REPLY
AVVIO

CYBERSECURITY: LEVEL UP FOR 2025

INSPIRATION PACK FOR ENGAGING EMPLOYEES

MW MODERN WORKPLACE 2025

SECURE OUR WORLD

It’s Cybersecurity Awareness Month 2025 in October and this year’s theme is “Secure Our World”.

So, what does that mean?
It’s all about recognising that cybersecurity isn’t just an “IT thing” — **it’s everyone’s responsibility.** From the newest recruit to the CEO, we all have a role in protecting our digital spaces and keeping threats at bay.

The 2025 campaign zeroes in on four simple, powerful actions we can all take.

1. **Strong passwords & password managers**
   Create complex, unique passwords and let a password manager keep them safe for you.
2. **Multi-factor authentication (MFA)**
   Add an extra lock on the door with MFA, so even if a password slips, your account stays secure.
3. **Software updates**
   Keep your software and devices up to date to shut down security gaps before attackers can exploit them.
4. **Spotting & reporting phishing**
   Learn how to recognise those too-good-to-be-true emails and report them before they cause damage.

> “Cybersecurity in 2025 is a whole new game. Threats are smarter, sneakier, and evolving faster than ever, which means this is the year to get your people up to speed on the latest trends and tactics to stay safe.”
>
> **Craig Swanwick**
> Partner, Avvio Reply

SO, LET’S GET STARTED →

THE HIGH PRICE OF A WEAK LINK

Hackers have leveled up, have you?

Skipping out on a strong cybersecurity strategy isn't just risky, it can be downright catastrophic.

A single weak link, whether in your systems, your suppliers, or **especially your people,** can open the doors to attacks that halt operations, damage trust, and rack up staggering financial and reputational costs. The reality is that employees are often the first line of defence, **or the easiest way in,** making awareness and vigilance across your workforce just as critical as the technology you use. That's why a resilient Security Behaviour and Culture Programme isn't optional – **it's essential.**

43% of businesses reported having experienced a cyber breach or attack in the last 12 months. This corresponds to approximately 612,000 UK businesses

Cybersecurity Breaches Survey 2025 – GOV.UK

£300M

Marks & Spencer (M&S): Retail chaos and a £300M hit

In April 2025, M&S was rocked by a ransomware attack, believed to be executed by the Scattered Spider group using DragonForce tools, that began with a phishing compromise of a third-party IT contractor. The fallout was intense: online orders and click-and-collect services were offline for weeks, contactless systems failed, and supply chains faltered. Analysts estimate the disruption will cost the company around £300 million in operating profit, and its market value plunged by about £1 billion.

CURRENT THREATS

Threats are getting smarter. And so must your campaigns. These trends aren’t just buzzwords; they’re what your people need to know right now.

AI-POWERED THREATS

Cybercriminals are now using Artificial Intelligence (AI) and machine learning to up their game.

Think deepfake videos that look eerily real, voice clones that can "call from the CEO," and phishing emails that sound just like your boss. It's no longer just typos and dodgy grammar; it's slick, fast, and convincing. These are showing up in CEO fraud, payment scams, and even internal manipulation.

No longer can we rely on gut feeling or "it just looked dodgy" anymore. Training and awareness need to keep up with the pace.

85% of Cybersecurity professionals believe that the rise in cyberattacks is due to AI tactics.

CFO.com

CEO of world's biggest ad firm targeted by deepfake scam

Fraudsters cloned the voice and appearance of WPP's CEO, using a WhatsApp account and virtual meeting façade to try to trick staff into sharing money and personal details. Thanks to employee awareness, it was stopped in time.

SOCIAL ENGINEERING SURGE

Social engineering is a type of cyber attack that relies on human interaction to trick people into divulging sensitive information or take an action that compromises security – in a nutshell social engineers exploit human psychology to gain trust and manipulate victims.

Phishing emails are just the tip of the iceberg. We now need to be aware of vishing, smishing, pretexting, spoofing, baiting, whaling and tailgaiting techniques which target vulnerable people.

It's not about the tech; it's about exploiting human nature. Awareness, education and behaviour change are key.

"One example we've seen is that when we had new starters at the company we used to put a note out on LinkedIn to welcome them. But we noticed that those new employees would immediately be targeted by phishing scams, as it would be assumed they're an easy target who doesn't know the people and processes in the company very well yet."

Millicent Machell, HR Magazine

REPLY AVVIO

More than

90%

of cyberattacks start with a phishing email. Meaning human error, like clicking on a malicious link or attachment, is still the most common way breaches begin.

StationX.net

HMRC phishing attack

In 2024, HMRC detected unauthorized access to approximately 100,000 taxpayers' online accounts due to a phishing campaign by organised crime groups. The attackers used personal data obtained from external sources to impersonate legitimate users and fraudulently claim funds. While no direct financial loss occurred to taxpayers, the incident highlighted the vulnerability of government systems to social engineering tactics. The breach led to several arrests, and HMRC took immediate action by deleting compromised logins and removing erroneous data. The tax authority also collaborated with domestic and international law enforcement to address the incident.

CONFIGURATION MISTAKES

A configuration issue can be as simple as using weak passwords or a more complex problem, such as improperly set up firewalls.

Whilst your cybersecurity teams are responsible for your security systems, instilling the basic habits highlighted in this year's cybersecurity month theme will help employees safeguard themselves and your organisation.

Sooo... don't use weak passwords, don't use devices not authorised by your company and regularly update your software.

More than

8,000

servers were vulnerable to data breaches due to misconfigurations.

2023 report, Censys

Weak password leads to corporate collapse

A venerable 158-year-old UK transport company, Knights of Old (KNP), was brought to its knees in 2025 following a ransomware attack initiated by a single, easily-guessed employee password. The attackers, members of the "Akira" group, infiltrated the company and encrypted critical systems, including backups and endpoints.

They issued a ransom demand of up to £5 million, which KNP could not afford. Despite having cyber-insurance and aligned cybersecurity practices, the company couldn't recover and was forced to close, leaving 700 employees without jobs.

This case is a chilling reminder that it often takes just one vulnerable point to escalate into a full-blown crisis.

YOUR FIRST LINE OF DEFENSE

Understand the latest strategic approaches and new training opportunities to upskill your people - enabling them to protect themselves and your business.

NEXT-GEN METHODS TO TACKLE CYBER RISKS

SIMULATION-BASED TRAINING

Phishing and smishing simulations have been standard practice for years, helping employees spot suspicious emails and texts.

Now, companies are taking it a step further with deepfake simulations, recreating realistic scenarios like fake CEO videos or voice clones to train staff against sophisticated modern attacks.

Why it works: People remember what they do, not just what they read.

Core Health & Fitness simulates deepfake
Core Health & Fitness replaced outdated content with deepfake simulations and interactive modules, achieving a 5% average failure rate and a 4.7/5 employee rating.

BEHAVIOUR-BASED LEARNING

Adaptive behavior-based learning tailors content to each employee, adjusting in real time based on their responses and risk profile.

Why it works: Forget one-size-fits-all e-learning. This approach meets people where they are, giving them the right awareness and education exactly when they need it.

Adaptive Learning at DocuSign
DocuSign used an adaptive learning model that adjusts simulation difficulty to employees' skill levels, giving the Trust & Security team clearer insight into strengths and weaknesses around social engineering risks.

DATA DRIVEN DEFENCE

Instead of "training everyone the same way once a year", organisations should be using real data on employee behaviour to focus on the most vulnerable groups and adjust their strategy over time.

- **Leverage actual data and evidence,** instead of assumptions or generic best practices, to guide how your company protects itself.
- **Identify segments and prioritise training** for those who are more at risk or demonstrate poor cybersecurity behaviours - supporting the most exposed with targeted engagement activities.

Fortune 500 tech company reduces spear-phishing via data-driven insights

A Fortune 500 technology company with over 11,000 employees globally experienced a breach in summer 2022. Despite an advanced cybersecurity stack, comprising phishing simulations, governance tools, endpoint protection, and training, sophisticated spear-phishing attacks exploiting employee and vendor personal data succeeded. Executive leadership realised that traditional defenses were no longer sufficient and implemented the below:

Action taken

1. **Evidence-based:** Decisions were guided by quantifiable data on exposures, not assumptions.
2. **Tailored responses:** Protections and training were specific to actual vulnerabilities and roles.
3. **ROI-focused:** Security initiatives were justified with hard numbers, gaining executive buy-in.
4. **Measurable success:** A clear before-and-after assessment confirmed effectiveness.

Within 11 months, the company reported:

- No new data breaches.
- Significant drop in incoming spear-phishing and social engineering attempts.
- Reduced HR costs tied to poaching/churn.
- Estimated value exceeding $13,000 per employee annually, combining risk reduction, improved productivity, and other benefits.

FOSTERING A CULTURE OF SECURITY

Security behaviour and culture programmes' (SBCPs) are designed to transform employees from the weakest link into a strong line of defence by embedding good security habits and values into an organisation's culture.

SCBPs are structured initiatives within organisations that aim to improve how employees think about, understand, and act on cybersecurity in their daily work. They go beyond technical controls (like firewalls or encryption) and focus on the human side of security, shaping habits, awareness, and cultural norms so employees naturally make secure choices.

Core elements of a SBCP:

1. Awareness & Education
2. Behavioural Change/Reinforcement
3. Leadership & Culture building
4. Measurement and data-driven adjustment
5. Integration into daily work they cause damage

The Science Museum

The Science Museum Group wanted to understand whether its existing security training and compliance efforts were actually translating into safe behaviours among employees – or simply – checks on a compliance list. They aimed to gauge real behavioural change and the overall security culture, not just training completion.

Utilising the Human Cyber Index (HCI) they reviewed knowledge, intentions, and behaviour to shift from compliance to genuine, positive security culture. This enabled them to develop an insight-informed strategy, enhanced training, targeted interventions and reinforce secure habits.

"Organisations using security behavior and culture programs (SBCPs) have experienced a more effective use of cybersecurity resources as employees become competent at making independent cyber risk decisions."

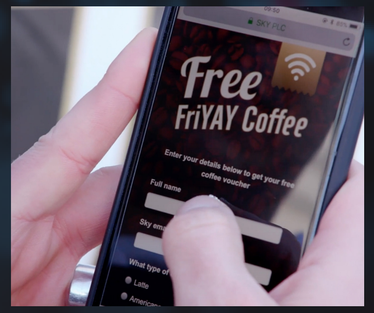
Gartner's Top Cybersecurity Trends for 2024.

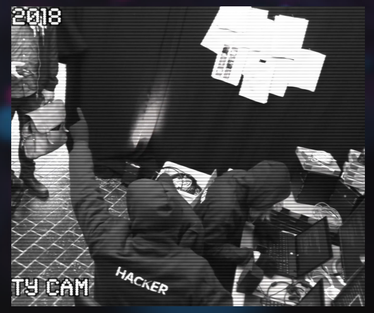
DON'T BE AFRAID TO DO SOMETHING A BIT DIFFERENT

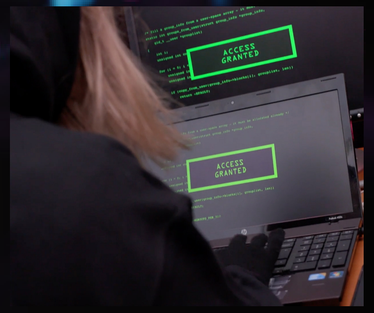
At Avvio, we know that cybersecurity threats aren't just about firewalls and software, they're about people.

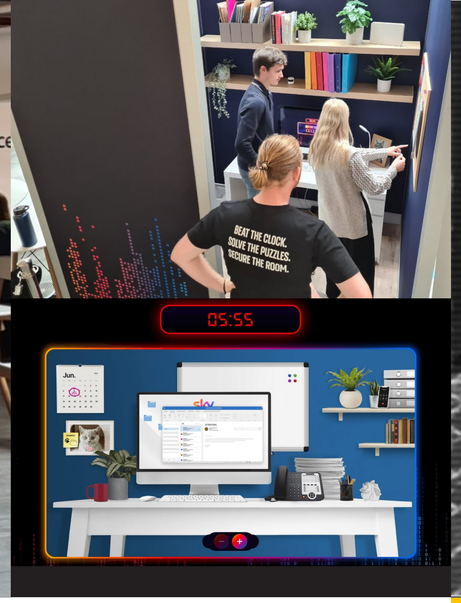
Human behaviour is often the deciding factor in whether a threat succeeds or fails. That's why we create highly engaging, memorable campaigns that bring a topic many see as dry or repetitive to life. From creative storytelling to interactive experiences, we make sure employees don't just hear the message, they remember it, act on it, and help keep your business secure.

People will forget what you said, but they will never forget how you made them feel. Engagement drives action, if cybersecurity training is boring, it won't stick. Investing in creative, fun campaigns turns awareness into behaviour.









CRACKING THE CODE: GAMIFIED CYBER TRAINING AT SKY

To strengthen cyber awareness across Sky, we designed an engaging Cyber Security Escape Room supported by a digital game. Employees were challenged to solve cyber puzzles in just six minutes to "secure the office" before time ran out.

The physical installation created a buzz onsite, while the digital version extended the reach across the business, giving thousands of colleagues the opportunity to take part. The gamified approach not only grabbed attention but also translated into measurable behaviour change.

Results showed a clear impact: Q4 phishing simulations saw a decrease in click-throughs, and reported incidents via Outlook increased. More than 7,000 learning moments were recorded through today@Sky, with over 6,250 unique players, exceeding the 2022 benchmark.

As one leader put it: "Following the Cyber Escape Room, we've seen a significant overall improvement in our cyber security efforts."

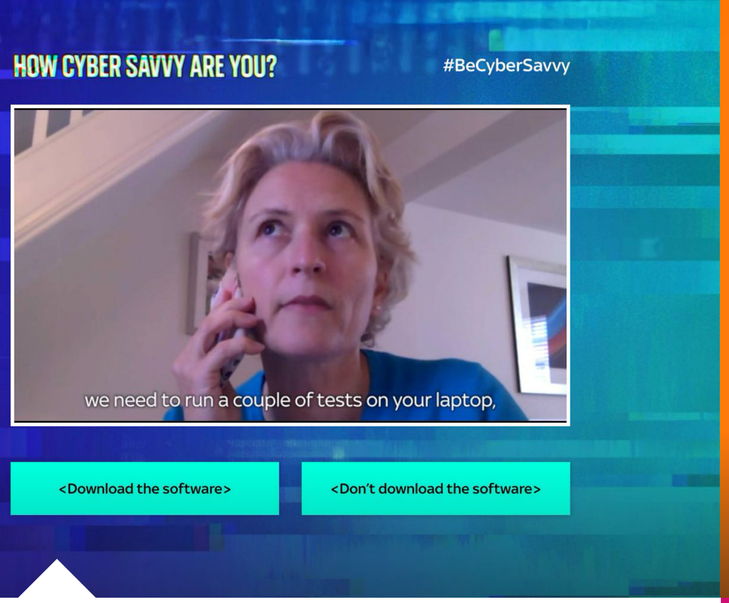
Watch the sizzle

A WI-FI STUNT: EXPOSING THE RISKS OF INSECURE NETWORKS

With employees constantly online, Sky wanted to raise awareness of Wi-Fi security. We created an experiential stunt offering free coffee, requiring staff to share "secure" details to claim their caffeine. Inside the venue, a hacker's pod revealed the risks of unsafe networks, with Sky-branded hosts on hand to educate colleagues on staying protected.

The live activity generated huge buzz, sparking conversations and curiosity onsite. But the real success came from filming the stunt and producing an engaging edit that was shared across Sky. This extended the impact far beyond the event itself, spreading the message in a dynamic, memorable way and ensuring employees across the business understood how to keep themselves and the company cyber safe.

Watch the sizzle



DECISIONS THAT MATTER: BUILDING CYBER SAVVY AT SKY

Avvio created a campaign to help Sky employees take personal responsibility for cybersecurity, reinforcing the message: "Look after Sky's security as you would your own."

We produced an interactive video, filmed via Teams, using a "choose your own adventure" decision-tree mechanic. Employees faced real-world cyber threat scenarios and chose how to respond, with each choice revealing different outcomes, making learning engaging and memorable.

The digital format delivered impact at scale while providing measurable insights into employees' cyber-savviness, helping Sky strengthen overall security awareness and resilience.

HARRY POTTER'S LAPTOP: A CYBER SECURITY CHALLENGE

With more people working from home, Sky needed to remind employees of their responsibility to protect company data. To make a serious, often dry topic engaging, Avvio created a playful "spotter" style game.

Employees were challenged to identify hidden security threats on Harry Potter's laptop. Each click revealed a popup with practical advice, turning the activity into an interactive learning moment.

The simple, cost-effective mechanic proved highly impactful, sparking attention and reinforcing key security behaviours. To ensure reach across the business, the game was also translated for Sky's Italian and German audiences.

PHISHING EXPOSED: RICHEMONT'S BOLD DIGITAL AWARENESS CAMPAIGN

Richemont's Group Security team wanted to educate employees on phishing and ensure they could handle cyber threats effectively. Avvio created a disruptive digital campaign for the intranet, transforming a typically bland topic into an engaging experience.

Using a modern, "loud" design with neon and glitch effects, the campaign combined cheat sheets, infographics, banners, and animated GIFs to educate employees on phishing and reinforce vigilance. The dynamic visuals kept cybersecurity front of mind, making the learning experience memorable while encouraging employees across the Group to stay alert and protect Richemont's systems and data.

STANDOUT CAMPAIGNS
FROM AROUND THE WORLD

LEGO CITY CYBER ATTACK SIMULATION

TAFE Queensland created a LEGO City simulation using over 25,000 bricks to teach cybersecurity in a hands-on, immersive way.

Students were divided into red (attackers) and blue (defenders) teams, with attacks causing visible disruptions, trains stopping, lights going out, and buildings “catching fire” via LEDs.

The exercise helped students experience real-world cyber-attack impacts, develop defensive strategies, and understand the importance of protecting critical infrastructure in a memorable, interactive setting.

CAPITAL ONE’S CYBERSECURITY TRAINING ARCADE

Capital One allowed employees to learn about cybersecurity risks in a fun and interactive way.

This was a great way to engage employees and teach them about phishing, malware, and other cybersecurity threats. This uses operant conditioning, which is a type of learning that occurs when we’re rewarded for our behavior.

When employees are rewarded for learning about cybersecurity, they’re more likely to continue learning and practicing safe behaviors.

UPPERSAFE’S DISTURBING MARKETING STUNT

Uppersafe, an internet privacy company, launched a provocative campaign to highlight the risks of unsecured home video security systems.

They staged a scenario where a hacker gains access to a family’s security camera, showcasing the potential consequences of lax cybersecurity measures.

This unsettling stunt aimed to grab attention and emphasise the importance of securing personal devices.

Watch video

KNOWBE4 – THE INSIDE MAN CYBERSECURITY WEB SERIES

KnowBe4 produced The Inside Man, an award-winning, Netflix-style web series that dramatises social engineering, phishing, and insider threat scenarios in short, thrilling episodes.

This format transforms traditional cybersecurity training into binge-worthy internal comms.

Watch trailer

READY TO GET PLANNING?

Big plans don't need to be complicated.

This quickfire guide gives you four clear steps to kickstart your Cybersecurity Awareness Month, without the overwhelm. Whether you're a seasoned planner or tackling this for the first time, just follow these prompts to build a campaign that connects, cuts through, and actually changes behaviour.

PRO TIP: If you're stuck, start small. One good story, told well, can do more than a whole month of wallpaper emails.

PIN DOWN YOUR PURPOSE & AUDIENCE

- What's the one key behaviour, feeling, or message you want to drive? (e.g., more phishing reports, stronger passwords, basic awareness)
- Who are you trying to reach? Office staff, remote workers, frontline, execs? Know their barriers and motivators to interacting with your efforts
- How cyber-savvy are they? Use past feedback or data if you have it

Tip: Focus on one specific, actionable goal like "Spot and report suspicious emails" rather than a vague aim such as "Raise cyber awareness." Clearer goals make it easier to plan, communicate, and measure your campaign's impact

RALLY ALLIES & AUDIT WHAT'S THERE

- Collaborate with cybersecurity SMEs across IT, HR, Legal, and Risk early. They'll help with facts, reach, and credibility
- Ask leaders and managers to champion the message. Security is everyone's business!
- Dig up last year's campaign and training to enable data-driven decisions: What worked? What flopped? What can you reuse or update? Check for training modules, intranet resources, or posters you can refresh. Don't reinvent the wheel!

Tip: Not everyone checks email. Can you use chat platforms, digital signage, screensavers, or physical posters? Don't forget team huddles, webinars, or "lunch and learns" for more personal engagement

MAP YOUR APPROACH

- Pick your channels: email, chat, digital signage, webinars, posters, team huddles
- Choose your tactics based on your audience and culture: simple reminders, stories, quizzes, challenges, or in-person talks
- Don't force "fun" if it doesn't fit. Credibility comes first
- Don't cram everything into the first week of October. Instead, plan weekly themes (phishing, passwords, MFA, updates) to keep things fresh and keep steady momentum

Tip: Build in time for feedback and optimising your approach, so you can tweak as you go

GET PERSONAL, TRACK & KEEP IT GOING

- Share real-life stories or "near-miss" examples from your own people (with their permission)
- Show how cyber risks affect not just the company, but employees' daily lives, families, and reputations
- Decide how you'll measure success: open rates, quiz completions, reports, feedback
- Don't stop in October. Keep the momentum with ongoing reminders, refreshers or onboarding

Tip: Share results with everyone; it builds trust and shows impact

CYBERSECURITY TERMS YOU NEED TO KNOW IN 2025

Vishing – voice phishing
Attackers use phone calls to trick victims into revealing sensitive information, like passwords, credit card numbers, or account details.

Example: *Someone calls pretending to be from IT, saying there's a problem with your account and asking you to "verify" your login info.*

Smishing – SMS phishing
Similar to vishing, but the attack comes via text messages.

Example: *You get a text claiming to be your bank asking you to click a link to "secure your account," but it actually leads to a fake website.*

Pretexting
The attacker invents a fake scenario (pretext) to manipulate someone into giving out confidential info.

Example: *Someone pretends to be a company executive or auditor and asks for sensitive HR or financial data under the guise of "urgent compliance checks."*

Spoofing
Attackers masquerade as a trusted source by faking email addresses, phone numbers, or websites.

Example: *Receiving an email that looks like it's from your CEO or IT department, but it's actually a hacker trying to steal credentials.*

Baiting
Attackers offer something enticing to get the victim to take an action, like clicking a link or plugging in a USB drive.

Example: *Leaving a USB stick labeled "Employee Salaries 2025" in the office, someone plugs it in, unknowingly installing malware.*

Whaling
A high-level phishing attack targeting senior executives or "big fish" (the whales).

Example: *A CFO receives a highly personalized email asking them to approve a fraudulent wire transfer.*

Synthetic fraud
The creation of fake identities or synthetic personas using AI-generated data, such as deepfake videos or voice clones, to deceive systems or individuals.

Example: *Fraudsters use a deepfake video of a CEO to trick a finance team into wiring money to a fraudulent account, like the WPP deepfake incident in the UK.*

Agentic AI
Artificial intelligence systems with the autonomy to make decisions and take actions without human intervention.

Example: *Hackers deploy agentic AI to automatically scan corporate networks for vulnerabilities and launch phishing attacks without manual input.*

Synthetic resilience
The ability of systems to defend against AI-generated threats by using AI-driven defense mechanisms.

Example: *A company implements AI-based monitoring that automatically detects and blocks phishing emails generated by AI, preventing a potential breach before it reaches employees.*

Zero trust architecture
A security model that assumes no user or device, inside or outside the organisation, should be trusted by default.

Example: *A remote employee attempts to access sensitive HR files from an unrecognized device; the system requires multi-factor authentication and restricts access until verified, stopping potential unauthorized access.*

Behavioral biometrics
Technology that analyzes patterns in human activity, such as typing speed and mouse movements, to authenticate users.

Example: *A bank detects an unusual typing pattern on a customer's account login and flags it as suspicious, preventing an impersonation attack.*

REPLY
AVVIO

WANT BACK UP?

You know your people. But if you want a sounding board, more inspiration, or extra hands, Avvio's here. We've helped teams turn cyber campaigns from "meh" to memorable. Ping us if you want to chat!

Cybersecurity is everyone's job, but making it stick is yours. Use this pack for what it is: a jumpstart. Make it yours. And if you want us in your corner, you know where to find us.

Contact: f.briscoe@reply.com

MW MODERN WORKPLACE
2025