WePurpose Technology

Modern Threats Hiding in Plain Sight: When People Become the Target

A Changing Threat Landscape

Every business today, no matter its size or industry, operates in a digital environment that never sleeps. Work happens across multiple devices, from homes, offices, and everywhere in between. Cloud platforms, shared documents, and instant communication have made collaboration easier than ever. Unfortunately, the same technologies that help us stay connected have opened the door to new risks that are harder to see, anticipate, and defend against.

Cyberattacks have always evolved, but something has shifted. Traditional malware and large-scale exploitation are now just one part of the picture. Attackers increasingly target the individual. They exploit human emotions such as curiosity, fear, and trust to gain access to systems and data. It is no longer just the IT infrastructure that is under threat, but the people who use it every day.

What makes this change so dangerous is how familiar it feels. Where old-style attacks once relied on spotting fake links or suspicious attachments, today's threats are woven into the daily flow of business. Messages look genuine, requests seem routine, and the platforms being used are ones we rely on to get work done. In this environment, a single click or reply can hand cybercriminals the access they need.

For small and mid-sized organisations, this can feel daunting, but it is not hopeless. Staying secure today is less about chasing the latest security product and more about understanding where real risk lies. It means recognising that people, not technology, are now the primary targets, and that sustained protection requires guidance, training, and managed support.

That understanding sets the stage for what follows. To tackle the modern threat landscape, we first need to explore how and why attackers turned their focus toward people, and why even the most careful employees can become the gateway for a cyber incident.

From Firewalls to False Confidence

For years, many businesses believed that protecting their systems meant building strong walls around them. Firewalls, antivirus software, and access controls were seen as the first and last lines of defence, creating the sense that if the perimeter was secure, everything inside would be safe. That approach worked when data and applications sat neatly within an office network, but it no longer reflects how modern work happens.

Today, information flows between personal devices, cloud services, and third-party applications that live far beyond the company firewall. Teams share files in real-time, join meetings from home networks, and use collaboration tools where business and casual communication blend together. In this constantly connected environment, the edge of the network has all but disappeared. Yet many organisations still rely on old assumptions, expecting yesterday's architecture to protect today's workforce.

Attackers know this. Instead of trying to breach hardened defences, they go after something much softer and far more predictable: human behaviour. They study how people interact, who approves payments, and what looks normal in internal communication. They pose as trusted colleagues, service providers, or even executives, turning trust into their key weapon rather than malware. The best technical controls can be bypassed in an instant if an employee is persuaded to share credentials, approve a fake invoice, or click on a convincing link.

This is where the sense of false confidence becomes most dangerous. A business can invest heavily in the latest tools, but if its people are not equipped to recognise manipulation, the risk remains. Only 6% say that their organisation's security policies are continuously updated based on emerging trends. In practice, that means most companies operate with outdated rules and training that fail to address how attacks actually work today.

Modern cybersecurity can no longer be treated as a box to tick. It is a shared responsibility that combines technology, awareness, and culture. Protection is no longer about building higher walls, but about creating smarter, more adaptable teams who understand how to respond when the unexpected happens. This shift in mindset is what enables true resilience, and it begins with recognising that awareness and partnership are our strongest forms of defence.

> Only 6% of security leaders say that their organisation's security policies are contiuously updated based on emerging trends.

Targeting the Weakest Link: How Humans Became the Prime Target

Attackers have discovered that the most effective way to penetrate an organisation is rarely through technology alone, but through the people who rely on it. Human nature, with all its strengths and weaknesses, has become the new frontier of cybercrime.

Curiosity leads someone to open an unexpected attachment. Empathy makes them respond quickly to what appears to be a colleague in need. Distraction results in a hasty click during a busy afternoon. Urgency, which cybercriminals often manufacture, pushes people to act before they think. These instincts are what make us efficient and cooperative at work, yet they are the same traits attackers manipulate to gain access.

The uncomfortable truth is that anyone can be fooled. Even trained, security-minded individuals can let their guard down at the wrong moment. Cybercriminals exploit psychology, not intelligence, crafting messages that bypass logic and appeal to emotion. They design requests that appear completely ordinary, embedding their deception within the everyday noise of corporate communication.

A well-timed message during a financial deadline or a genuine-looking request from a senior leader can be enough to breach even the most aware teams.

Training programmes are a critical first step in addressing this challenge, and most businesses recognise this. In fact, 87% of respondents say that their organisation trains its employees to spot cyberattacks at least once a quarter. This commitment shows that organisations understand the human element is central to modern security. Yet there remains a gap between awareness and execution, with 33% still fearing mistakes and human error in handling of email threats by employees. Training alone cannot counteract the pace and sophistication of attacks that evolve faster than internal education can adapt.

The key lies not in assigning blame, but in building resilience and support. A culture where staff feel encouraged to report a suspicious message, rather than embarrassed by a mistake, is far more effective than one driven by fear.

Managed protection services can reinforce this by providing real-time monitoring, ongoing behavioural insights, and continuous updates that adapt alongside the threat landscape. When people are supported rather than singled out, they become an active line of defence instead of a potential vulnerability.

This human-centric approach bridges the gap between awareness and action, leading into the next vital question: how did attacks that once relied on crude impersonation evolve into today's highly personalised, AI-driven campaigns?

The Evolution of Human Targeted Attacks

Phishing has come a long way from the clumsy, poorly written scams that once filled inboxes. In its early days, a fake bank message or a suspicious lottery win was easy to dismiss. The errors were obvious, and the approach was scattershot, relying on quantity rather than quality. Today's reality is very different. Modern phishing is crafted with precision, designed to impersonate real people, legitimate companies, and even the internal systems businesses use daily. The once-obvious red flags have been replaced by professional-looking messages that mirror the tone, layout, and timing of genuine communication.

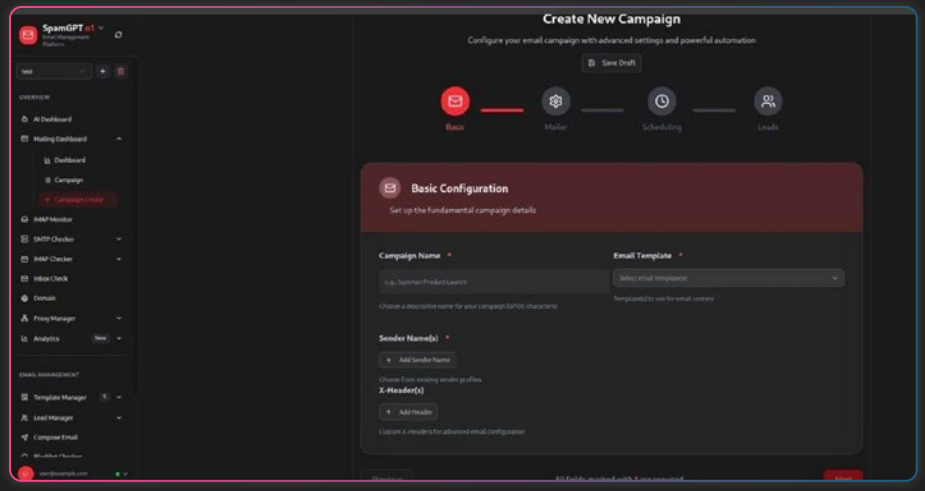
This transformation is driven by the power of automation and artificial intelligence. Attackers no longer need to manually write each message or research their targets individually. They use AI tools to analyse language patterns, business hierarchies, and communication styles, creating messages that look authentic and relevant. The result is multi-channel deception that's difficult to distinguish from legitimate interaction, spreading through email, chat platforms, and social messaging systems with equal effectiveness.

SpamGPT highlights how far this evolution has come. It is an AI-powered spam and phishing toolkit marketed on underground forums, designed to compromise email servers, bypass spam filters, and automate large-scale phishing campaigns with ease.

Its features mimic enterprise marketing platforms, including campaign management, SMTP and IMAP setup, deliverability testing, analytics, and an integrated AI assistant known as “KaliGPT,” which generates tailored phishing content and optimises campaigns for greater success.

By lowering the barrier to entry, SpamGPT offers inbox placement guarantees, spoofing capabilities, SMTP cracking training, and real-time monitoring, effectively making professional-grade spam operations available to less-skilled attackers.

As these tools continue to develop, the gap between technical defences and attacker sophistication grows wider. Standard filters, blacklists, and detection systems struggle to keep pace when every message is context-aware and continuously refined by machine learning. Awareness training must now evolve in parallel, focusing on behaviour, verification, and culture rather than rule-based identification.



Modern Attack Types Every Business Should Know

Business Email Compromise

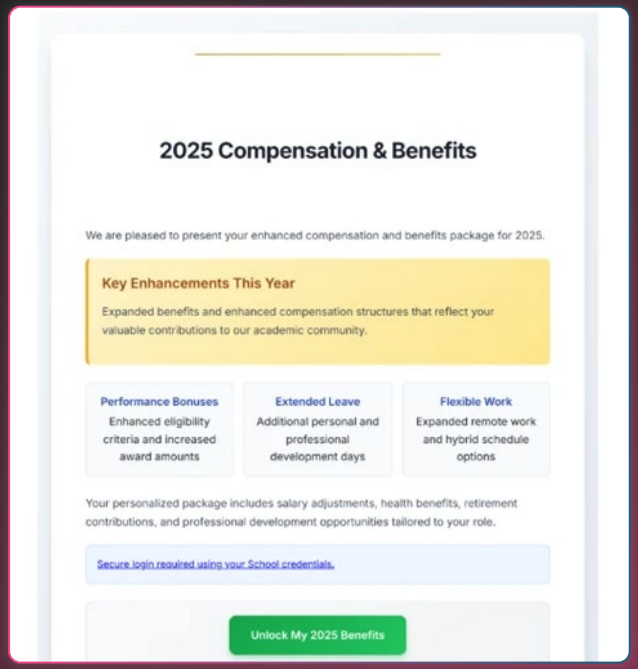
Among the most financially damaging types of targeted attack, Business Email Compromise (BEC) relies not on technical intrusion, but on deception and trust. In a BEC scenario, attackers hijack or convincingly spoof an executive's email account, often imitating senior figures such as the managing director, finance lead, or CEO. The goal is simple: trick an unsuspecting employee into transferring money, changing payment details, or supplying sensitive information.

These emails are remarkably convincing. Attackers research internal structures, study writing styles, and mimic legitimate communication flows. A message may appear from the finance director requesting an urgent wire transfer, or from HR updating payroll details. Others pose as suppliers chasing overdue invoices, or even as senior staff requesting a batch of gift cards to "thank the team." Each request is framed as normal business activity, making it difficult to flag as suspicious.

Statistics highlight how effective this subtle manipulation has become. Business Email Compromise emails achieve an average 28% open rate, with 15% of targets replying to the message. Even more alarming, 16% of all financial losses associated with cybersecurity incidents are directly linked to BEC. With these numbers, the threat is no longer a niche concern but a mainstream business risk.

Traditional security solutions struggle to contain this type of attack. Secure email gateways and spam filters, designed to detect malware or bulk spam, often miss BEC attempts because they contain no malicious links or attachments. The communication itself is the weapon.

Protection requires layers beyond basic filtering. Strong authentication such as multi-factor authentication can prevent account hijacking, while behavioural monitoring can spot activity that falls outside normal user patterns. Continuous awareness also plays a vital role: when employees are encouraged to pause and confirm suspicious requests, the strength of human validation becomes the most reliable last line of defence.



28% Open Rate

15% Reply Rate

Business Email Compromise

Session hijacking is one of the more covert threats businesses now face. Instead of stealing passwords, attackers steal the session tokens that keep a user securely logged in to cloud or web applications. These tokens act as digital passes that prove a person's identity once authenticated. When stolen, they allow cybercriminals to step directly into an existing, trusted session without ever needing to know the password.

This tactic effectively bypasses many of the safeguards that organisations rely on. Multi-factor authentication, strong passwords, and single sign-on protections all fall short once a valid session token has been compromised. The attacker simply resumes where the legitimate user left off, with full access to systems, emails, and business data. Tokens are traded openly on illegal marketplaces, sometimes costing as little as $10 per session, giving almost anyone the ability to exploit stolen user access for profit.

As businesses increasingly rely on cloud services and browser-based applications, the opportunities for token theft multiply. Each connected device, app, and session represents another possible foothold for a cybercriminal. Once inside, attackers can exfiltrate data, impersonate the user, or deploy additional malware to entrench control.

Reducing exposure to this type of attack requires vigilance and continuous oversight rather than one-time security checks. Continuous monitoring and behavioural analytics can detect when a session acts unusually, such as a login from a new region or a sudden flood of data transfer. Combining these insights with robust endpoint security and regular token renewal helps close a gap that technology alone cannot eliminate.

This evolution in attack methods mirrors a wider shift in how cybercriminals operate, moving from the inbox to the platforms where day-to-day collaboration happens.

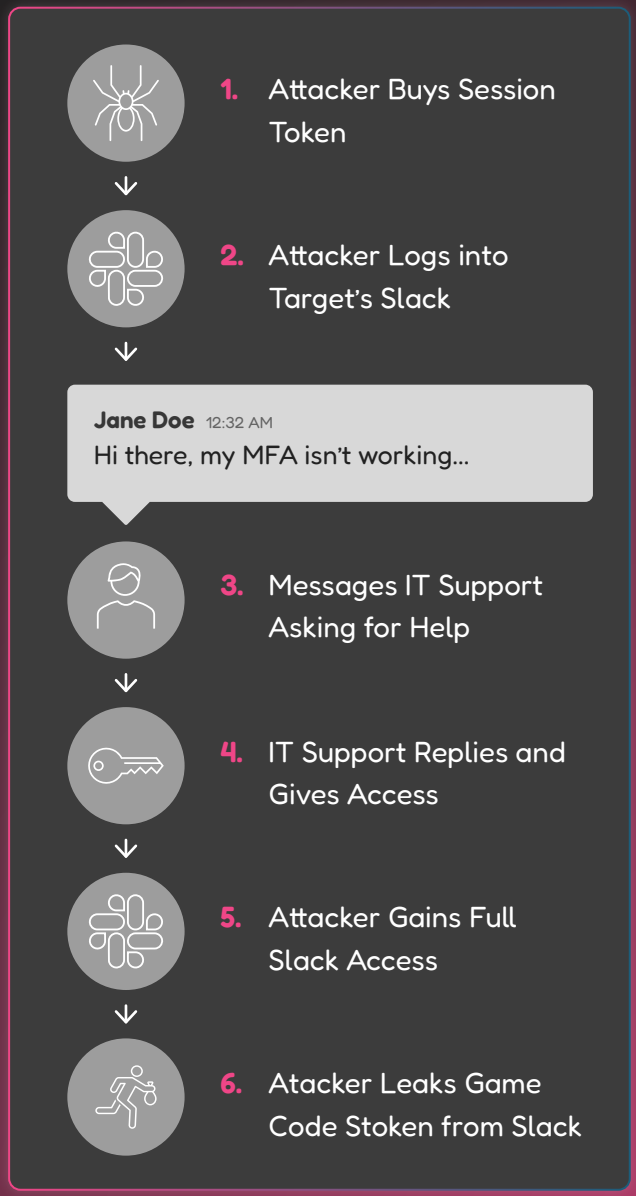
Collaboration Platform Attacks

Collaboration tools like Microsoft Teams, Slack, and SharePoint have become the beating heart of modern business communication. They make teamwork fast and convenient, allowing projects to move forward even when teams are scattered across multiple locations. However, this constant connectivity also gives cybercriminals a new and highly effective channel through which to operate. When a message appears to come from a colleague, many users instinctively trust it, creating the perfect environment for deception.

Attackers exploit this trust to launch phishing and session hijacking attacks within these platforms. Instead of arriving by email, fraudulent messages and malicious links appear within familiar chat threads or shared documents, seamlessly blending into day-to-day communication. Once a single account is compromised, an attacker can move laterally through the organisation, sending infected files or requests for access that appear completely legitimate. It is no surprise that 89% of organisations report having seen at least one advanced attack targeting their collaboration platforms.

The breach at Rockstar Games provides a striking example of this type of attack. The incident began when a threat actor purchased stolen session cookies on a criminal forum. Using those tokens, they logged directly into the company's Slack workspace, bypassing authentication. The attacker then messaged IT support, claiming that multi-factor authentication was not working and asking for help with access. Believing the request was genuine, IT provided additional credentials. Within minutes, the attacker had full access to the internal Slack environment, ultimately leaking source code from a major upcoming release.

This attack illustrates how integrated collaboration environments blur the boundaries of internal and external trust. A message that looks ordinary within a secure workspace can in reality be a vehicle for compromise. Effective protection depends on layered monitoring, verification processes for internal requests, and a culture where employees are comfortable questioning unusual activity.



ClickFix Attacks

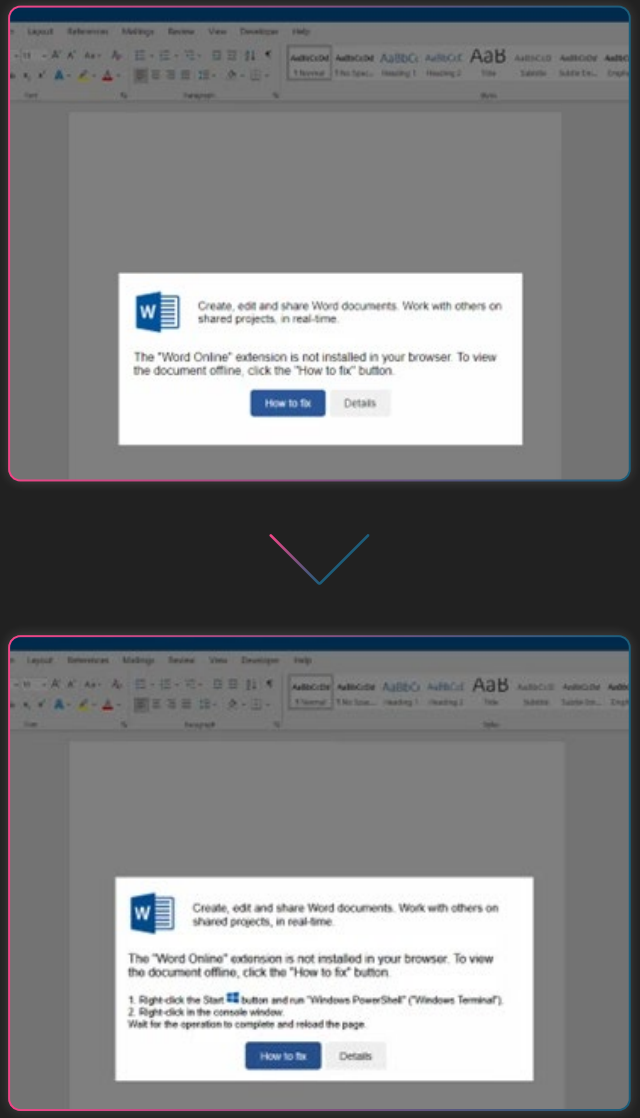
ClickFix attacks are engineered to take advantage of one of the most common user reactions in technology: the instinct to fix a problem quickly. In these schemes, cybercriminals display realistic pop-ups or prompts that appear to come from trusted software, encouraging users to “approve access,” “re-enable security,” or “fix a detected issue.” The messages are designed to look and feel authentic, often borrowing the exact design cues, branding, and tone of legitimate applications or operating systems.

The sophistication of these attacks has accelerated alongside the growth of cloud and web-based services. What once looked like an obvious fake warning has evolved into prompts that appear directly inside browsers or collaboration tools, adding credibility and urgency. The method is highly effective precisely because it plays on trust and compliance. Even security-conscious employees can be prompted into immediate action when a message appears to come from a familiar application claiming something has gone wrong.

Recent research shows how widespread the problem has become. ClickFix-style attacks increased by 500% during 2025 and now account for 8% of all reported cyber incidents, the second-highest category behind phishing. The increase demonstrates that attackers are successfully adapting psychological manipulation for modern, cloud-first environments.

What makes ClickFix particularly dangerous is that these pop-ups often instruct users to override genuine security measures such as authentication requests or update warnings. In doing so, employees unknowingly grant attackers the access that technical controls are designed to prevent. The best defences against this type of attack combine user awareness, browser-level security policies, and behavioural monitoring that can detect suspicious authorisation activity.

This manipulation of urgency and authority reinforces a central idea that runs throughout modern cybercrime: it is not always the software that fails first, but the human instinct behind the click.



SVG Phishing

SVG phishing is a newer and sophisticated attack technique that has becoming increasingly common. Instead of attaching a traditional file that might be scanned or blocked, attackers embed JavaScript and other executable code within harmless-looking image files, most commonly scalable vector graphics (SVG). When these images are opened or uploaded into trusted platforms, the hidden code activates, redirecting recipients to malicious websites or harvesting credentials directly within the browser.

What makes this attack so effective is that the file type itself does not appear suspicious. SVG images are widely used in websites, presentations, and email signatures because they scale cleanly and load quickly. Tools such as AutoSmuggle have been specifically designed by attackers to inject malicious code into these images, streamlining the process of creating weaponised files that evade security controls. To the recipient, the SVG seems entirely legitimate, yet a single click can trigger a script that silently connects to an external server or prompts a user to sign in again, capturing their credentials in the process.

The rise of SVG phishing is reflected in its sheer volume. In 2025 alone, there were more than 2 million detected incidents within a single month. This rapid surge highlights how attackers continue to exploit the grey areas between convenience and security. Standard email security solutions often treat image files as low-risk, allowing these threats to slip through unnoticed.

Protecting against SVG phishing requires the same blend of user education and technical enforcement used for other human-focused threats. Employees should be cautious when unexpected image files appear, even if sent by familiar contacts, while security teams must ensure that file-content scanning and sandboxing extend to all attachments and embedded scripts.

Notification Abuse

Notification abuse takes advantage of the familiarity and urgency created by trusted digital services. Attackers craft malicious prompts or system notifications that appear identical to legitimate alerts from well-known platforms, such as DocuSign, Adobe Sign, or PayPal. These messages typically claim that a document needs to be signed, an account must be verified, or a payment is pending approval. The goal is simple: convince users to click immediately, bypassing inspection and scepticism.

Because genuine notifications from these platforms are so common in daily business activity, the fraudulent versions blend seamlessly into routine communication. A user who regularly signs contracts through DocuSign or processes payments through PayPal may see little reason to investigate further, especially when the timing coincides with real work processes. Once clicked, these links often direct the user to fake login pages designed to harvest credentials or inject malicious payloads masquerading as software updates.

Attackers rely heavily on the psychology of compliance. The notifications are designed to look pressing yet ordinary, prompting individuals to respond before they lose access or delay an urgent transaction. Even vigilant employees can mistake these prompts for genuine messages, particularly when they mimic company-wide systems that use similar branding.

While email filters and secure gateways may catch some of these attempts, notification abuse often targets the spaces that sit outside traditional protections, such as mobile push notifications or direct browser prompts. Staying protected requires combining awareness training with technical controls that verify the authenticity of source domains and restrict automatic pop-ups requesting user action.

By exploiting the appearance of trusted communication, this form of attack reinforces how attackers adapt their methods to target daily workflows.

Real-World Lessons: How One Mistake Became a Data Breach

The story of the 150-year-old UK logistics firm Knights of Old is a powerful reminder of how a single lapse can unravel even a well-established business. In 2023, the company suffered a catastrophic ransomware attack that brought its entire operation to a halt. What began as a simple instance of password reuse quickly escalated into a full-scale breach, ultimately leading to the company's collapse.

The attack began when the Akira cybercrime group exploited a reused employee password to gain initial access to internal systems. From there, the attackers spread laterally across transport and finance networks, encrypting servers and demanding a ransom of nearly £5 million to restore access. The company's backup systems, which were thought to offer protection, failed during recovery. Within weeks, the business that had operated for over a century and a half was unable to fulfil orders or service clients.

The immediate impact was devastating. Knights of Old entered administration, costing more than 700 jobs and erasing approximately £15 million in shareholder value. Despite investing over £100,000 annually in IT infrastructure, the company's defences were compromised by weaknesses that could have been avoided. Password hygiene was poor, multi-factor authentication was inconsistently applied, and backup strategies lacked regular verification, leaving the business vulnerable when disaster struck.

Even cyber insurance fell short. With a policy covering only £1 million, the firm discovered that inadequate coverage can compound the consequences of a breach. The incident revealed gaps not just in technical security, but in strategic oversight and risk management.

The lesson is clear: cybersecurity resilience is not defined by the size of a company's budget but by the quality of its planning and partnerships. True protection relies on continuous improvement, informed guidance, and external support from security specialists who understand how to align processes, technology, and people. For smaller businesses, the collapse of Knights of Old is a sobering example of what can happen without proactive collaboration and managed protection.

The Cost of Ignorance: Counting the Hidden Impact

The collapse of Knights of Old shows that the greatest cost of a cyber incident is rarely the ransom itself, but everything that follows. When systems go offline, operations stop. For many organisations, every lost hour means missed orders, idle staff, and damaged customer relationships that take months to rebuild. Downtime has a direct financial impact, but the wider effects ripple through every part of the business, from supply chain delays to disrupted cash flow and customer churn.

Yet financial loss is only part of the picture. Once an attack occurs, most companies face additional costs they never budgeted for: legal action, regulatory penalties, and forensic investigations that can run well into six figures. In sectors that handle personal or contractual data, compliance failures can attract steep fines, especially when it becomes clear that preventable gaps in policy or oversight contributed to the breach.

Rebuilding trust with customers and suppliers is often the longest and most expensive task of all. Reputation, once damaged, is difficult to restore, and for many small and mid-sized businesses, it can mark the end of a trading relationship entirely.

Cyber insurance may soften the blow, but it rarely covers every aspect of loss. Reputational damage, staff overtime, lost productivity, and the long-term cost of business interruption are difficult to quantify and almost impossible to recover. The difference between prevention and recovery often comes down to timing and awareness. Investing early in proactive defence, training, and continuous monitoring costs a fraction of the expense of rectifying a full-scale breach.

The good news is that change is achievable. Businesses that act now to strengthen their defences can significantly reduce risk and build greater confidence in their digital operations. The next step is understanding how to make those improvements in a structured, sustainable way, starting with a strategy that treats people, process, and technology as equal pillars of protection.

Building a Human-Smart Defence

If the true cost of a cyber incident lies in what happens after the breach, then the real value of cybersecurity lies in prevention. Building a resilient defence begins with a balanced approach that combines three pillars: People, Process, and Technology. Each plays an essential role, and success depends on how well they work together rather than how advanced any single solution might be.

The first pillar, **People**, recognises that human behaviour is both a potential risk and a powerful defence. Regular awareness training and continuous education turn staff from passive recipients of policy into active participants in protection. Simulated phishing exercises, clear guidance on incident reporting, and leadership engagement all reinforce vigilance and accountability. When employees understand why attacks happen and feel empowered to act, mistakes can become early warnings instead of disasters.

The second pillar, **Process**, provides the structure. Defined procedures for access management, data handling, and incident response ensure consistency and reduce uncertainty when pressure is high. Well-tested backup strategies and recovery protocols mean that even if a failure occurs, operations can return to normal swiftly and confidently. Processes should evolve alongside new threats, ensuring that outdated policies do not create avoidable vulnerabilities.

Finally, **Technology** ties the framework together. Multi-factor authentication, continuous endpoint monitoring, and automated patching strengthen technical defences, while cloud security controls and behavioural analytics provide the insight needed to detect anomalies before they escalate. Technology, however, is only effective when it supports people and processes rather than replacing them.

Perhaps the most important ingredient is **Culture**. A workplace where employees can report suspicious activity without fear of blame creates an environment of trust and shared responsibility. With expert guidance and managed support, even small businesses can achieve enterprise-level protection. Cybersecurity is not an unattainable goal; it is a continuous journey, one that becomes far more manageable with the right partner beside you.

How WePurpose Technology Can Help

We believe that cybersecurity is not just about responding when something goes wrong, but about staying one step ahead. Our role goes beyond providing a helpdesk, we act as a proactive partner, watching over your systems, guiding your teams, and ensuring your defences evolve as the threat landscape changes.

Through continuous monitoring, our team identify unusual activity before it becomes a problem. We deliver ongoing awareness training that keeps your staff alert to the latest scams and deception tactics. We also align the right technologies with your business goals, ensuring that solutions like multi-factor authentication, endpoint protection, and secure cloud configurations work together smoothly rather than in isolation. This joined-up approach provides stronger, smarter protection tailored to how your business actually operates.

Most importantly, we make security accessible. Good protection should not be limited to large enterprises or businesses with complex IT teams. With the right guidance and support, every organisation can achieve a level of security that matches its ambition and appetite for growth. If you are ready to take a confident step forward and strengthen your defences, our team is ready to help, start the conversation with us today.

WePurpose Technology

+44 (0)1463 572042 | **www.theapprenticestore.co.uk** | info@theapprenticestore.co.uk