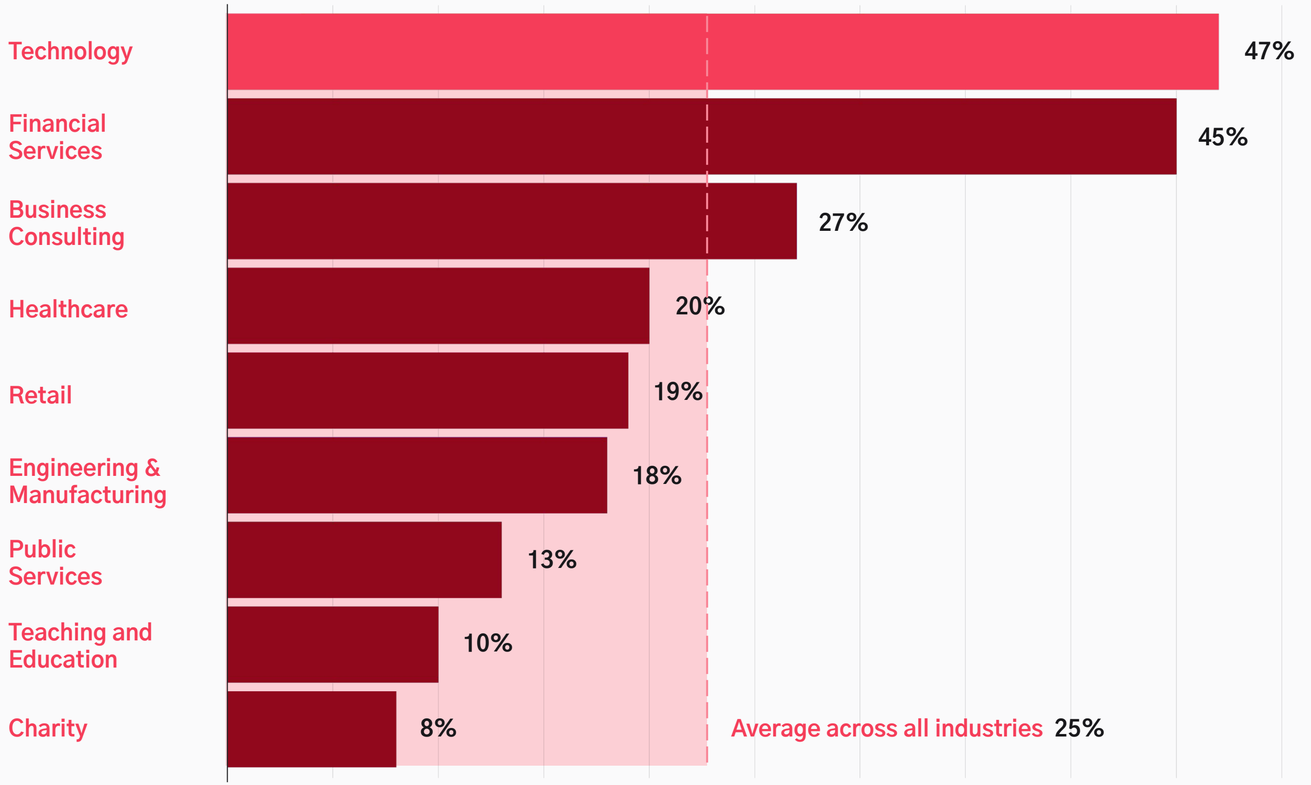


Mistakenly falling for a phishing scam.

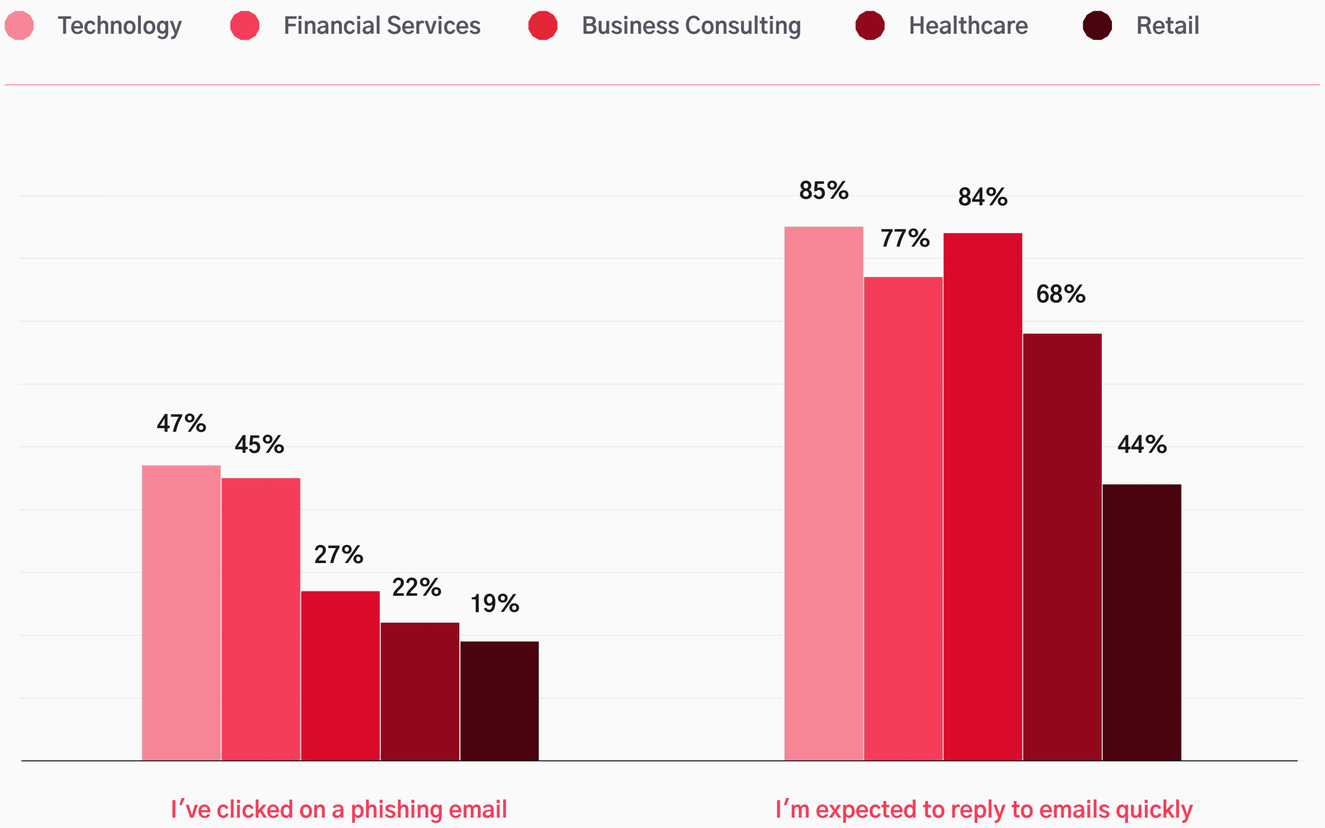
One in four survey respondents (25%) said that at some point during their career they've clicked on a link in a phishing email at work.

Workers in the Tech industry were the most likely to click on links in phishing emails, with nearly half of respondents in this sector (47%) admitting they had done so. It goes to show that even the most cybersecurity savvy people can make mistakes. They were closely followed by employees in Banking and Finance (45%).

Employees that have clicked on a phishing email at work by industry.



Impact of quick-to-click cultures on susceptible to phishing attacks.



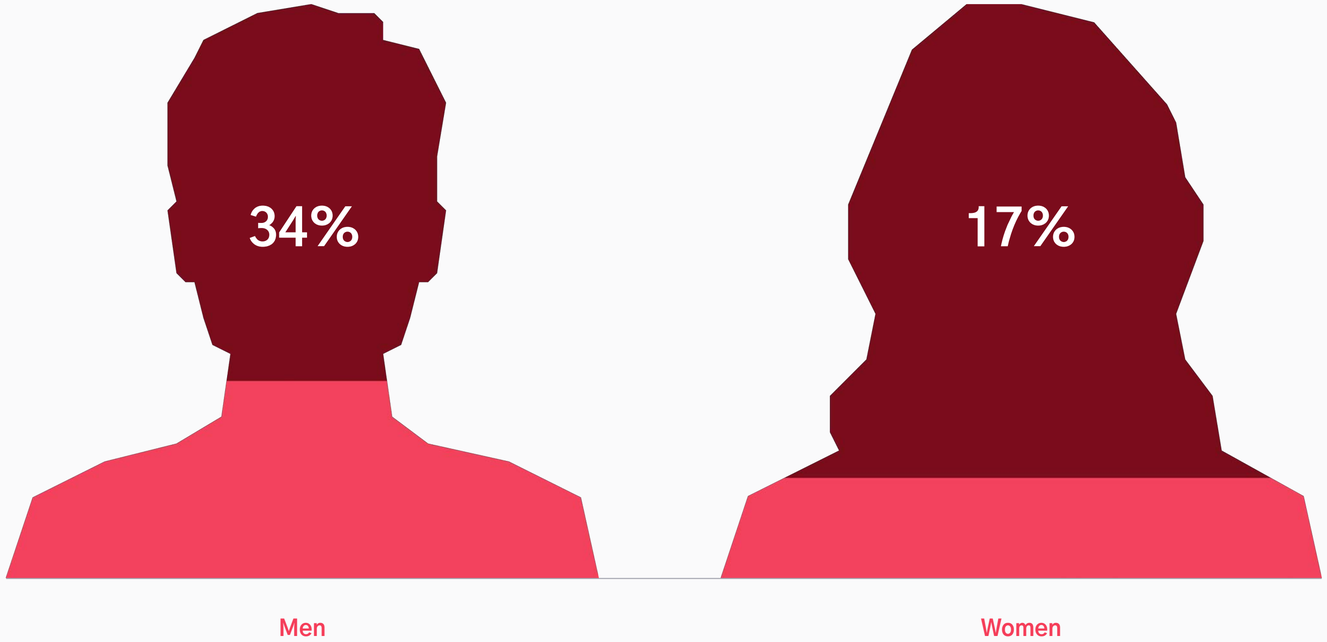
Interestingly, people in the Tech industry were also the most likely to agree that there is an expectation in their organization to respond to emails quickly (85%), while 77% in the Financial sector said the same.

And, when you consider that these two industries were also among the most likely to have clicked on a phishing email, we can start to see the correlation between quick-to-click cultures and phishing vulnerabilities. It's no wonder that a number of academic reports have repeatedly shown that time pressure negatively impacts decision accuracy.

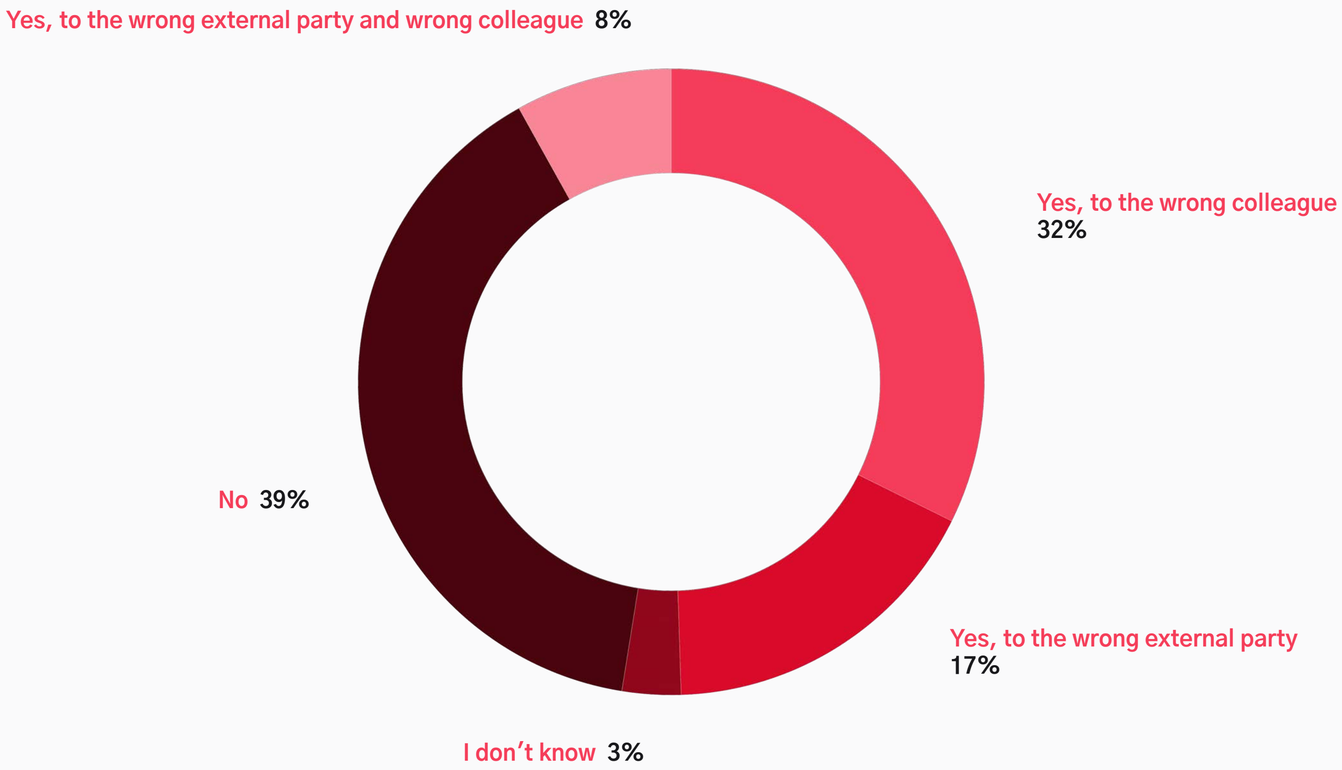
Our research also revealed that men were twice as likely as women to fall for phishing scams, with 34% of male respondents saying they have clicked on a link in a phishing email versus just 17% of female respondents.

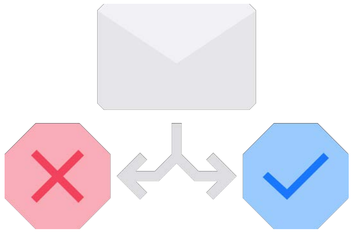
While researchers do not fully understand why gender difference is a factor in phishing attacks, it is known that men – on average – are more likely to take risks than women. This could explain why men are more likely to click on links in phishing emails. It also shows us that demographics matter to phishing – something we go on to investigate further in this report.

Employees that clicked on a phishing email: Men vs. Women.



Percentage of employees that have sent a misdirected emails.



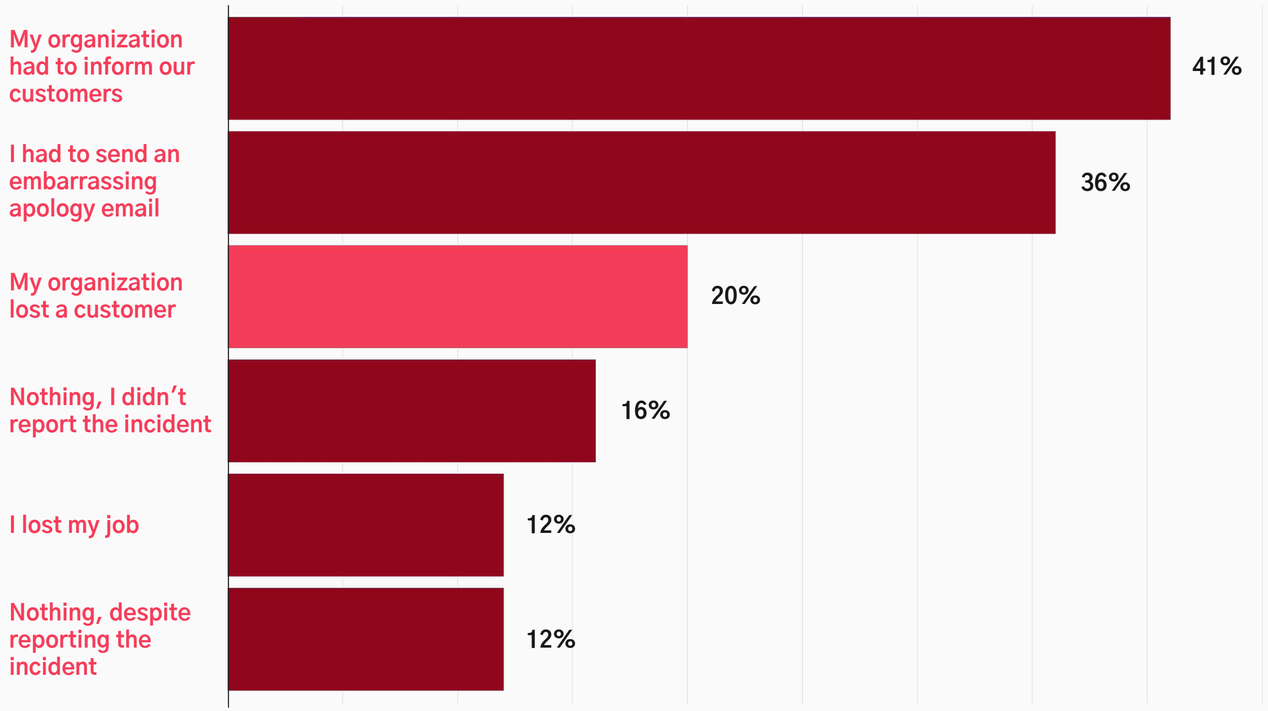


Mistakenly sending emails to the wrong person

Another mistake with security repercussions is sending company emails to the wrong person – something the majority (58%) of employees said they've done.

Of these misdirected emails, nearly a fifth (17%) were sent to the wrong external party while 8% had sent an email to both the wrong external party *and* wrong colleague.

The consequences of sending a misdirected email.



The consequences of sending an email go far beyond just red-faced embarrassment.

Misdirected emails were the number one cause of online data breaches reported to data protection regulators in 2019. And, in addition to reporting these breaches to regulators, businesses also have to report data loss incidents to their customers.

Not only is this embarrassing, it also breaks the trust you had with your customers and causes significant damage to the relationship you built. This can dramatically affect future deals and acquisitions.

In fact, our survey revealed that one in five companies (20%) lost customers as a result of the error, while one in ten workers said they lost their job.

R 1

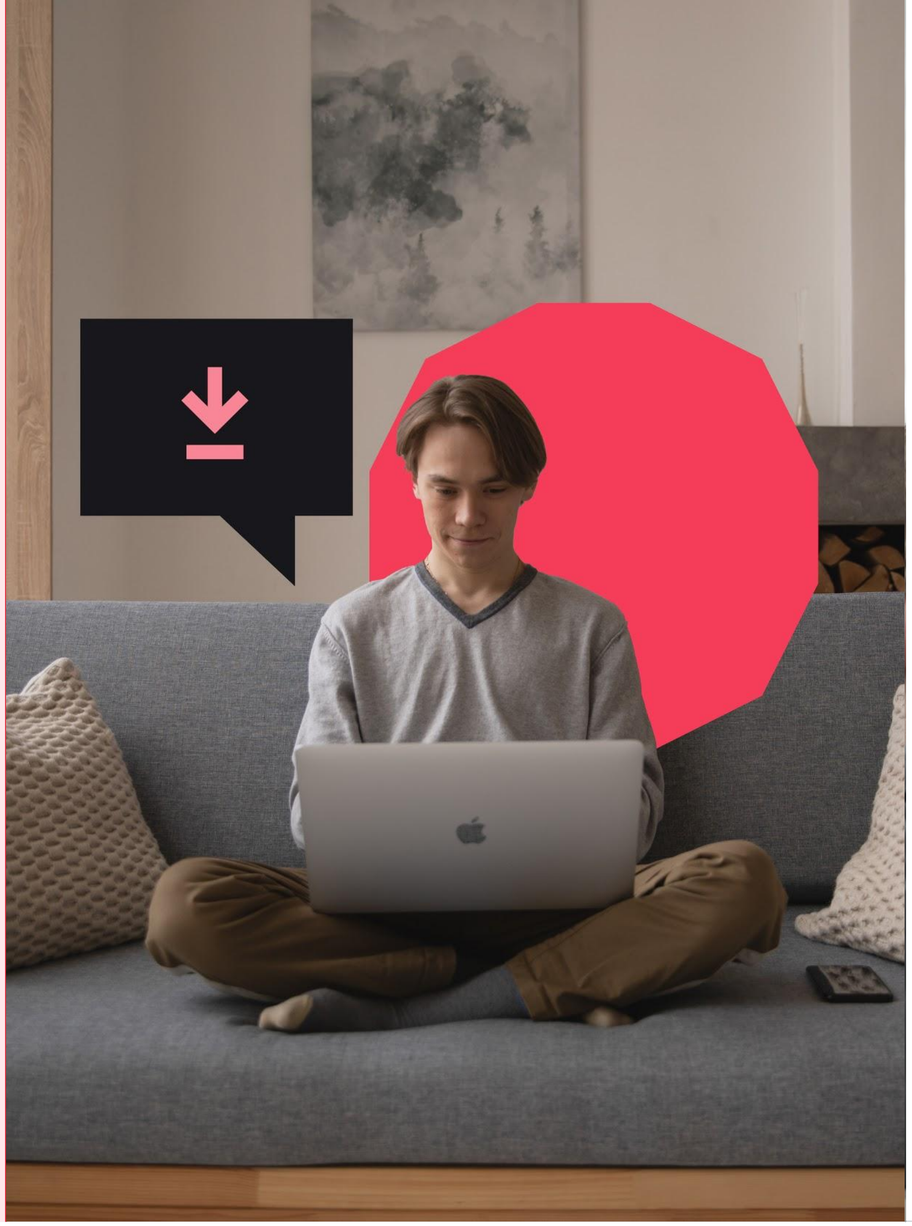
Err is
man

06

CHAPTER 2

Why do these mistakes happen?

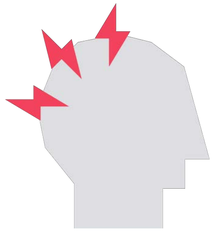
13



CHAPTER 3

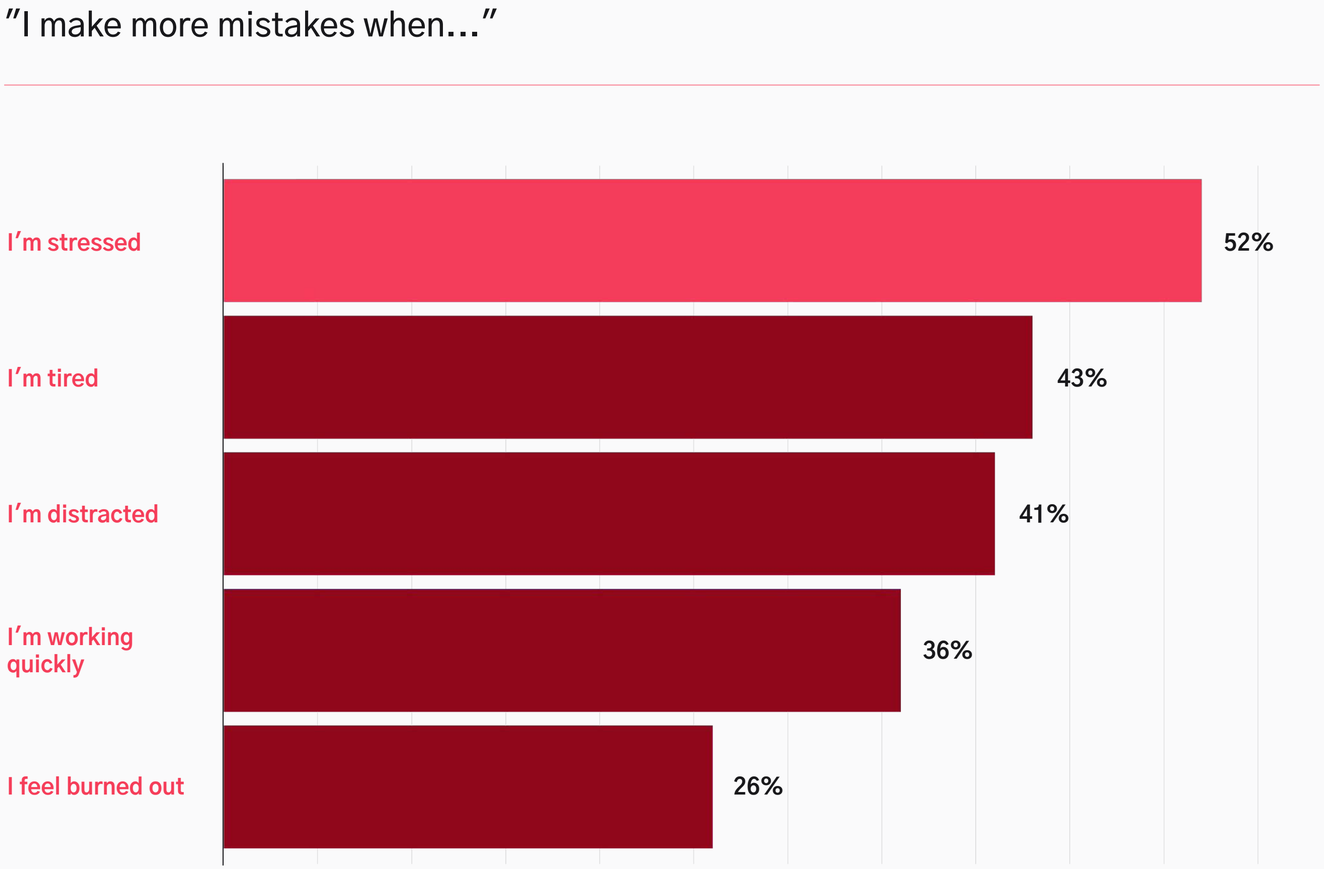
Why
demogr
and cult
matter

21

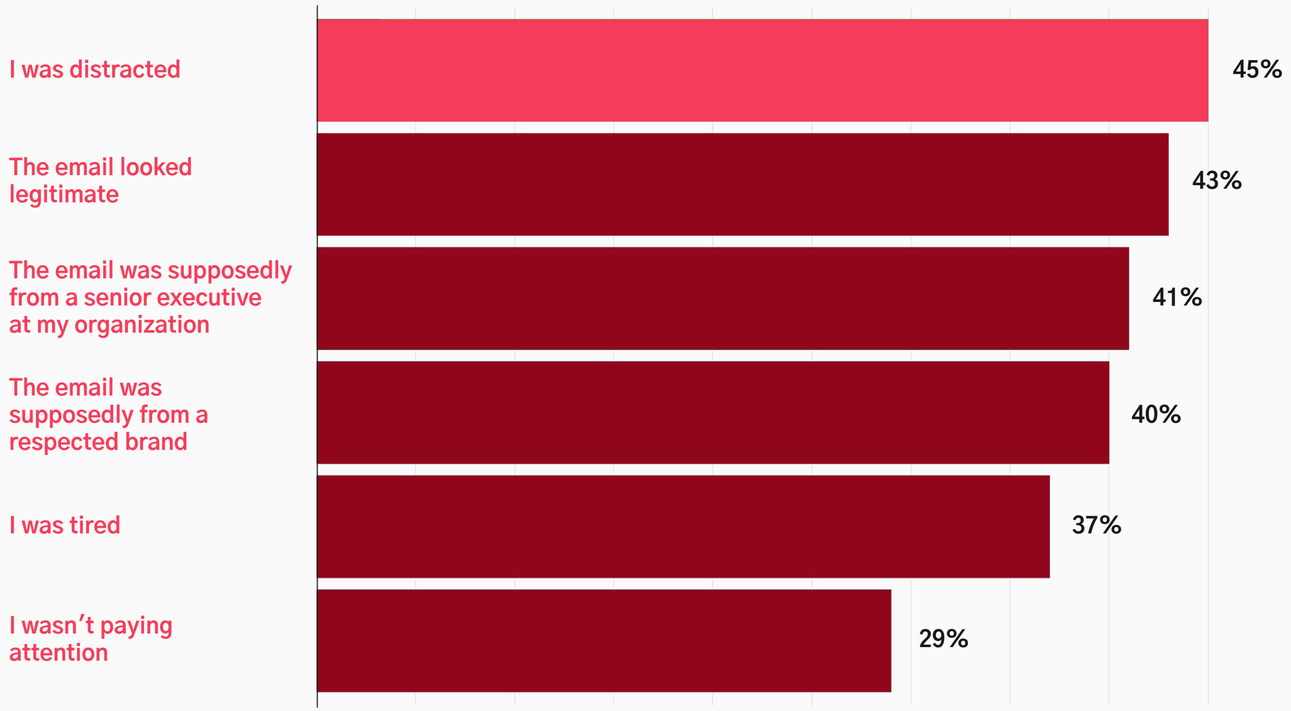


The majority of employees make more mistakes when they are stressed, while over two-fifths say they are more error-prone when they are tired and distracted.

Younger employees seem to be more affected by stress than their older co-workers, though. Nearly two-thirds of workers aged 18–30 years old (62%) said they make more mistakes when they are stressed, compared to 45% of workers over 51 years old.



Why employees clicked on phishing emails.



Driven to distraction

Nearly half of respondents (47%) cited distraction as the top reason for falling for a phishing scam.

With 57% of workers admitting they're more distracted when working from home, the sudden shift to remote-working could open employees and businesses up to even *more* risks.

Stanford professor Jeff Hancock explains, "Working in unusual environments can be stressful and distracting. Prior to the pandemic, people were used to operating in distinct spaces – home, work, social – and we had different ways of understanding the world in each space. The events of 2020 mean these spaces have blurred, and we've had to quickly learn new ways of operating and this has its challenges."

When I’m at work, for example, I adopt my ‘superhero’ persona; I’m confident and I’m alert. When I’m at home, though, my shield is down. I don’t expect to receive a threatening email from a hacker pretending to be my boss, demanding an urgent request. And as the cues for me to adopt my ‘work mode’ shield aren’t there, I might not react in the way I would while at the office.

Jeff Hancock

HARRY AND NORMAN CHANDLER PROFESSOR OF COMMUNICATION

Stanford University

Deception and trickery

Other reasons for clicking on phishing emails included the perceived legitimacy of the email (43%) and the fact that it appeared to have come from either a senior executive (41%) or a well-known brand (41%).

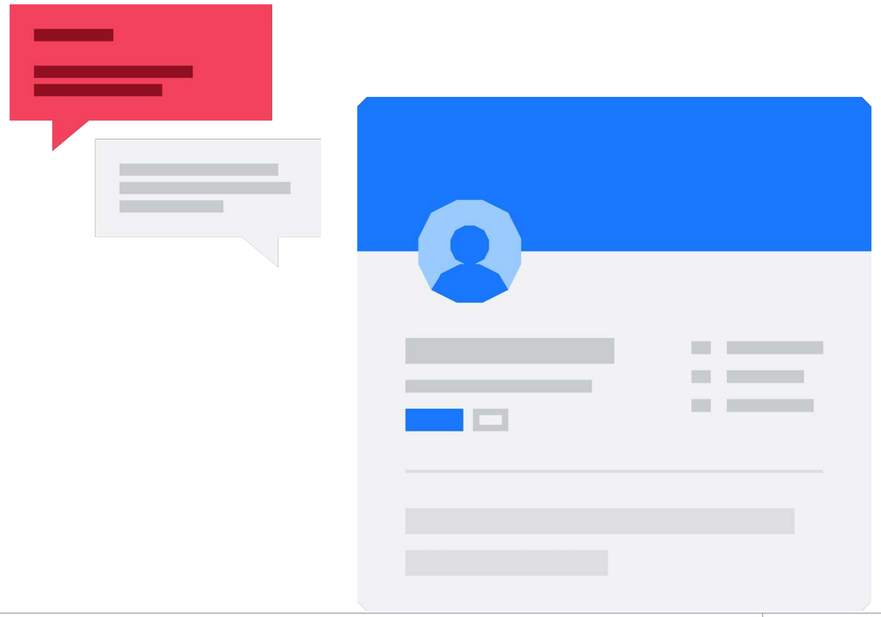
Impersonating someone in a position of trust or authority is a common and effective tactic used by hackers in phishing campaigns. Why? Because they know how difficult or unlikely it is to ignore a request from a senior executive who is asking you to urgently send strategic and important information for an upcoming meeting.

And, with so much publicly available information about people's lives online, hackers can easily crawl through social media sites and company websites to find valuable information about your role, responsibilities, and professional relationships.

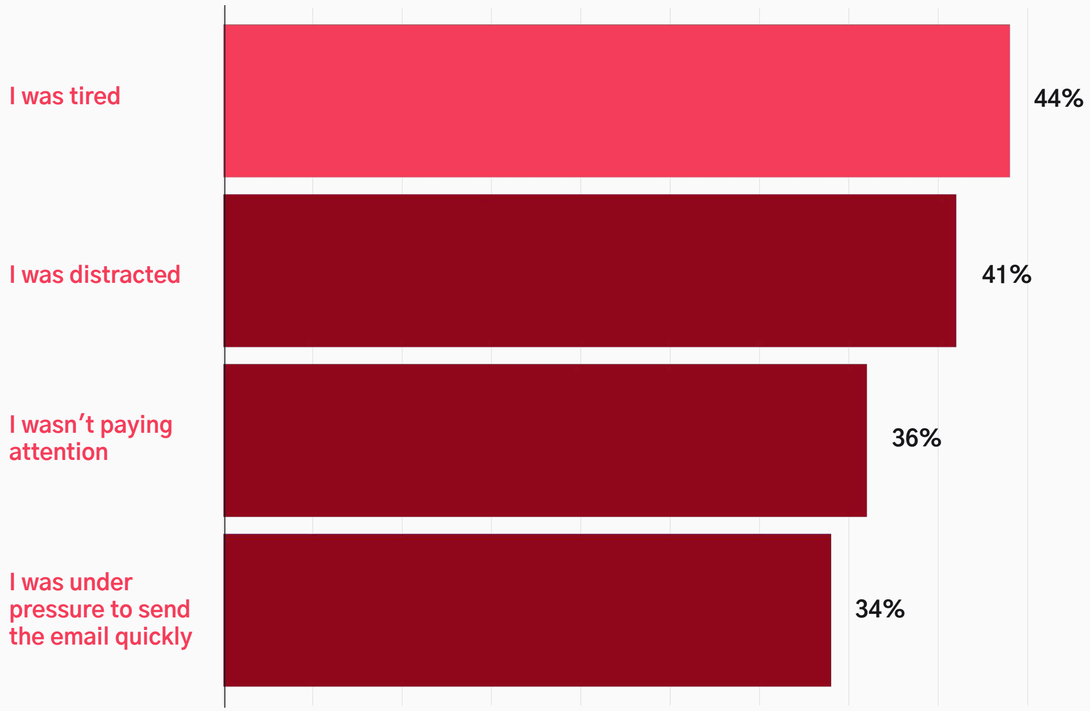
With this information, the attacker can impersonate someone in your network and create a credible narrative, using clever social engineering techniques and coercive language to convince you to comply with their requests.

This idea of network disruption, Hancock argues, is what makes phishing so effective. He explains: "Everyone has 'known' and 'unknown' networks. The known network is made up of friends, family, colleagues and others that we want to know, such as a new client. The unknown network is made up of strangers, and includes bad actors such as phishers and scammers.

However, our use of technology and the way in which interfaces have been designed means these two networks now overlap – in our inboxes or on our social media feeds – and it's become much harder to tell who you do and don't know, or who you can trust. For example, if a hacker spoofs the identity of someone in your 'known' network, like a customer, colleague or vendor, the likelihood of you clicking on that email is much higher."



Why employees send a misdirected email.



Feeling fatigued

Respondents cited feeling tired as the top reason for why they had accidentally sent an email to the wrong person (44%), while 37% said they fell for a phishing scam because of fatigue.

The shift to remote working and new ways of communicating are not helping our levels of tiredness, suggests Hancock.

"Having a conversation on Zoom is a very different experience than having a conversation in person. When you're face-to-face, for example, you don't stare directly at someone for long periods of time when they're talking. Now and then, you look away.

"However, on Zoom, you have an audience – sometimes of multiple people – constantly staring directly back at you. All the while, we are unable to move because we have to keep our head in the frame. It's intense and exhausting, especially if you are doing it many times a day."

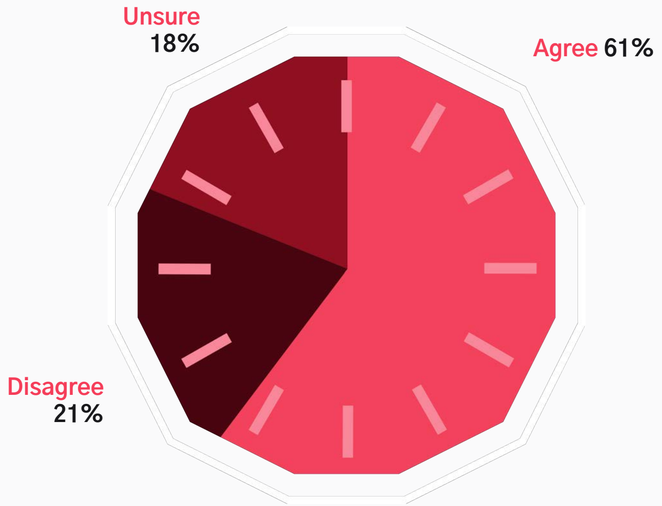
Cutting employees some slack

It's concerning that stress and fatigue cause people to make more mistakes when you consider that the overwhelming majority of employees surveyed (93%) said they were either tired or stressed at some point during the working week.

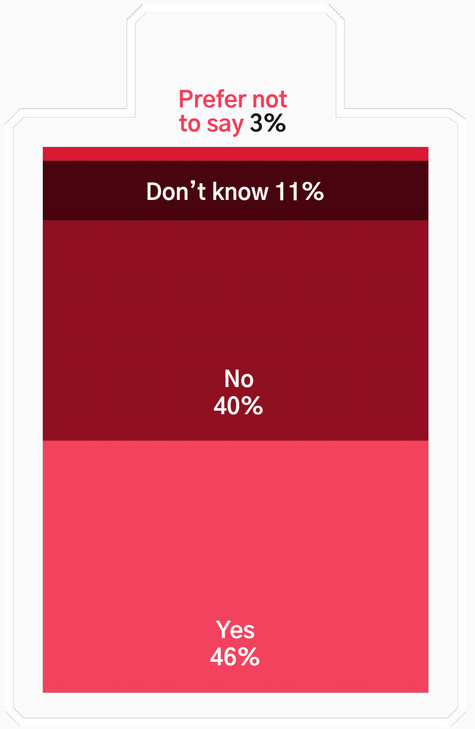
This isn't helped by the fact that nearly two-thirds of employees feel chained to their desks, with 61% of respondents saying there is a culture of presenteeism in their organization that makes them work longer hours than they need to.

Perhaps more worryingly, nearly half of employees (46%) have experienced burnout in their career.

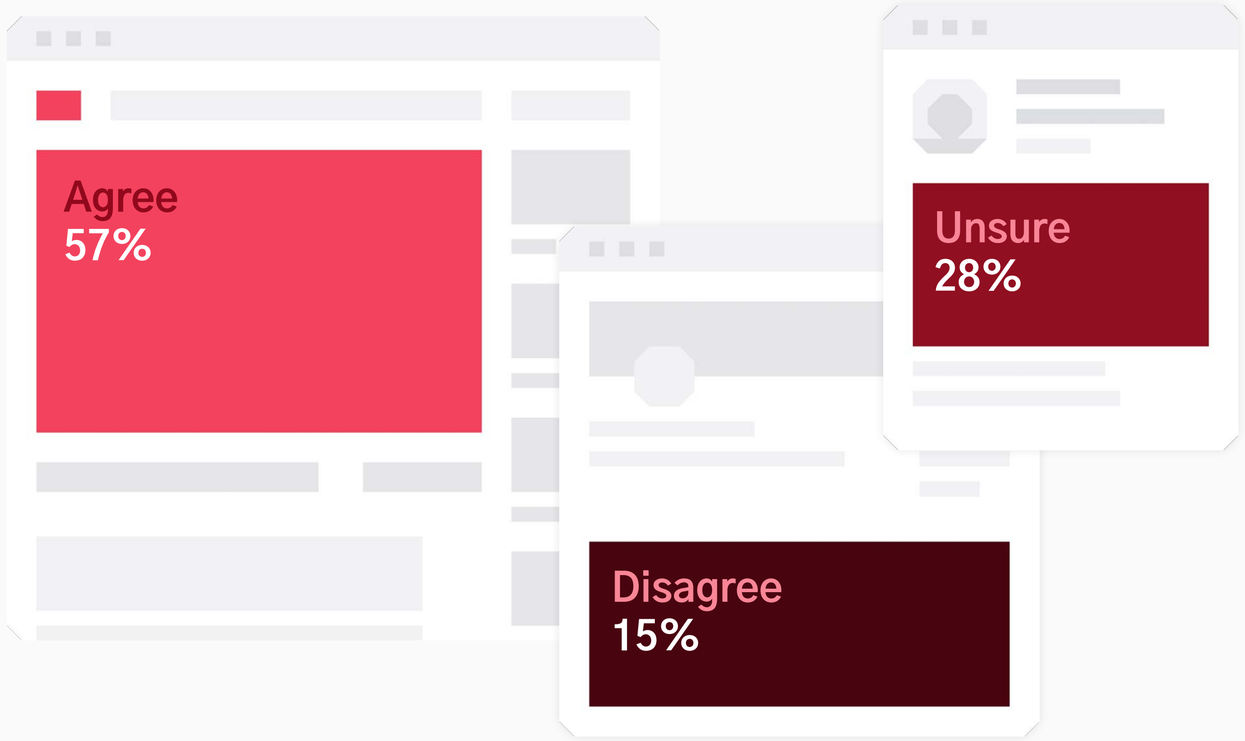
"There is a culture of presenteeism in my organization that makes me work longer hours than I need to."



Employees that have experienced burnout at work.



"I'm more distracted when I work from home."



Not only do these feelings of stress, fatigue, and distraction impact employees' health and wellbeing, but they could also explain why incidents of human error are happening at work *and* at home, especially given that employees are more likely to feel distracted when working outside of their normal office environment.

Something needs to change.

"Understanding how stress impacts behavior is critical to improving cybersecurity," said Hancock. "In 2020, people have experienced extremely stressful situations that have affected their health and finances, against a backdrop of political uncertainty and social unrest, while simultaneously juggling the demands of their jobs. It's been overwhelming.

"The problem is that when people are stressed and distracted, they tend to make mistakes or decisions they later regret. And sadly, hackers prey on this vulnerability. Businesses need to educate employees on how hackers might take advantage of their stress and explain the scams people could be susceptible to."

CHAPTER 3

Why demographics and culture matter

21

The age factor

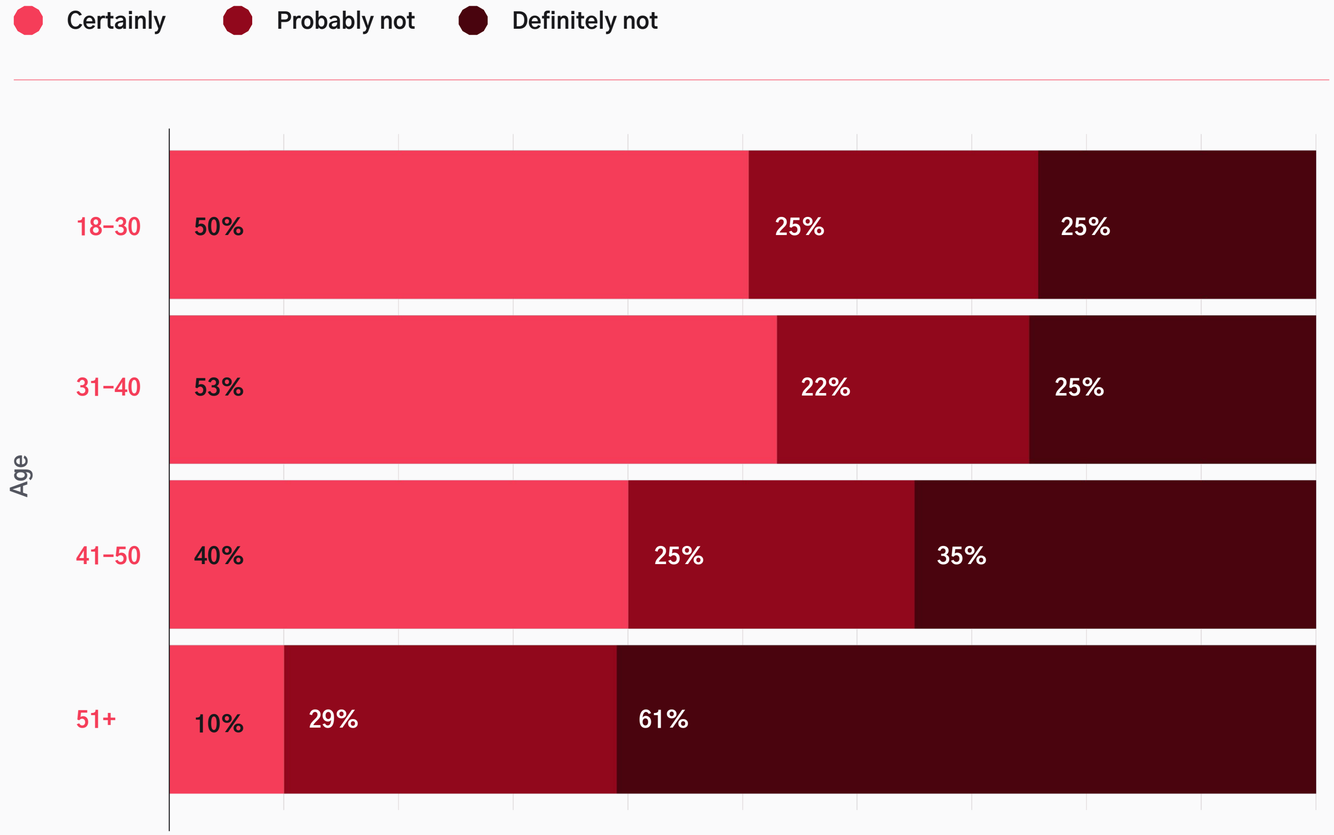
Age has a significant impact on people's cybersecurity behaviors.

Younger workers were 5x more likely to admit to errors that compromised their company's cybersecurity than older generations, with 50% of 18–30 years olds saying they've made such mistakes versus just 10% of workers over 51.

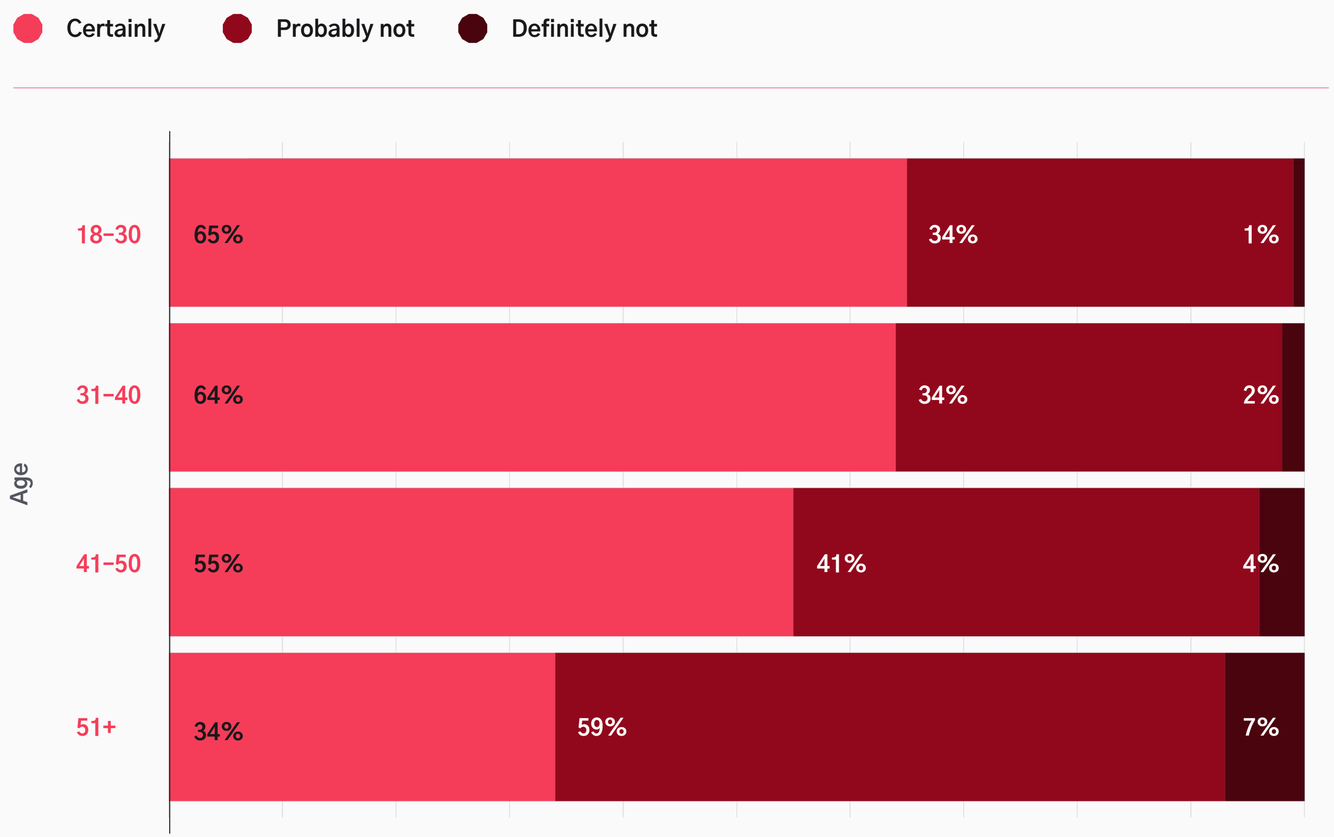
The reasons for this disparity, Hancock believes, may be because younger workers are actually more aware that they have made a mistake and are more willing to admit their errors.

For older generations, he explains, self–presentation and respect in the workplace are hugely important. They may be more reluctant to admit they've made a mistake because they feel ashamed due to preconceived notions about older generations and technology and don't want to "lose face".

Employees that have made mistakes with security repercussions, broken down by age.



Employees that have sent a misdirected email, broken down by age.



Younger workers were also nearly twice as likely to send a misdirected email, with 65% of 18–30 year olds saying they'd sent an email to the wrong person compared to just 34% of those over 51.

Older workers, however, were the least likely to report the incident. 23% of over 51s said that, despite making the error, they didn't report it to their IT team versus 13% of 18–30 year olds.

This shows that businesses need to "deshame" the reporting of mistakes.

Another Tessian study revealed that data security incidents happen 38x times more often than IT leaders think. This lack of visibility into employee behavior is damaging businesses' cybersecurity posture. Companies need to create a security culture that encourages employees to report their mistakes to IT, and provide clear channels for them to do this. Support teams should also be trained to offer reassurance when a security incident happens.

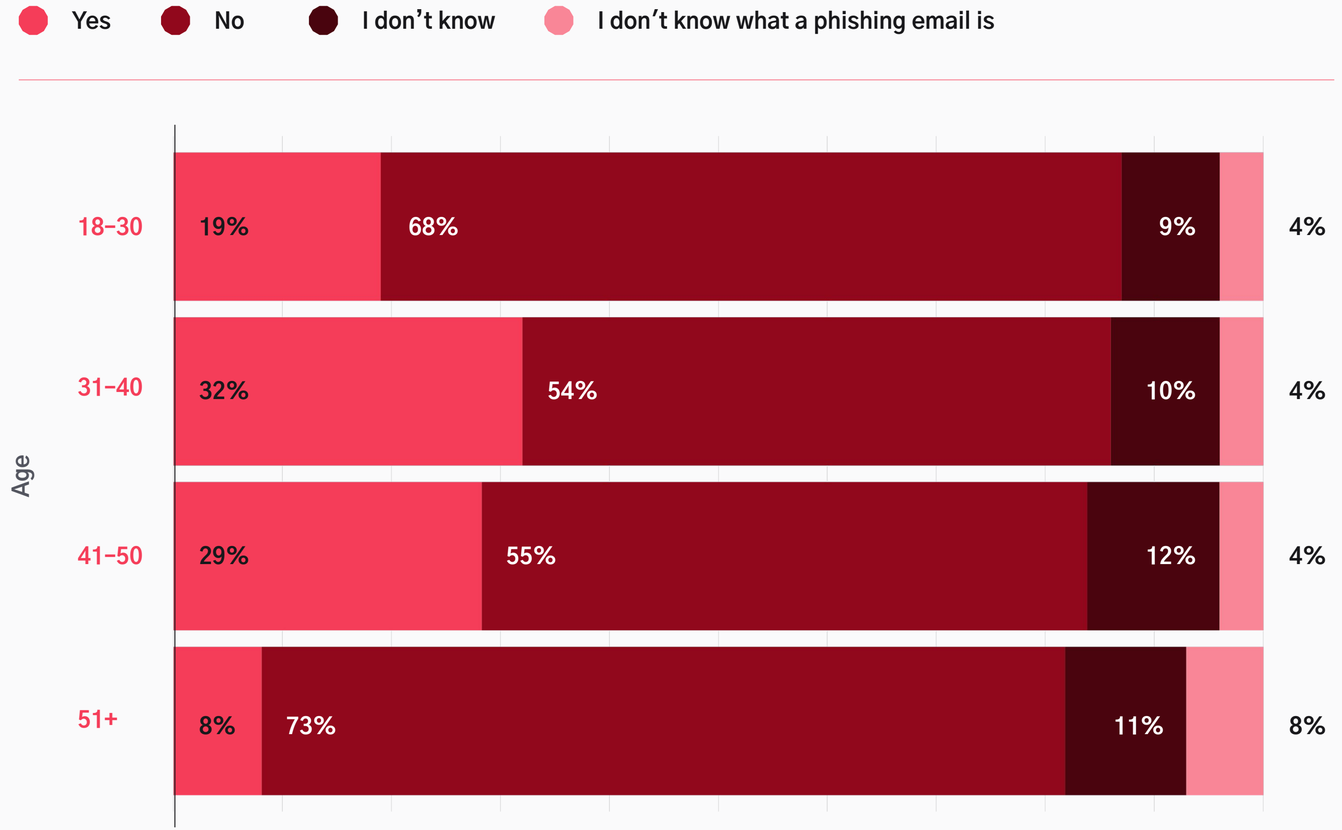
Age is also a factor in people's susceptibility to phishing scams.

Nearly three-quarters of respondents who admitted to clicking a phishing email were aged between 18-40 years old. In comparison, just 8% of people over 51 said they had done the same. However, the older generation were also the least likely to know what a phishing email was.

"The older generation have, in many ways, the potential tools and mindsets needed for detecting phishing attacks. They have more life experience, they are more involved in their community, and they tend to have strong, close networks which means they are good at detecting when something doesn't 'feel' quite right," said Hancock.

However, Hancock also adds that a percentage of the older generation may find it harder to spot phishing scams, simply because they are less experienced with these kinds of attacks on email.

Employees that click on phishing emails, broken down by age.



Flipping the script on training

Training is incredibly important in raising employee awareness. But it needs to be tailored if it's going to resonate and stick.

"A one-size-fits-all approach won't work," said Hancock. "Different generations have grown up with tech in different ways, and security training needs to reflect this. That's not to say that we should think that people over 50 are tech-illiterate, though. Businesses need to consider what motivates each age group and tailor training accordingly.

"Being respected at work is incredibly important to an older generation, so telling them that they don't understand something isn't an effective way to educate them on the threats.

Instead, businesses should engage them in a conversation, helping them to identify how their strengths and weaknesses could be used against them in an attack."

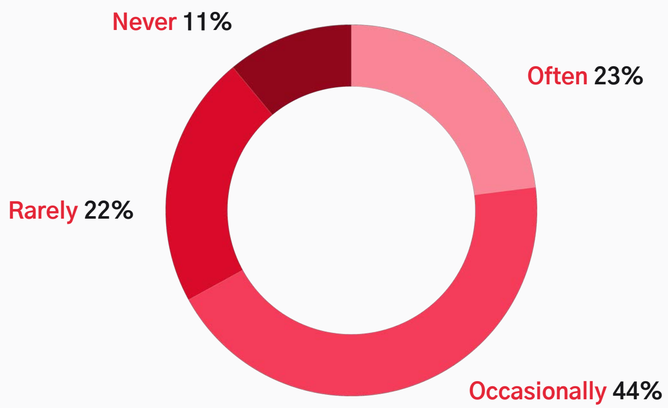
"Many younger employees, on the other hand, have never known a time without the internet and they don't want to be told how to use it. This generation has a thirst for knowledge, so teach them the techniques that hackers will use to target them. That way, when they see a scam, they'll be able to unpick it and recognize the tactics being used on them."

One way to achieve this is by investing in security solutions, like Tessian, that use machine learning to automatically detect threats on email and then explain what was suspicious about the message via clear, educational warnings to the user. This in-situ training, provided by contextual, in-the-moment alerts, not only prevents mistakes from happening, but also educates employees on the tactics hackers use.

CONCLUSION

Preventing mistakes from happening

Percentage of employees that think about cybersecurity at work.



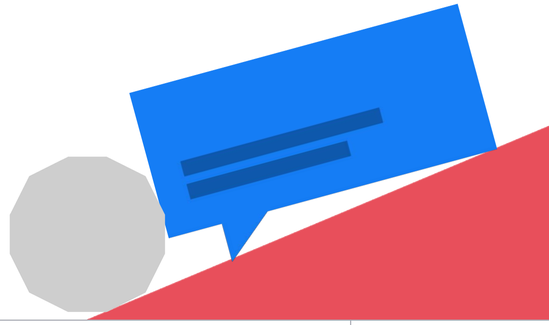
It’s all too easy to place the blame of data breaches on people’s mistakes.

However, businesses have to remember that not every employee is an expert in cybersecurity. In fact, a third of our survey respondents said they rarely or never think about cybersecurity when at work. They are focused on getting the jobs they were hired to do, done.

When faced with demanding to-do lists, stress and distractions, people’s cognitive loads become overwhelming and mistakes happen. To successfully prevent mistakes from turning into serious security incidents, businesses have to take a more human approach.

They need to take the burden of security away from employees and empower them to work – however and wherever they want – in a safe way.

Training and policies help. However, combining them with machine intelligent security solutions that automatically alert individuals of potential threats in real-time and explain why the email they are about to send or have received is a risk, is more powerful in preventing mistakes before they turn into breaches.



And this is where Tessian comes in.

By alerting employees to the threat in-the-moment, our solutions help override impulsive and dangerous decision-making that could compromise cybersecurity. With explainable machine learning, Tessian arms employees with the information they need to apply conscious reasoning to their actions over email, making them think twice before doing something they might later regret.

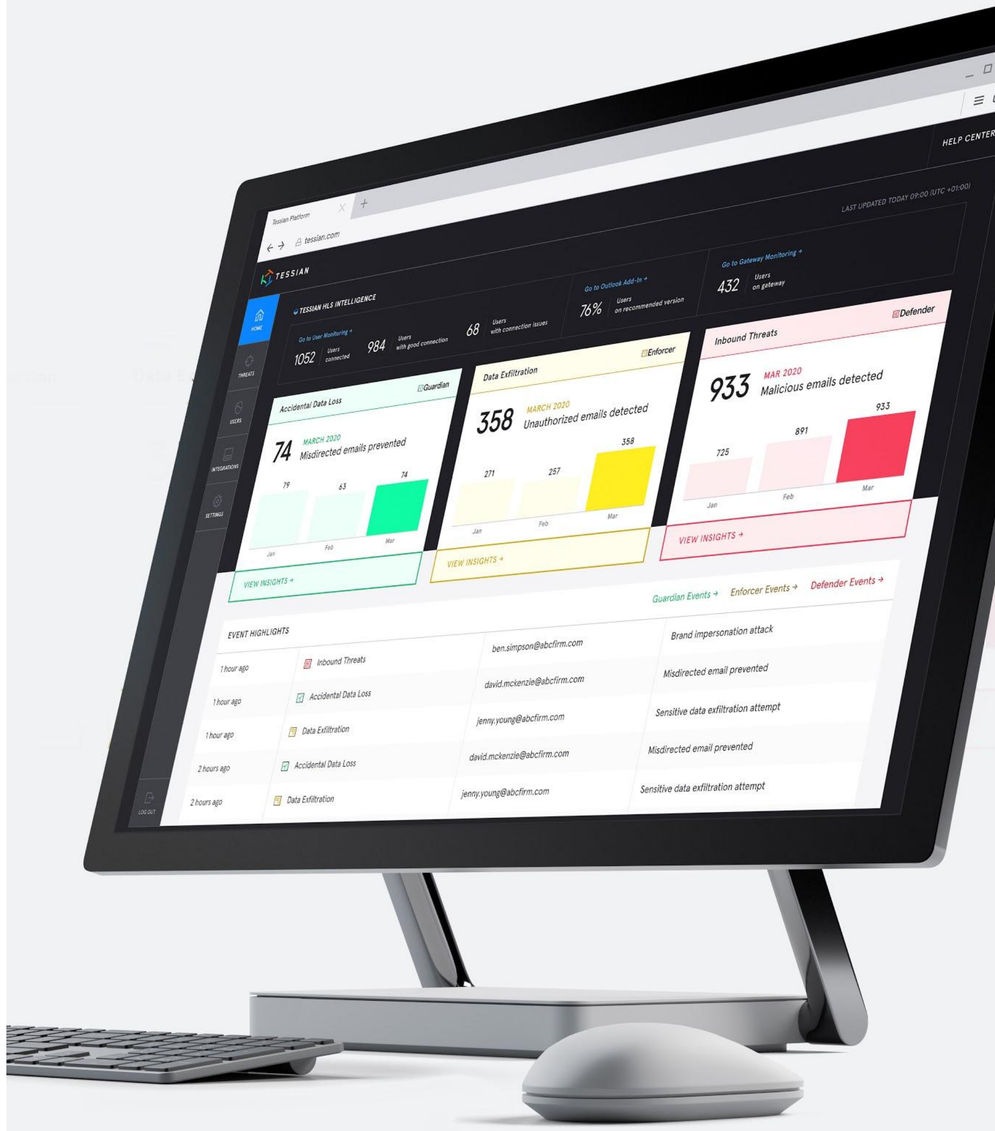
If we come back to this idea that mistakes are a part of learning, then this approach is a hugely powerful way to help improve people's cybersecurity reflexes.

"People learn best when they get fast feedback and when that feedback is in context," said Hancock. "So not only will these real-time, contextual alerts reduce risks, it will also improve your human security layer."

In turn, businesses can also learn from the valuable insights within their email data sets. They can see how these risks change over time and benchmark their risk levels against industry peers. And with greater visibility into the behaviors of their riskiest and most at-risk employees, businesses can tailor security training and policies to influence and improve staff's cybersecurity behaviors.

We call this Human Layer Security.

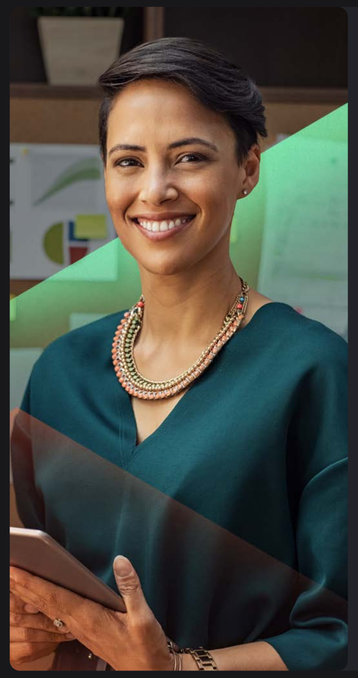
Only by protecting people and preventing their mistakes can businesses ensure data and systems remain secure, and help people do their best work.



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 Sequoia, Accel and Balderton and has offices in San Francisco and London.

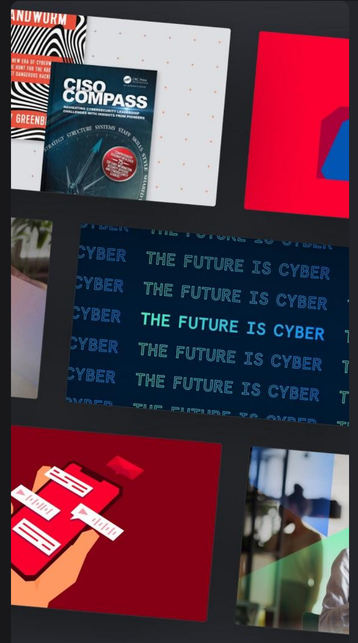
TESSIAN.COM



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 →

About Jeff Hancock

Jeff Hancock is the Harry and Norman Chandler Professor of Communication at Stanford University.

He and his team specialize in using computational linguistics and experiments to understand how the words we use can reveal psychological and social dynamics, such as deception and trust, emotional dynamics, intimacy and relationships. Professor Hancock is well-known for his research on how people use deception with technology, and his work has been published in over 80 journals. Hancock's TED Talk on deception has been seen over 1 million times and he has also featured as an expert in media outlets such as the New York Times, CNN, CBS and the BBC.

About OnePoll

In April 2020, Tessian commissioned OnePoll to survey 2,000 working professionals: 1,000 in the US and 1,000 in the UK. Survey respondents varied in age from 18–51+, occupied various roles across departments and industries, and worked within organizations ranging in size from 2–1,000+.

Share this report

TESSIAN.COM/RESEARCH →