SECURITY AWARENESS: TOP 5 METHODS TO HELP STAFF RETAIN INFORMATION

As an Information security professional, you understand the importance of a robust learning programme: well-constructed content that informs and engages staff. Nevertheless, if learning retention isn't achieved then your programme will fail.

What is Learning Retention?

Search on the web and you'll find various definitions of what learning retention is and how to achieve it.

For us, in the business of instilling a culture of Information Security Awareness, we have managed to distil the message somewhat:

It's the art of getting information into users' heads and keeping it there.

What learning and retention strategies can you deploy to ensure staff retention rates?

5 Methods for knowledge Retention

Below are retention techniques you can use in your staff awareness programme that will ensure content is not just learned but helps instil a culture.

1. Tell a Story: Give them information they can relate to

Relate learning topics that are applicable to your trainees' home and working lives.

Information security policies and procedures are boring. Let's first face up to this undeniable truth. The endgame is to get employees to comply with your organisations' information & cyber security policies & procedures. But simply telling staff that they need to comply is proven not to work.

Instead, you need to get staff engaged in broader concepts of information security. The easiest way to engage people is to focus on stuff that they care about. Such as the security of their finance records, data that social media companies hold on them, what online retailers know about their shopping habits and what information Google can see about you when you initiate a search. It's these sorts of facts that resonate with users. Why? Because if they care — the information will stay in their heads. When you have them on your side, you can deliver the critical work-related information they need and the chances of them retaining it have increased tenfold.

2. Quiz Them

Now that the learners are listening, you need to test & quiz them.

Running imaginative and thought-provoking quizzes not only helps to cement the information into learners heads but it also provides you with metrics to demonstrate a return on investment. Employers should consider the culture of their organisation when developing quizzes. For example, would your employees react well to a learning league, complete with medals of achievement or could they conversely feel patronised?

3. Relate the learning material to the real world

Develop learning materials that are related to trainees' everyday occurrence will help them connect.

As we mentioned in point 1, the information you are imparting needs to resonate and elicit a positive reaction. Similarly, the content being delivered should bear some resemblance to their own working experiences and environment. Simply avoiding using 'Americanisms' for example, in a UK based workplace is a good first step. Including screen-shots of your work systems' functionality, referring to your own policies and mentions of your industry sector all help to decrease user apathy and increase retention.

4. Repeat: Active participants are more likely to remember

Organisations so often categorise learning as a 'tick box' exercise.

When compliance and best-practice advice stipulates employees should undergo learning, it's very tempting from a financial and logistical viewpoint to throw some eLearning in front of them, get them to confirm they have done it and move on. This is a particularly dangerous path to take in relation to Information Security when you consider that around 80% of all data breaches have a human element to them and that the consequences of such can have a majorly detrimental effect on the organisation. Regular, imaginative and varied training should be considered an ongoing process.

5. Review, measure and demonstrate

Design your learning content that requires staff to review and summarise what they have learned.

But also allow you to review, measure and demonstrate the effectiveness of the programme. As mentioned previously, use regular quizzes to gather metrics and confirm the information is getting into their heads. Also, run real-world testing scenarios against the learners, this will demonstrate that the learning is working and give you the data in order to fine-tune the content accordingly. Showing year-on-year progress and improvement also validates the training in the first place and provides you credence in front of the board.

Next Level Security Awareness Learning

The key to ensuring learning retention is to expand the way a brain absorbs and holds on to information – ***it's getting information into users' heads and keeping it there.***

INSPIRE
EMPOWER
ENGAGE
MEASURE
get in their heads.

eRiskology™ by
RISK CREW

Ensure learning is retained with the eRiskology™ programme — the most engaging learning system for today's learners.

INSPIRE

Face-to-face Workshops present staff with current security topics they can relate to.

EMPOWER

Interactive Training Narrated by subject matter experts who presents current methodologies and best defences.

ENGAGE

Continual Learning Stream of videos, webinars, podcasts, infographics, bulletins, tips and alerts.

MEASURE

Get Cultural Awareness & ROI Results. KPIs & simulated social engineering attacks confirm behavioural changes.

LEARN MORE ABOUT eRiskology™

Contact Risk Crew for more information

☎ +44 (0) 20 3653 1234 ✉ information@riskcrew.com 🌐 riskcrew.com