Cybersecurity awareness training

Employees can often be the weakest link in an organisations IT security. They are frequently exposed to sophisticated phishing and ransomware attacks resulting in serious cybersecurity breaches. We see these breaches reported to us on a daily basis, where an end user has suddenly found that their password has been compromised, or they've been tricked into making a payment to a fraudulent bank account. Training employees to recognise these attacks and avoid them is vital.

Did you know Cyber Training is now mandated?

The Information Commissioners office (ICO) is the UK body that is responsible for prosecuting organisations that fail to keep data safe. In December 2021 the ICO issued new guidance saying that they expected that all staff and volunteers that have access to data, should receive cyber awareness training as part of their induction, and before they are given such access. Furthermore, they mandate that training should be ongoing for all employees, and that an organisation should be able to demonstrate completion of training and management of non-attendees.

What is KnowBe4's training?

Delivering regular cybersecurity training, that is engaging, effective and that can be evidenced and managed, can be quite an admin challenge. That's why ramsac have partnered with KnowBe4 – who offer the world's largest library of cyber training, on a platform that automates most of your management obligations.
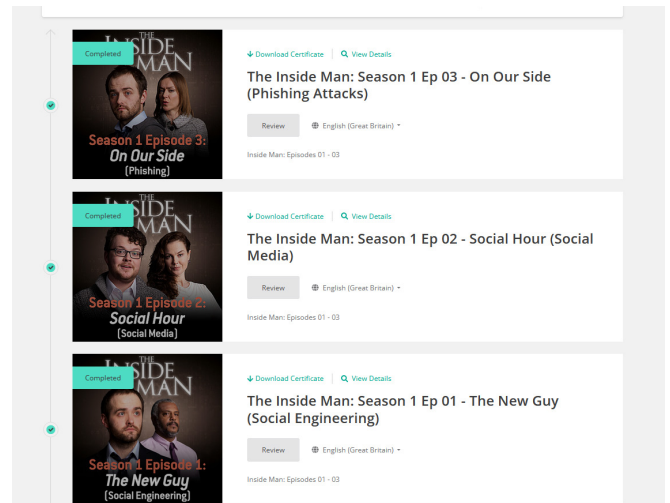
KnowBe4 offers a vast library of content, including interactive modules, videos, games, posters and newsletters. Organisations can tailor training campaigns which can be scheduled to land in a user's inbox each month. The interactive training gives users a fresh new learner experience that makes learning fun and engaging, with our own favourite being a series of learning that feels more like watching a Netflix drama! And in the background, the platform records who has and hasn't completed the learning, and reminds non attendees – and their manager, if they are falling behind.

KnowBe4
Human error. Conquered.

ramsac
the secure choice

Why is KnowBe4 so effective?

This is not tech heavy, dryly delivered content. The most popular resource is 'The Inside Man' an award-winning original series that delivers security awareness principles embedded in each episode that teach your users key cybersecurity best practices and makes learning how to make smarter security decisions fun and engaging. From social engineering, insider threats and physical security, to vishing and deepfakes: 'The Inside Man' reveals how easy it can be for an outsider to penetrate your organisation's security controls and network. But it's delivered in a way that's entertaining – meaning users won't resent the activity and learning happens without feeling like an arduous task.

And because it's delivered regularly for a few minutes each month, it keeps the subject matter fresh and at the front of mind – and it stays up to date with changing threats and trends.

- **Engaging, enjoyable learning**

- **Delivered in 10 minute monthly chunks**

- **Trackable and managed via a portal that ramsac will report on for you**

Test and train

Cybersecurity training is vital (and mandatory) for organisations, but it is also really important to test employees outside of the training environment, to understand the effectiveness of the training. Using KnowBe4 Phish testing, ramsac will carry out simulated phishing attacks, ensuring that every user receives a very realistic phishing email at least 4 times a year (although this can be increased to monthly). The emails mimic real phishing emails and if the user clicks on a link they will be taken to a safe web page, that highlights what they have just clicked on and offers them an immediate online training session on how to spot attacks in the future. We recommend organisations combine both Phish and Security Awareness Training as you should always test AND train users. If organisations use both solutions, the results of phish tests can be used to adapt training, to provide extra training for those that need it.

To be truly secure – you must train your users to recognise how they can keep your organisation secure and test them to ensure they understand.