Security awareness training:

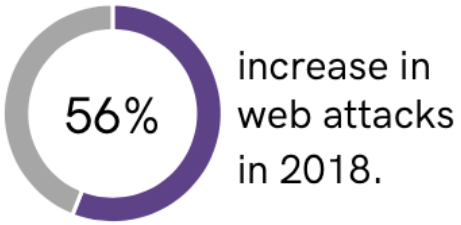
3 big reasons why an annual webinar is not enough

Given that 49% of organisations have faced critical security consequences as a result of employee errors, the need for security awareness training for all employees is undeniable, but how frequently must this be delivered to impactfully reduce threats? This article outlines why, in order to mitigate against cyber attacks, training must be delivered significantly more frequently than on an annual basis.

1. Security threats are evolving rapidly

Germany's AV-Test Institute holds one of the world's largest collection of malware samples and, ***each day***, over 350,000 new samples are registered. With such an incredible pace of change, security awareness training material must be continuously reviewed and communicated to ensure that employees are receiving the very latest intelligence to help them defend against the very latest cyber attacks.

Delving into the detail, it's immediately clear how such a speedy evolution of threats is impactful on the end user. Symantec's 2019 Internet Security Threat Report revealed that web attacks increased 56% over the course of last year, with enterprise ransomware up 12% over the same period. A growth in attack numbers brings increasing diversification and sophistication of tactics from cyber criminals: prior security best practice can quickly become out of date. As a result of



the 400% growth in SSL based phishing in the second half of 2018, previous advice that employees should trust websites where there's a padlock in the address bar must be updated. Similarly, Microsoft Office documents now make up 48% of malicious email attachments vs 5% a year previously: annual updates are demonstrated to be insufficient to keep employees abreast of the kind of attacks they should be looking out for.

Given that 34% of organisations now consider unaware employees to be their ***biggest*** security vulnerability, it's crucial that adequate time and resource is allocated to ensuring that end users are provided with the latest know-how they need to help them mitigate against the cyber threats they're facing today.

2. Your employees won't remember the training

In order for end users to act as your first line of defense, it's crucial that training content remains forefront of mind so this can be recalled instantaneously in the face of malicious activity.

So how frequently does training need to take place in order to deliver this level of retainment? Well, the Ebbinghaus 'Forgetting Curve' is a commonly accepted theory of memory retention which proves that as much as 79% of training content is forgotten within 31 days of delivery without reinforcement. This is very bad news for an annual program of security training: should an employee face an attack just ***one month*** after completing the course, almost ***4 out of 5*** of the tell-tale signs of malicious activity they learnt then will now be missing, significantly impeding their ability to prevent cyber criminals from

gaining a foothold in your organisation.

Annual security awareness sessions are also problematic due to the sheer volume of information that needs to be communicated. From phishing and password attacks to social media malware and data protection, the growth and evolution of threats means that annual webinars may begin life as a short and succinct session but often quickly evolve into something long, unwieldy and unengaging. Having reviewed over 6.9 million educational sessions, an MIT study concluded that the optimal length of a video based training session is less than 6 minutes. Further research of 1.3 billion video plays by Wistia indicated that the first 3 minutes of a video achieve considerably greater engagement than those which follow. These factors are a firm advocation of a 'little and often' approach to security awareness training in order to maximise recall: annual training simply doesn't cut the mustard.

Another key practice that should be used as an element of a security awareness learning journey is testing: this has been demonstrated to improve recall of knowledge by as much as 38%. Follow up of annualized or induction-based security training is often lacking but facilitating a simulation or a 5 – 10 question test covering the key learnings can have a considerable impact on an end user's ability to remember crucial security know-how should they face an real-life attack. It's also a great way to measure that users have fully understood and absorbed their training.

3. The regulators say so

We all love to hate them but the regulators and analysts base their advice on the latest cyber security intelligence and they are unanimous in their endorsement of a program of regular, continuous security awareness training.

The UK's National Cyber Security Centre includes 'User Education and Awareness' in its top 10 steps for cyber security, insisting that 'all users should receive ***regular*** training on the security risks to the organisation', these sentiments being echoed by ISO 27001 (A.7.), Control 17 from the Center of Internet Security ('Implement a Security Awareness Program') and analyst house, Gartner.

Both ISO 27001 and the CIS doubly emphasise the regularity of the training by insisting that organisations must 'plan and implement a programme of awareness, education and training ***throughout the employment lifecycle (not just at induction)***' and that 'an effective cyber defense training program is ***more than an annual event; it is an ongoing process***' respectively.

Gartner, too, encourages an ongoing program of security awareness training, stating that

"Implement a programme of awareness, education and training throughout the employment lifecycle - not just at induction"

ISO 27001

'security and risk management leaders must invest in tools that increase awareness and influence behavior that supports security business objectives through computer-based training', going on to endorse 'solutions in the market that are capable of producing measurable improvements in employee security behavior'. Gartner are not alone in supporting an ongoing program of training which demonstrates continuous improvement, with ISO 27001 requiring that the organisation 'carry out skills, knowledge, competence and awareness assessments', whilst the CIS mandate that 'training is repeated periodically, measured and tested for effectiveness'.

About Purplephish

Looking to quickly and easily empower your employees to prevent cyber attacks? Purplephish's security awareness and real-world phishing simulation solution is proven to reduce user susceptibility to today's biggest threats.

Demonstrate the reduction in risk across your organisation via our industry-leading suite of dashboards as your users undertake a regular, ongoing training program, encompassing tried-and-tested methods guaranteed to ensure key security knowledge is forefront of mind should they come under attack.

Sources: State of Industrial Cybersecurity 2018, Ebbinghaus 'Forgetting Curve': A Contribution to Experimental Psychology, EY Global Information Security Survey 2018 – 2019, 2019 Symantec Internet Security Threat Report, MIT Study: How Video Production Affects Student Engagement, Wistia Research (https://meetmaestro.com/resources/blog/how-long-should-your-video-be), Test-Enhanced Learning: Taking Memory Tests Improves Long-Term Retention (Henry L. Roediger, III, and Jeffrey D. Karpicke, Washington University, St Louis)