CyberSmart

The SME Mobile Threat Report

Introduction

Mobile phones, they're ubiquitous. Although it's less than three decades since the launch of the first internet-enabled phone (**Nokia's 9000 Communicator**, for readers looking for an excellent pub quiz question), there's not much we don't use mobile devices for — dating, banking, food shopping, navigation and, increasingly, work.

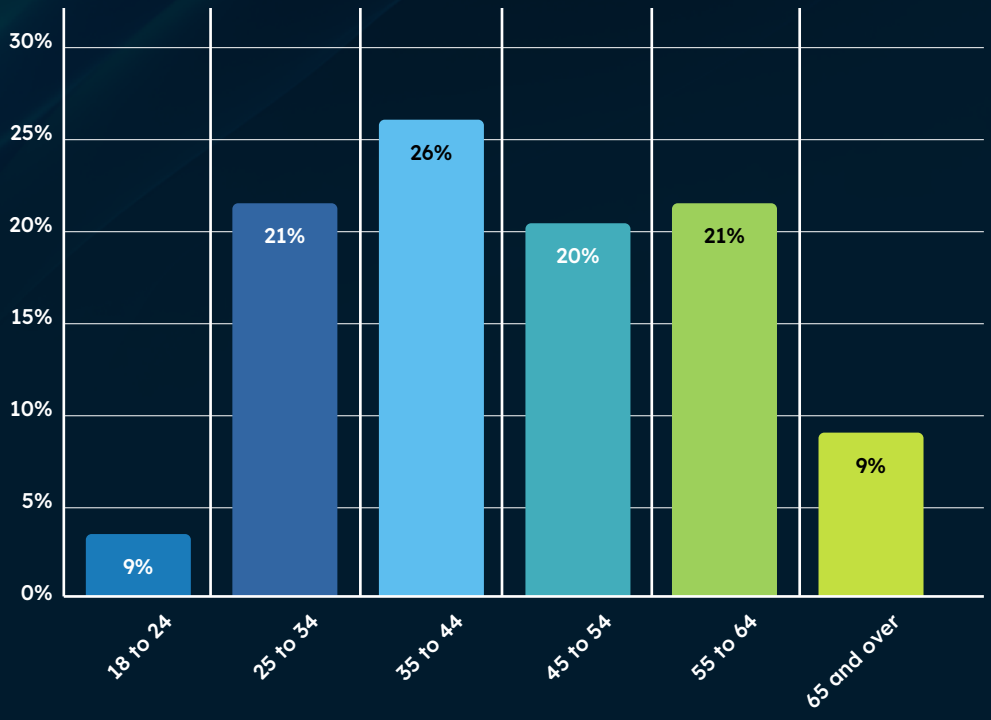
Practices like bring your own device (BYOD) – employees using their personally owned devices for work purposes – and **remote working**, have been revolutionary for small businesses. These new ways of working, unthinkable just a few decades ago, have dramatically reduced the costs of doing business and ushered in an age where employees can work from just about anywhere.

However, at the same time, the use of mobile devices (particularly personal devices) for work brings risks with it. Indeed, mobile-specific threats are one of the fastest-growing forms of cybercrime.

The stats make for pretty grim reading. Between 2022 and 2023, global mobile cybercrime saw a **147% increase**, from around 2 million per month to nearly 5.5 million. What's more, it appears that many businesses are ill-equipped to deal with the threat. **42% of organisations** report that vulnerabilities in mobile devices and web applications have led to a security incident.

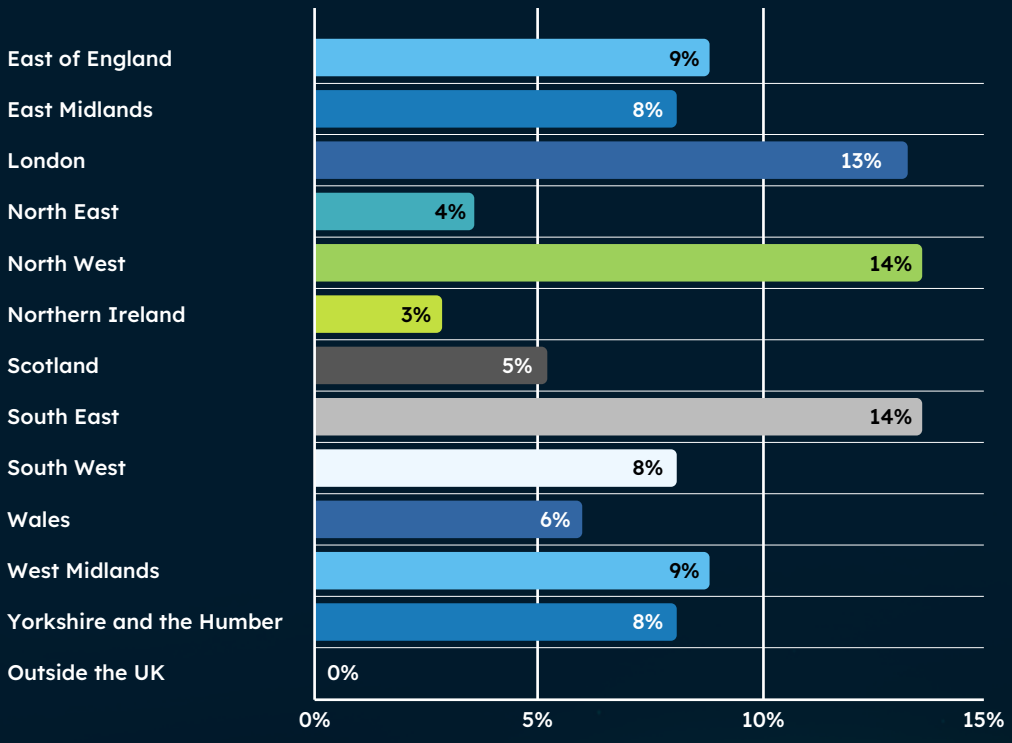
With all this in mind, we decided to probe a little deeper. How are the UK's small businesses tackling mobile security threats? To find out, we surveyed, 250 UK CEOs from companies with under 250 employees, across a wide geographical and sectoral range (see table below).

How old are you?



Response count **250**

Where do you live?



Response count **250**

Which sector do you work in?

1st	Retail	15%
2nd	Information technology	13%
3rd	Property and construction	10%
4th	Other sector	9%
5th	Business, consulting and management	8%
6th	Engineering and manufacturing	6%
7th	Accountancy, banking and finance	6%
8th	Hospitality and events management	5%
9th	Healthcare	4%
10th	Leisure, sport and tourism	4%
11th	Teaching and education	3%
12th	Creative arts and design	3%
13th	Transport and logistics	2%
14th	Insurance and pensions	2%
14th	Sales	2%
16th	Environment and agriculture	1%
16th	Marketing, advertising and PR	1%
16th	Media and internet	1%
19th	Charity and voluntary work	1%
19th	Information research and analysis	1%
19th	Performing arts	1%
19th	Recruitment and HR	1%
19th	Social care	1%
24th	Energy and utilities	0%
24th	Law	0%
24th	Public services and administration	0%
27th	Law enforcement and security	0%
27th	Publishing and journalism	0%
27th	Science and pharmaceuticals	0%

We asked them how they're using mobile devices within their organisations and the security protections they have in place. What follows are results of this study, providing an accurate picture of SMEs' mobile defences in 2024.

What mobile threats do small businesses face?

Before we delve into the results, it's worth considering the mobile-specific cyber threats SMEs face. Although this is by no means an exhaustive list, here are a few of the key threats.

Mobile Phishing

Mobile phishing attacks have **grown at a consistent rate of 85% annually** since 2011. And, as we'll see from our survey, this is one of the biggest threats to SMEs.

Banking Trojans

Between **the first half of 2019 and the first half of 2024**, UK internet banking fraud cases skyrocketed. Much of this is being driven through mobile devices. For example, more than **300,000 Android users** may have downloaded **banking trojan** apps through the Google Play Store.

Mobile Malware

Malware such as **ransomware** has long been one of the most common and lethal cyber threats. Unsurprisingly, cybercriminals have continued to adapt how they launch attacks, with mobile devices now providing fertile ground for scams.

What's more, this threat is on the rise. In a 2022 study, mobile malware was found on **1 in 20 Android devices.** Meanwhile, according to Kaspersky, **10.1 million mobile malware attacks** were blocked in the first quarter of 2024 alone.

Malicious Apps

Despite Apple and Google's stringent security criteria for anything available through their app stores, malicious apps remain a huge problem. For example, security researchers **flagged hundreds of fake apps to Google last year**, warning millions of users could be affected.

And, the apps on our phones don't need to be malicious to be harmful. It's estimated more than **75% of all published apps** have at least one security vulnerability.

Insecure Wi-Fi and network spoofing

One of the key benefits of BYOD and remote working is employees' ability to work from anywhere. However, it also comes laden with risk. Open or "free" Wi-Fi in places such as cafes or on public transport are notorious for man-in-the-middle and similar attacks where cybercriminals intercept and monitor network traffic – posing a huge security risk to anyone accessing sensitive company data.

Poor updating hygiene for apps

In much the same way as desktop, unpatched mobile operating systems and applications can contain exploits and vulnerabilities that attackers take advantage of to steal corporate or personal data.

Insider threats

Readers of our **SME cost of living crisis report** will remember that insider threats were a key concern for small business leaders. And, unfortunately, that's unlikely to have changed. Between 2023 and 2024, there has been a **28% increase** in insider-driven data exposure, loss, leak, and theft events.

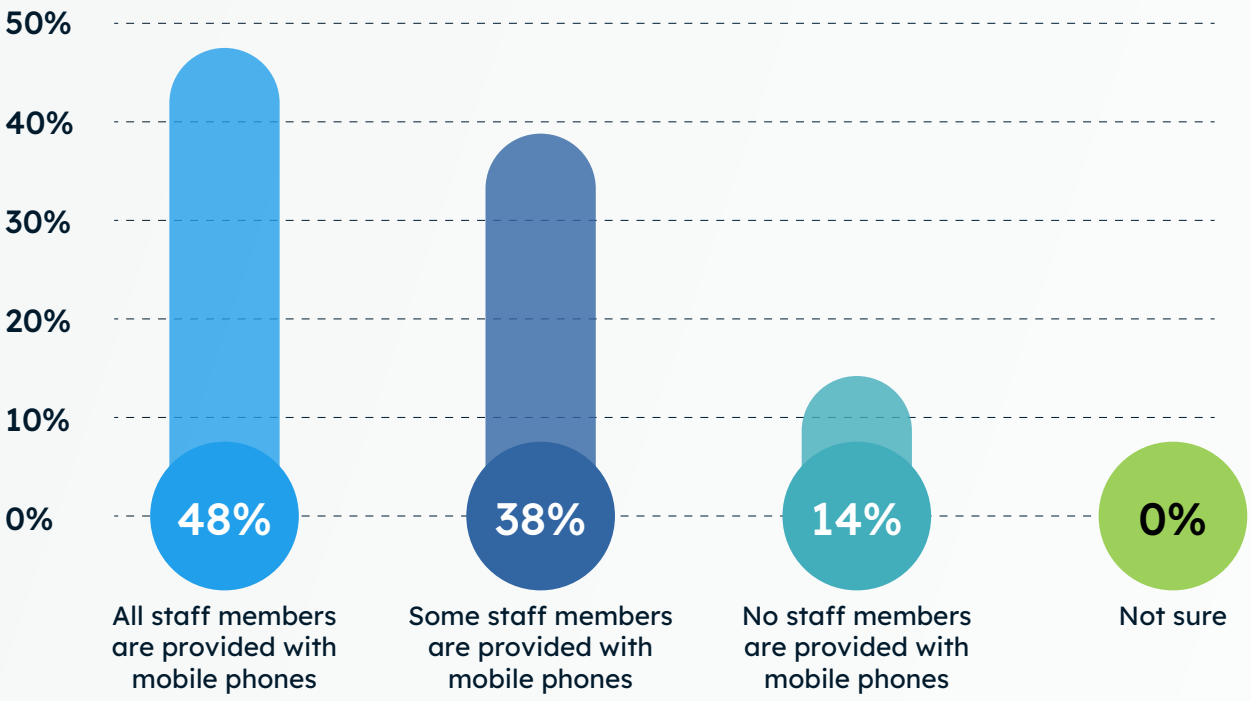
Whether unwittingly through clicking on phishing links, being duped by **social engineering techniques**, or maliciously, the threat of staff exposing a business remains.

Our findings

We've covered the mobile threats SMEs face, but what can our research tell us about security practices within small businesses?

SMEs are increasingly using personal mobile devices for work.

Does your business/workplace provide mobile phones for any your staff members to use for work purposes?

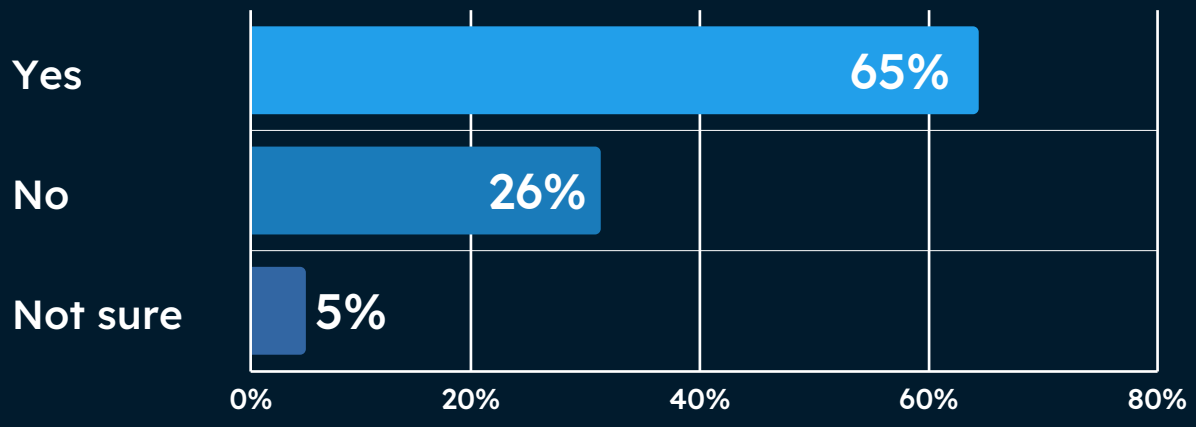


Response count **250**

BYOD policies can offer dramatic CapEx savings, something that's particularly important for small businesses that are often compelled by circumstance to track every penny. Therefore, it's somewhat predictable to see that 60% of organisations expect their employees to use mobile devices to carry out work tasks, despite not providing all of them with work phones.

Indeed, 65% of those businesses that don't provide all staff members with mobile phones expect staff to use personal devices.

You said that you only provide some staff members with mobile phones or that no staff members are provided with mobile phones. Do these members of staff complete work-related tasks using a personal mobile phone instead?



Response count 130

There's nothing wrong with this in principle. As we've previously mentioned, BYOD policies are essential for many modern SMEs. However as we'll see in the next section, it can present problems.

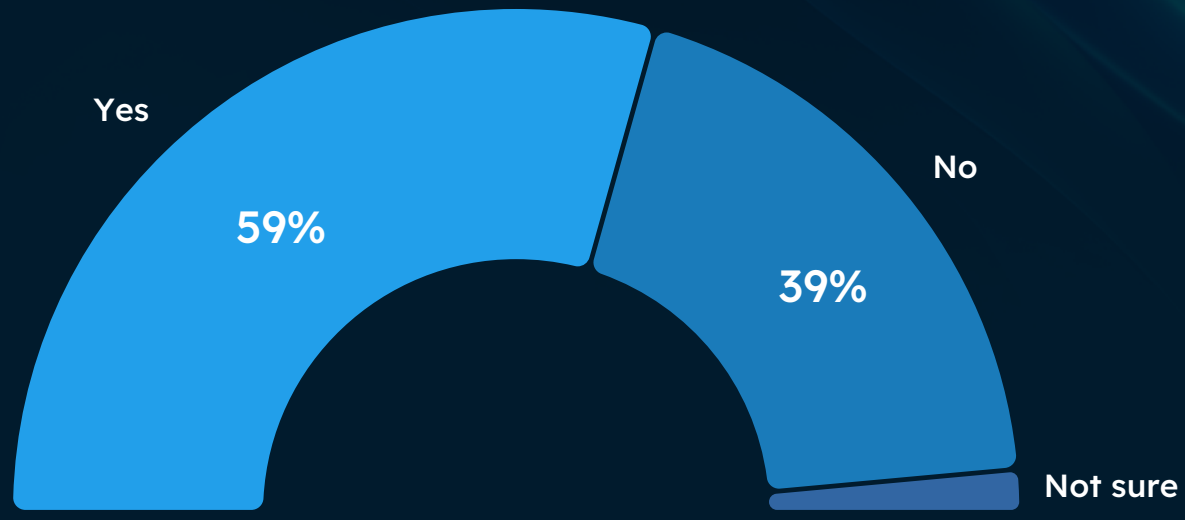
Many SMEs don't have a mobile code of conduct for staff

For any business adopting a BYOD policy, staff must understand what's expected of them from a security perspective. For example, you might stipulate that employees must never connect to an unsecured Wi-Fi network without using a VPN. Or, have rules in place about how regularly patches and updates must be run.

A clear code of conduct or security policy can help prevent your businesses from being exposed to unnecessary risks.

Therefore, it's concerning to see that although 59% of small businesses do have a code of conduct for completing work-related tasks on personal devices in place, a large chunk (39%) don't.

Does your organisation have a code of conduct for completing work-related tasks on a mobile phone?

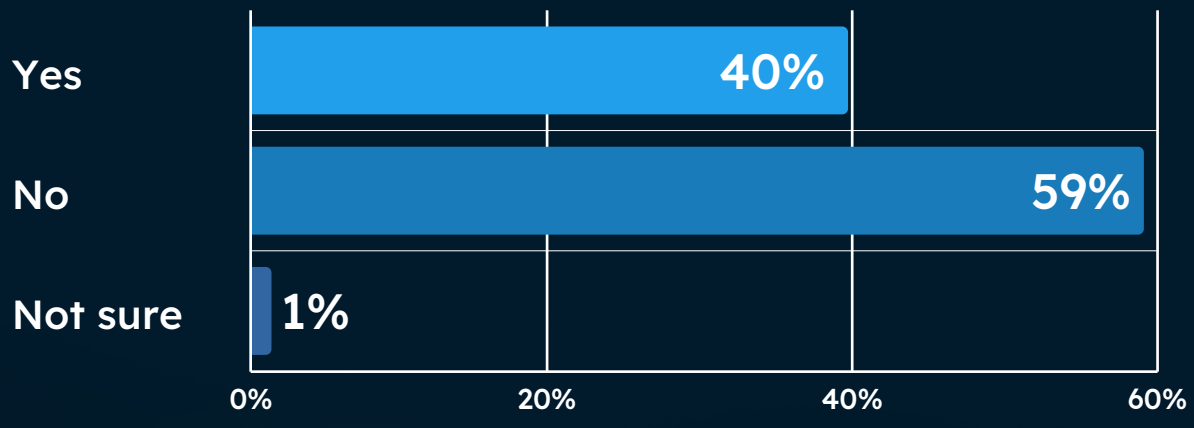


Response count 250

These organisations are potentially exposing themselves to many risks, from insider threats to man-in-the-middle attacks.

Most SMEs don't provide mobile security training for staff

Are your staff members required to complete any mobile phone security training as a part of their role?



Response count 250

As we saw in the previous section, it's deeply concerning that many small businesses are implementing BYOD programmes without clear security and conduct policies in place. However, our research uncovered an area of even greater concern.

The majority (59%) of our respondents said that they don't provide any mobile phone security training for staff. Without training on how to identify and avoid cyber threats or what safe online behaviour looks like, these businesses are courting potential disaster.

According to research from Cybint, **95% of cyber breaches** stem from some sort of human error, or, in simple terms, could have been prevented. This is also backed by older **research from Stanford University and Tessian** which puts the figure at 88%.

Whichever figure you prefer, that's a lot of preventable cyberattacks. And, by not providing security awareness training to staff, it's exactly these kinds of breaches that small businesses are risking.

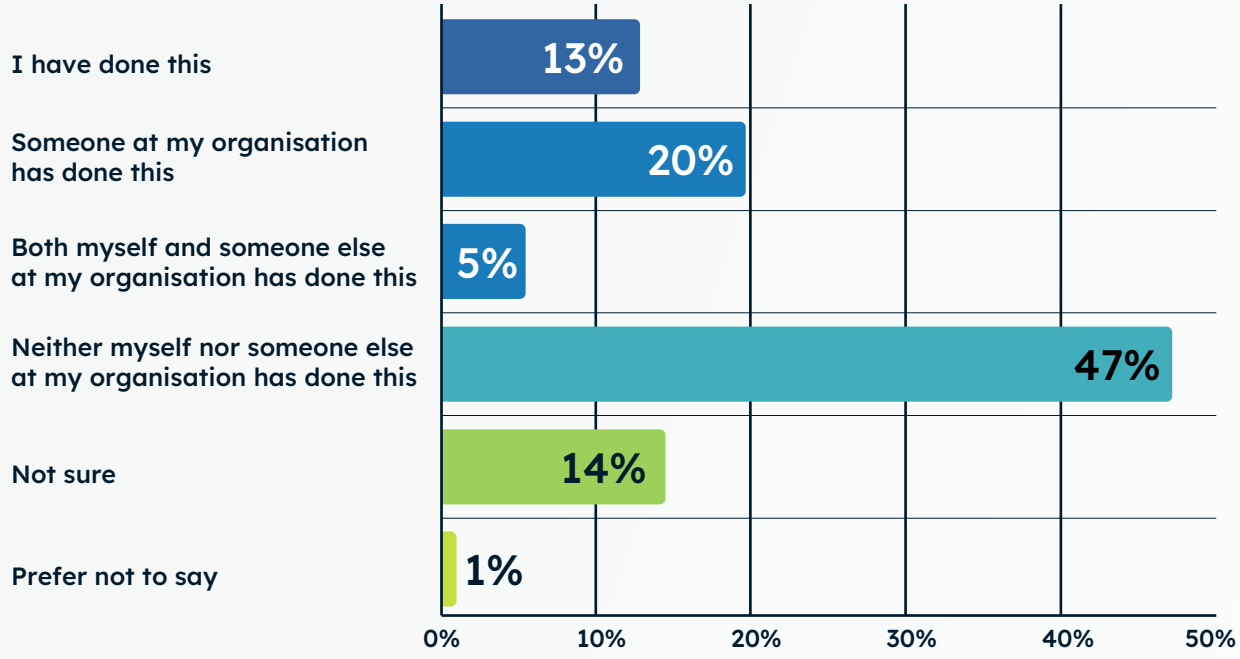
In mobile security, this could be anything from staff clicking on a phishing link (more on which later) to working from an unsafe network or even unwittingly unleashing a banking trojan on company systems. The key point is that training is one of the most effective ways to prevent this and protect your business. After all, forewarned is forearmed.

What are the consequences of SMEs' security practices?

Thus far, we've unearthed some worrying findings about UK SMEs' mobile security. But what are the consequences of this? Are SMEs being attacked as a result? Here's what our respondents told us.

Over a third of SME staff have clicked on a malicious link

Have you, or anyone at your organisation, ever clicked on anything malicious (such as a phishing link) when working from a mobile phone?



Response count **250**

According to the Department for Science Innovation & Technology (DSIT), **84% of all UK** businesses have received some kind of phishing attack in the last 12 months. So, we asked SME leaders whether they or anyone at their business had clicked on a malicious link via mobile.

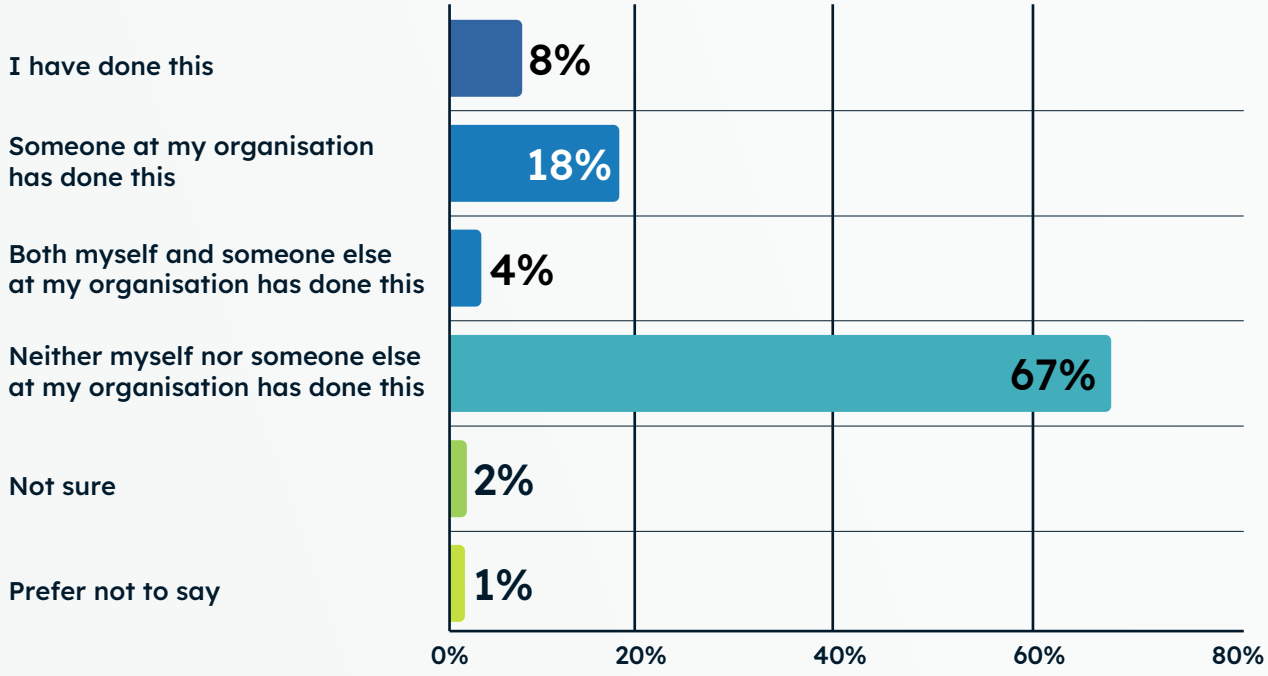
Although almost half (47%) of small business leaders responded no, some 38% reported that someone within their business had clicked on a phishing link – still a high number. What's more, the real figure is likely to be somewhat higher given that a further 15% were either unsure or preferred not to answer.

This poses a real risk for small businesses. The UK has lost £1.7 billion to **phishing scams** in the last year, while the average cost of a breach to an SME ranged between **£2,240 and £17,190**. Worse still, phishing scams are often used to launch much nastier cyber threats such as ransomware and banking trojans.

However, this threat can be greatly weakened by simple security awareness training. If staff know what to look out for and how to identify potential scams, they're far less likely to click on a malicious link or expose the business to risk.

Almost a third of SMEs report losing mobile phones containing sensitive data

Have you, or anyone at your organisation, ever lost or had mobile phone stolen containing sensitive corporate information?



Response count **250**

30% of respondents reported losing or having stolen a mobile phone containing sensitive corporate information. While this might appear more of an OPSEC (operational security) problem than a cybersecurity one, a mobile device falling into the wrong hands poses a cyber threat.

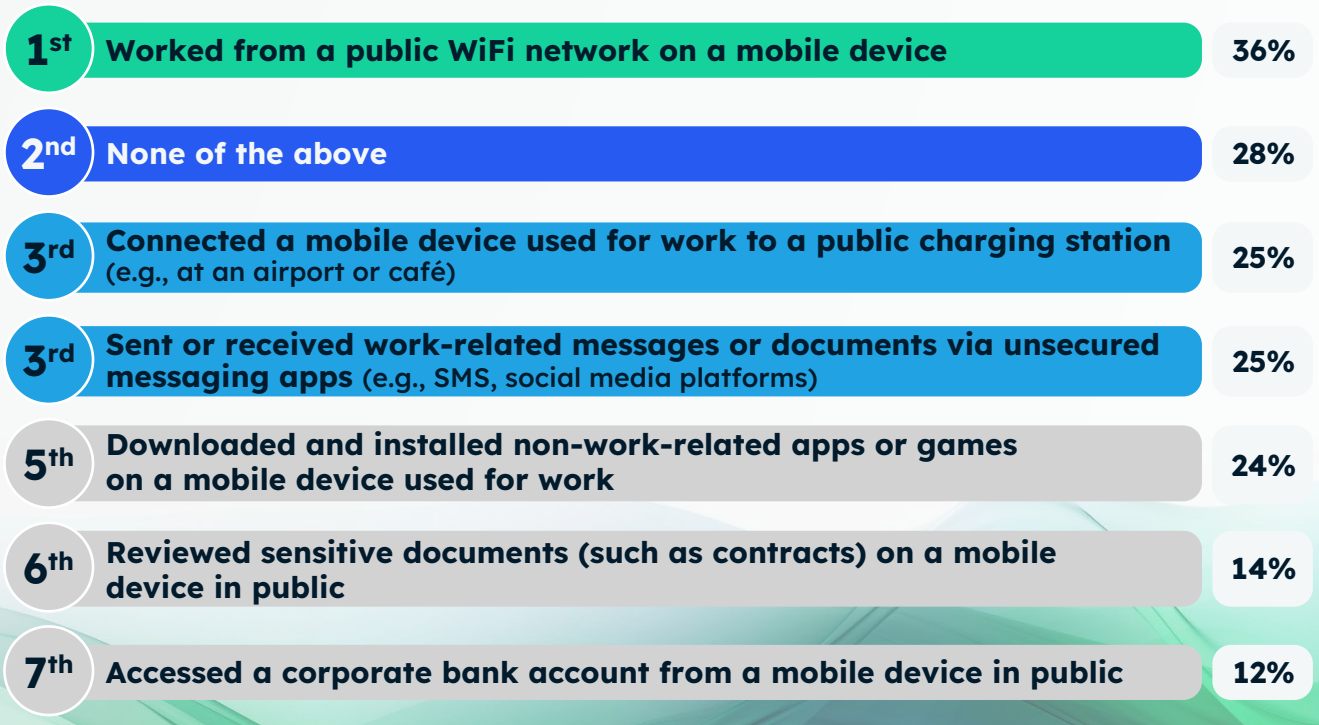
Not only does it risk providing cybercriminals with access to sensitive data and internal systems, but the device could also be used to launch further attacks on partners and customers.

Of course, however rare it might be, things do get lost or stolen and staff make mistakes. These are inevitable costs of doing business. Nevertheless, when a device with sensitive data or access to corporate systems goes missing, acting quickly and decisively is key. It's a lot like a medical emergency, often, what happens in those first few minutes will determine the outcome.

To be able to respond quickly and shut down any risk, small businesses need a policy in place for what happens if a work-owned or BYOD device goes missing. In addition, staff need to be familiar with this policy to allow them to react quickly.

SME staff are engaging in risky behaviour

Have you, or anyone at your organisation, ever done any of the following? [Select all that apply. Please note that 'mobile device' refers to both company-owned and personal mobile phones]



7th	Allowed a friend or family member to use a mobile device that contains corporate data	12%
9th	Stored corporate passwords or login credentials on a mobile device without encryption	11%
10th	Forwarded corporate data to a personal account	9%
10th	Used a mobile device to access corporate networks or data while abroad without informing the IT department	9%
12th	Synced corporate emails or files to a personal device without IT department authorisation	5%
13th	Made a large corporate payment (Over £10,000) in public on your mobile device	4%
14th	Not sure	4%
15th	Prefer not to say	1%

Response count **250**

While not as eye-catching as stats about phishing and lost corporate devices, it's the day-to-day cyber hygiene of SME staff that raises the most concern. This risky behaviour suggests a low level of mobile security awareness among employees.

For example, a quarter of respondents admitted using a mobile device for work at a public charging station (e.g., at an airport or café), and 36% of respondents have worked from a public WiFi network on a mobile device.

A further 9% admitted to forwarding corporate data to a personal account, and 11% admitted to storing corporate passwords or login credentials on a mobile device without encryption.

These are all behaviours that put businesses at risk of breach. However, all could be mitigated by clear, businesswide policies for mobile use and security awareness training.

What can we conclude?

Despite some SMEs adopting safe mobile security practices, it's clear that there is a significant number that are engaging in risky behaviour – putting businesses in real peril.

However, it's important to note that there are several mitigating circumstances leading to this. Most obviously, there's the cost. Large enterprises are far more likely to implement security awareness training for mobile devices and implement a code of conduct. This just isn't a luxury afforded to most SMEs, who don't have the resources or time to really invest in their cybersecurity.

In addition, there's clearly a security awareness problem for some small business leaders when it comes to mobile threats. The move to using mobile devices hasn't been a neat, seamless process for many SMEs. Instead, BYOD has often been adopted quickly, out of necessity, due to events like the COVID-19 pandemic and shrinking budgets. As a result, SMEs and their staff just aren't aware of the scale of the threats.

Finally, the cybersecurity industry needs to make security more accessible for SMEs through training, guidance and practical solutions. Small businesses make up 99% of the UK economy and form the supply chain of its government and major businesses but, too often, they're being left behind. It's time we change this.

What can SMEs do to improve their mobile security?

We've established that mobile security poses a real security risk for many small businesses. But what are some practical measures SMEs can take to improve their cybersecurity?

Establish a Mobile Security Policy

Create a clear mobile security policy that outlines acceptable use, security requirements, and guidelines for personal devices (BYOD). This policy should evolve with changing technologies and threats to remain effective.

Alongside this, define the roles and responsibilities of both staff and your organisation regarding mobile device security. Doing these two things should help employees develop safer security habits and respond quickly and decisively if an incident occurs.

Educate Employees

Conduct regular training sessions to educate employees about mobile security best practices. This can include subjects like recognising phishing attempts, using multi-factor authentication, and the importance of securing sensitive data.

What you prioritise will depend on the knowledge gaps within your organisation but aim for little and often as your approach. Little, because no one learns best by bombardment. Often, so that your people get into the habit of thinking about cybersecurity regularly.

Also, look to foster an environment where employees feel responsible for maintaining security standards and talk regularly about threats.

Use Mobile Device Management (MDM) software

Deploy MDM software to manage, secure, and monitor mobile devices. MDM allows you to remotely manage tasks such as wiping data from lost or stolen devices and enforcing strong password practices.

Review your mobile security measures

Review the mobile security measures you're asking staff to use. Are all devices using **multi-factor authentication** (MFA)? If not, mandate that all staff have it switched on. This adds a vital extra layer of protection against unauthorised access.

Coupled with this, you should also ensure employees use Virtual Private Networks (VPNs) when accessing company resources remotely, especially over public Wi-Fi networks. This encrypts data in transit and protects against eavesdropping.

Regularly update apps and software

Even the most secure software develops vulnerabilities over time. When it does, developers will release updates and **patches** to close any potential loopholes cybercriminals could exploit. So ensure all staff regularly update all software and applications on mobile devices to protect against vulnerabilities. This includes operating systems, apps, and antivirus tools.

Implement data protection strategies

Use encryption for sensitive data stored on mobile devices. This ensures that even if data is accessed without authorisation, it remains unreadable without the decryption key.

On top of this, establish secure data backup procedures, such as the **3-2-1 rule**. Backing up your data regularly can help protect your data from attacks like ransomware, as you'll always have a spare copy even if cybercriminals do manage to breach your defences.

If in doubt, seek guidance from the experts

If you're unsure what to do to improve your mobile security, ask! The National Cybersecurity Centre (NCSC) offers plenty of free resources such as **this guide on BYOD security.**

We also recommend seeking out a managed service provider (MSP) that understands your needs. There are many UK MSPs who cater to small businesses and can help you get a handle on your business's mobile security.

Use a tool to tie everything together

Alongside working with a security provider that understands the needs of small businesses, we also recommend using a mobile security tool designed for SMEs.

CyberSmart Active Protect for mobile safeguards your devices, people, and company data from mobile-specific security threats. Compatible with all major MDM software, our app scans for security misconfigurations, unsafe apps, malicious content and more. And, all while ensuring the privacy of personal messages, locations, and browsing history.

It also includes security policy templates and distribution to help you build a safer security culture. And, when coupled with our Active Protect desktop app it provides security awareness training to help upskill your staff's cyber skills.

To find out more, get in touch, we'd love to show you how it can help your business achieve complete cyber confidence.

CyberSmart