

Over 40 per cent of SMEs have been attacked

New research reveals that the frequency and success of phishing attacks on SMEs, over the last twelve months has shot up

‘With 97 per cent of people unable to identify a sophisticated phishing email, Williams further emphasised that employee training is essential’

Shocking new data on the impact of phishing has been revealed by new research amongst 250 IT decision-makers at UK SMEs. CybSafe, the intelligent security awareness, behaviour and culture solution provider, has revealed that 43 per cent of them have experienced a phishing attempt through impersonation of staff in the last 12 months. Of those impersonation phishing attempts, it was discovered that two-thirds (66 per cent) had suffered a successful attack.

Businesses in CybSafe's survey admitted to taking minimal action to correct this: less than half of those featured in the research (47 per cent) claimed to already have a cyber security training and awareness programme in place.

Interestingly, respondents saw email phishing as a much greater threat than phone phishing. Pitted against nine other potential threats, email phishing was perceived to be the second most pressing threat (37 per cent). By contrast, phone phishing was believed to be the least (8.8 per cent) urgent threat to business.

Oz Alashe, CEO, CybSafe says: "The continued dominance of phishing presents a huge opportunity for the channel. Businesses often aren't running a security awareness and training programme. Those that are, often aren't seeing benefit from it; their people are still being phished, and their human cyber risk isn't visibly being reduced. For the channel, both of these scenarios present an opening."



CybSafe's report echoes warnings in the Government's own Cyber Security Breaches Survey published earlier this year, which found that phishing attacks were the most common security attacks on businesses and charities in the UK.



Human instinct

Holly Williams, (pictured) Technical Director of cybersecurity firm Secarma, a cybersecurity specialist and penetration tester, has further cautioned businesses against relying on human instinct to defend against these phishing attacks.

Speaking at a recent security event in Manchester she urged: "Your users shouldn't be your business' first or last line of defence. There should be several lines of defence between me sending an email to the user and it being delivered. A user shouldn't be able to completely derail business operations just by opening an email."

Williams advised that rather than relying on employee action, businesses should increase visibility on their internal network to better deal with subsequent attacks.



"If you know the roles employees are supposed to be performing and improve your awareness of commands being executed, you can then detect when users appear to be behaving unusually and start implementing behavioural analytics to combat phishing attacks."

Commenting that phishing attacks play a part in 90 per cent of all data breaches, she continued: "Phishing is a go-to for attackers, but there's confusion over where it sits in the attack chain. The end result of a phishing attack is very often not just something simple like gathering credentials; it's one part in a larger story to gain access to systems."

With 97 per cent of people unable to identify a sophisticated phishing email, Williams further emphasised that employee training is essential in recognising the signs of a malicious email, but if businesses are leaving their phishing defence down to human reliability, then they will be far more vulnerable to attacks.

A panel of fellow security experts highlighted the increasing sophistication and volume of phishing attacks, and consequently the growing risk to UK businesses. Last year, 14 billion phishing emails were sent – two for every person on the planet.

Stephen Crow, Head of Defensive Securities and Compliance at hosting firm UKFast, explained, "We've seen the complexity of phishing attacks increase dramatically in the first half of this year. Fake chains are being created between board and senior directors asking staff to perform tasks and act fast."

He added: "Often employees are scared to question the request if it has come from higher up. There are lists of email addresses you can purchase online or even obtain for free. It's a numbers game for hackers: the more you send out, the more likely you are to catch somebody."

Advice to businesses concerned over the increasing number and convincing nature of fake emails is to limit the assignment of admin privileges, particularly for SMEs where one person could be responsible for multiple tasks or roles, to lower the number of employees with access to sensitive data who are more of a target for threat actors.

James Turland, Cybersecurity Manager at professional services network PWC, encouraged businesses to implement defences at three stages: "People, process, technology; you need to put interventions at each of these and not be complacent." ■



About Cybsafe

CybSafe is a British cyber security and data analytics company. CybSafe's artificially intelligent software platform leverages science, data and cognitive computing technology to provide the world's first truly intelligent awareness, behaviour and culture solution. CybSafe is headquartered at Level39, the prestigious technology community based in Canary Wharf, London.

About UKFast

UKFast provides dedicated servers, cloud services and colocation to more than 5,000 government, public sector and commercial organisations, with a wide-ranging product portfolio including Infrastructure as a Service, DR as a Service and its cloud offering, eCloud®. Alongside its product range, UKFast has five fully owned, custom-built data centres and its cybersecurity arm Secarma specialises in ethical hacking and penetration testing.

The family of businesses owned by founders Lawrence and Gail Jones employs 450 people, with UKFast directly employing more than 350.

Contact details

www.cybsafe.com
www.ukfast.co.uk