CYBERSECURITY

Five ways to stop phishing in its tracks


Nelen/Shutterstock

With rapid remote-working rollouts being implemented across industries, enterprises have never been so susceptible to cyberattacks, with phishing among the most common threats. Here are five ways organisations can keep themselves safe in the coronavirus era

Kate O'Flaherty

1 Keep up to date with changing risks

The coronavirus crisis has resulted in many office employees working from home and with this has come a surge in phishing attacks. As remote working became the norm in April, Google's Gmail blocked 18 million COVID-19-related malware and phishing emails every day.

With phishing attacks on the rise, it's important businesses are up to date with the threats they face. Recent phishing attempts are often COVID-19 themed, with threat actors impersonating government organisations such as the World Health Organization to solicit fraudulent donations or distribute malware.

One type of phishing, called spear phishing, sees attackers target users via an email from a trusted sender to lure them in. This type of phishing attack often targets remote workers, with hackers impersonating an organisation's admin or human resources team to encourage users to click on a malicious link or transfer money.

"To help prevent these kinds of attacks, organisations need to set up email authentication policies as a de facto security measure for their domain," says Andy Kennedy, engineer at Google Cloud.

2 Train remote workers to spot phishing attempts

Employees are a firm's first line of defence from phishing attacks. They need to understand why phishing is a threat, why they specifically might be targeted, what a phishing attempt looks like and what to do if they see or click on a suspicious link, says Amanda Finch, chief executive of the Chartered Institute of Information Security

This requires training. "The more comprehensive the better," says Finch. For instance, instead of simply emailing advice, organisations should share examples of phishing emails that show employees what to look for and stage mock attacks to demonstrate how easy it is to be fooled.

Cybersecurity training is essential, agrees Professor Kevin Curran, Institute of Electrical and Electronics Engineers senior member and professor of cybersecurity at Ulster University. "There has recently been a new movement where security teams send phishing emails containing fake malware to their employees, which when activated simply leads users to a site highlighting their mistake and educating them on the dangers," he says.

3 Use two-factor authentication and strong passwords

Cybercriminals often make phishing attempts to steal users' credentials and access sensitive company data. It's therefore a good idea to implement two-factor authentication as an extra layer of protection, says Carl Wearn, head of e-crime at Mimecast. "This should be considered by every security leader."

A solid extra layer of protection is provided by security keys, such as the Yubico YubiKey, which are proven to prevent phishing, says Andrew Shikiar, executive director of the FIDO (Fast IDentity Online) Alliance. He cites the example of software giant Google, whose 85,000 employees use security keys to access online services. "Not one has been successfully phished," he says.

In addition, good password hygiene is integral to help stop phishing attacks. "Ensure employees don't mix personal and work credentials, and use a good password manager to generate sufficiently complex passwords," says Harman Singh, managing consultant at Defendza.

At the same time, users should be discouraged from using the same password across multiple services. If one password is revealed in a data breach, this will allow an attacker to gain access to multiple accounts.

4 Assess and improve technology controls

While training employees is crucial, technology can help to stop remote workers falling victim to phishing attacks. This is especially important when one mistake could lead to the compromise of entire business systems and expose sensitive information. "If technological controls are weak, an employee clicking on a legitimate-looking email could lead to a compromise of the underlying system," says Defendza's Singh.

Therefore, as well as examining admin rights, securing systems and implementing network segmentation, Singh recommends enhancing email security with technical controls. "These can work together in a layered structure to ensure senders' legitimacy and make sure email isn't spoofed," he says.

In addition, keep anti-virus and anti-malware software up to date, says Ulster University's Curran. "Some phishing emails can be detected by anti-virus tools," he says. "However, it is important teams inform management or the IT department when they receive a suspicious email. This allows IT teams to identify how an email managed to get through their system and consider updating their software."

5 Create the right culture

It's true that employees are a firm's first line of defence, but at the same time it's important not to blame users if a phishing attack does get through. "Provide users with an easy way of reporting these attacks," says Kevin Breen, director of cyberthreat research at Immersive Labs.

Javvad Malik, security awareness advocate at KnowBe4, agrees. "It is vital employees are given easy and convenient ways to report issues," her says. This could be as simple as a button to allow employees to easily and quickly report a suspected phishing email.

But if remote workers are tricked into opening a malicious email, firms should be careful not to create a culture where they do not report it for fear of reprisal. "If employees can spot and report phishing attempts, it can actually help you when you might have missed something otherwise," says Breen. "It's not all about the technical. While people can be a weakness, they can also be your strongest asset."