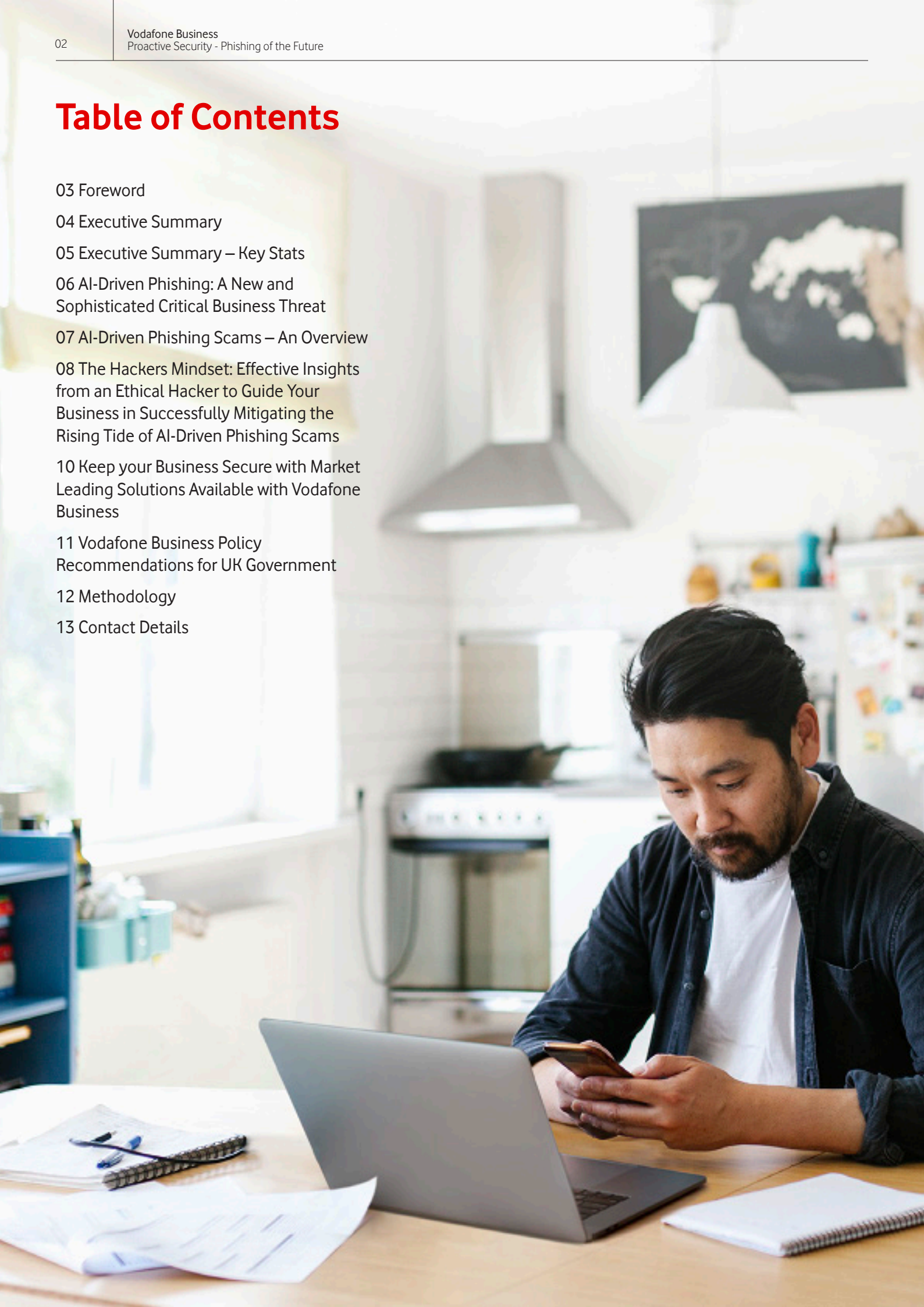
# Proactive Security - Phishing of the Future

Artificial intelligence is helping cyber criminals create phishing scams that are more sophisticated than ever. Here's how your business can stop them in their tracks!

vodafone business

# Table of Contents





# Foreword

Welcome to the **Vodafone Proactive Security - Phishing of the Future Report**, a brand-new cybersecurity report designed to drive awareness of the rising threat of artificial intelligence (AI)-driven phishing scams and the strategies businesses can employ to detect and mitigate them.

At Vodafone Business, we want to empower businesses to stay ahead of these emerging threats and safeguard the trust of their customers, partners and employees.

In today's interconnected world, the sophistication and speed of cyber threats are growing at an extraordinary rate. With close to two decades of experience in this field, I have witnessed an evolution in the tactics used by cybercriminals that demands constant vigilance as well as a willingness to adapt.

One of the most pressing threats on the horizon is the use of AI to create increasingly sophisticated phishing attacks. These AI-driven scams are designed to bypass traditional security measures and prey on the trust we have in our communications, making them a formidable challenge for businesses everywhere.

AI-driven phishing represents a seismic shift in the cyber threat landscape. Criminals can now craft hyper-personalised attacks, mimicking voices, individuals, emails, and even messages, with alarming accuracy. These capabilities are empowering malicious actors to deceive not just individuals, but entire organisations, with AI being used to study and exploit vulnerabilities at exceptional levels.

As a result, businesses must act now, resilient cybersecurity is no longer just about protecting networks—it's about building a culture of security that anticipates these sophisticated threats and embeds cybersecurity into every aspect of the organisation.

To drive awareness of this emerging threat, Vodafone Business has launched a new campaign, 'Proactive Security – Phishing of the Future'. As part of this campaign, and to gain a clearer understanding on just how effective AI is at helping cybercriminals to breach businesses, we have partnered with renowned ethical hacker Katie Paxton-Fear.

Katie was challenged to 'hack' entrepreneur Chris Donnelly's business using AI-driven phishing methods – and the results were fascinating. Head over to the @VodafoneBusinessUK YouTube channel to see for yourselves how the exchange played out.

Having supported UK businesses with their cybersecurity needs for more than three decades, we believe that preparing for this next generation of cyber threats requires more than just advanced technologies. Businesses also need to consider the education and awareness of every individual within the organisation.

Beyond the wider findings of the report, we learned that 94% of businesses in the UK did not feel adequately prepared to manage more sophisticated AI-driven phishing scams. This highlights an opportunity to equip them with the right solutions to keep their sensitive and commercial data protected, and avoid falling foul of regulatory responsibilities.

Thank you for joining us on this critical journey toward a more secure digital future for all. I hope this report will not only inform, but inspire, proactive action in the face of evolving cyber risks. Together, we can turn this challenge into an opportunity, by strengthening our collective defences and protecting what matters most – keeping our businesses – the foundation of our economy – safe and secure.

By Steve Knibbs, Head of Vodafone Business Security Enhanced (VBSE), Vodafone Business UK

# Executive Summary

This new 'Proactive Security – Phishing of the Future' report explores the evolving landscape of AI-driven phishing attacks and the critical vulnerabilities they present to organisations today.

To help build it, we spoke to a combined 3,000 UK business leaders and employees in organisations operating across the length and breadth of Britain, spanning all sizes and sectors. In doing so, we wanted to find out how aware they were of the rising threat of sophisticated AI-driven phishing scams, and whether their business was suitably prepared to mitigate them.

By leveraging AI, cybercriminals are now crafting highly sophisticated and personalised phishing campaigns that bypass traditional security defences, posing significant risks to businesses of all sizes.

Vodafone Business research underscores the scale of the challenge: over the past two years, more than half (55%) of business leaders, alongside 45% of employees, reported being targeted by a phishing scam. The data also reveals a concerning gap in detection skills. While the majority of UK business leaders expressed confidence that their teams could spot and mitigate phishing attacks, two-thirds of employees failed to do so. This gap highlights the need for comprehensive training and advanced cybersecurity measures to address threats effectively.

The study also highlighted an 'age gap' in awareness, with younger staff aged 18 to 24 appearing more likely to fall for AI-driven phishing scams than their older peers. Gen Z staff were more likely than most to fall victim, with nearly half (47%) having not updated their password for more than a year, and two in 10 (19%) having never changed it at all.

This report provides key insights and actionable recommendations to help businesses strengthen their defences against AI-driven phishing threats. We've even partnered with a renowned ethical hacker to divulge secrets from a cybercriminal's perspective.

From investing in intelligent detection tools to embedding cybersecurity awareness across all levels of an organisation, the strategies outlined here are designed to empower businesses to counteract the heightened risks AI presents in the phishing landscape. By proactively addressing these vulnerabilities, companies can protect their people, data and operations from this emerging threat.

# Executive Summary - Key Stats

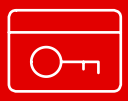
Updating cybersecurity protocols regularly is essential for businesses to protect sensitive data, comply with the UK's stringent data protection laws, such as the Data Protection Act and GDPR, and safeguard business continuity. As cyber threats grow, staying secure helps avoid data breaches, costly fines, and operational disruptions, ultimately protecting business reputation and resilience.

Key insights from the Vodafone Business Proactive Security – Phishing of the Future study includes:

94% of businesses did not feel adequately prepared to manage the rising threat of AI-driven phishing scams.

Despite four-fifths (78%) of workers agreeing they could confidently spot a phishing attempt, only a third were able to correctly distinguish a scam video or email from the real thing.

A third of UK businesses have provided no cybersecurity training for their staff in the last two years.



Junior staff leave themselves the most exposed to hackers, with nearly two-thirds (62%) having social media profiles that are open to the public, compared to two-fifths (40%) of Brits.

More than half of UK businesses have no response plan in place to deal with an advanced AI-driven phishing attack. Meanwhile, a third had provided no cybersecurity training for staff across the last 12 to 24 months.

Two-fifths (40%) of employees were confident they could recognise a voice call phishing scam, while two-thirds (63%) said they would spot a text message scam.

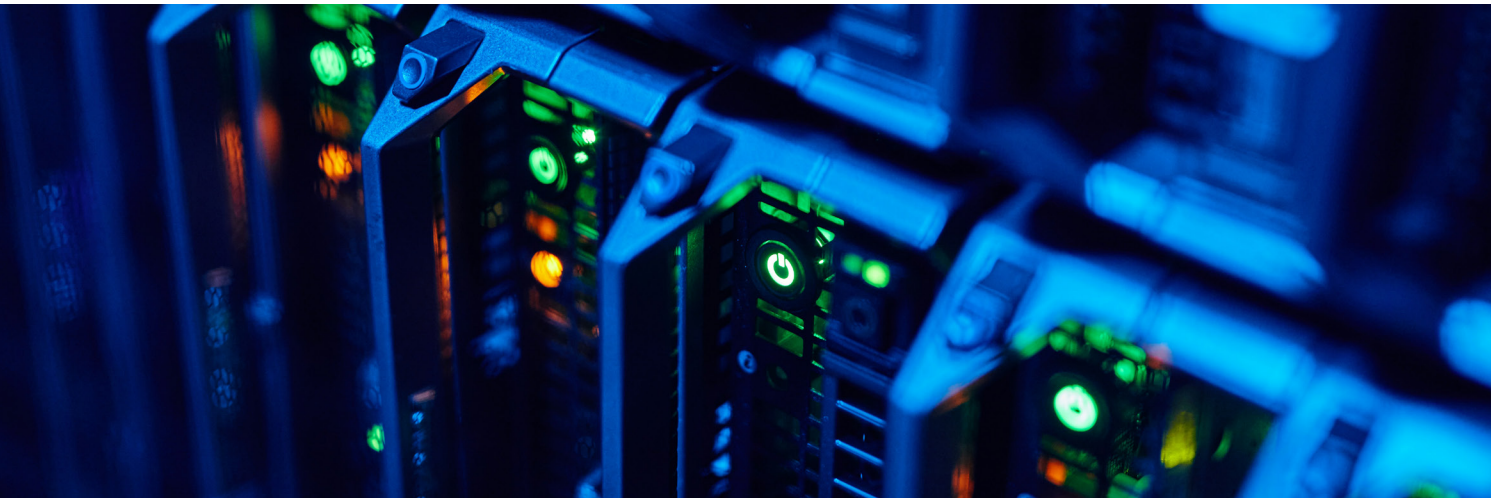
Only 36% of organisations use phishing simulations or similar tests to measure employees' ability to recognise cyber-threats.

Upon receiving a suspicious email, a third (36%) of young employees would either forward it to a colleague to verify or 11% would simply ignore it.

Only 42% of businesses are using automated systems to monitor and respond to human-error incidents, such as phishing, improper data handling or security misconfigurations.

More than two-thirds (67%) of young workers say the cybersecurity training they have received is not adequately tailored to the needs of their role.

# AI-Driven Phishing: A New and Sophisticated Critical Business Threat



The rise of AI-driven phishing scams is posing an increasingly significant threat to businesses across the UK, as cybercriminals leverage artificial intelligence (AI) tools to create more sophisticated, convincing, and targeted attacks.

Traditional phishing tactics often rely on poorly written, easily recognisable emails; however, AI is now enabling scammers to generate highly personalised messages that mimic legitimate correspondences, making them harder to detect. This advancement in phishing sophistication challenges even the most vigilant employees, putting businesses at greater risk as a result.

One major factor in this escalation is generative AI's ability to scrape vast amounts of public data. This can help create highly customised messages that often reflect individual roles, interests, and even specific projects. Scammers can now target executives, employees and business partners with contextually relevant content, creating a false sense of legitimacy.

These AI-generated messages can appear to come from trusted sources, such as colleagues or company leadership, making them more likely to deceive recipients into divulging sensitive information or clicking on malicious links.

Additionally, AI-driven voice and video phishing, or "vishing", is on the rise. Scammers are increasingly using AI to clone voices and mimic video calls, adding a layer of authenticity to their attacks. This introduces another dimension to the threat, as people are often more trusting of verbal or visual communications compared to emails. Such tactics can pressure employees into bypassing standard security protocols, especially in high-stakes or urgent scenarios, increasing the likelihood of a breach.

**94%** **of UK businesses did not feel adequately prepared to manage the rising threat of AI-driven phishing attacks.**

Regarding business preparation and confidence, Vodafone Business found that 94% of UK businesses did not feel adequately prepared to manage the rising threat of AI-driven phishing attacks. In addition, 78% of business leaders were 'confident' that their employees could successfully identify a sophisticated AI-driven phishing attack. In reality, however, two-thirds fail to do so.

To counter these threats, businesses should invest in advanced cybersecurity training and AI-driven detection tools that can recognise patterns in phishing attempts. Educating employees on recognising AI-driven phishing tactics is also key, as is maintaining strict protocols around information sharing. As cybercriminals continue to evolve their methods, businesses must be proactive. The first step is recognising that traditional defence measures may no longer suffice against the growing sophistication of AI-driven scams.

To find out more about the range of market-leading cybersecurity solutions available from Vodafone Business, visit:
**www.vodafone.co.uk/business/cyber-security-solutions**

# AI-Driven Phishing Scams – An Overview

Each of the following AI-driven phishing types leverage AI to increase the believability and impact of attacks, highlighting the need for heightened awareness and verification practices.

**Spear Phishing and Deepfakes:** AI allows attackers to create highly personalised spear phishing emails, targeting specific individuals by using data from social media and other public sources. Deepfake technology can generate realistic audio or video of trusted contacts, such as executives, to add credibility and urgency to fraudulent requests.

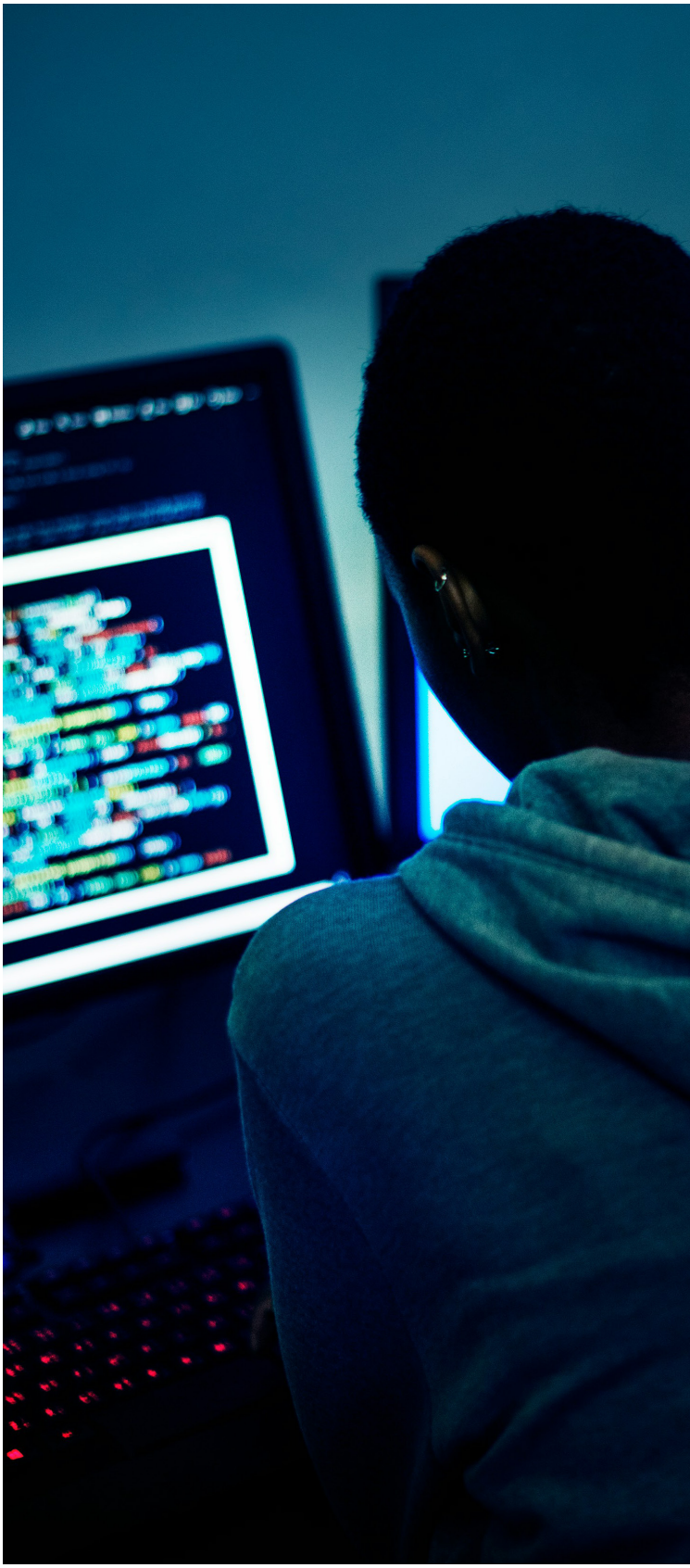
**Chatbot Phishing:** Attackers can create malicious chatbots that mimic legitimate customer service or support tools. These AI-driven bots engage users in realistic conversations, tricking them into sharing sensitive information or clicking on malicious links.

**Natural Language Processing (NLP) Phishing:** AI models trained in natural language processing can craft phishing messages that sound authentic and are difficult to distinguish from legitimate communications. By generating grammatically correct and contextually appropriate messages, these scams avoid the typical errors that often give phishing attempts away.

**Business Email Compromise (BEC) with AI:** Using AI to analyse a company's communication style, attackers can craft emails that closely mimic the tone and content of high-ranking employees. These messages often request financial transfers or sensitive information, relying on AI-driven accuracy to avoid detection.

**Social Media Phishing and Social Engineering:** AI tools can scrape social media for details about a user's life and relationship, which can then be used to craft personalised phishing messages. These messages often exploit personal or emotional triggers, increasing the likelihood of a response.

**Phishing Kits with AI Automation:** Some attackers use AI-driven phishing kits that automate the creation of phishing emails and landing pages tailored to various industries or demographics. These kits enable rapid deployment of highly effective campaigns with minimal effort from attackers.



# The Hacker's Mindset: Effective Strategies to Help Your Business Mitigate AI-Driven Phishing Scams

**By Katie Paxton-Fear**,
Ethical Hacker and Lecturer,
Cyber Security, Manchester
Metropolitan University

As an ethical hacker, basically a cybersecurity expert who tests systems for vulnerabilities to help organisations improve their security, with permission and in a legal, constructive way, I was delighted when Vodafone Business approached me with a challenge: attempt to hack the business of a renowned entrepreneur to demonstrate just how far cybersecurity phishing has evolved thanks to artificial intelligence.

What came next saw me sitting in the London office of Chris Donnelly, co-founder of Lottie, a health-tech platform for care homes. Here, I put together an AI phishing strategy in an attempt to persuade one of his employees to send business funds to a fictious company at the supposed behest of Chris himself. I can reveal that a combination of public facing data, social media and a cloned sample of Chris' own voice was used to set up the scam. However, you'll need to head across to the @VodafoneBusinessUK YouTube channel to find out whether I was successful or not.

As someone who has navigated both sides of the cybersecurity fence – carrying out bug bounties - a program where organisations reward individuals for finding and reporting security vulnerabilities in their systems or software - as well as educating the next wave of digital security experts at Manchester Metropolitan University – I staunchly believe businesses today need to approach AI-driven phishing with a hacker's mindset. That means always thinking one step ahead, and building defences that evolve alongside the threats.

By combining advanced detection systems, smarter training, rigorous testing and real-time incident responses, organisations can remain resilient in the face of increasingly sophisticated cyber threats. AI may have raised the stakes but, with the right approach, businesses can use this same technology to protect their people and data, turning the tables on attackers.

So, which cybersecurity defence strategies should your business consider when combatting advanced AI-driven phishing attacks?

The first step is to **use AI in return**. Advanced AI-driven detection systems are designed to recognise suspicious patterns, detect unusual language, and flag behaviours that could signal an attempted breach. When trained to spot signs of AI-generated messages, these tools become the first line of cybersecurity defence. They can help identify phishing attempts before employees ever encounter them, reducing the risk of human error, which remains one of the most common vulnerabilities exploited in these attacks.

Another key defence strategy is enhancing access controls through **Multi-Factor Authentication (MFA) and Zero Trust** frameworks. MFA ensures that employees authenticate through multiple channels, which prevents attackers from getting in even if they have valid credentials. The Zero Trust model—assuming that no user or device is trusted by default—requires constant verification of every request and interaction. This way, even if attackers gain access to one system or device, they can't easily pivot to compromise the entire network.

**Employee training**, however, is where organisations can make the most impact. AI-driven scams are getting smarter, meaning employees need to be equally savvy to recognise and resist them. Training programmes should go beyond the basics, incorporating simulations that mirror real AI-generated attacks. From my experience, giving employees hands-on exposure to these kinds of scenarios helps build a deeper level of awareness, especially among those in high-risk positions like executives or finance teams.

**Automated incident response systems** add a crucial layer of security, offering rapid, real-time responses to potential phishing attacks. These systems can detect and isolate compromised accounts or devices within seconds, helping to limit exposure before significant damage occurs. When an alert is raised, automated responses allow security teams to focus on strategic actions instead of scrambling to contain a breach after the fact.

**Regular security audits and realistic penetration testing** are equally important. Simulating the latest AI-based phishing techniques during testing reveals gaps in defences that might otherwise go unnoticed. With each simulation, companies can: fine-tune their response plans; create stronger protocols; and empower employees with better tools to more effectively detect and report phishing attempts.

**Verify all invoices** thoroughly before processing any payments, ensuring that you're checking the sender's email address matches official records and watching for subtle discrepancies in domain names, which are often a red flag. Cross-reference invoices with known contacts or internal records to confirm legitimacy.

**Managing your online presence** is also vital. Limit the personal information you share on social media, as AI algorithms can gather even the smallest details to create convincing fake messages. Regularly update your privacy settings and be cautious when accepting friend requests or messages from unknown sources. Additionally, avoid posting details like upcoming trips, work schedules or personal connections, as these can be exploited by phishing attackers.

**Utilising jailbreaking techniques**, the art of "tricking" deceptive chatbots into disclosing information or performing actions they were programmed to avoid, can be an effective strategy for mitigating AI-driven phishing scams. By bypassing standard restrictions, users can explore the underlying functionalities of chatbots, identifying manipulative behaviors or hidden prompts designed to extract sensitive information.

Lastly, **intelligence sharing** is one of the most underutilised, yet essential, tools for cybersecurity teams today. AI-driven phishing techniques often spread rapidly across industries, so threat intelligence networks are crucial for staying informed on emerging tactics. Through my work with Vodafone Business, I've seen how valuable collaboration between companies and cybersecurity providers can be in protecting against these attacks.

Katie Paxton-Fear

# Keep your Business Secure with Market Leading Solutions Available with Vodafone Business

No matter the size of your organisation, Vodafone Business offers a range of proactive cybersecurity solutions to help keep you and your sensitive data protected, 24/7.

## Proactive people

**CybSafe** - is a cloud-based human risk management platform that helps reduce security risks by measuring, understanding and improving people's security decisions and behaviours.

## Proactive processes

**Penetration Testing** - We can simulate an attack on your businesses network to find weaknesses in your cyber security controls.

**Cyber Security Exposure Diagnostics** - Scans the user environment to collect and analyse data helping the customer identify improvements that should be made towards their cyber security.

**Phishing Awareness** - their way through defences. Phishing awareness tests can help your business understand your security awareness level.

**Vulnerability Assessment** - Service that helps to pinpoint existing vulnerabilities in a customer's infrastructure.

## Proactive technology

**Managed Extended Detection and Response** - Monitoring, Management and Response service. We provide you with notifications and advice on cyber threats and act with remediation quickly and cohesively, using the latest technologies and a combination of automated workflows with a skilled analyst team.

**Secure Web Gateway with Zscaler** - ZIA: secures users as they connect to services and applications over the internet for general internet access or using Software as a Service a applications such as Microsoft 365.

# Vodafone Business Policy Recommendations for UK Government

## Vodafone Business recommends the following policy initiatives to help the UK Government in its mission to support businesses as they combat advanced AI-driven cybersecurity threats:

1. **Incentivise Cybersecurity Adoption:** Introduce financial incentives such as tax breaks, grants or subsidies for businesses that invest in cybersecurity measures, including training and certification.

2. **Launch a 'Cyber Safe' PR Campaign:** Develop a nationwide PR campaign to promote Cyber Resilience Centres (CRCs) and the Cyber Essentials certification among businesses of all sizes.

3. **Reallocate Funding for Local Cybersecurity Training:** Reallocate funds within the National Cyber Security Strategy budget to support targeted local initiatives for businesses, focusing on effective engagement programmes.

4. **Enhance Cybersecurity and Skills to Prevent AI-led Cyber Attacks:** Promote the development and adoption of AI-driven cybersecurity tools and provide training to businesses on preventing AI-driven cyber-attacks.

5. **Expand Cyber Resilience Centres (CRCs):** Establish additional CRCs in underserved regions and enhance the capabilities of existing centres to offer tailored support to businesses.

# Methodology

Vodafone Business commissioned Walr, an independent market research agency, to conduct online research among 1,000 business leaders and 2,000 office workers aged 18+ across the UK.

The fieldwork took place from 3rd to 7th October 2024.

Walr employs MRS-certified researchers and strictly adheres to the MRS Code of Conduct.

# Contact Details

For further information on anything disclosed in this Vodafone Business report please contact:

**Leon Garwood**
Corporate Communications Manager, Vodafone Business UK

leon.garwood@vodafone.com
+44 07568 962 571