PSYCHOLOGY OF HUMAN ERROR 2022

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

EXECUTIVE SUMMARY

In 2020, we published a study with academics at Stanford University looking into why mistakes happen at work and the impact these mistakes had on cybersecurity. At the time of publication, the world was at the peak of the global pandemic.

18 months later, offices are starting to open back up and hybrid working has become the norm, so we wanted to find out how this has impacted people's abilities to make cybersecurity decisions at work.

So what did we find out?

Remote or hybrid working is causing distraction and affecting people's cognitive loads. This has resulted in a higher percentage of people making mistakes that compromise company security - such as a clicking on a phishing email or sending data to the wrong person - as a result of fatigue and distraction, versus the figures we reported 18 months ago.

Business Email Compromise has become more successful. More than half of employees (52%) said they fell for a phishing email in which a cybercriminal impersonated a senior executive - up from 41% in 2020, while click-through rates on phishing emails whereby threat actors impersonating well-known brands dropped.

Organizations are taking tougher action in response to mistakes which result in data being compromised. The percentage of people who lost a customer or a client due to an employee sending an email to the wrong person increased from 20% in 2020 to 29% in 2022.

The findings in this report illustrate why a human approach to cybersecurity is needed, especially as hybrid working environments remain in place.

Once again, we have collaborated with Jeff Hancock the Harry and Norman Chandler Professor of Communication at Stanford University and expert in trust and deception, to explain how the past 18 months has influenced security behaviors online and how factors like Zoom fatigue could be hindering people's abilities to stay focused.

26%

of employees have clicked on a phishing email at work in the past year

40%

of UK and US employees have sent an email to the wrong person in the last 12 months

50%

of people say they are more distracted when working from home

56%

of employees have received a scam via text message, and 32% complied with the request in the scam message

45%

of UK and US employees have experienced burnout in the last 12 months

36%

of employees believe they have made a mistake at work that has compromised security in the last 12 months

58%

of employees say their team is understaffed as a result of colleagues leaving

52%

of people clicked on a phishing email because it looked as though it had come from a senior executive at the company - up from 41% in 2020

TABLE OF CONTENTS

01

MISTAKES AT WORK ARE STILL COMPROMISING SECURITY...

...but they’re happening less and less frequently...

In fact, 36% of the employees we surveyed said they are very or pretty certain they have made a mistake at work that has compromised security in the last 12 months, down from 43% in July 2020.

But what kind of mistakes are they making?

ACCIDENTALLY SENDING EMAILS TO THE WRONG PERSON

Two in five respondents (40%) admitted to sending work emails to the wrong person in the last 12 months, with 18% saying they sent an email to the wrong colleague. This is a significant drop from the 32% of people who said they'd sent an email to the wrong colleague in 2020.

The percentage of employees who sent an email to the wrong external party stayed the same at 17%, while an additional 5% said they had sent an email to the wrong colleague and the wrong external party.

Another error experienced by 39% of employees was sending an email with the wrong attachment. Just less than one fifth (15%) of respondents said they'd sent an email with the wrong attachment to an external party – potentially breaching confidential information.

MISTAKES WHEN SENDING EMAILS

2 in 5

respondents sent work emails to the wrong person

Almost 1 in 5

respondents sent an email to the wrong external party

Almost 2 in 5

respondents sent a work email with the wrong attachment

THE CONSEQUENCES OF SENDING AN EMAIL TO THE WRONG PERSON

While people are being a little more careful on email, the consequences of sending an email to the wrong person have become much more severe since our last report ☹

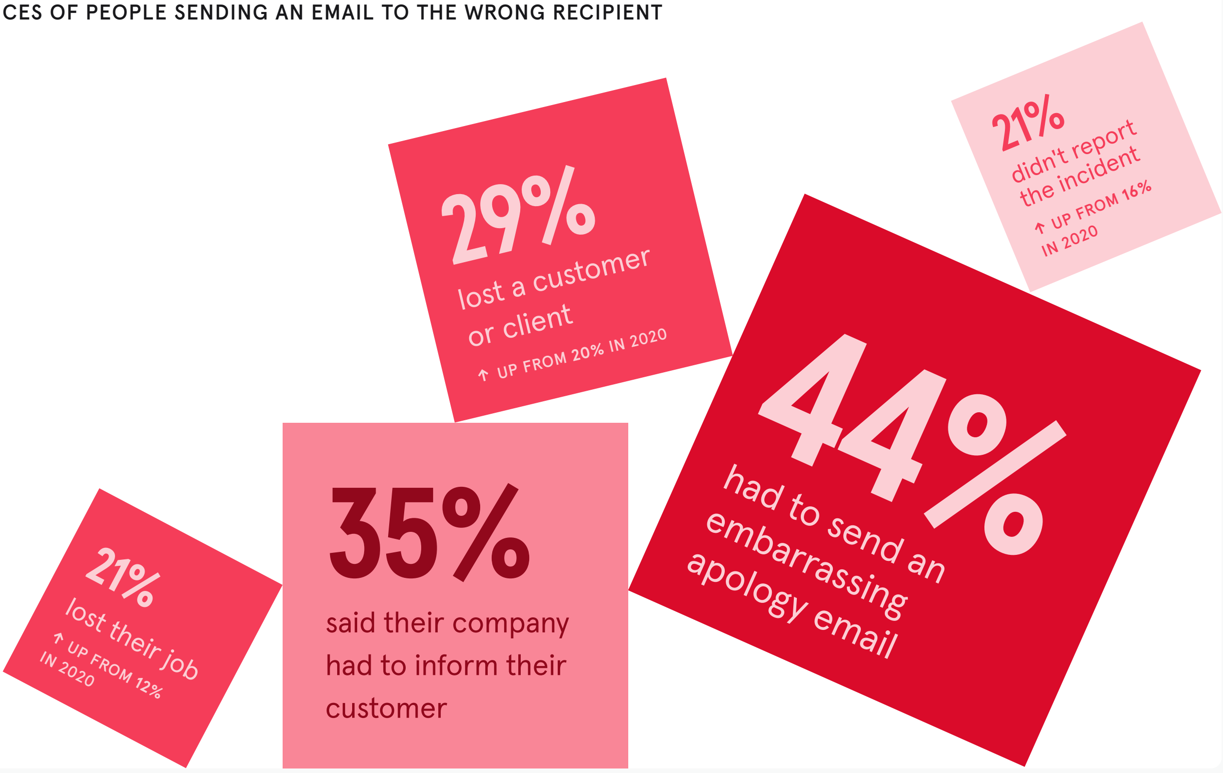
More and more breaches caused by misdirected emails were reported to regulators. In the first nine months of 2021, the number of breaches reported to the Information Commissioner's Office, caused by data being sent to the wrong person, was 32% higher compared to the same period in 2020.

As well as reporting these breaches to regulators, businesses need to report data loss incidents to their customers - something that 35% of respondents said they had to do following their mistake. Not only is this embarrassing, it causes significant damage to the trusted relationship you built with customers. In fact, nearly a third (29%) said their business lost a client or customer as a result of sending an email to the wrong person - up from 20% in 2020.

What's more, one in four respondents (21%) said they 👎 lost their job - a huge increase from the 12% we previously reported.

Perhaps it's little surprise, then, that the percentage of people who didn't report the incident increased, with 21% of employees saying they didn't tell their IT team about the mistake - up from 16% in 2020.

CONSEQUENCES OF PEOPLE SENDING AN EMAIL TO THE WRONG RECIPIENT



“Rewards are far more effective than punishment. If employees feel uncomfortable when working with a security team, that security team will never hear about the most important mistakes and problems early enough.

So rather than scaring employees into compliance, encourage employees to engage with security by creating positive security experiences so that you can cement a partnership mindset between security teams and staff.

Those positive incentives will help combat security nihilism and build strong security cultures.”

Josh Yavor
CHIEF INFORMATION SECURITY OFFICER AT TESSIAN

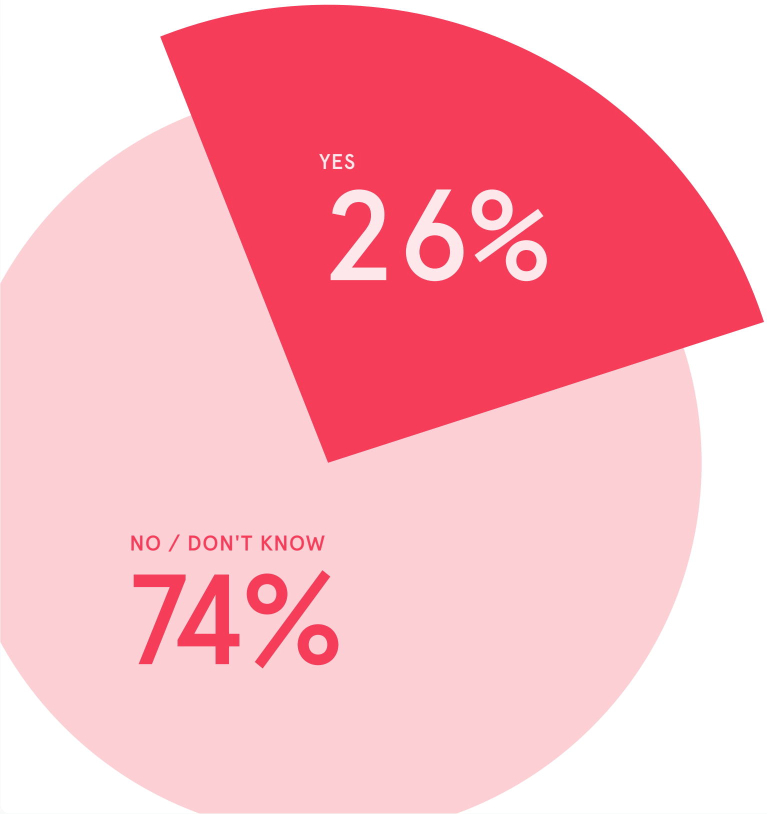
PEOPLE ARE FALLING FOR PHISHING ATTACKS

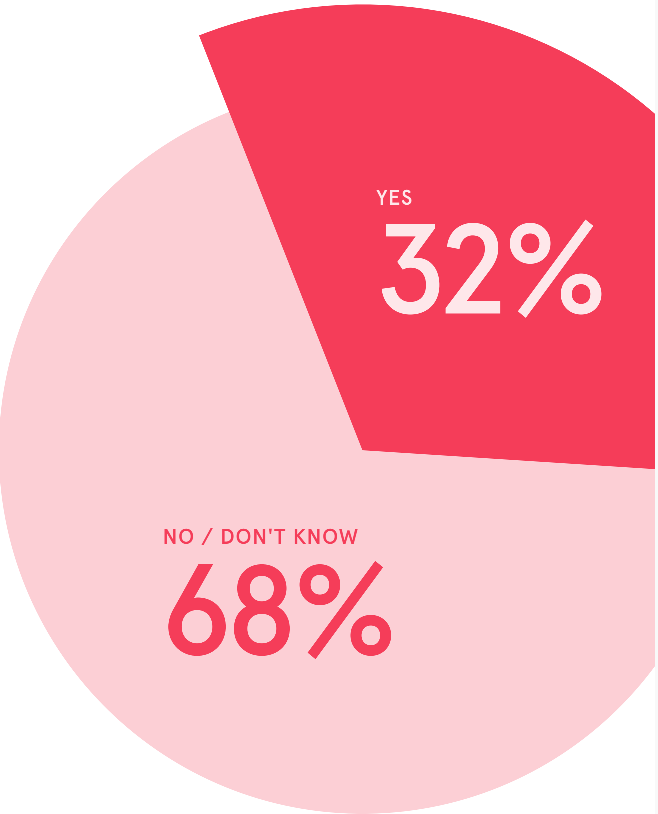
Just over one in four employees (26%) said they had fallen for a phishing scam at work in the last 12 months – up very slightly from 25% in 2020.

In addition to phishing emails, we also asked respondents whether they'd received phishing attacks via SMS. We found that the number of smishing attacks increased dramatically during the pandemic, and 56% of people we surveyed said they received a scam via text message in the last 12 months.

A third of those who received one (32%) complied with the request – a higher percentage than those who clicked on a phishing email.

EMPLOYEES WHO FELL FOR A PHISHING EMAIL IN THE LAST 12 MONTHS ↘





EMPLOYEES WHO FELL FOR A SMISHING ATTACK IN THE LAST 12 MONTHS ↗

> "Until recently, very few people outside your 'known' networks would be able to reach you via ✉ SMS and, therefore, we considered it a pretty secure and reliable channel.
>
> But now, that's not the case.
>
> As we shop online and are prompted to share our mobile number, we now receive text messages from contacts we don't know – so messages are legitimate, and others aren't. Because many people do not expect to be scammed via their texts, SMS has become a really effective attack vector."

Jeff Hancock
HARRY AND NORMAN CHANDLER PROFESSOR OF COMMUNICATION AT STANFORD UNIVERSITY

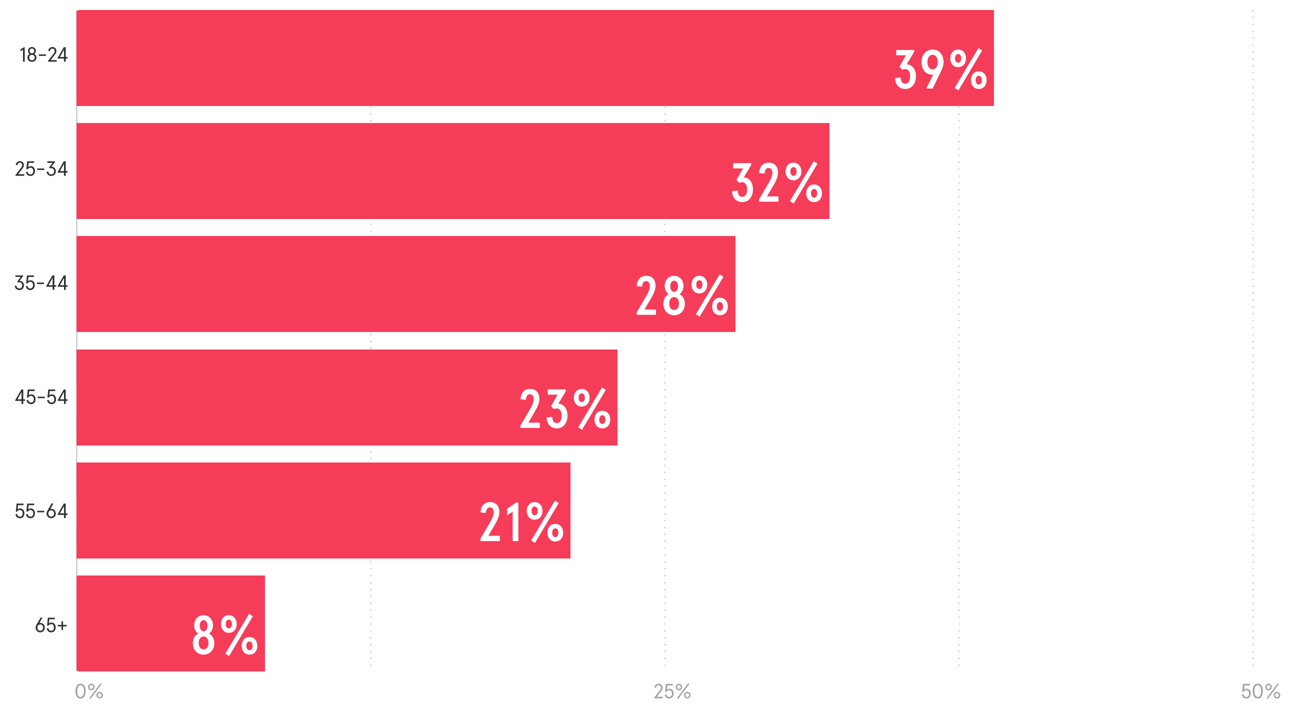
THE AGE FACTOR

Similar to our 2020 report, age is a key factor in phishing fallibility.

The percentage of employees who admit to falling for phishing scams at work decreases with age, and younger employees are 5x more likely to click on phishing emails than older employees, with 39% of 18–24 year olds admitting to doing so versus 8% of those over 65 years old.

Interestingly, older respondents were more susceptible to smishing attacks, compared to the younger employees, with 33% of respondents over 55 years olds complying with the request in a smishing scam versus 24% of 18–24 year olds.

EMPLOYEES WHO FELL FOR A PHISHING EMAIL IN THE LAST 12 MONTHS, BY AGE:



In our previous report, Hancock explained that this may be because the older generation were less experienced with phishing attacks, and therefore less likely to spot the signs of a scam. This could explain the higher percentage of smishing susceptibility in older age groups.

This year, Hancock also remarked on the shift in the types of scams targeting different age groups. He said, "In 2020, Covid-19 was the powerful hook used to phish people, preying on uncertainty and tapping into people's basic human need for health and safety, but now we see more scams centered on crypto targeting younger generations, tapping into that human need for greed."

DEPARTMENTAL DIFFERENCES

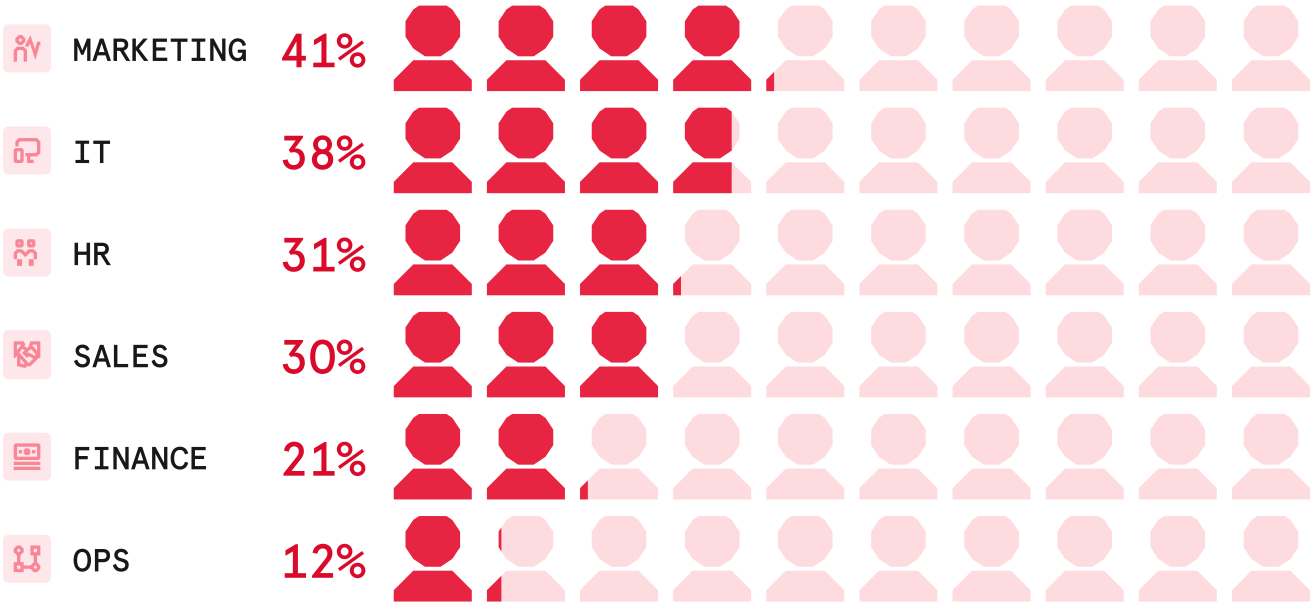
Phishing click-through rates also varied depending on the department that employees worked in.

Employees in marketing departments were twice as likely to fall for a phishing scam than employees in the finance department, and almost 4x more likely than those working in operations.

To Yavor, these findings highlight why security awareness training must account for differences in security cultures and behaviors across different departments.

He said, "Employees in highly regulated functions like finance, operations and legal have to comply with strict data regulations on a daily basis, and this means security risks are frequently top of mind. This will likely impact the security cultures in these departments and, consequently, the behaviors of the employees within them."

EMPLOYEES WHO CLICKED ON A PHISHING EMAIL IN THE LAST 12 MONTHS, BY DEPARTMENT



02

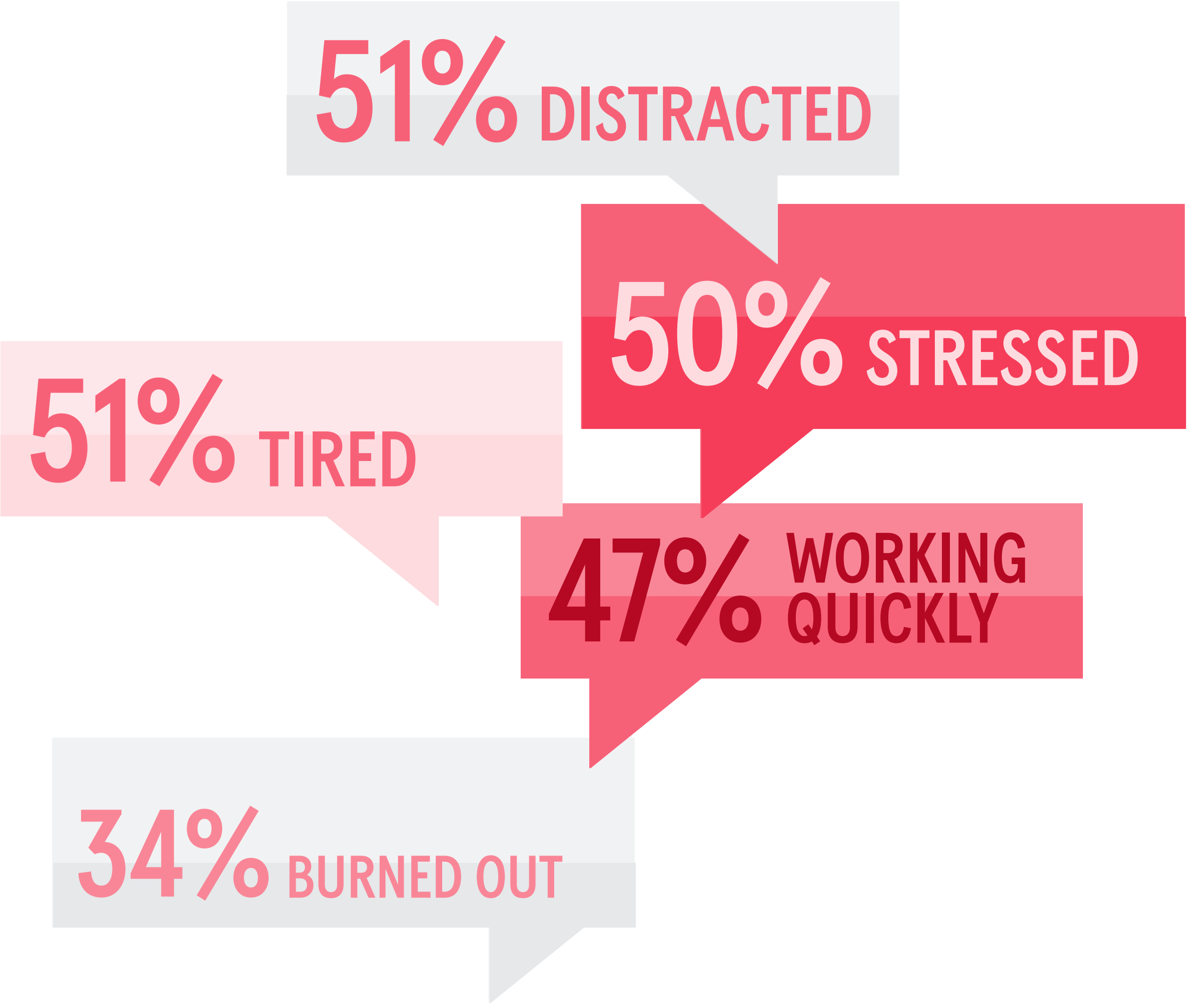
WHY DO THESE MISTAKES HAPPEN?

In the last 12 months, people have been more likely to make mistakes as a result of fatigue, stress and distraction – indicating the impact that behavioral factors can have on company security.

Over half of employees (51%) said they make mistakes at work when tired – up from 43% in 2020 – and 50% saying they make mistakes at work when they are distracted – up from 41% in 2020.

Working remotely hasn't helped matters. Half of employees surveyed (50%) say they are more distracted when working from home, while 43% say they are more stressed.

PEOPLE MAKE MISTAKES AT WORK WHEN THEY ARE...



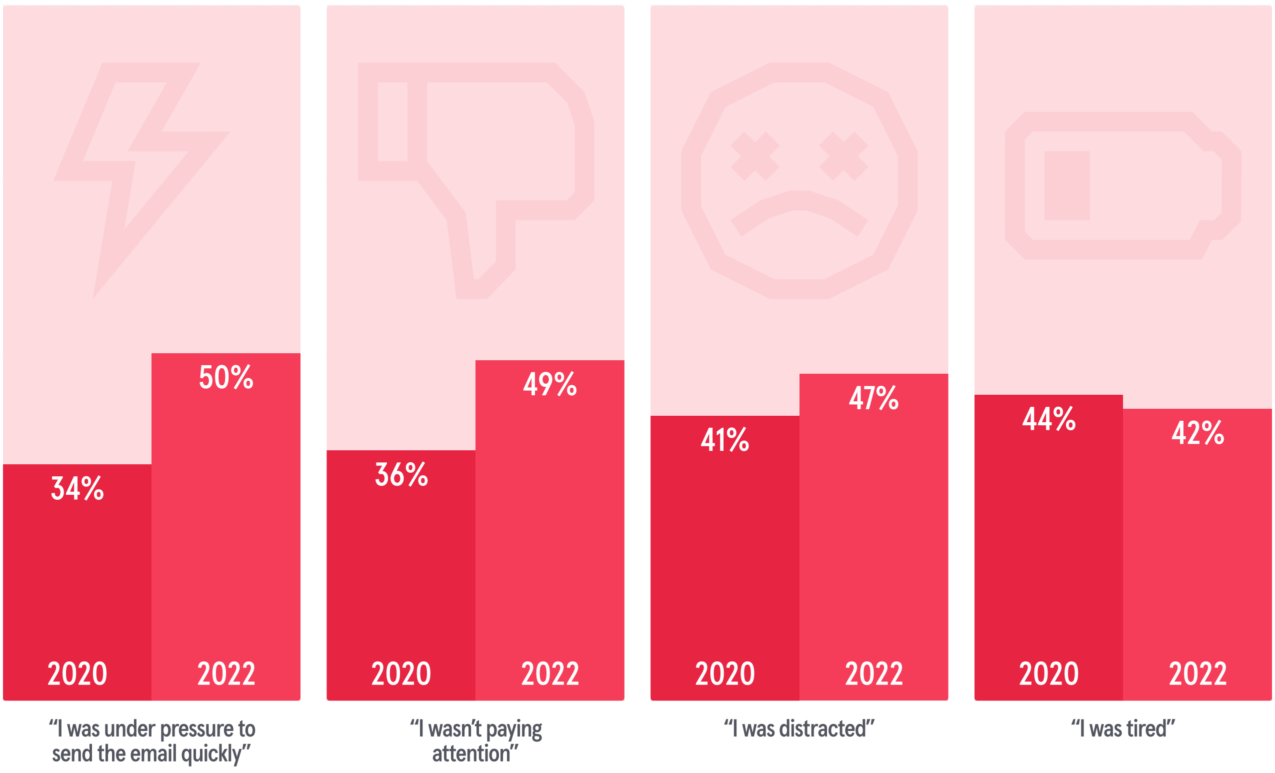
WHY EMPLOYEES SEND EMAILS TO THE WRONG PERSON

When we asked employees why they believed they had sent an email to the wrong person, half of respondents said it was because they were under pressure to send the email ⚡ quickly – up from 34% in 2020. This was closely followed by distraction and fatigue.

The data shows that since our last report, and since working environments changed to a hybrid model, people are more likely to make mistakes because they are working quickly and because they weren't paying attention.

Hancock said, "Businesses need to consider how hybrid working environments impact people's cognitive load – their ability to pay attention based on how many things they are juggling. When our cognitive loads are overwhelmed, that's when mistakes happen. Focusing on improving employees' mental health in these new ways of working not only impacts wellbeing and people's productivity – it also impacts security. Put simply, good mental health can improve cybersecurity in the organization."

WHY EMPLOYEES SENT EMAILS TO THE WRONG PERSON



WHY EMPLOYEES FALL FOR PHISHING EMAILS

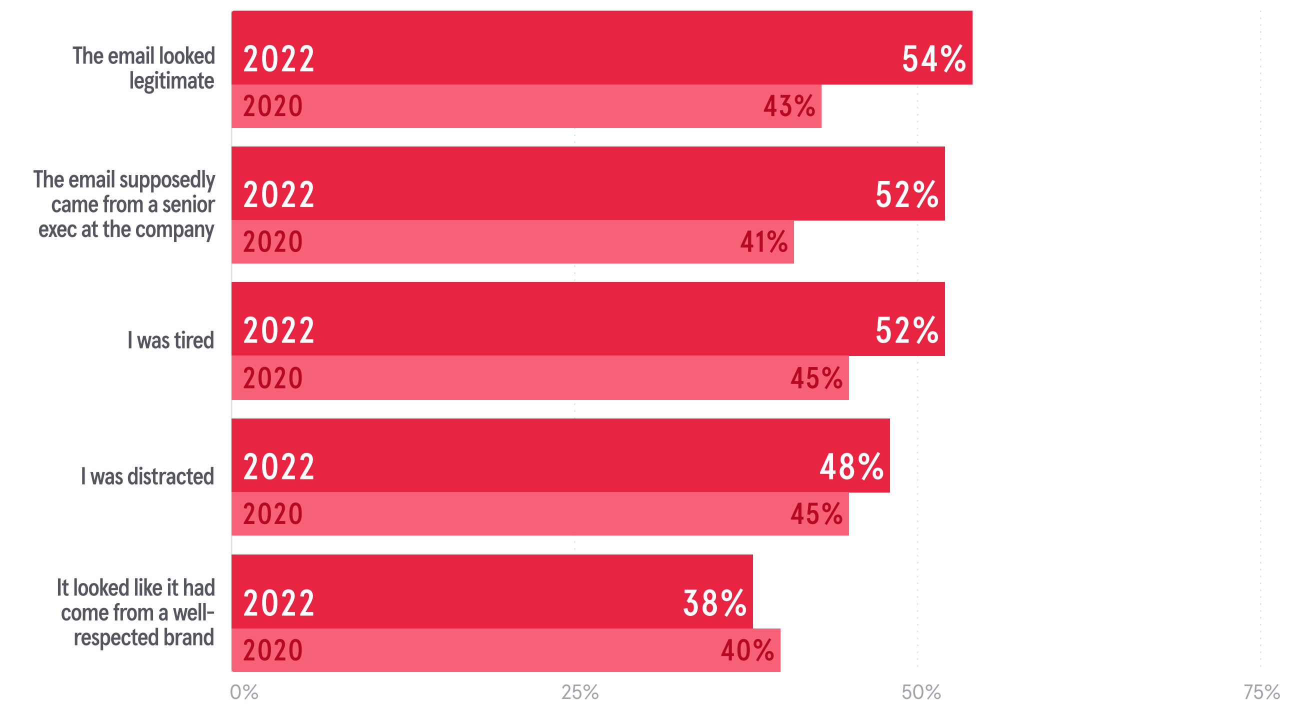
We can see that tiredness and distraction were, again, a reason for people to fall for phishing emails.

And cybercriminals know this; a 2021 report we published found that most phishing attacks are sent during the afternoon slump, between 2pm and 6pm, when people are more likely to be tired or distracted.

Another factor, though, is that inbound threats – the socially-engineered phishing attacks received by employees – have become harder to detect.

When asked why they fell for phishing scams in the last 12 months, 54% of employees said it was because the email looked legitimate – a big increase from the 43% reported in 2020. This was closely followed by 52% of respondents saying it was because the email looked as though it had come from a senior executive at the company – up from 41% in 2020.

WHY PEOPLE FELL FOR PHISHING SCAMS AT WORK



And these types of impersonation scams are effective.

In 2021, the FBI reported that Business Email Compromise (BEC) attacks caused $1.8 billion of losses - up 14% on the previous year. In fact, the percentage of respondents who said they fell for a phishing email whereby the threat actor was impersonating a well-respected brand dropped from rates reported in 2020.

> “There are several core principles of influence and one of them is social proof.
>
> A stronger version of social proof is one that invokes authority.
>
> As humans, we are deferential to authority so if our default is to ‘do what the boss says’, and a cybercriminal impersonates a senior executive at the company, it increases the probability that the attack will work.”

Jeff Hancock
HARRY AND NORMAN CHANDLER PROFESSOR OF COMMUNICATION AT STANFORD UNIVERSITY

So not only are behavioral factors like fatigue and stress hindering employees’ abilities to spot phishing scams, but cybercriminals are delivering more and more sophisticated (and believable) attacks.

"Attacks are becoming more sophisticated because there is so much information about ourselves online now.

The attacker knows more about their target than the target knows about the attacker and they'll use that asymmetry to craft more targeted attacks and make their targets like them or trust them more.

With a basic understanding of human psychology, attackers will build a relationship with their targets and center their scams on the things that get people's attention – greed, attractiveness, confidence and fear – to successfully hack their victims 🕵"

Jeff Hancock
HARRY AND NORMAN CHANDLER PROFESSOR OF COMMUNICATION AT STANFORD UNIVERSITY

BURNED OUT

The media has widely reported how the pandemic has increased levels of stress, while working remotely has left people working longer hours

Our data tells a similar story.

45% of UK and US employees say they are burned out - the same figure we reported at the peak of the pandemic in July 2020. What's more, the majority of respondents (56%) believe there to be a culture of presenteeism which means they work longer hours than they should - all, once again, adding to people's cognitive loads.

This feeling of being 'chained to the desk' has only been exacerbated by the trend of people leaving their jobs on a huge scale - dubbed The Great Resignation. In fact, 58% of UK and US employees say their team is understaffed as a result of their colleagues leaving this year.

> "The big factor in the Great Registration is the loss of culture. When people work closely together for a long time, they understand each others' working behaviors and communication patterns. An individual can usually tell if an email is legitimate, based on the relationship they built with that person; they have common ground and can provide context to what they're saying. That is really hard to fake in phishing attacks. But if that person leaves the company, the context is lost or skewed, which increases the opportunity for a successful phishing attack on a newer, less culturally-embedded employee."

Jeff Hancock
HARRY AND NORMAN CHANDLER PROFESSOR OF COMMUNICATION AT STANFORD UNIVERSITY

03

SO...
WHAT NOW?

THE IMPACT OF HYBRID WORKING

Hybrid work is here to stay; and that's going to impact your company's security in more ways than you might have thought.

Not only do security teams have to think about the risks associated with Bring Your Own Device and network security, but organizations are also going to need to address how hybrid working impacts people's working and security behaviors.

Think about how the technologies that enable hybrid and remote working influence the cognitive loads of employees. A recent study by Jeff Hancock and his team showed that virtual meetings fatigue is real, and people are suffering from cognitive overload because of it. And when people are cognitively loaded, they can't multi-task and are less likely to see warning signs in phishing emails, for example.

They found that women and people of color are most likely to suffer from Zoom fatigue and, with this in mind, it's so important to tailor security support for these individuals. Because, as Hancock says, "if the criminals behind the phishing attacks know which employees are overwhelmed and distracted, they're going to target those people."

You also need to consider how hybrid meetings – with attendees both in the office and dialing in from home – will affect people's security behaviors. Hancock adds, "The person calling into the meeting via Zoom has to work a lot harder to be perceived as present and work harder to communicate non-verbally. Overtime, that's going to impact their levels of fatigue and their ability to pay attention."

A simple fix is to encourage workers to take regular breaks, particularly between virtual meetings and step away from screens to help prevent cognitive overload caused by Zoom fatigue. Stanford researchers also recommend implementing "no-video meeting" days and, if video is not necessary for specific meetings, making "video off" mandatory so that no one feels the pressure to keep it on. If you want to find out if your employees or colleagues are fatigued, you can ask employees to take the Stanford Zoom Exhaustion and Fatigue (ZEF) Scale and find solutions to help reduce it.

A longer term solution is to build a strong security culture and create an environment where employees can do their work while avoiding security risks. How? Read on →

BUILDING SMARTER SECURITY CULTURES

Throughout this report, we've shown that when employees are overwhelmed and stressed, they make mistakes that compromise security.

It's human nature.

To address this, organizations need to take a more human approach to security, helping employees make the right security decisions on channels like email, and making it easy for them to remediate mistakes before they turn into security incidents.

Machine intelligent security solutions like Tessian automatically detect threats and alert employees in-the-moment, explaining what was suspicious about the message via clear, educational warnings to the user. This in-the-moment coaching not only prevents mistakes from happening, but also educates employees on the tactics hackers use.

This approach helps nudge people to adopt safer security behaviors, overriding impulsive decision-making and encouraging employees to think, consciously, before they click. Over time, behaviors improve and risk levels decrease, especially as security teams can leverage the intelligence provided by the platform to identify their riskiest and most at-risk employees, and tailor security training and policies for individuals that need more help online.

By empowering employees to make security decisions, people become another layer of defense in the enterprise and this, in turn, helps alleviate the burden and stress experienced by those in the security operations team.

Understanding how factors like stress impacts behavior is so important to improving cybersecurity, especially in these new ways of working.

A human-first approach to security can support people and help secure the data and systems they need to get their jobs done.

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.

Methodology

In January 2022, 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+.

Learn More About How Tessian Prevents Human Error on Email.

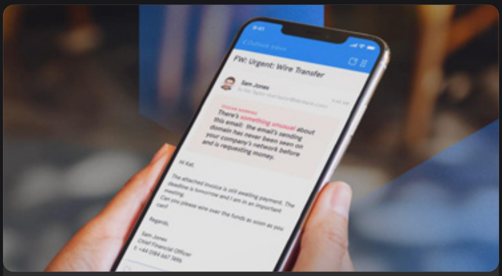
Tessian's mission is to secure the human layer by empowering people to do their best work, without security getting in their way.

WANT TO LEARN MORE?

TESSIAN DEFENDER

Prevent Inbound Email Attacks that Bypass Legacy Email Security Solutions

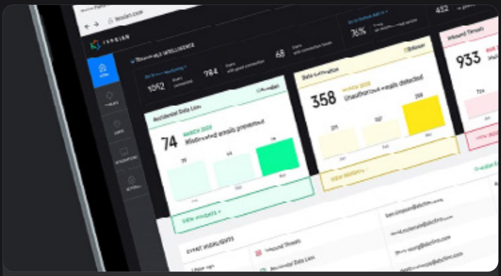
LEARN MORE →



TESSIAN GUARDIAN

Automatically Prevent Accidental Data Loss

LEARN MORE →



BOOK DEMO

See Tessian in Action

LEARN MORE →

See Tessian in Action.

Automatically stop data breaches and security threats caused by employees on email.

FIND OUT MORE →

TESSIAN

Tessian Cloud Email Security intelligently prevents advanced email threats and protects against data loss, to strengthen email security and build smarter security cultures in modern enterprises.