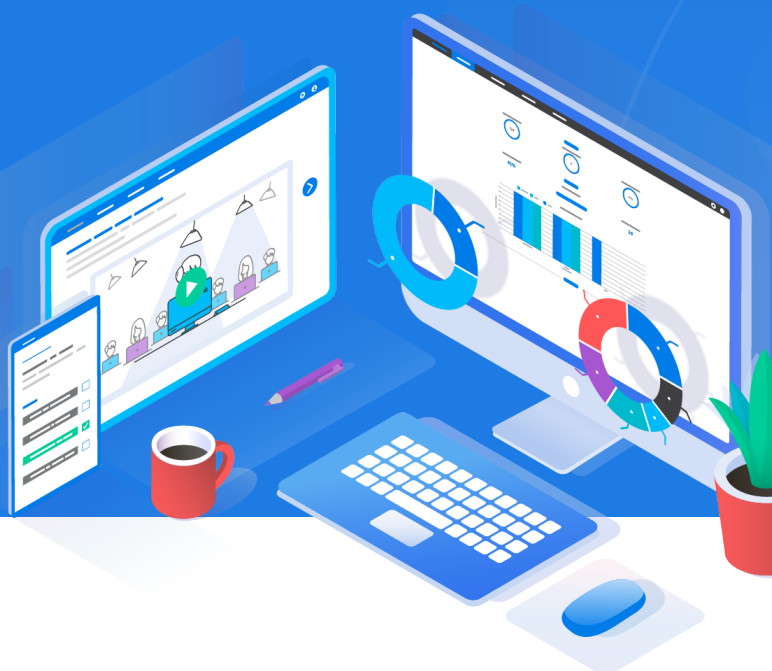
THE ULTIMATE CYBER SECURITY AWARENESS TRAINING TOOL



Dunedin

It's very much common knowledge that while the huge shift in remote working has improved employee satisfaction and productivity, it has also brought with it a whole new set of problems, security being one of them.

While the majority of the population are tackling the pandemic together, cybercriminals see the massive change in the way we work as their opportunity to strike. With the world coming out of their protective office bubble and setting up in a home office environment, it's becoming much more difficult to ensure security is replicated in everyone's homes and across everyone's devices.

Dunedin IT

HUMAN ERROR IS THE ONE THING NO SECURITY SOLUTION CAN PREVENT

While there is a great abundance of security products to ensure hackers can't gain access to your customers' computer/laptop, cyber criminals can still sometimes manage to slip through the net and are successful purely down to human error. Here are the different ways in which cyber criminals can get to your customers:

PHISHING

Phishing emails are the quickest ways for cyber criminals to act. A phishing email is sent to a large number of recipients at random, with the expectation that only a small amount of the percipients will respond. These sorts of emails encourage the recipients to click malicious links that encourage them to enter their details, in which can then be used for fraud or identity theft.Spear-phishing emails are what it says on the tin. **SPEAR PHISHING**

Spear-phishing emails are what it says on the tin. They are designed to intentionally target a single recipient in the organisation. Cybercriminals spend time on researching colleagues and job titles in organisations, and will pose as them asking them to click links, send information etc. For example, posing as the CEO asking a team member to purchase a gift card for a client.

EDUCATING YOUR CUSTOMERS' EMPLOYEES IS KEY

It's unlikely that your customers have carried out full, extensive cyber security training for their employees to avoid the above. This is because a lot of SMBs believe that due to their size, they could fall victim to a cyber-attack. However, SMBs are the main target for cyber criminals for this exact reason. They know that SMBs are the demographic least likely to expect it and therefore be prepared for it.

usecure, a global provider of innovative security solutions, identified this and therefore created a simple, cost-effective training tool that your customers and their employees can use whenever, from wherever they are.

Dunedin

Usecure is made up of different components to ensure every area of cyber security is covered:

ULEARN | AUTOMATED SECURITY AWARENESS TRAINING

Drive secure user behaviour with automated security awareness training. Deliver bite-sized video and interactive security awareness training, tailored to each user's unique vulnerabilities.

UPHISH | AUTOMATED PHISHING SIMULATION SOFTWARE

Monitor and reduce user vulnerability to sophisticated phishing. Learn how susceptible your users are to ultra-targeted spear-phishing campaigns or enable continual simulations and monitor vulnerability trends over time.

UBREACH | EMAIL EXPOSURE CHECKER

Identify and safeguard your users' exposed email accounts. uBreach monitors thousands of data dumps, paste sites and breached data forums, locating exposed email accounts before they can be leveraged for targeted attacks.

UPOLICY | SIMPLIFIED POLICY MANAGEMENT

Keep users up to date with proactive policy management software. Ensure users are up to date on relevant policies.

FOR MORE INFORMATION CONTACT YOUR ACCOUNT MANAGER TODAY ON 0330 058 1701

SALES@DUNEDINIT.CO.UK

Dunedin