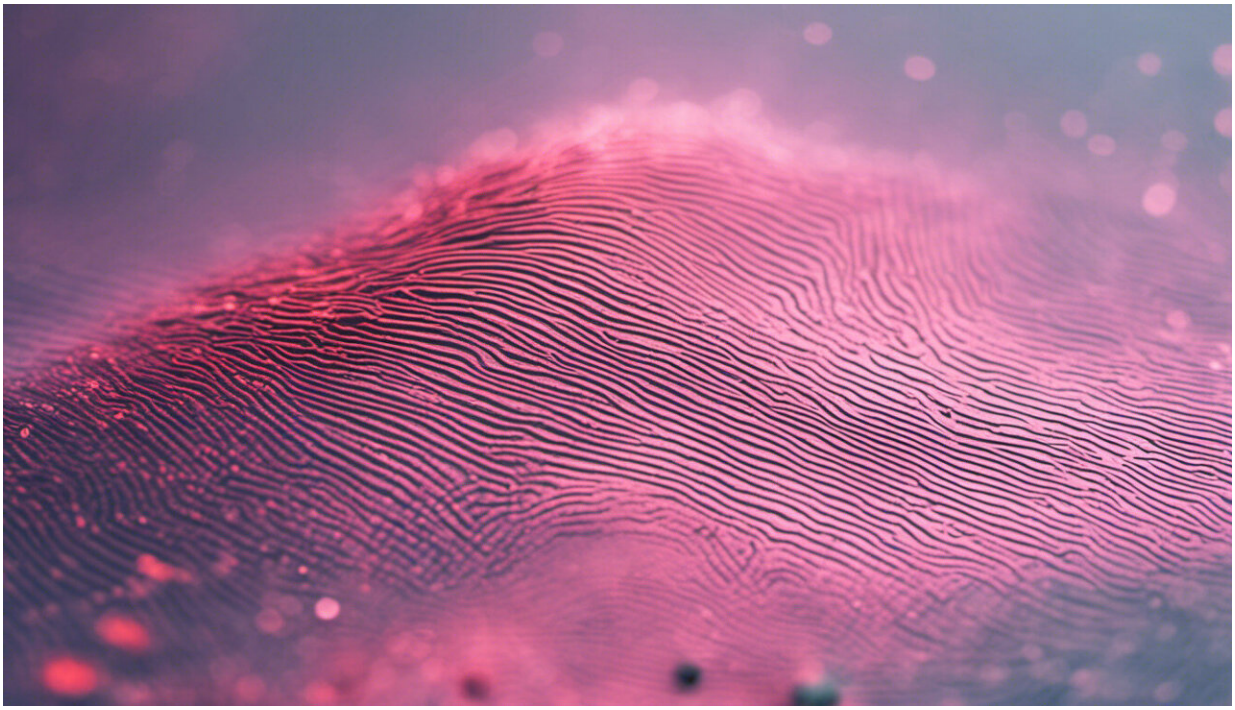
Phishing scams are becoming ever more sophisticated

March 16 2017, by Emma Williams And Debi Ashenden



Credit: AI-generated image (disclaimer)

Companies are bombarded with phishing scams every day. In a recent survey of more than 500 cyber security professionals across the world, 76% reported that their organisation fell victim to a phishing attack in 2016.

These scams take the form of emails that try to persuade staff to download malicious attachments, click on dodgy links, or provide personal details or other sensitive data. A targeted "spear" phishing email campaign was blamed for instigating the recent cyber attack that caused a major power outage in Ukraine.

Even more worryingly, phishing attacks are now the most popular way of delivering ransomware onto an organisation's network. This is a type of software that typically encrypts files or locks computer screens until a ransom is paid. The amounts demanded are generally quite small, meaning that many organisations will simply pay the ransom without, of course, any guarantee that their systems will be unlocked. In the face of these phishing attacks, employees have become the frontline of cyber security. Reducing their vulnerability to phishing emails has therefore become a critical challenge for companies.

Disciplinary problems

As organisations struggle to contain the threat, one idea that is gaining traction is the potential use of disciplinary procedures against staff who click on phishing emails. This ranges from the completion of further training to formal disciplinary action, especially for so-called "repeat clickers" (people who respond to phishing emails more than once). They represent a particular weak point in cyber security.

This is not necessary – nor, indeed, is it a good idea. For a start, we still don't understand what causes people to respond to phishing emails in the first place. Research is only just scratching the surface of why people may respond to them. Email habits, workplace culture and norms, the degree of knowledge that an individual has, whether an employee is distracted or under a high degree of pressure – there is varied understanding of online risks, all of which may influence whether people are able to identify a phishing email at a particular point in time.

Unfortunately, this means that there are still more questions than answers. Are some job roles more vulnerable due to the types of task that they engage in? Is training effective in educating staff about the risks of phishing attacks? Are employees able to prioritise security over other workplace demands when necessary? Among these unknowns, focusing on a disciplinary approach seems premature and risks sidelining other efforts that may be more effective.

Targeted phishing attacks are also becoming increasingly sophisticated and difficult to spot, even for technical users. Recent attacks (on PayPal and Google, for example) demonstrate this.

It is now incredibly easy to craft a fraudulent email that looks very similar, if not almost identical, to a legitimate one. Spoofed email addresses, the incorporation of accurate logos, correct layouts and email signatures, can all make it difficult to distinguish a phishing email from a genuine one.

Keep calm and carry on

Phishers are also very good at creating scenarios that maximise the likelihood that people will respond. They instil a sense of panic and urgency by things like mimicking authority figures within an organisation to create a sense of crisis. Or they focus on the potential negative impact of failing to respond. When we acknowledge the increased sophistication shown in the phisher's arsenal, it becomes more difficult to justify penalising employees for falling victim to their trickery.

Simulated phishing attacks are often used as a way of increasing awareness among employees. While there have been suggestions of improved click rates following such programmes, a comprehensive evaluation of the range of potential impacts on employees is lacking.

And some research points out the potential that employees merely give up trying to deal with the threat as it seems like a losing battle.

A culture of blame and victimisation may also make employees less willing to admit to their mistakes. Either of these outcomes is likely to damage the relationship between an organisation's security personnel and its other employees. In turn this will have a negative impact on the organisation's security culture. It suggests a return to an authoritarian role for security, which research shows is a step backwards if we are to fully engage employees in security initiatives.

Mitigating an organisation's exposure to phishing attacks represents a complex and evolving challenge. The recent #AskOutLoud campaign by the Australian government to encourage people to ask for a second opinion when they receive a suspicious email provides a good example of how this challenge can begin to be addressed. It encourages conversation and shared experiences. Using this approach can ensure employees feel empowered and encouraged to report suspicions, a vital element in maintaining cyber security.

Research is clear that cyber security depends on open dialogue, participation from employees when it comes to developing solutions and trust between an organisation's security personnel and other staff. As the old cliché goes: you're only as strong as your weakest link. It's therefore imperative that all employees are supported in order to be an effective front line in their organisation's defence.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation