Cyber Security Awareness Month Toolkit 2025

Your guide to creating a cyber secure culture for 2025 and beyond. Featuring insights, frameworks, best practices and opinion from cyber security awareness leaders.

CYBER SECURITY AWARENESS MONTH

State of the sector

2025 has seen a seismic shift in general levels of awareness, appreciation and understanding of the risk cyber security breaches present to business, customers and consumers alike.

That the general public could see the connection between a social engineering attack on a popular high-street brand, and their very real inability to buy specific items online or even on the shelves in shops, has helped bring home the consequence of inadequate cyber behaviours and defence.

But what should that mean for cyber security professionals in 2026, and their approach to cyber security training, awareness and human risk management?

We outline our thoughts and some helpful guidance along with the views of other CISO's on the frontline of cyber secure cultures.

82%

of cyber breaches contain HR data such as payroll - Lab1

Source: Lab 1 https://tinyurl.com/4u38f7v6

66%

of CISOs agree that human risk is the top cybersecurity threat their organisation faces

*Source: Proofpoint https://tinyurl.com/42d3h2jj

95%

of data breaches tied to human error

Source: Mimecast https://tinyurl.com/8u9ftm89

74%

of employees would violate a cyber security policy to achieve a business objective. - Gartner survey

Source: Gartner https://tinyurl.com/mt5n5nva

$200k

median ransom payment in 2024

Source: Checkpoint https://tinyurl.com/ms29v28z

Changing behaviours: Positive not punitive

Fear and punitive messaging alone are far less effective than constructive, empowering and contextually relevant strategies that fit with your people's real-world daily routines.

Cyber awareness programmes should allow employees to experiment, witness consequences and gain feedback for their actions, creating a proactive always-on security culture.

Once and done e-learning is not enough, as proven by psychologist Hermann Ebbinghaus - his well referenced Forgetting Curve shows a rapid decline in memory retention 24 hours after learning. However, regular spaced reviews and prompts of information over time can improve long-term retention which helps influence behaviours.

That is why we believe cyber secure organisations are those that intrinsically link cyber awareness to culture where there are multiple moments that trigger the senses helping employees to understand and become more mindful of their actions.

Blue Goose co-owner and strategy director, Ben Watson, has led cyber awareness campaigns for more than 15 years with leading financial, health and retail organisations.

'We know that 'affective security' – the desire to protect an organisation out of loyalty to it – is a powerful weapon when it comes to information security,' he says.

'A business that has embedded a positive culture and belief in its purpose, can leverage that commitment to ask for support on a broader range of issues – including compliance and cyber security.'

Changing behaviours:
Positive not punitive

Consider applying three behavioural science models:

THE COM-B MODEL

Capability requires employees to have the necessary knowledge and skills, incorporating both psychological and physical aspects. This could involve training or workshops to build confidence and competence.

Opportunity includes external or environmental factors (like resources, time, or supportive social norms) that enable behaviour change. You can create opportunities by adjusting work environments or fostering supportive cultures.

Motivation refers to both conscious decision-making and unconscious drives that prompt employees to change behaviors. Motivational interventions may include feedback, incentives, or making desired behaviours more attractive.

THE HABIT LOOP

The Habit Loop model focuse son three stages: cue, routine and reward.

Cue triggers a behaviour, like a notification or meeting agenda prompt.

Routine is the action your employees take, such as sharing feedback or recognising peers.

Reward follows, providing positive reinforcement like praise, points, or progress badges. This loop, when repeated, helps turn intentional actions into automatic workplace habits, making desired behaviours around cyber awareness more consistent and ingrained into organisational culture over time.

THE B=MAP MODEL

Stanford behavioural scientist BJ Fogg says a behaviour occurs if **Motivation, Ability and Prompts** are all present - so a campaign must ensure tasks are simple, appealing and prompted at the right time.

> "It should never be hard for the employees to engage in a campaign. They shouldn't have to go looking for it, it should come to them."
>
> **Ben Watson,** bluegoose

What does a cyber secure culture look like?

There are many factors and responsibilities required across an organisation to successfully embed a cyber secure culture. Ask yourself to consider where you are across these five core characteristics:

LEADERSHIP

Executives and managers demonstrate and communicate the importance of cybersecurity, actively encourage secure practices, and model desired behaviours.

INTEGRATION

Cybersecurity extends beyond IT; every department (from HR to finance to operations) knows its role and duties in keeping data and systems secure.

CONTINUOUS

Ongoing, engaging training (including simulations and practical exercises) ensures staff know how to spot threats like phishing, create strong passwords, and follow policies.

OPENNESS

Employees are encouraged to report incidents and share concerns without fear of blame. Secure culture prioritises learning over punishment and builds trust in internal channels.

ENABLING

Security is framed as supportive of organisational goals - not a barrier to operations - so staff see the value and relevance in their daily roles cyber security.'

Sound of the CISO

We capture voices from a selection of CISOs and cyber security awareness experts about where the focus should be for the year ahead.

"Rapport isn't built in a crisis. CISOs need to engage the board before an attack happens, educating them and establishing trust."

Matt Malone, a board director and former partner, Head of Risk Consulting at KPMG

"Cybersecurity needs to shift from fear to empowerment; culture is the most powerful tool we have."

Jessica Barker CBE, advisory board member, UK Government Cyber Security Advisory Board

"Awareness alone does not equate to security. Organisations must go further by equipping users with the tools, training and support needed to act securely in an increasingly complex, AI-riddled digital environment."

Param Vig, Chief Information Security Officer, Solventum

"CISOs need to frame cybersecurity as a business enabler, not just a cost centre. Show how security investments drive customer trust and long-term resilience."

Myrna Soto, ex-CISO at Comcast and former partner, Head of Risk Consulting at KPMG

"It [behaviours and awareness] has to start at the top: The CEO or whoever has to go through the same process as everyone else, for example if they need a new identity badge."

Sunil Patel, Information Security Officer at River Island

Big six for 2026

1. ONLINE VS OFFLINE. THE RIGHT CYBER INTERFACE.

More than ever before, your workforce is online. They might not be in communal physical spaces very often at all. But this is making your job harder. You have to cater for ever more irregular work-patterns, processes and locations. However, it is making the connection to non-online employees even more complicated.

2. DOUBLE DOWN ON SOCIAL ENGINEERING

The attack on UK retailer M&S was reportedly the result of someone impersonating an employee to gather confidential passwords. It was done well, but better understanding and awareness would have prevented it. Now is the time to leverage that incident to upskill your people.

3. THE E-LEARNING IMPERATIVE

As part of a wider cyber awareness strategy, e-learning is a guaranteed opportunity to interact with all colleagues about cyber security. Your e-learning should be engaging, essential and relevant. Located within the real world of your collagues work, it must resonate with all employees and leave them wanting more.

4. SMALL, EASY AND OFTEN

People are open to cyber training like never before. But it will always want to be on their terms. So, e-learning aside, not big clunky programmes, but short, sharp, memorable interventions that get to the heart of a learning point quick. Little and often.

5. HOME/WORK

The relationship between the two has never been closer or more critical. Often, they're one and the same. So it's a win-win: secure the workplace by securing the home. Employees will thank you for it. And you'll benefit as a result too.

6. GIVE THEM WHAT THEY WANT

And as an exertion to the home/work dichotomy, give your employees what they want further, by helping them help secure their family members. Be that teenage sons, elderly grandparents, or those embarking on a digital journey for the first time.

Family guide for employees: helping their families stay cyber safe

Home life and work life are interchangeable like never before. Which means how family members manage their own information security is more important than ever. Here's a breakdown of the risks your family members face and how you can help them. Take a look, download it, and share it with your people.

Elderly

Phone and Vishing Scams

Be aware of fraudulent calls claiming to be from trusted institutions like banks, tax authorities or government agencies. Scammers often create urgency by threatening arrest, frozen accounts, or legal action. Always verify independently by calling official numbers and never make payments or share details over the phone.

Phishing and Smishing Scams (Email and SMS text Messages)

Do not click on links in unexpected emails or texts claiming suspicious account activity, prize winnings, or urgent requests for verification. Legitimate organisations do not ask for personal details or passwords via these channels. Report and delete suspicious messages without responding.

Fake Online Shopping and Subscription Traps

Avoid websites that offer “too-good-to-be-true” deals, free trials that convert to costly subscriptions, or sellers on social platforms who take payments without delivering goods. Confirm the legitimacy of retailers before purchasing or providing card details.

Grandparent Scam

Scammers impersonate grandchildren or other relatives in distress, requesting urgent money via wire transfer or gift cards. They often ask to keep the call secret to avoid detection

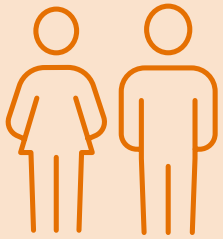
Tech Support Scams

Beware of unsolicited phone calls or pop-up messages claiming your computer or device is infected or compromised. Scammers may try to gain remote access or charge for fake repairs. Official providers never call unsolicited - hang up and never give control of devices to strangers.

Government and Pension Impersonation Scams

Scammers posing as government or pension officials may threaten to stop benefits or demand repayment of bogus debts. They often ask for payment via gift cards, wire transfers, or other untraceable methods. Remember official bodies do not demand immediate payment this way, so always check independently.

Teenagers



Manage Privacy and Oversharing

Teach teens to use strong privacy settings on social media and remind them to “Stop and Think” before posting anything that could affect their reputation or safety.

Verify Online Shopping Deals

Teach teens to check website legitimacy carefully before making purchases; if a deal sounds too good to be true, it probably is.

Use Strong Passwords and Account Security

Help set up strong, unique passphrases for their accounts and enable MFA wherever possible.

Address Cyberbullying Proactively

Encourage open communication so they feel comfortable reporting any harassment or inappropriate behavior online. Reassure them they are supported.

Be Wary of Phishing and Scams

Educate them to recognise phishing attempts and suspicious links, especially in emails and social media messages.

Younger Children / First-Phone Tweens

Understand In-App Purchases and Trials

Explain that “free” apps or trials may lead to unexpected charges; teach them to ask before downloading or approving any purchases.

Teach Safe Information Sharing

Clarify what personal information is and why it should never be shared online, including names, addresses, schools, or phone numbers.

Encourage Open Communication

Prompt children to talk about anything online that makes them uncomfortable or unsure, fostering an ongoing dialogue.

Set Up Parental Controls and Monitoring Tools

Use tools like Google Family Link to monitor online activity while allowing a safe amount of independence. Customise limits based on their age and maturity.

Disable Public Location Sharing

Ensure location tracking is disabled on devices or restricted so only trusted family members can see their location.

Tips for everyone in the family

Protect Passwords and Use a Password Manager

Use password managers to generate and store strong, unique passwords and enable multi-factor authentication on all accounts where possible.

Be Suspicious of Phishing Emails and Calls

Always verify the sender or caller before clicking links or providing any personal information. When in doubt, contact the organisation directly using official contact details.

Regularly Update Devices and Software

Enable automatic updates for operating systems and applications to protect against newly discovered vulnerabilities.

Robocall Scams

Automated calls ask seemingly innocent questions ("Can you hear me?") to record voice samples for identity fraud or deliver false warranty or prize claims. Pause when you answer and wait for the caller to identify themself. End the call if suspicious.

Use Secure Networks

Avoid using public Wi-Fi for personal or financial transactions. Use a VPN or mobile data for secure connections or wait until home networks can be accessed safely.

Clean Up Digital Footprints

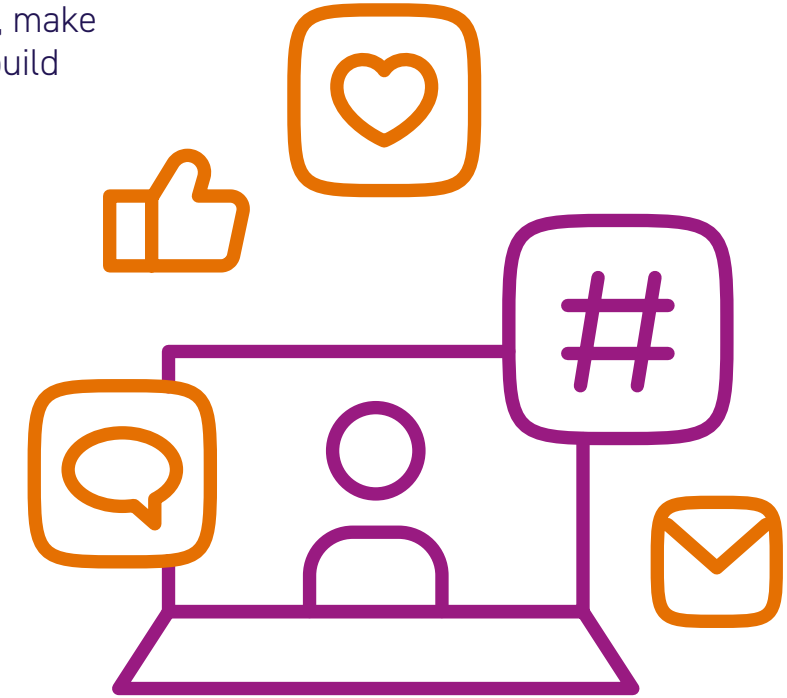
Remove unnecessary apps and email accounts. Delete all instances of sharing confidential identity documents or personal information online where possible.

Inspiring human-centred cyber secure campaigns

Style and substance matter. Your campaign efforts should be memorable, but they must also be meaningful, and resonate with both employees' working and individual lives. Only when both elements are considered and dealt equally are you likely to hit on genuine success.

Your campaigns also need ROI. That can come in many forms, from communication-orientated measures - number of views; likes; completions; comments; forwards - to the more broadly impactful: reduction in clicks; improvement in personal security; fall in data breaches. It's important to decide up front what represents success, make sure you have a benchmark and build your campaign around it.

Below we highlight a selection of impactful campaigns and strategies:



Campaigns that hit the mark...

COMPUTACENTER

Winner: Best campaign

Winner: Plan of the Year

The company needed a new approach to cut through traditional communications to change employee attitudes and behaviours.

Blue Goose worked with them to build their #BeReady campaign which combined live action gaming with training, to win the game and save the company. Employees had to repel an imminent cyber attack by completing training and answering cyber security questions correctly.

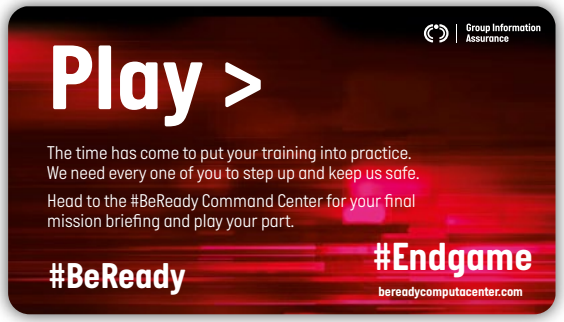
www.bluegoose.co.uk/case-study-computacenter/

IoIC Awards 2021 WINNER BEST SINGLE CAMPAIGN

Cyber Security Awards WINNER

WINNER WINNER


Handle with care
Be safe
Be secure
#BeReady


Group Information Assurance
Play >
The time has come to put your training into practice.
We need every one of you to step up and keep us safe.
Head to the #BeReady Command Center for your final mission briefing and play your part.
#BeReady
#Endgame
bereadycomputacenter.com


Henning Wehn
visits Computacenter


GET CYBERFIT
WITH AGENT B
• Assess your cyber score
• Detox your data
• Build cybersecurity muscle
• Protect your loved ones
• Keep in shape while on a well-earned break

Campaigns that hit the mark...

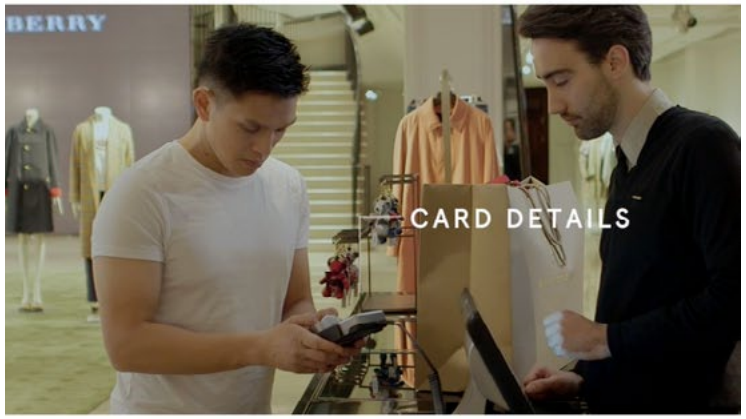
BURBERRY

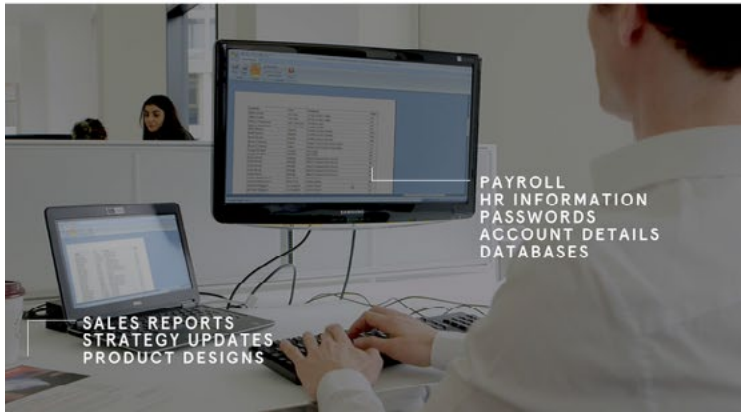
Burberry needed a message and look and feel that reflected their world and resonated with their people. The challenge was to find an approach that would reach across 33 countries and territories. One that would resonate effectively and influence the behaviours of a diverse range of professionals with varying skill sets.

www.bluegoose-cyber.co.uk/work/burberry


DATE OF BIRTH
EMAIL ADDRESS
PURCHASE HISTORY
DRESS SIZE
EMPLOYEE ID
NAME


BE AWARE WHEN WORKING
IN A PUBLIC PLACE


BERRY
CARD DETAILS


PAYROLL
HR INFORMATION
PASSWORDS
ACCOUNT DETAILS
DATABASES
SALES REPORTS
STRATEGY UPDATES
PRODUCT DESIGNS

Campaigns that hit the mark...

RICHEMONT

Richemont required a single security/safety awareness camapaign and elearning programme.

We developed the BE AWARE BE SECURE campaign - a long-running to campaign to engage its global workforce of 29,000 employees in 12 languages.

A creative storytelling approach was adopted commissioning British crime author Paddy Magrane.

www.bluegoose.co.uk/case-study-richemont/


Against the clock - episode 2
BIG LOSS
Martina loses more than her phone
BE AWARE BE SECURE


AGAINST THE CLOCK
SEASON 2
BE AWARE
BE SECURE
SEASON FINAL
A CHAOTIC OPPORTUNITY
WATCH THE LAST EPISODE NOW

Contact

blue goose for expert support in delivering your cyber and information security initiatives.

Ben Watson
Managing Director
benw@bluegoose.co.uk

CYBER SECURITY AWARENESS MONTH