Reignite your cyber security knowledge: tools to boost your expertise

Our toolkit is designed to point you in the direction of industry leading insights and conversations. Arming you with the knowledge to engage with your people and senior leaders confidently.

CYBER SECURITY AWARENESS MONTH

The importance of cyber and information security education

As the advancement of technology grows so does our reliance on it to make our lives easier and more efficient.

An increased loss of information from the use of AI tools, the sophistication of phishing tactics growing and outdated systems from the sheer volume of apps we are required to remember to update. Aside from this:

- The UK Government has proposed the implementation of a new cyber security and resilience bill to strengthen the UK's defences. The bill underscores the importance of investing in regular training and awareness programmes for employees.
- EY's latest global cyber security leadership insights study spoke to leaders from across the globe and different sectors. The report highlighted that in the wake of AI, prioritising cyber security training to equip employees against cyber threats is a top priority.
- SANS (leading security awareness network) recently published their report which highlighted the key human related risks organisations are most concerned about - with social engineering at the top at 89% and AI fourth at 31%.

53%

of businesses reported being attacked once a month or more in 2024.

*Source: UK Cyber Security Breaches Survey

Cyber security training reduces security risks by

70%

*Source: keepnetlabs.com

Follow that voice...

Blogs of interest that will make you think twice:

IRA WINKLER

What should human risk management really be?

Ira is a leading voice in cyber security and his phrase “are we just putting lipstick on a pig?” referencing awareness and human risk management is a key point.

FORRESTER.COM

The silent threat in cyber security: burnout

Jinan Budge globally leads Forrester’s awareness, behaviour, and culture coverage in security. Her research reveals our overemphasis on technology, neglecting the core of our cyber-defenses: people and its impact on their wellbeing.

SANS.ORG

The CISO’s guide to AI: Embracing Innovation While Mitigating Risk

Insight into how CISO’s can manage, guide, and lead AI’s adoption whilst balancing progress and protection.

Campaigns that hit the mark...

The National Protective Security Authoritative (NPSA)

Think before you link

The NPSA launched an app allowing users of social media and professional networking sites, such as LinkedIn and Facebook, to better identify the hallmarks of fake profiles used by foreign spies and other malicious actors.

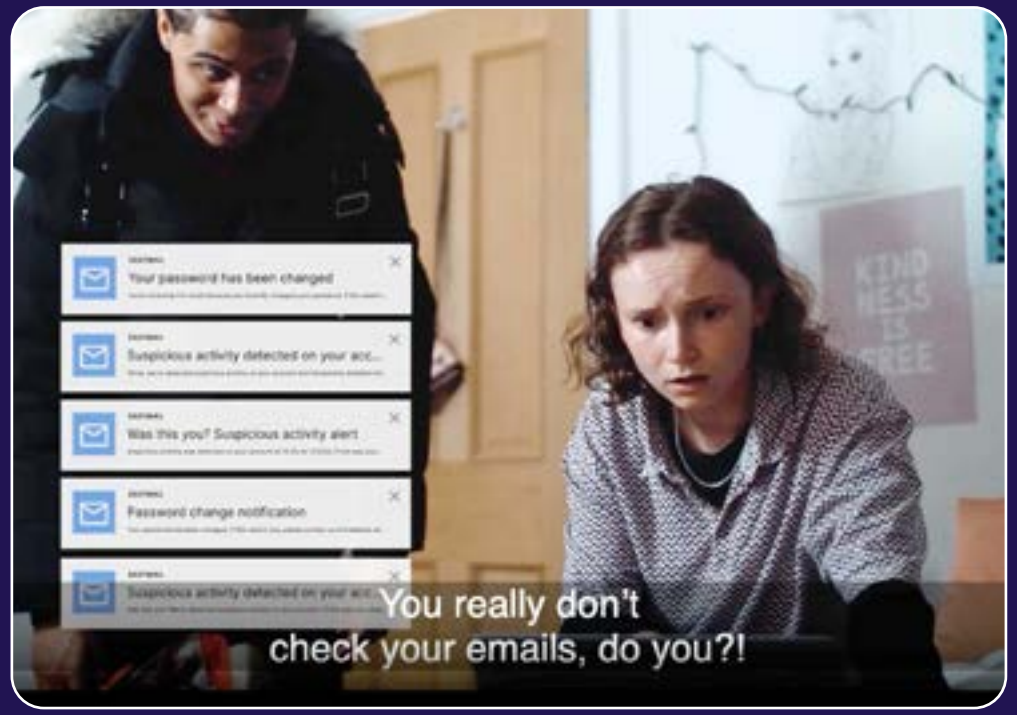
The app has been developed with behavioural scientists to include features such as a profile reviewer, which will help individuals identify potentially fake profiles and report anything they deem suspicious. They also created a series of videos that effectively illustrated the impact fake profiles could have.

Campaigns that hit the mark...

NATIONAL CYBER SECURITY CENTRE

CyberFirst Navigators

CyberFirst Navigators is a campaign designed with young people in mind, but its content and approach make it a valuable resource for adults seeking to improve their knowledge. It also helps bridge the generational gap in digital literacy and enable adults to have more informed conversations with young people about online safety.



Campaigns that hit the mark...

BANK OF ENGLAND

IoIC shortlisted for game changer

Blue Goose worked with the BoE to use the strength of the Bank's walls as a creative metaphor in their awareness campaign.

The walls represent the historical security of the Bank – but they also underline how security threats have changed. Hackers can attack from afar so physical defences alone are no longer enough.

www.bluegoose.co.uk/case-study-bank-of-england/

SHORTLISTED

SHORTLISTED

IoIC Awards

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.

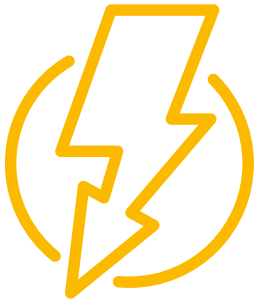
www.bluegoose.co.uk/case-study-computacenter/

IoIC Awards 2021 WINNER BEST SINGLE CAMPAIGN

Cyber Security Awards WINNER 2021

WINNER WINNER

Resources that deliver a shock factor...



HAVE YOU BEEN PWNED?

Web security expert Troy Hunt created the widely used site Have I Been Pwned to help users see where their email address has been compromised. A simple tool to see where your credentials have been part of a data breach.

MAP YOUR SECURITY BEHAVIOURS TO RISK RELATED OUTCOMES

SebDB is a cyber security behaviour database. It was originally built by CybSafe, but is now maintained by cyber security professionals on a global scale.

WHAT ARE THE MOST COMMONLY USED PASSWORDS?

Nordpass have been mapping out password habits for the past 5 years and you can filter by country and / or industry to see the top used.

DATA ON THE GO

CIFA's award winning video features a live stunt in a coffee shop capturing the reactions of members of the public as their personal data is revealed. Think Starbucks, but next level.

HUMAN FACTOR SECURITY WITH JENNY RADCLIFFE

Jenny Radcliffe, known as "The People Hacker," is a leading ethical hacker who has collaborated with FTSE 100 companies and appeared on ITV's This Morning.

Her podcast, The CISO's Voice, explores social engineering practices, the threat landscape, and the importance of resilience in leadership. She interviews CISOs from various sectors, including legal and healthcare.

Contact

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

Alison Jiggins
Lead Cyber Consultant
alisonj@bluegoose.co.uk