

Quarterly Cybersecurity Threat Report

APRIL 2026



Defending against mobile
cybersecurity threats



Contents

- 01 Defending against mobile cybersecurity threats
- 03 Foreword
- 04 Mobile phones: the top security risk to businesses today
- 06 Phishing and smishing: multi-channel campaigns
- 11 Malicious apps: mobile malware disguised as trustworthy tools
- 13 Outdated software: an open door for cybercriminals
- 15 Mobile security matters more than ever
- 16 Why Vodafone Business?
- 16 Thank you to our partners



Foreword

Most of us rely on our mobile phones and connectivity without a second thought. They're with us from the moment we wake up, helping us manage work, home life and everything in between. Over time, they've quietly become the hub of our digital lives, holding our identity, finances, passwords, photos, messages and work tools in a single device.

We use them everywhere: on trains, in cafés, on hotel Wi-Fi and constantly on the move. For many people, they're essential to daily life. So when something goes wrong, the disruption is often far greater than we expect.

For businesses, mobiles are no longer just useful gadgets. They're critical to how work gets done. Yet despite their importance, they often perceived as not needing the same level of security attention as other workplace technology.

That's a growing problem. Phones now bring every part of our digital world together. Work emails sit alongside family WhatsApps, while corporate apps share space with banking, shopping and social media.

This blend of personal and professional use means a significant amount of sensitive data now lives in one environment. Add to that how we actually use our phones: on the move, on small screens, switching rapidly between tasks. Attention is lower, and that makes mobiles an increasingly attractive target for cyber criminals. Research shows that mobile devices are now a primary attack surface, with continuous targeting of mobile users¹. They are simultaneously one of our most powerful productivity tools and one of our biggest security risks.

Vodafone supports over 310 million mobile customers across 15 countries worldwide². We understand the importance of protecting not just devices, but the people who rely on them.

In this report, we explore the biggest mobile threats, how to spot them, and what you can do to keep your business protected.

Jenn Didoni,
Cloud, Security & Managed
Services Director,
Vodafone Business



1. [ENISA Threat Landscape report 2025](#)
2. [Vodafone annual report 2025](#)



Mobile phones: the top security risk to businesses today

Across Europe, there are more mobile connections than people, with around 122 to 146 subscriptions for every 100 people³.

Mobile-based attacks now account for more than 42% of all cyber incidents⁴. For businesses, this shift matters. Smartphones and tablets now hold everything from company email and customer contacts to banking apps and sensitive files, making them an appealing entry point for criminals.

The speed at which businesses are switching to mobile platforms in their operations is increasing too. Vodafone is seeing businesses in Europe migrating more sales channels online as well as consumers shifting from cash to digital payments via mobile phones and smartwatches. In fact, these trends have driven a 14% year on year increase in the value of mobile money transactions⁵. This surge in mobile usage presents a significant opportunity for businesses, but it also expands an attractive channel for cybercriminals.



3. [Digital 2026: Global Overview Report — DataReportal — Global Digital Insights](#)
4. [ENISA Threat Landscape report 2025](#)
5. [Vodafone annual report 2025](#)



For years, security strategies focused on PCs, servers, networks and firewalls. But the way we work has changed. Remote working, cloud apps and always-on connectivity mean employees now access business systems from anywhere, often on personal devices outside the corporate network.

Attackers have adapted just as quickly. They target the mobile phone: always connected, always in hand, and typically less protected than laptops, desktops or servers⁶.

Look at how your teams use their phones today: replying to customer emails, messaging

suppliers on WhatsApp, collaborating on Teams or Slack, approving payments, accessing sales or booking tools, sharing documents or running social channels. If this sounds familiar, mobile security isn't optional, it's essential.

For small and mid-sized businesses, where over a quarter still don't provide mobile security training to employees⁷, and security layers are often lighter, the compromise of a single device can rapidly escalate into wider breaches, data loss or financial fraud.

Top Mobile Security Threats in 2026

- 1  **Mobile phishing and smishing**
- 2  **Mobile malware (apps)**
- 3  **Operating system vulnerabilities and spyware**
- 4  **Network attacks (man in the middle and interception)**
- 5  **SIM swap and Identity hijacking**



6. [Lookout Mobile Threat Landscape Report Q2 2025](#)

7. Vodafone Business Research, conducted by Savanta, 2026



1. Phishing and Smishing: multi-channel campaigns



Social engineering is when criminals pretend to be someone you trust to steal sensitive information like passwords, payment details, or access to your business. These scams can come as emails (phishing), texts (smishing), fake websites, or phone calls (vishing) and attackers often use several of these together to make their request seem more believable and trick you into giving away something valuable⁸.

According to ENISA, phishing remains the leading way cyberattacks begin, with **60% of security incidents starting from a single fraudulent message**⁹. Today's attackers reach you wherever you're most likely to see and react quickly. That means on mobile via SMS, WhatsApp (or other chat apps), voicemail and even social media DMs.

In recent Vodafone research, over half of businesses surveyed had seen an increase in phishing attempts and 70% were more worried about mobile security attacks than 12 months ago¹⁰.

The diagram on the next page shows you the steps attackers take to create and implement a typical multi-channel phishing attack.

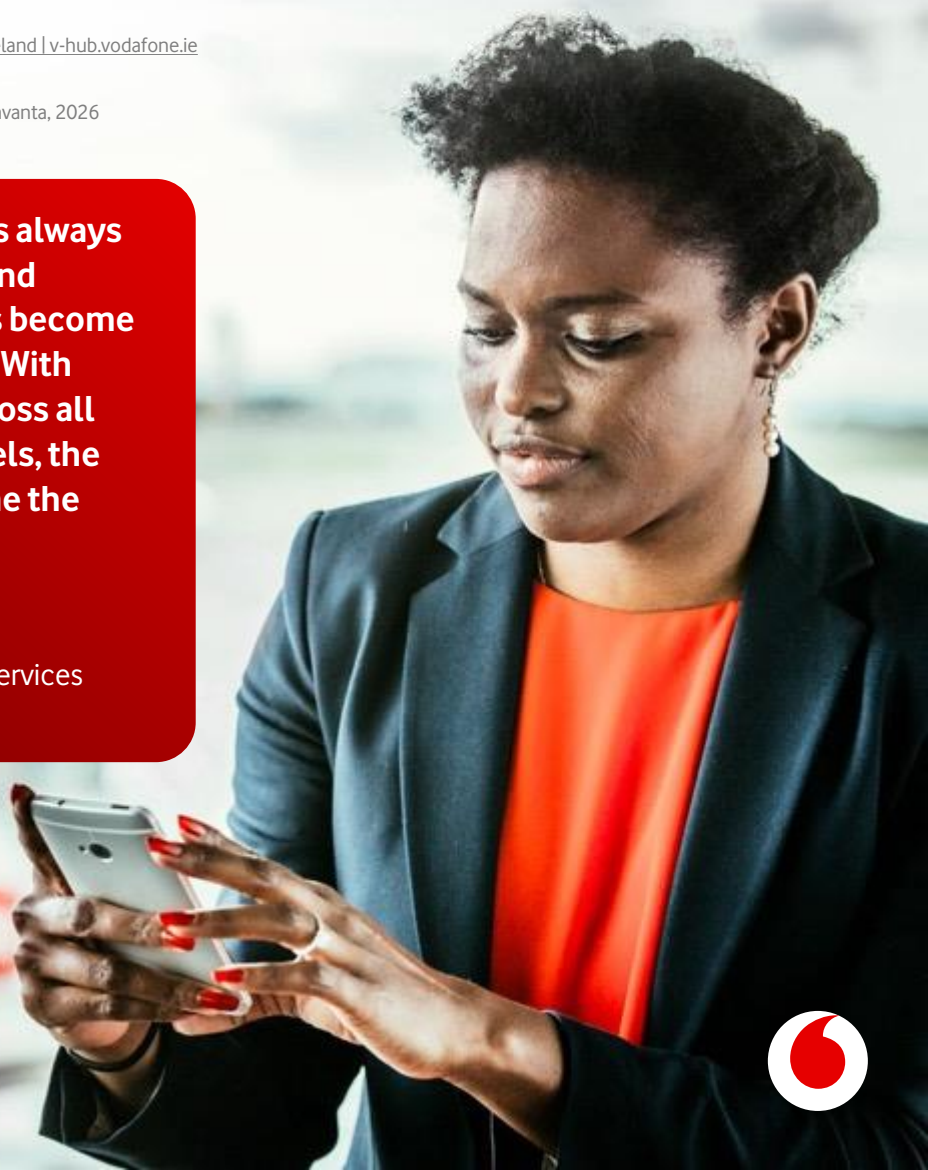
8. What are phishing scams? | V-Hub | Vodafone Ireland | v-hub.vodafone.ie

9. ENISA Threat Landscape report 2025

10. Vodafone Business Research, conducted by Savanta, 2026

“Because your mobile is always on, always connected and always within reach, it’s become the number one target. With phishing expanding across all communication channels, the smartphone has become the central point of risk”

Jenn Didoni,
Cloud, Security & Managed Services
Director, Vodafone Business



ATTACK Flow

2 First contact

Attackers send phishing emails or messages using spoofed identities, urgency, or malicious links/attachments.

Defend through enabling anti-phishing tools and teaching employees to check sender details and URLs.

4 Redirect

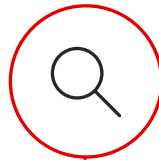
Attackers push victims to fake login pages, bogus payment portals, remote-access tools, or request multi-factor authentication (MFA) codes/passwords.

Defend through using strong password management like MFA, URL filtering, and conditional access controls.

6 Internal spread

Attackers access internal files, escalate privileges, or send internal phishing from compromised accounts.

Defend through applying least-privilege, using anomaly detection, and maintaining strong incident response processes.



1 Research

Attackers scan public info (LinkedIn roles, email formats, suppliers, recent announcements) to craft convincing messages.

Defend through reducing oversharing; train staff to spot social engineering clues.

3 Secondary contact

Attackers reinforce the scam through phone calls to appear legitimate.

Defend through verifying unexpected requests using known, trusted contact details, not the ones provided.

5 Extract/deploy

Attackers steal credentials, bypass MFA, install malware, or trigger fraudulent transactions.

Defend through monitoring for unusual logins and risky sign-in patterns.

7 Final objective

Attackers commit fraud, steal data, deploy ransomware, or exploit business email compromise.

Defend through multi-layered security and ongoing staff awareness.



Why mobile phishing works

Phishing messages on mobile are designed to catch you off guard. They often look like something you trust, such as a text from your bank, a delivery update or even a voicemail from your IT team, urging you to “verify your account” or “confirm a security code”. And on a small phone screen, with notifications arriving all day, it is easy to glance, tap and move on. But that single tap could give attackers access to your accounts or allow malware onto your device.

Criminals have established vast networks of people and technology to drive their mobile phishing campaigns. From dedicated ‘scam centres’ with hundreds of employees, to ‘SIM farms’ with several hundred thousand SIMs sending and receiving messages, the scale and sophistication of the scam ecosystem is growing every day.

Criminals are also getting more creative. Some are using equipment, known as SMS blasters, that mimics mobile towers to send mass SMS

messages to any phone in the area¹¹. SMS blasters are highly portable and can be stored in the back of a car, or even on a motorbike, allowing the fraudsters to drive around busy urban areas and reach many thousands of potential victims. You do not need to have shared your number for a blaster to find you. They simply broadcast the scam to every device in range, hoping someone will react before thinking.

Mobile phishing can be anything from a simple scam message sent to thousands of phones, right through to a highly targeted attack which is researched and personalised for an individual or an organisation. When you layer in the use of AI-driven ‘deep fake’ technology, along with tools which allow scammers to modify the calling number appearing on your phone, the level of threat has never been higher. It is therefore essential to stay alert to unexpected messages and calls, even if they appear to come from a trusted source.

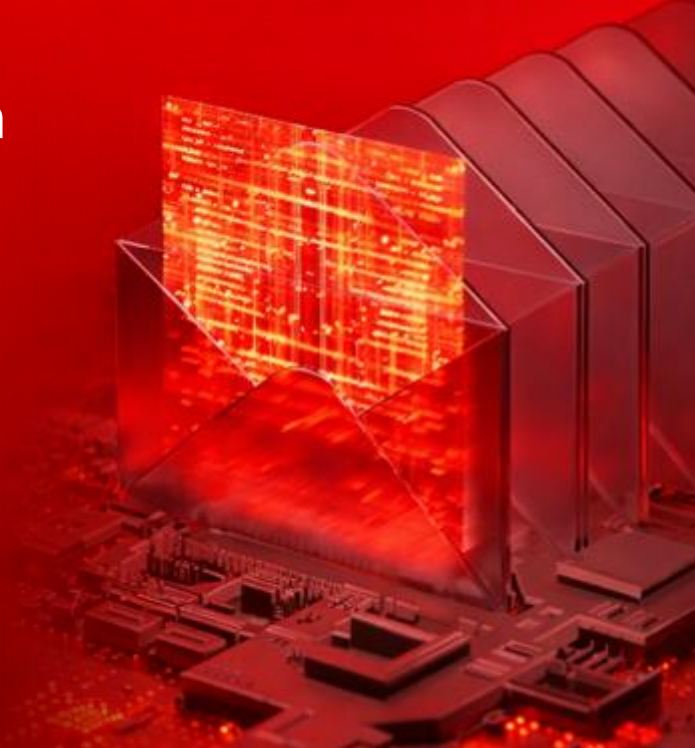
“Scams have reached a vast, unprecedented scale, and many of them start with a call or message received on a mobile phone. SMEs are a popular target, but by remaining vigilant and taking the time to validate any new requests, you can protect your business and keep the scammers at bay”

Morgan Ramsey,
Senior Manager, Global Fraud, Vodafone.



The scale of the problem is growing

Microsoft Security is seeing phishing and identity-based attacks rise fast, with a jump of around 30% over a three-month period¹² and security experts at mobile security firm, Lookout, report a 20% increase, over three months, in enterprise mobile phishing encounters, underlining a clear shift: attackers are aiming their scams directly at our phones¹³.



People over technology

Businesses are especially vulnerable to these scams because people are at the heart of how organisations run. Recent Vodafone research saw 41% of organisations allowing full unrestricted access to company resources on personal devices with no robust security measure or tools in place¹⁴. This is where an employee's judgment often becomes both the first and last line of defence against phishing. Attackers know this and take full advantage.

There is also a confidence gap at play. In a Vodafone survey of small businesses with 78% of leaders believing their staff could spot a sophisticated phishing attempt, yet when tested, nearly two thirds of employees missed a genuine phishing message¹⁵.

In other words, many people feel sure they would not fall for a scam until a convincing one appears on their device.

That overconfidence is exactly what cybercriminals rely on. One timely, believable message, seen briefly on a lock screen, is often all it takes. Once someone taps a malicious link and enters their details on a fake login page, attackers can steal passwords, take over accounts and even gain access to wider business systems. A single text can quickly snowball into something far more serious, such as a data breach, financial fraud or a ransomware attack.

¹². [Microsoft Digital Defence Report 2025](#)

¹³. [Lookout Mobile Threat Landscape Q2 2025](#)

¹⁴. Vodafone Business Research, conducted by Savanta, 2026

¹⁵. [Vodafone: Proactive Security – Phishing of the Future](#)



What can you do about it?

A combination of awareness and a few protective technologies can dramatically cut mobile phishing risk:



Make phishing awareness part of everyday work: short, practical reminders work far better than long, one off training sessions. Show your teams real examples of phishing emails and texts, and call out the tell-tale signs such as urgency, unknown senders, strange links or unexpected requests for passwords or payments. Running the occasional safe phishing test can help keep everyone alert. Check out our phishing awareness poster at the end of this report.



Build a culture of pause and check: encourage everyone to verify before they act. Any unexpected request for money, login details or sensitive information, whether it comes through text, WhatsApp or email, should be checked using a second trusted method. A quick call to a colleague or supplier using a known number can stop a scam in its tracks.



Switch on the protections you already have and strengthen them: make sure email spam and phishing filters are on and regularly updated. Consider adding specialist mobile security software such as Lookout Security, Microsoft Defender or Trend Micro Mobile solutions. Most importantly, turn on multi factor authentication (MFA) for all key systems including email, banking and cloud apps. This simple two step check can stop almost all automated attacks¹⁶, and it gives you an extra layer of protection even if a password is compromised.



Know what to do when something goes wrong: even with good habits, mistakes can happen. What matters is acting quickly. Make it clear who staff should contact if they click a suspicious link or share information by accident and reassure them that they will not be blamed for speaking up. A simple plan that covers who to alert, how to secure accounts and how to reset passwords can prevent a small slip from turning into a major incident.

¹⁶. Microsoft: [One simple action you can take to prevent 99.9 percent of attacks on your accounts](#)



2. Malicious apps: mobile malware disguised as trustworthy tools

Mobile malware is simply malicious software designed to target smartphones and tablets. It often arrives through an app that looks completely genuine, whether it is a game, a utility, or something claiming to help with work. Behind the scenes, that app may have been tampered with or created solely to hide malware. Once it is installed, the malware can quietly get to work, stealing sensitive information like contacts and saved passwords, tracking locations, listening in on activity or even giving an attacker remote access to the device.

Malware, however, does not only come from apps. It can also slip in through a suspect email attachment or a website that triggers an automatic download on your phone.

To give a sense of scale, around one in twelve cyber incidents can be traced back to a compromised mobile app, often one that was installed from outside an official app store or cleverly disguised to appear safe¹⁷.

It's common for employees to use their personal phones for work and/or freely install apps on company-provided mobiles, if no technical controls are in place. Bring-your-own-device (BYOD) is convenient and often necessary and downloading the latest app to make work easier is common. But this flexibility also opens the door to cyber risk.

The “ChatGPT” app trap

In early 2025, cybercriminals took advantage of the buzz around AI tools to spread malware to businesses in Europe. They circulated a fake app called “ChatGPT” (posing as an official mobile client for the popular AI chatbot). Many employees, eager to try new productivity tools, downloaded it without suspecting any danger. Unfortunately, once the app was installed, it secretly implanted a backdoor on the device, giving attackers full access. This campaign hit dozens of small businesses; over 50% of known victims were in Austria, Germany and Portugal¹⁸.

This reinforces why teams should always pause before downloading apps, stick to official app stores and treat any “latest tool” with a healthy degree of caution.

17. ENISA Threat Landscape Report 2025

18. Small business security warning - new malware is spoofing tools such as ChatGPT, Microsoft Office and Google Drive, so be on your guard | TechRadar



Even trusted stores can slip up

Even trusted app stores have, on occasion, seen malicious apps slip through their review processes. In one recent case, security researchers uncovered hundreds of harmful apps that had been downloaded tens of millions of times before they were detected and removed. These apps posed as legitimate tools such as photo editors and games. This highlights that while using reputable app stores significantly reduces risk compared to sideloading apps from unknown sources, no platform is completely immune and determined attackers may still find ways to bypass security checks.

What can you do about it?

Strengthen app habits and device security to keep malicious apps and malware out of your business:



Keep devices and apps up to date: updates matter more than most people realise. Both app updates and operating system updates fix security gaps that attackers rely on. Set devices to update automatically where possible and encourage your team to install updates as soon as they appear. Delaying them leaves the door open for malware.



Stick to trusted app stores: keep things simple. Encourage staff to install apps only from official stores like Google Play or Apple's App Store. Avoid downloading apps from links, pop ups, forums or unofficial stores, as these are some of the most common ways malware spreads.



Manage devices wherever you can: if your business has even basic IT support, mobile management tools can make a real difference. Mobile Device Management, or MDM, lets you control which apps can be installed, set essential security features like PINs and encryption, and push updates remotely. Vodafone Secure Device Manager is a great place to start.



Pay attention to app permissions: if an app asks for access it does not need, take it as a warning sign. A torch or calculator has no reason to access your contacts or microphone. Help staff get into the habit of questioning unusual permission requests and avoiding apps that ask for too much. On managed devices, consider limiting high risk permissions such as Accessibility access, which is often abused by malicious apps.



Add extra protection on mobile: a reputable mobile security or antivirus app, like Lookout Mobile Endpoint Security, Microsoft Defender for Endpoint or Trend Micro Mobile solutions, can add another strong layer of defence by detecting known threats and warning users about dangerous sites.





3. Outdated software: an open door for cybercriminals

Mobile operating systems like Android and iOS, along with the apps we use every day, are just software. And like any software, they can contain bugs or security gaps that criminals are quick to exploit. When one of these weaknesses is discovered, companies such as Google or Apple will usually release an update to fix it. But if devices are not updated in good time, those known gaps stay wide open for attackers.

The challenge is that many mobile devices in use today are running older software and missing important security patches. Research shows that more than 30 percent of Android phones are estimated to be running on versions of the operating system that no longer receive security updates¹⁹.

Lookout's data highlights why this matters. They have seen a sharp rise in attacks on devices that are not fully updated, including a significant jump for both Android and iOS year on year²⁰. On top of missing updates, common weak spots in business devices include not setting a device lock, leaving encryption switched off or falling behind on basic security settings²¹. Something as simple as an employee not using a passcode, or running an OS version from two years ago, can turn their phone into an easy target.

From research by ENISA, 21% of security incidents involve exploiting a software vulnerability where attackers use a known flaw in software to break in²². Many mobile malware incidents and breaches succeed because attackers take advantage of misconfigurations and unpatched software, exploiting weaknesses that should already have been fixed. It is a reminder that keeping phones updated and correctly set up is one of the simplest and most effective ways to stay protected.

¹⁹. Digital Information World

²⁰. Vodafone/Lookout Quarterly reporting 2024/25

²¹. Vodafone/Lookout Quarterly reporting 2024/25

²². ENISA 2025 Threat Landscape Report



What 2025 taught us about unpatched devices

On iPhones, Apple had to rush out an emergency update for a zero click exploit. Attackers could send a malicious iMessage that installed spyware without the user doing anything at all. The message did not even need to be opened. Although this type of attack is usually seen in high level espionage, it showed how simply receiving a message could infect an iPhone that was not up to date. The patch closed the gap, but only for people who installed it²³.

“Most organisations tightly manage laptops, but mobile devices remain a weak spot. Without a central way to enforce updates security is left to chance, and attackers know exactly where to look.”

Pedro Peixe Ribeiro,
Head of Cyber Security Vodafone Business



What can you do about it?

Keeping software up to date is one of the simplest and most cost effective ways to stay secure. Here is how to stay on top of it:

- 1 Phase out outdated devices:** phones and tablets that no longer receive updates are a genuine risk. Plan to replace them, especially if they handle customer information, payments or access business systems. If you cannot replace them straight away, limit what those older devices can do so they do not become an easy entry point for attackers.
- 2 Switch on automatic updates:** this is the quickest win. Make sure every work phone and tablet is set to update apps and the operating system automatically. Most updates install overnight with little to no disruption, and it removes the need for staff to remember to do it themselves. A short reboot is a small step that keeps devices protected.
- 3 Set a clear, simple update rule:** keep the message easy to follow. If a device is used for work, it must stay up to date. Encourage employees to install updates as soon as they are prompted or to leave their device plugged in overnight so updates can run. A quick monthly “update check in” can help everyone build the habit.
- 4 Use tools to keep track where possible:** if you already use mobile management tools or mobile security apps, take advantage of their built-in monitoring. Many will flag devices that are missing updates or running old software, and some can even restrict access to business systems until updates are applied.
- 5 Act quickly when urgent patches appear:** when a major security flaw hits the news or a vendor releases an emergency update, move fast. Let your team know quickly, clearly and directly to update their devices.

23. Apple Zero-Click Flaw in Messages Exploited to Spy on Journalists Using Paragon Spyware



Mobile security matters more than ever

For each of the key risks outlined in this report, there are proactive ways to protect against them. Even with limited IT resources, businesses of all sizes can take practical, manageable steps right away to strengthen their security. By helping employees spot and avoid phishing, by being strict about where apps come from and what they can access, and by keeping devices up to date, businesses can significantly boost their mobile protection. None of this requires big budgets, just a focus on the basics and sometimes additional help from a specialist partner.

Concentrating on these three areas is a smart and realistic place to start. Think of them as the three points in your mobile security chain that need the most reinforcement: people and their choices (phishing), the apps they install (malware), and the software running on their devices (updates).

At Vodafone Business, we are optimistic. The risks are real, but the solutions are accessible to every business. With the right awareness and simple, proactive steps, you can enjoy all the productivity and flexibility that mobile technology brings without unnecessary worry. It is about acting early, not reacting after something has gone wrong.

With vigilance, good day to day practices and the support of partners like Vodafone, businesses can build strong mobile security and embrace the benefits of a mobile first workplace with confidence.

“At Vodafone we continue to raise security standards by independently testing our networks and working with industry partners to strengthen resilience. But while we build security into the network, the rising frequency of non-technical attacks means users also play a vital role in staying secure”

- Pedro Peixe Ribeiro, Head of Cyber Security Vodafone Business



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



For more information and tailored cybersecurity solutions, visit [Vodafone Business](#).

This newsletter is for informational purposes only and reflects the threat landscape as of Q1 2026. Recommendations are based on publicly available data and best practice guidelines but may not be suitable for all organisations. Vodafone Business accepts no liability for actions taken based on this information. For tailored cybersecurity advice, organisations should consult with cybersecurity professionals.



How you stay safe



- Verify using official channels
- Never share passwords of MFA codes
- Pause-urgency is a red flag
- Report anything suspicious to IT/security

Email



Urgent action!

→ **Reset password** ←

Red flags

- Unknown sender
- Old Links
- Urgent tone

SMS



Your package is delayed

→ **Click to verify** ←

Red flags

- Unknown number
- Shortened URLs
- Urgent language

Phone call



I'm here IT

→ **Share your code** ←

Red flags

- Pressure
- Requests info
- Unknown caller

Social media



Is this you in the photo?

→ **Click to see!** ←

Red flags

- Fake profiles
- Unexpected DMs
- Odd-looking links

