vodafone business

Quarterly Cybersecurity Threat Report

SEPTEMBER 2025

Defending the small to mid-sized business: the rise of AI-driven cyber attacks

Contents

Foreword

At Vodafone Business, we know cyber security can feel overwhelming. That's why we've created the Cybersecurity Threat Report, a regular snapshot of the latest threats, drawn from our global network, **1.5 million users**, and expert partners. It's designed to help you stay informed and take practical steps to protect your business.

In our May research, **49% of small and mid-sized enterprises (SMEs) ranked cyber security in their top five priorities**, yet many don't know where to start.

Think of cyber security like your health, you might not notice a problem until it's too late. That's why establishing proactive, healthy routines , like regular exercise, and getting expert advice are important. You don't need to be a cyber expert; you just need the right tools and support to stay protected.

This edition focuses on **AI**, a game-changer for productivity, but also for cybercriminals. AI is helping attackers move faster and smarter, and the financial impact of cyber crime is expected to rise by nearly **50% in the next three years** because of this[1].

While attackers only need to succeed once, your defences must work every time. Understanding today's threat landscape is the first step to staying secure.

Let's look at what this means for your business.

Andrzej Kawalec

Head of Cyber Security,
Vodafone Business

1. Stylus Media

The AI dilemma

AI is revolutionising how we work, helping businesses save time, cut costs, and deliver better customer experiences. But it's also taking cyber crime to the next level.

Cyber criminals are now using AI to launch faster, smarter, and more convincing attacks. According to the National Cyber Security Centre, AI will almost certainly make elements of cyber intrusion operations more effective and efficient, leading to an increase in frequency and intensity of cyber threats[2]. It's not just the volume that's rising, but the speed as well: hackers can now encrypt multiple devices in less than five minutes[3]. This isn't just a concern for IT teams, more than half of employees say AI is making scams harder to spot[4].

At the same time, many businesses are starting to use AI in their own operations, like automating customer service or analysing data. But 69% of small to mid-sized organisations don't have the right security measures in place to safely deploy these technologies[5].

This means they could accidentally expose sensitive data or create new entry points for attackers.

The scale of AI-powered attacks means no business is too small or too remote to be go unnoticed. If you're online, you're on the radar. For small and mid-sized businesses, the risk is real. You're big enough to be a target but often don't have the same security resources as larger firms.

So, businesses face two big challenges: protecting themselves from AI-powered cyber attacks and making sure their own use of AI is secure.

The good news? You don't need complex solutions. What you need is a simpler, smarter approach to cybersecurity — one that helps you understand the risks and act.

Let's break down the top threats and how to protect your business.

> "It used to make little sense for attackers to go after smaller businesses. They had less valuable data to steal, fewer digital systems to target, and attacks were expensive. Today, the average SME has more data than ever, a digital environment to rival large businesses, and they're cheaper and easier to attack, especially with AI. The economics have changed — and small and medium-sized companies must move fast to keep up."

Andrzej Kawalec

Head of Cybersecurity, Vodafone Business

2. NCSC:For detailed information on the impact of AI on cyber threat, refer to National Cyber Security Centre (NCSC) available under the Open Government Licence (nationalarchives.gov.uk)
3. Microsoft
4. CybSafe
5. WEF

3 Security threats you need to know about

1. Identity hijacking

What is it?

Identity hijacking, commonly carried out through phishing or social engineering, is when a cyber criminal impersonates someone trusted, such as a colleague, supplier, or executive, to trick employees into revealing sensitive information or transferring funds. For example, an attacker might send a convincing email that appears to come from the company's finance director, urgently requesting a payment to a new bank account. If an employee complies, the business could lose thousands of pounds in minutes.

For SMEs, the consequences can be especially damaging; operations may be disrupted while the breach is investigated, sensitive customer or business data could be exposed, and the resulting loss of trust can lead to lost clients and long-term reputational harm. Unlike larger organisations, SMEs often lack the resources to recover quickly, making identity hijacking not just a cybersecurity threat, but a serious business risk.

How is it evolving with AI?

In some attacks cyber criminals are now using AI to clone voices and impersonate trusted figures like your IT team. These fraudulent calls sound real and often ask for sensitive info like login details. In early 2025, voice phishing, known as vishing, accounted for over 60% of phishing attacks seen by Cisco Talos[6]. With AI, scammers can now target businesses at scale, automating calls, gathering personal data, and mimicking tone and speech to deceive employees.

> "Speech-capable large language models (LLMs) have been around for years, but they didn't sound very "human" until now. Suddenly, the voice an employee hears at the end of the phone can sound just like someone they know; a colleague from work, their boss, or even a close friend or family member. It's enabling real-time, fraudulent conversations that sound just like speaking to a real person."
>
> - **Andy Linham,**
> Principal Strategy Manager,
> Vodafone Business

SME employees often juggle multiple roles, leaving little time to scrutinise every email. That makes it easier for these types of attacks to slip through the cracks.

With **94%** of businesses feeling unprepared for these advanced threats, the urgency to act has never been greater[7].

6. Cisco Talos
7. Vodafone

Lookout: Phishing isn't just email anymore

Cyber criminals are getting creative — and more convincing. According to Lookout, phishing now goes far beyond your inbox, with a sharp rise in **vishing** (voice phishing), **smishing** (scam texts that look legit) and **quishing** (fake QR codes that lead to malicious websites) [8].

Take quishing for example: attackers play on people's impulse to scan QR codes and place fake codes in everyday places like train stations or parking meters, tricking people into handing over sensitive information.

Even more worryingly, these tactics are often combined into **hybrid phishing attacks**, and these multi-channel scams are even more successful at bypassing your defences and catching employees off guard.

How to defend against identity hacking

Train your team regularly to spot suspicious messages and impersonation attempts. Ongoing training helps employees stay sharp and confident in identifying red flags before they click.

Set up verification processes, like using code words for sensitive requests as well as multi-factor authentication.

Stay alert to new tactics like deepfakes and multi-channel scams and educate your teams on them.

8. Lookout

2. Malware

What is it?

Malware is **malicious software** designed to steal data or disrupt your systems. It can cause major disruption to day-to-day operations and damage relationships with customers and partners. It often enters through phishing emails, apps, downloads or compromised suppliers, and once inside, it can spread to other businesses in your network.

If your business is infected, attackers could use your systems to target your clients or partners, making you the weak link in the supply chain. This can lead to lost contracts, reputational damage, and even legal trouble if sensitive data is exposed. In today's connected business environment, protecting against malware isn't just about safeguarding your own company, it's about maintaining trust and reliability across the entire supply chain.

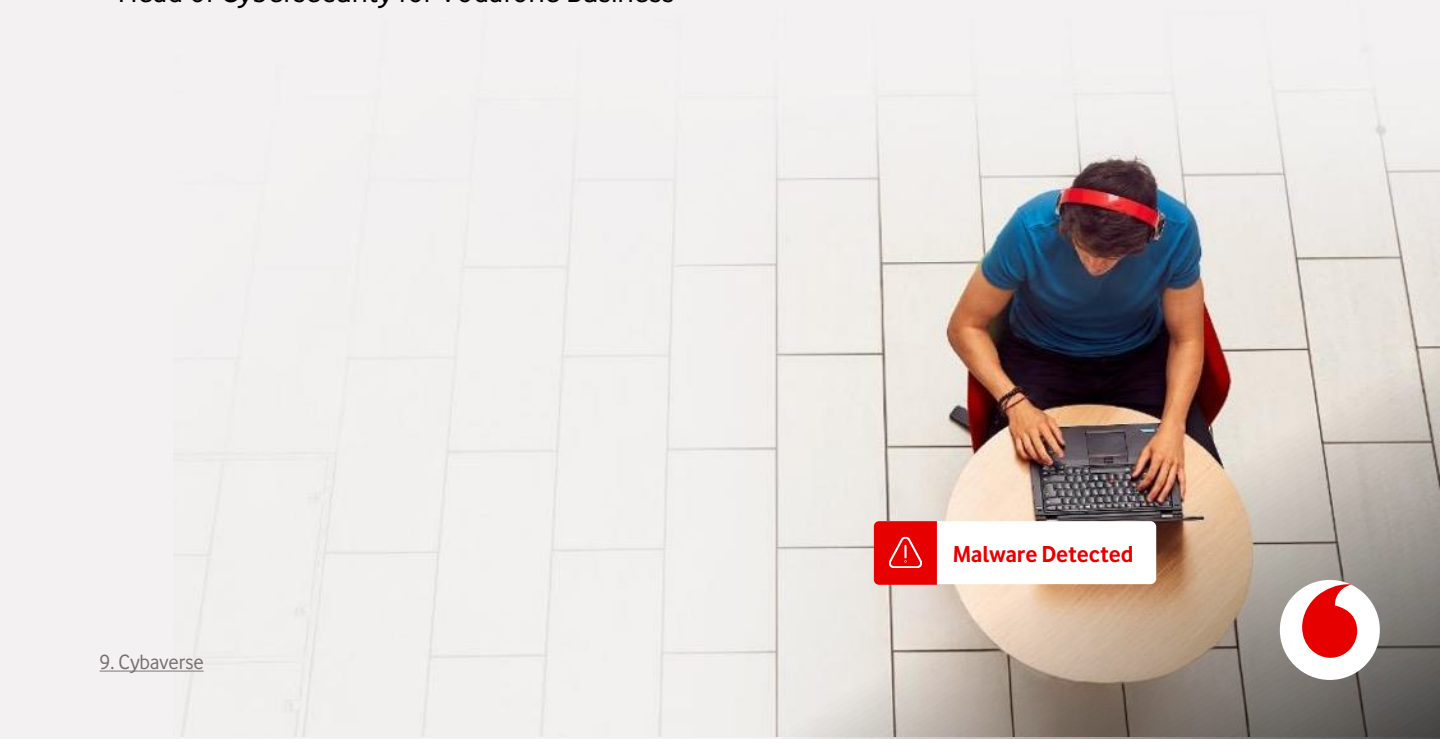
How is it evolving with AI?

Attackers are starting to use AI to make malware smarter. This adaptive malware is beginning to learn, adapt, and change its tactics to avoid detection, making traditional antivirus tools less effective. This emerging threat is gaining attention and is expected to grow .

Businesses with minimal security tools and low visibility and control over their supply chain risks can be more susceptible to malware.

> "Today, malware is targeting a wide range of devices to reach employees. People are using more apps and cloud services than ever before, at work and in their personal lives, and cyber criminals are looking for vulnerabilities across the entire environment."

- **Pedro Peixe Riberio,**
Head of Cybersecurity for Vodafone Business



9. Cybaverse

Hackers are hijacking AI to build better attacks

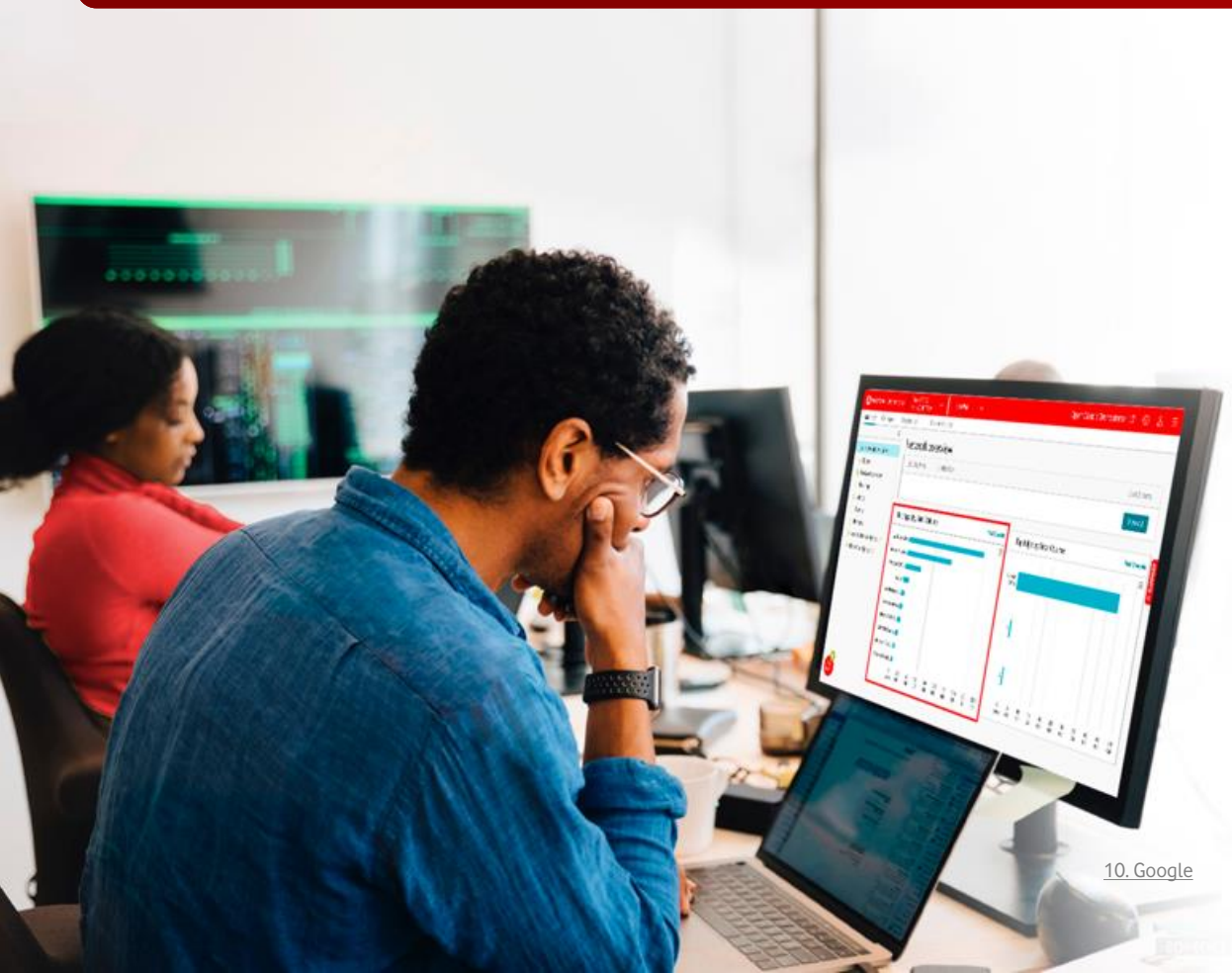
Cyber criminals are now trying to use AI tools to speed up and scale their attacks. They're asking tools to explain how malware works, rewrite harmful code in different languages, and even help them profile potential victims[10].

While tools often have built-in safeguards, some hackers are now selling "jailbroken" versions that strip away those protections, making it easier to create and spread malware.

The malware can be hidden in attachments that look like invoices or meeting invites, and with AI, can easily be translated into multiple languages for more relevance to the victim.

How to defend against adaptive malware

- **Use modern antivirus tools** that detect unusual behaviour, not just known threats.
- **Implement simple policies** like blocking downloads from unverified sites and enforcing software updates. These close off easy entry points for cyber criminals.
- **Assess the partners you work** with using cyber risk scoring tools to spot vulnerabilities in your supply chain that adaptive malware could take advantage of.



10. Google

3. Ransomware

What is it?

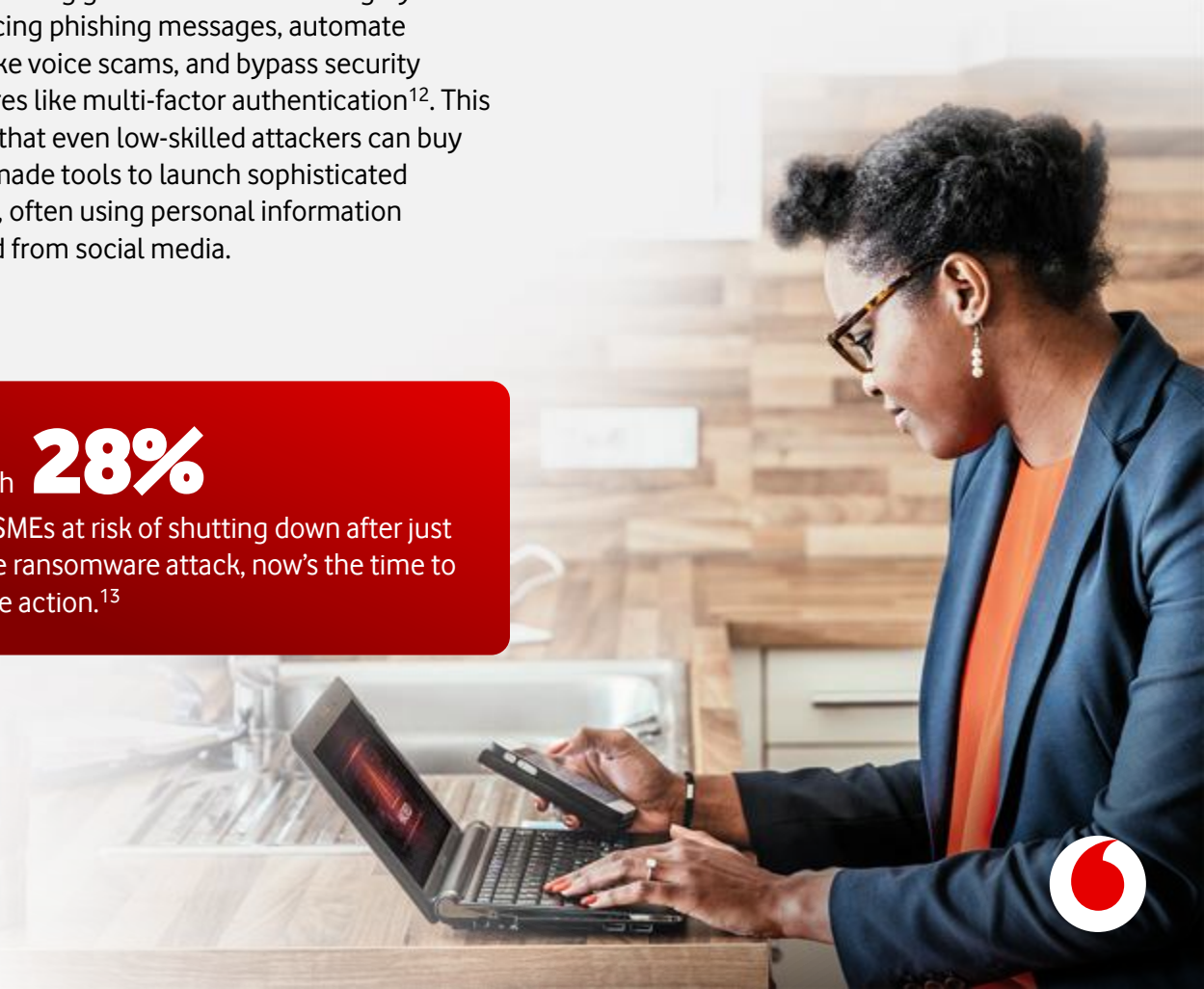
Ransomware is a type of malware that locks you out of your data or systems until you transfer funds to the attacker. And it's not just the very big companies that are the targets. A recent report showed they only accounted for 2.6% of the attacks, it's companies with 11-1000 employees that were most affected, making up 64% of incidents in the last quarter[11]. The real cost of an attack isn't the ransom, it's the downtime, lost productivity, data recovery, legal and regulatory issues and reputational damage that does the most harm.

How is it evolving with AI?

Recent research reveals that AI is transforming how ransomware is created, deployed, and scaled. Ransomware-as-a-service (RaaS) groups are now using generative AI to craft highly convincing phishing messages, automate deepfake voice scams, and bypass security measures like multi-factor authentication[12]. This means that even low-skilled attackers can buy ready-made tools to launch sophisticated attacks, often using personal information scraped from social media.

> "RaaS makes it easier for attackers to coordinate multiple methods to get into a target's network. They spread their bets by calling, texting, and emailing targets with personalised, fraudulent messages. It makes ransomware communications look and sound incredibly authentic, even for people who are well-versed in threat tactics."
>
> - **Andy Linham,**
> Principal Strategy Manager,
> Vodafone Business

With **28%**
of SMEs at risk of shutting down after just one ransomware attack, now's the time to take action.[13]



11. Coveware
12. Zscaler
13. Vodafone

From browsing to breach

Microsoft has reported a sharp rise in ransomware attacks over the past 18 months, and once attackers get in, they can start causing damage within minutes[14]. Cybercriminals are now using AI to build detailed employee profiles and launch highly targeted scams[15]. AI can replicate your writing style, mimic company branding, and even generate fake websites with realistic testimonials, all designed to trick employees into clicking, sharing, or paying.

The risk grows when work devices are used for personal activities like shopping or browsing. These habits can expose employees to malicious links and fake sites, giving attackers more opportunities to strike.

How to defend against Ransomware

- **Use Multi-Factor Authentication** (MFA), it's like adding a second lock to your front door. Even if someone gets a password, they still can't get in without a second form of ID.
- Make sure all **software and systems are up to date**; those updates often fix security gaps hackers love to exploit.
- **Have a back up plan.** If you lose access to your critical systems, make sure you know how to recover them quickly.
- **Train employees on what to do if something goes wrong.** If systems go down or a ransom message appears, they should know exactly who to contact and what steps to take.

14. Microsoft
15. Microsoft

Summary

Cyber threats are real but protecting your business doesn't have to mean a complete security overhaul. Here's how to strengthen your defences with minimal disruption:

1 **Train your team**

Run regular security awareness sessions and phishing simulations. Help staff spot scams and know exactly what to do if something seems off.

2 **Keep things clean and current**

Update software, apps, and antivirus tools regularly. Back up your data to secure cloud and offline storage, and frequently test those backups. Only give employees access to what they truly need and ensure you delete access for anyone leaving your business.

3 **Get expert support**

Partner with a security specialist to set up smart tools that detect threats early, including managed services that monitor your systems 24/7. A partner can also help you build a clear action plan in case of an attack.

Have a look at **our cybersecurity checklist** for more detail on how to implement these recommendations or visit the **Vodafone V-Hub knowledge centre** for free resources and training.

Why Vodafone Business?

We work with some of the world's top technology providers to help businesses tackle today's biggest cybersecurity challenges, including the growing risks from AI-driven threats.

Using global threat intelligence, advanced tools, and expert support, we help businesses of all sizes stay protected. Because we believe every organisation deserves strong, affordable cybersecurity.

That's why we've created our '**Secure Employee**' package, designed specifically for businesses like yours. It focuses on simple, cost-effective ways to protect your people, wherever they're working.

Here's what included

Security assessments
Continuously monitor your systems to spot and fix vulnerabilities in real time.

Security awareness and training
In partnership with CybSafe, we help your team build better security habits through behaviour-based training and real-time support.

Email and cloud protection
With solutions from Trend Micro and Microsoft, you get strong protection across devices, email, cloud apps, and web access.

Mobile threat management
Lookout Mobile Security uses the world's largest AI-driven dataset to protect against mobile threats.

Vodafone Business CyberHub
A free platform for Vodafone Business security customers that helps you manage your cyber resilience and stay ahead of emerging threats.

We also offer

Managed security services
In partnership with Google, Microsoft, Lookout, and Trend Micro, we provide 24/7 monitoring and protection, so you don't have to do it alone.

Network security
With support from Zscaler and Fortinet, we help secure your connections and infrastructure, including firewalls and data protection.

Thank you to our partners

Microsoft · Google · CYBSAFE · Lookout · cisco · zscaler · TREND · FORTINET

For more information and tailored cybersecurity solutions, visit **Vodafone Business**.

vodafone business

vodafone business

Cybersecurity checklist: protect your business from AI-driven cyber threats

Cyber threats are evolving fast, especially with AI in the mix. But protecting your business doesn't have to be complicated. **Here's a simple, actionable checklist to help you stay one step ahead.**

1. Build a cyber-savvy team

Start with free training

SafetyCulture offers a great free course to get your team up to speed.

Test their instincts

Run phishing simulations to see where people slip up and then offer targeted training to boost their confidence.

Need something more advanced?

We partner with CybSafe to deliver tailored cybersecurity awareness programmes. Just ask us.

2. Practice smart cyber hygiene

Keep everything updated

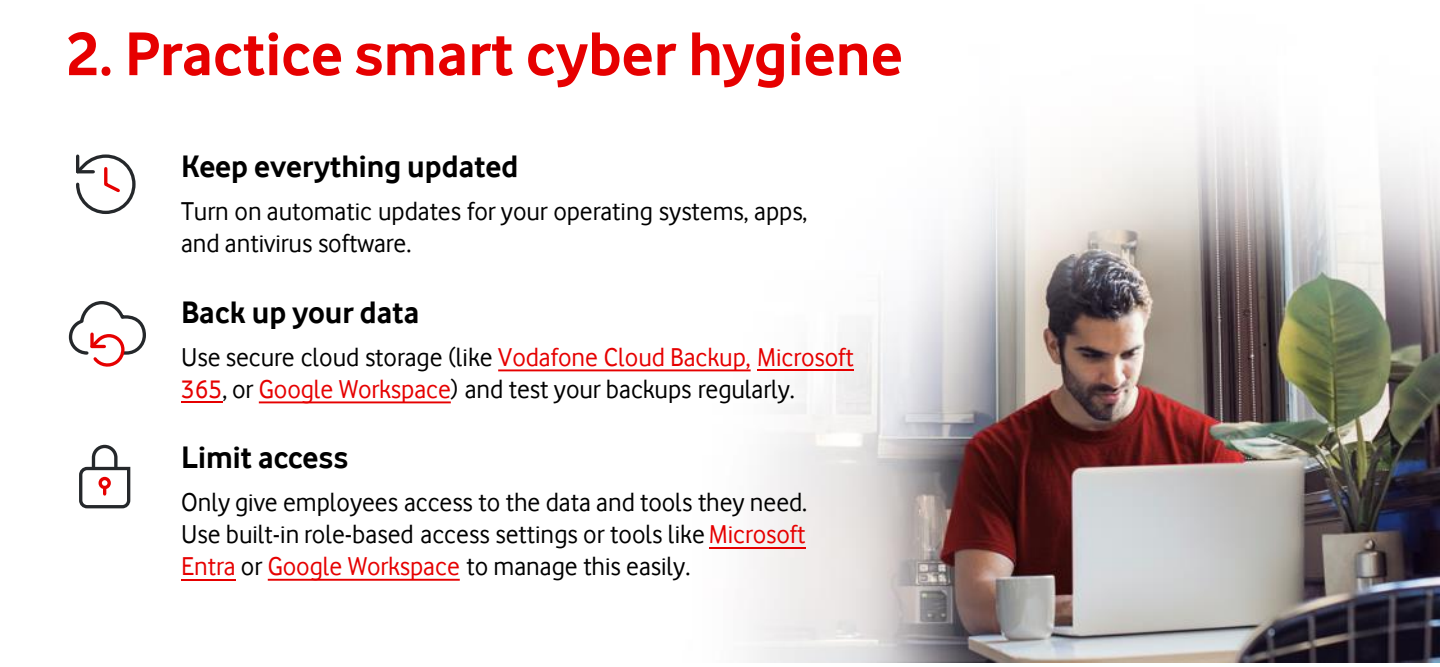
Turn on automatic updates for your operating systems, apps, and antivirus software.

Back up your data

Use secure cloud storage (like Vodafone Cloud Backup, Microsoft 365, or Google Workspace) and test your backups regularly.

Limit access

Only give employees access to the data and tools they need. Use built-in role-based access settings or tools like Microsoft Entra or Google Workspace to manage this easily.



3. Use the right tools

(without breaking the bank)

Choose smart security tools

Look for solutions that detect both known threats and unusual behaviour. Great options for SMEs include:

Trend Micro Worry-Free | Lookout Mobile Security | Microsoft Defender

Consider managed services

Let experts monitor and respond to threats for you. Vodafone Business can help you find the right fit.

4. Know your risks and those of your suppliers

Get a free cyber risk score with every Vodafone Business security solution via our CyberHub platform.

Dig deeper with tools like SecurityScorecard to assess third-party risks and get detailed reports on your own organisation.

5. Be ready to respond

Create a response plan

Include steps like disconnecting affected devices and notifying your team.

Set clear policies

Outline what's expected from employees when it comes to security.

Use free templates

There are plenty of great ones online to help you get started quickly.

Together we can
vodafone business