ADVERTISING FEATURE

Digital security solutions

Angelo De Silva is founder of IT consulting firm AlphaClick IT Solutions.

The importance of cyber awareness

Despite the growing cost of data breaches, and the growing regulatory obligations when it comes to privacy and security, many Australian organisations still fail to include cyber awareness training when it comes to bolstering their cyber defences.

Cyber security incidents continue to increase in frequency, scale and sophistication, while hurting their targets more than ever.

The average cost of each cyber breach globally hit a record $6.2 million in 2022, up 2.6 per cent from the year before, according to IBM Security.

The rise was even more significant in Australia, jumping 3.4 per cent to hit an average of $2 million per breach.

After stolen or compromised credentials, phishing scams are the vector most favoured by attackers (and often the vector by which credentials are first compromised). Rather than targeting exploits or defeating technical defences, phishing attacks primarily succeed by tricking staff into doing their bidding.

Clumsy generic phishing attacks are easy to identify and are often picked up by spam filters before they land in inboxes.

However, more sophisticated spear-phishing attacks choose their victims with care, targeting them with well-crafted emails delivered at the most opportune moment.

The number of spear-phishing attacks has increased nearly sevenfold since the start of the pandemic, according to McKinsey.

Cybercriminals are taking advantage of the increasing number of remote workers, who may be more susceptible to phishing scams due to lax security hygiene and a habit of collaborating with colleagues and bosses primarily through email and chat apps rather than face to face.

Rather than just targeting the big end of town with spear-phishing attacks, cybercriminals are turning their attention to SMEs, which are often seen as easy targets.

The consequences can be severe, with around 60 per cent of SMEs going out of business within six months of a data breach or cyber attack, according to the United States' Securities and Exchange Commission.

Despite this growing threat, organisations of all sizes often forget about the human element when assessing their cyber defences, says Angelo De Silva, founder of AlphaClick IT Solutions, an Australian IT consulting firm.

While there is growing awareness of the need for improved cyber security, many organisations focus on the technical aspects, such as addressing the Australian Cyber Security Centre's "Essential Eight". These recommendations extend from installing patches and blocking Office macros to restricting administrative privileges and enabling multifactor authentication.

While the Essential Eight offers a solid baseline for any organisation looking to improve its cyber security posture, De Silva says it must be accompanied by cyber awareness training to ensure that staff can act as an effective last line of defence against attacks like spear phishing.

"When you raise the need to arm their people with the knowledge to detect and thwart attacks like spear phishing, many organisations will tell you that they can't spare the time for even a one-hour training session to cover the basics," he says.

> "If you stop and think about the impact of a successful cyber attack in both lost time and money, that one hour seems like a small price to pay to keep your business safe."
> Angelo De Silva

"If you stop and think about the impact of a successful cyber attack in both lost time and money, that one hour seems like a small price to pay to keep your business safe."

Along with the ability to spot spear-phishing scams coming from external sources, cyber awareness training can also help staff thwart business email compromise (BEC) attacks which seemingly come from within.

By compromising email accounts in order to impersonate business leaders, business email compromise attacks aim to trick underlings into handing over sensitive data, paying bogus invoices or transferring money offshore.

"Cyber awareness training isn't just about teaching people to spot these kinds of attacks, it is also about teaching them what to do if someone suspects they have fallen for one of these attacks," De Silva.

"A swift and precise response can make a significant difference to the amount of havoc that attackers can wreak if they do manage to trick one of your people."

As businesses look to curb costs amid ongoing economic turmoil, they can make the mistake of thinking that technical counter-measures such as spam filtering and firewalls eliminate the need for a more well-rounded cyber security strategy which incorporates aspects like cyber awareness training and data backups.

No single layer of defence is foolproof. Instead, different cyber security measures are designed to work in unison to offer the most robust protection, De Silva says. True cyber risk mitigation does not just focus on defending against cyber attacks, but also on minimising the impact of successful attacks.

"Today, data is one of any organisation's most important assets and a cyber breach can often leave a business unable to get back on its feet," he says. "When all else fails, data backups can save the day.

"Looking to save money by skimping on something like backups is a false economy when it leaves your entire business at risk."