CARELESS CLICKS

COULD YOUR TEAM
SPOT A CYBER ATTACK?

Foreword

In an interconnected – and often volatile – world, the threat of cybercrime is ever-present.

Hackers have become more sophisticated and pervasive in their efforts to extract the valuable personal and commercial information that banks and other financial services companies hold. Changing working habits like remote and hybrid working have further heightened the risk if employees use unsecured public networks, like those in coffee shops.

We've all seen phishing emails. You may even have clicked on one (and felt your heart race as the panic grows). Some phishing attacks are targeted at individuals, so while they're distressing, especially if personal information is compromised, they won't generally cause an organisation-wide incident.

But other phishing emails could be a more serious ransomware or malware attack, with the potential to bring down entire company systems. Figures show that nearly 60% of UK companies experienced a ransomware attack in 2024 – a 10% rise on the previous year.

We're all well aware of the operational disruption an attack like this could cost, not to mention the reputational damage and potential fines that come with it. For example, in 2023, the FCA fined Equifax Ltd more than £11m for its role in one of the biggest cybersecurity breaches in history – specifically, failing to manage and monitor the security of UK consumer data it had outsourced to its parent company in the US.

Every employee, at every level, plays a role in ensuring good cybersecurity practices but the evolving threat means that they don't always have the awareness and knowledge to spot and report an attack. This is why organisational culture and digital resilience are so closely linked – positive behaviours stem from sound reporting processes, strong IT systems and, of course, regular training.

To understand whether employees' attitudes and behaviours could be putting their company at risk of a cyber attack, we surveyed 200 finance professionals in the UK. Their responses are detailed in this report. We also spoke to cybersecurity expert Dr John Kingston about the current threats and what firms can do to protect themselves, and three leading financial services experts, with years of experience in regulatory compliance on how to embed good practices in your culture.

Vivek Dodd
CEO and Co-founder
of Skillcast

Contents

Contributors

Dr John Kingston

Dr John Kingston has more than 25 years' experience in the cybersecurity field, and a background in AI and law. He is also a member of the Nottingham Trent University's Cybersecurity Research Group, which researches and implements security measures to protect against cyber breaches.

Katharine Leaman

Katharine has worked in financial services for over 30 years in insurance claims, giving investment advice, regulation and banking compliance. Katharine has been European Head of Regulatory Compliance at Standard Chartered Bank and spent over a decade at the UK's regulator, the FSA (now FCA) in senior policy and supervision roles. Katharine's expertise is in technical areas of the rules such as Market Abuse, CASS, SMCR and Outsourcing. As well as issues that have a broader regulatory focus such as market conduct, non-financial misconduct, conduct risk, operational resilience, and consumer duty.

David Kenmir

David Kenmir has 35 years of regulatory experience, including five years as a Managing Director at the FSA and 14 years as a Risk and Regulatory Partner at PwC. Having retired from PwC last year, he is building a plural career, part of which includes taking on the role of Chair of Skillcast's new Advisory Board and has become an INED at a start-up bank.

David has extensive regulatory experience and has worked with many organisations on the strategic and day-to-day challenges they face. He has broad expertise in Financial Crime, including s166 reviews and Enforcement cases.

Scott Morris

Scott has over 40 years of banking and compliance leadership experience, acquired across a number of global banking organisations, as well as a regulator and professional body.

Scott has extensive experience in creating and directing large teams across different regions. Throughout his career he has taken on senior roles in Compliance and Anti-Financial Crime, operating at Board, Senior Advisor, Managing Director and Executive Vice President levels.

How secure are your ~~systems~~ people?

No matter how you slice it, humans are at the root of every cyber attack – whether it be everyday errors and misjudgement, or negligence and malicious insider attacks.

It might be more obvious in the case of phishing where someone has inadvertently clicked on a link, or when weak passwords have compromised an account.

But it's also easy for criminals to exploit vulnerabilities in networks and software when they haven't been patched or updated; when security settings aren't configured properly; and threat detection and response processes are poor.

So the question to ask is not how secure your *systems* are but how secure are your *people*?

Driving good practices is a leadership team that prioritises cybersecurity, with investment in IT infrastructure, clear and regularly communicated polices, and training to build knowledge and awareness across the workforce.

Many leaders, of course, recognise the threat of cyber crime. According to government figures:

- 75% of all businesses say it's a 'high priority' for their management team
- It's more likely to be a high priority in larger businesses compared to medium sized ones (98% vs. 93%)
- 61% of firms in finance and insurance have named cybersecurity a 'very high priority', just behind information and communications (65%)

Yet figures like these – like our own survey results on page 8 – show that there's still work to be done before all firms prioritise cybersecurity and follow best practices.

The changing face of cyber crime

We've all heard of email phishing, where people are persuaded to share sensitive details – but what about vishing (voice calls), smishing (SMS), spear phishing (highly targeted/personalised messages), or even whaling where senior executives are asked to disclose top level sensitive information?

As one report makes clear, cyber criminals are working 'smarter, not harder', using technologies like artificial intelligence (AI) and taking a more strategic approach. AI enables hyper-personalisation on a mass scale and could be used to build a relationship – and then manipulate – employees via their work or even personal channels.

The expert view: ‘Hackers target humans because they’re more likely to be deceived’

Dr John Kingston, senior lecturer in cybersecurity at Nottingham Trent University explains the biggest threats facing organisations today, and how they can protect themselves and their employees.

Cybersecurity threats like phishing have been around decades and they’re still common today. The government reported 84% of businesses experienced phishing from 2023-24 and another half had some form of cybersecurity threat.

There are still growth areas like malware on mobile phones, which is a more open market compared to computers. A recent trend is hackers targeting cryptocurrency, where we saw the biggest theft in history this year.

The role of AI

Artificial intelligence (AI) tools help hackers create sophisticated attacks by improving the quality of writing. Poor quality content used to be one of the telltale signs in the past.

But the biggest recent change to the industry is the use of deepfake AI.

The UK engineering group, Arup, was targeted in early 2024. Cyber criminals set up a video conference but the employees who joined weren’t real – their faces and voices were cloned using AI. The business was duped into transferring £20m over 15 transactions.

When working virtually, there’s no way to verify who you’re speaking to and deepfake has become that sophisticated, it’s hard to tell the difference. Of course, there are more technical cyber threats in an organisation or system but it’s easier to deceive the humans involved.

Flexible working: a new threat?

Home Wi-Fi networks, especially if you live in a terraced house, are often secure because they’re password protected. But anyone who can get close can theoretically hack it, it’s just likely that they would be spotted first.

Stats show a quarter of Brits work from a coffee shop once a week – but public Wi-Fi is less secure. The biggest threat is keyloggers, a type of malware where cyber criminals record every key pressed, which gives away card details, email addresses or passwords. Connecting to a mobile hotspot is also just as risky as public Wi-Fi.

“The physical security of home Wi-Fi is not bad at all and there’s not much reason to be worried. However, if you’re working from a public venue, like a coffee shop, security can be a big issue.”

Fortunately, most organisations protect against this by encouraging employees not to use public Wi-Fi or implementing tools like two-factor authentication (2FA).

The impacts of a breach:

Reputation

If you're in an industry where financial details must be kept secure, your reputation can take a big hit. For example, cybersecurity firm CrowdStrike caused a global IT outage in 2024, after a software update left them vulnerable – pretty embarrassing.

Regulatory

Back in 2015, a hacker tried the simplest form of attack (an SQL injection that uses malicious code to hack databases) on broadband provider TalkTalk's website – and it worked. They got access to its customer database that contained data like card details. The database wasn't encrypted, which led to a record fine from the Information Commissioner's Office (ICO) of £400,000. After a few years, GDPR came into effect and it's estimated the fine would have been at least £52m.

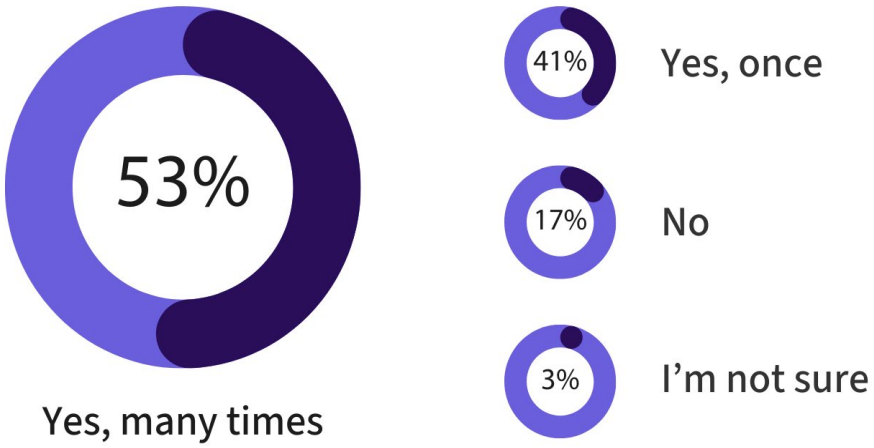
Bankruptcy

Regulatory fines are increasing with GDPR. The ICO states businesses are liable to pay fines up to £17.5m, or 4% of their annual turnover, depending on which is higher. Fines paired with loss of trust can be incredibly damaging for businesses and some will struggle to recover.

Survey results

Just how prevalent are cyber attacks in financial services and how well prepared are employees to respond to them? We polled 200 UK professionals working in the sector today to find out how their attitudes, behaviours and competencies are protecting their company's data and reputation – or putting them at risk.

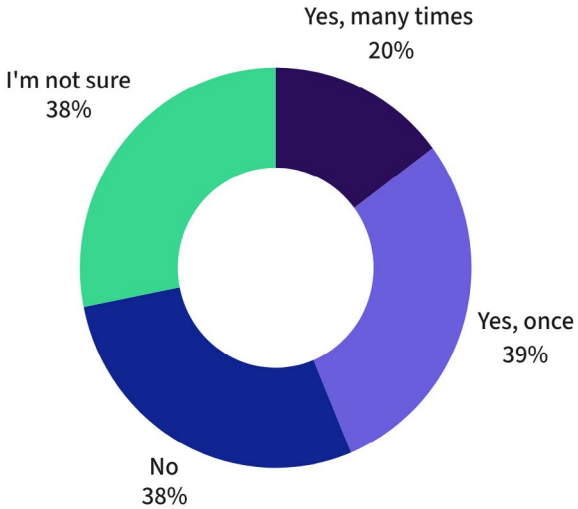
Q.1 Have you ever experienced a cyber attack attempt (e.g. phishing emails, malware) at work in the last 12 months?



Insight: UK businesses experienced around 7.78 million cyber crimes in 12 months, according to government figures – so it's not surprising most (82%) respondents say they've been targeted. Hopefully, these attempts were recognised quickly and appropriately actioned – however, the high-profile breaches that have been seen across the world over the past year underline the need for vigilance.

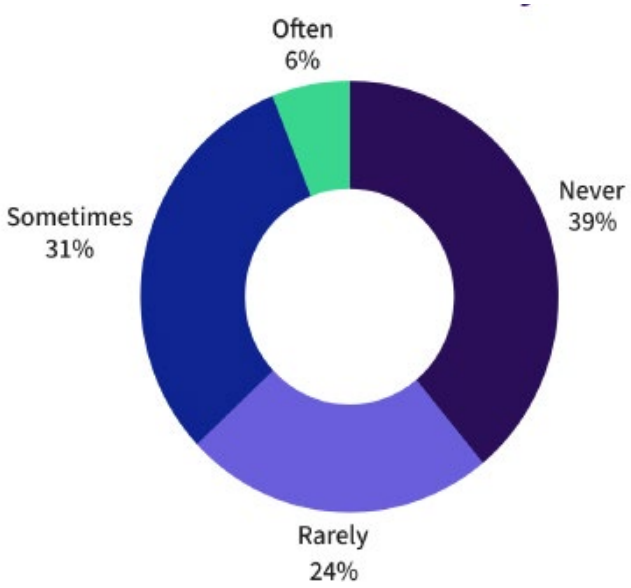
A fifth of our survey respondents also said they hadn't seen an attempt or they didn't know. So, they're either fortunate, work for a company with strong IT defences, or – more concerningly – didn't recognise that it was a potential phishing email in the first place.

Q.2 Have you ever clicked on a link or opened an attachment in an email or message that you later believed might be part of a phishing scam or cyber attack?



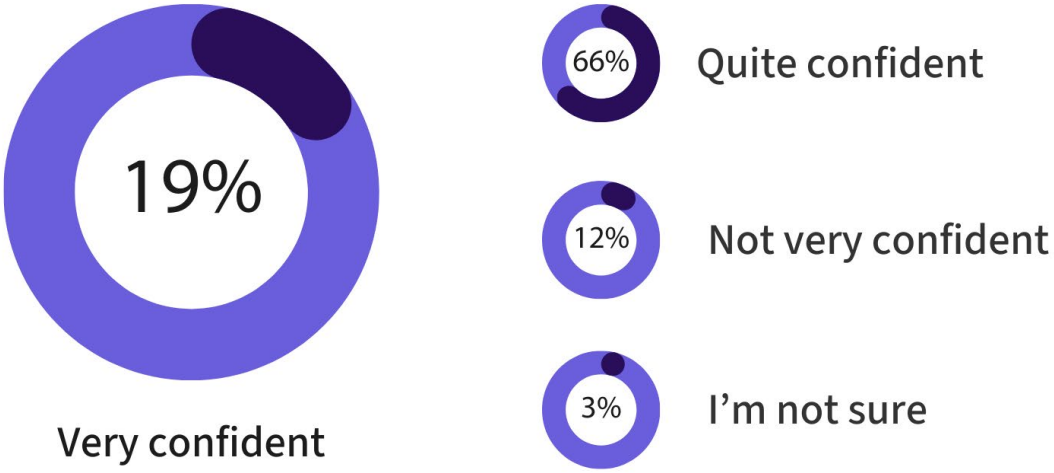
Insight: Well over half (59%) admit to clicking on a link or opening an attachment, which is understandable given how convincing these communications have become. A momentary lapse of judgement is all it takes for a busy employee to click carelessly. They may also let their guard down when working from home. The good news is that over a third (38%) say they haven't, suggesting high levels of awareness in some firms.

Q.3 How often do you use weak or easy-to-guess passwords (e.g. "password123", your pet's name, etc.) for work-related accounts or systems?



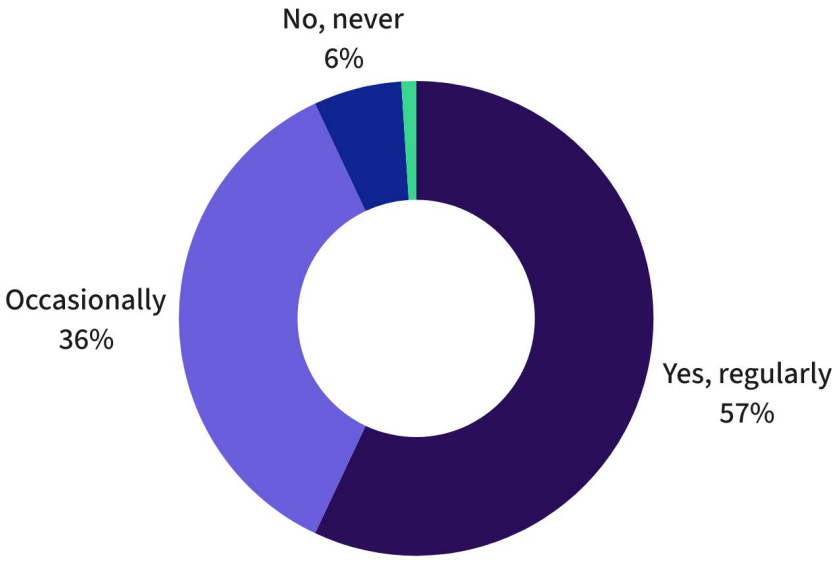
Insight: With so many accounts – and passwords – to manage, it's tempting to pick an obvious word to avoid having to reset the login details. Yet weak passwords are easy to hack and while it's reassuring that nearly two-fifths never use them, most (55%) do so at least sometimes, and 6% often use them.

Q.4 How confident are you that you could spot a possible cyber attack?



Insight: It's interesting to see that the vast majority of (85%) say they're confident they could spot a cyber attack – despite 59% clicking on links or attachments that could have been part of a phishing attempt. This may be down to their perhaps outdated assumptions of what an attack looks like versus the highly sophisticated reality we see today.

Q.5 Does your workplace deliver regular cybersecurity training and advice?



Insight: Training is a key part of reducing operational risk as set out in the FCA Handbook – so it's worrying that 7% of respondents say their workplace doesn't offer it. And while it's great that 57% receive regular training, those who only undertake it occasionally (36%) could also be putting their firm at risk. With threats changing all the time, and people often consumed by their day job, regular updates and reinforcement of key messages ensures that good practices are embedded within the workplace culture.

Test your knowledge

When cyber criminals attack

On a busy Monday morning at N.E. Bank, Sam, a mortgage adviser, absent-mindedly clicks a link in an email that looks like it's from IT. Without realising, he activates sophisticated malware that quickly harvests login credentials and sensitive customer data. The malware spreads through the bank's network, exploiting vulnerabilities and establishing backdoors for cybercriminals.

As systems slow down and customer data becomes inaccessible, it becomes clear the company has been hacked.

What should Sam do now?

a) Google the problem and try to fix it alone

b) Carry on working – there are deadlines to meet

c) Report the incident to the IT/security team and line manager straight away

d) Turn the computer off and on again

Could you spot a phishing email?

Not every unsolicited – spam – email is a cyber attack. Some are the result of dubious marketing practices from businesses you've often never heard of, for products you have no interest in buying. While annoying, these emails are not necessarily illegal.

Phishing emails, on the other hand, are illegal. They could be an attempt to extort money from the recipient (as with lottery or romance scams), or compromise IT systems by extracting passwords and other data, or installing malware or ransomware. And while attempts are getting more sophisticated, there will still be telltale signs if you know what to look for.

To: sam@ne-bank.com

From: John@ne-bank_security-team.com **[email domain looks convincing but isn't real]**

URGENT ACTION NEEDED: YOUR ACCOUNT HAS BEEN SUSPENDED

Dear Sam,

I hope this email finds you well. This is John from IT at N.E. Bank. **[right name and company]**

We've detected unusual login attempts on your workstation (ID: NE-2458) this morning at 9:47 AM. As a precautionary measure, we need you to update your credentials immediately.

Please click here to securely update your password: [N.E. Bank Secure Login Portal] **[clear attempt to obtain details]**

This is time-sensitive. If not updated within 30 minutes, we'll need to temporarily suspend your account access as per our new cybersecurity protocol. **[adds urgency]**

If you have any questions, don't hesitate to reach out to me directly on ext. 5566. **[makes it look legitimate]**

Thank you for your help in keeping our data secure.

Best regards,
John Smith
Head of IT
N.E. Bank

A culture of compliance, not complacency

As we've seen, knowledge is key to identifying and preventing a cyber attack taking hold of your company systems – but it doesn't happen by chance. It's part of an overall culture of compliance, where transparency and accountability are prioritised. Training isn't treated as a tick-box exercise but something that empowers people to make the right decisions.

We spoke to three experts, who've built their careers in financial services regulation and who're part of the Skillcast advisory board. Here, they explain how firms can embed good practices into their teams.

'Recognise your blindspots – and make compliance training fun'

Every organisation has its blind spots when it comes to information security. They may be reactive in responding to the latest regulation, rather than proactively promoting the sound processes and behaviours that enable them to comply in the first place.

Firms are particularly vulnerable during times of business change like restructuring a department or following a merger or acquisition. In today's world, restructuring is highly complex, partly because technology is so embedded within organisations. You need to factor in information security, confidentiality, access control (to software, devices and physical spaces), changes in reporting lines, and whether interim performance assessments are needed as responsibilities are handed off.

People often don't associate compliance training with fun, but trust me, it can be. One of the most enjoyable things I recommend is conducting scenario testing. One of the most fun things you can do at work – especially if you don't have a team-building budget – is create a scenario and throw it at the team unexpectedly.

For example, you could plan a scenario where the company's chairman has been kidnapped by hostages who've locked him in a meeting room, and there's a gunman in the building. Then, announce that the attackers have also unplugged all your servers. What's your resilience plan? Not only is it fun and engaging, but it also tests resilience for real. It inspires your team, encourages teamwork and helps you prepare for unforeseen events.

- Katharine Leaman, CEO of Leaman Crellin

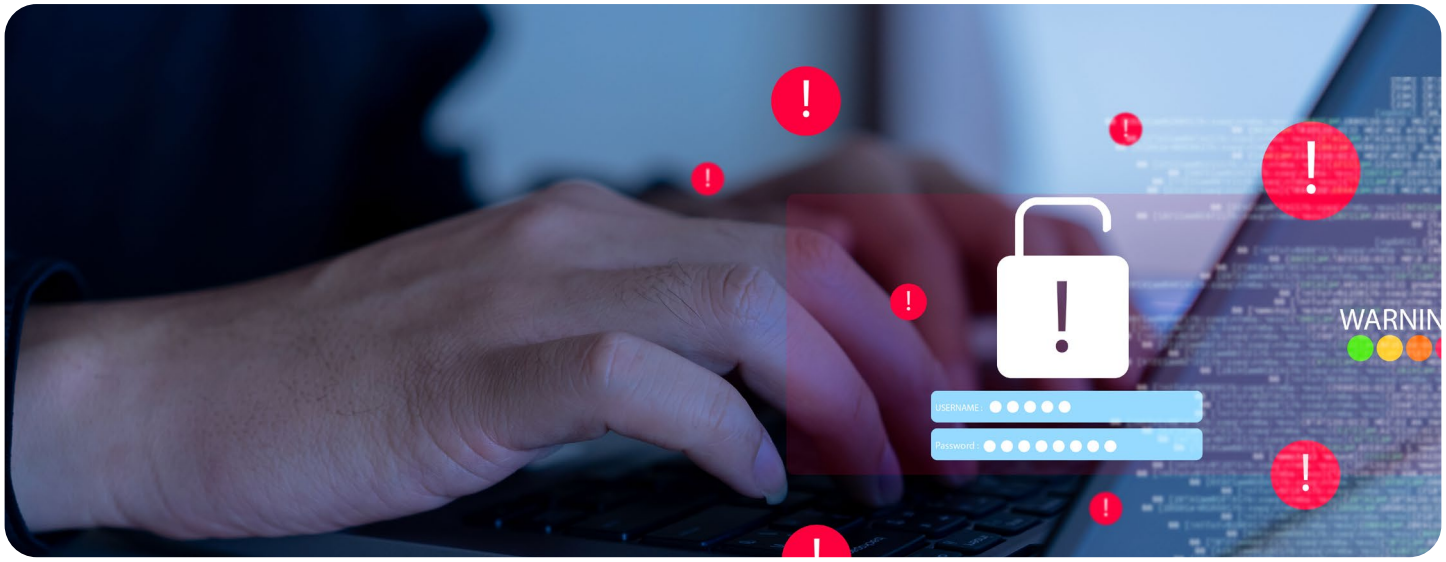
‘Recognise the changing face of cyber attacks’

Banking, like many industries, often struggles to keep up with the growing threat of cyber terrorism. This is no longer just an isolated issue, it’s now happening at the level of entire countries. It is suspected that Russia and other state actors are targeting European health services. In fact, our own **health services** experienced a major disruption, and while it hasn’t been officially confirmed, we strongly believe it was a coordinated attack at a country-wide, systemic level.

In the past, people used to talk about the risks of carrying confidential information like having it in your briefcase while on the train. Over time, it shifted to things like data sticks, and now we have laptops and other tools that, if compromised, can cause significant damage to the bank’s operations and reputation.

Although there’s a lot of encryption and security measures in place to prevent these issues, unfortunately, breaches still happen. On top of that, banks have been heavily criticised for their tech vulnerabilities. There have been a number of high-profile fines as well as outages. Outages, whether they’re caused by equipment breakdowns, natural events like floods or cyberattacks, can cause severe disruption for customers, especially if they’re unable to make critical payments or receive their wages.

-Scott Morris, Senior Adviser at StoneTurn



‘Manage your data well and build a healthy level of scepticism in your teams’

In today’s data-driven world, you’ve got to start with the basics, establishing control over where data is stored and managed. This process begins with design and continues through to building, deployment, testing and beyond. Everything needs to be framed within a strong policy and process environment, which must also include proper training for the relevant staff.

When it comes to the broader workforce, beyond just the technical teams managing these systems, it’s about fostering a culture where people are aware of the risks. They need to question things when necessary and be cautious like not clicking on suspicious links in emails, even if they’re not directly involved in the technical side of things.

-David Kenmir, Chair of Skillcast’s advisory board and INED

‘Preventing a cyber’ attack

Carrot, stick – and training

Carrot: Rewards people for getting it right.

Stick: Penalties for those who get it wrong (anything from poor practices to negligence).

Training: Introduce courses on common threats and how to look out for them.

It’s always worth sharing stories of people who have fallen prey to cyber attacks because it’s more memorable. If you have been the victim of a cyber attack, put out notices telling your employees that you are being targeted, and provide clear instructions on what they can do to contain the attack.

Businesses should already be implementing intrusion detection systems, firewalls and other security measures to protect against technical risks. There are also a number of other ways organisations can reduce the risk:

Penetration testing: Organisations manufacture an attack to check for vulnerabilities, which is an effective method for overall security.

Self-phishing: An organisation will typically send out phishing emails to its workforce and any employee who clicks it will get a response letting them know. This is a good training technique as employees can learn from it.

2FA: Adding an extra layer of security to email or system logins with 2FA works pretty well. But SMS is more vulnerable to hacking, so much so, Microsoft now sends authentication codes through WhatsApp – the more secure messaging option because it’s end-to-end encrypted.

Policy: Creating a policy for prevention is probably the best method but put someone in charge of driving it forward and making sure it's followed.

Password crackers: Run password crackers on your organisation to find out how easy it is to get past them. A lot of employees will still use basic words and many of them use a capital letter at the start and special character at the end. Introduce a policy on the best type of password – a passphrase is considered the most secure these days.

-Dr John Kingston shares his tips for avoiding a cyber attack

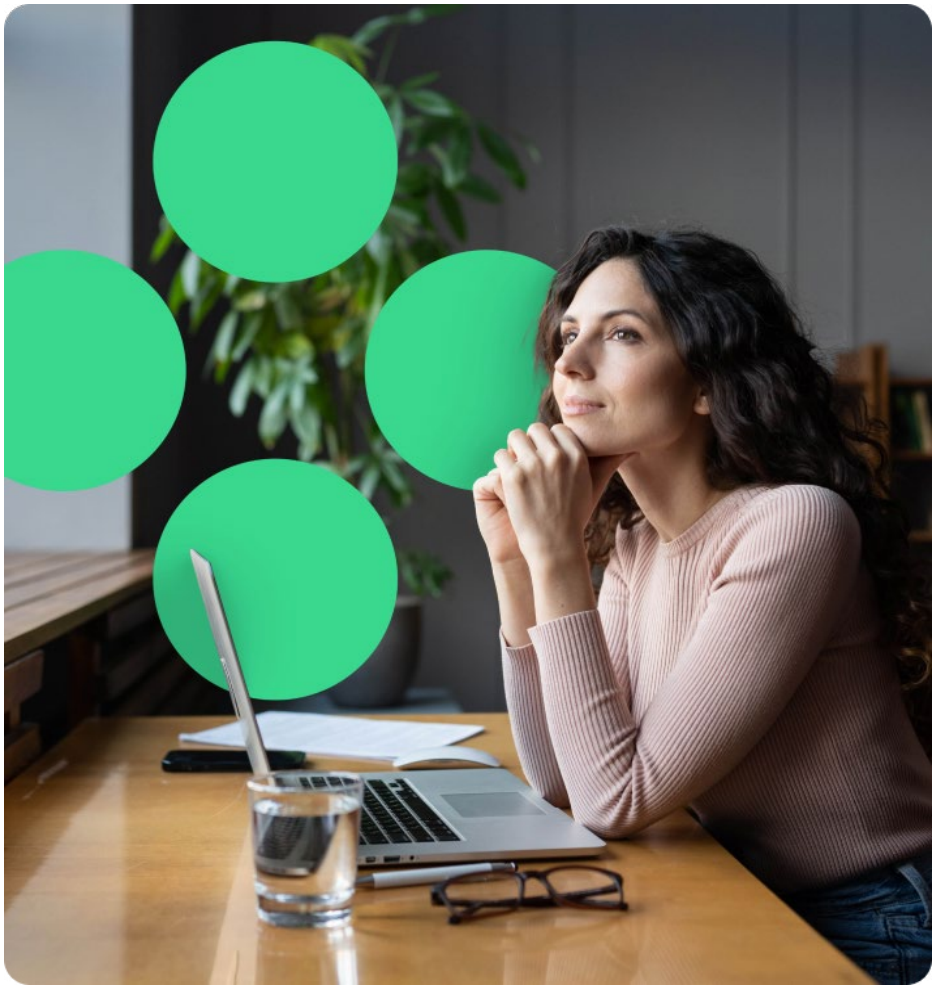
Conclusion

Cybersecurity threats are complex and ever-changing – but getting the basics right can go a long way. Our survey showed that while many employees are confident they could spot a malicious attack, this isn't always reflected in their day-to-day behaviours. Choosing stronger passwords and not carelessly clicking on links are some of the simplest yet most effective steps we can all take to protect both ourselves and the firm, but not everyone is doing it.

A culture that prioritises transparency, accountability and knowledge of the risks is key to building resilience, and this requires regular, relevant and engaging training.

As a result, employees are empowered to raise concerns, whether about systems, people or processes, while best practice becomes second nature. Leaders recognise that resilience is a collective responsibility, not one that falls to individuals alone, and that cybersecurity must be underpinned by clear policies and procedures that are understood and communicated frequently. They also need to be ready to take action if an individual fails to comply.

While it takes time to maintain technical infrastructure, develop policies and provide training, that investment will deliver returns many times over if it means avoiding the disruption, fines and reputational fallout associated with an attack. Even if you're fortunate enough to avoid a serious incident, creating an environment where people can get on with their job securely and with confidence unlocks wider business benefits, from product innovation to talent retention to customer confidence.



skillcast

About Skillcast

Skillcast helps companies build ethical, inclusive and resilient workplaces. It provides content and technology to digitise and streamline compliance processes and manage them from a single compliance portal. Its product range includes a Learning Management System with comprehensive off-the-shelf compliance course libraries, a Policy Hub, Staff declarations, Anonymous surveys, CPD tracking, and Compliance registers for gifts, expenses, PA dealing, and whistleblowing.

To start your free trial

Call us on +44 20 7929 5000

Visit www.skillcast.com/free-trial

Or scan the QR code below