520.743.7554
info@computerdimensions.net
www.computerdimensions.net

Phishing Awareness Training Neglect Comes Back to Haunt Businesses

In a volatile risk atmosphere, nothing has been more of a threat than phishing. This one hub is the starting point for most of today's most devastating cyberattacks from ransomware to credential compromise. Google has registered 2,145,013 phishing sites as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months). That's not slowing down either. After a banner year for phishing risk in 2020, it was hard to believe that there was any more real estate for phishing to climb. Unfortunately, that wasn't the case – and companies who slacked on security awareness training during the pandemic are paying the price.

Phishing is still experiencing triple-digit growth in 2021 – up almost 300% over 2020's record-breaking numbers in May and June respectively – and companies in every sector are getting hammered with attacks. An astonishing 80% of IT professionals in a recent survey said that their organizations have faced an increase in the number of phishing attacks that they're combatting in 2021. Unfortunately, more phishing attempts has translated into more phishing attack disasters for many companies. An estimated 74% of respondents in the same survey said that their companies had been successfully phished in the last year.

Phishing attacks against businesses are commonly fueled by dark web data, and there's plenty for cybercriminals to choose from. A flood of records stolen in past data breaches has made its way to the dark web including an estimated 22 million new records in 2020 alone. Experts had already estimated that 65% of the information on the dark web at the start of 2020 could harm businesses and this influx of stolen information provides abundant fresh fuel for cybercrime, increasing everyone's risk.

This is important for businesses to remember: the top cause of data breaches is still human beings. Specifically, errors made by employees. It is far too easy for cybercriminals to concoct compelling phishing messages that can fool employees into handing over credentials or opening a ransomware-laden document – 48% of malicious email attachments are Office files. Employees also fear missing out on an important message far more than they fear unleashing malware or falling for a phishing attack. An estimated 45% of employees click emails they consider to be suspicious anyway "just in case it's important."

In a survey of responses to phishing simulations, every industry had problems with employees clicking on a phishing email. CyberNews reports that 1 in 3 employees are likely to click the links in phishing emails, and 1 in 8 employees are likely to share information requested in a phishing email.

Phishing resistance and security awareness training is a proven method to mitigate phishing risk. Companies that engage in regular security awareness training that features phishing resistance have up to 70% fewer cybersecurity incidents. But many companies have deprioritized training in the chaotic scramble of the business world in the last year, even as phishing risk climbed and employees who were

520.743.7554
info@computerdimensions.net
www.computerdimensions.net

not trained to work remotely took the plunge. Plus, even if training is happening it's done in such a desultory way that employees don't receive enough training on the correct threats. All in all, far too many companies are courting disaster by neglecting training.

The danger to your organization is real and it is growing. Employees at companies of any size in any industry are prime targets for cybercrime because they will click phishing email. The numbers don't lie: employees are regularly getting and falling for phishing emails every day. In a recent study of North American staffers, experts discovered that:

- 67% of clickers (13.4% of overall users) submitting their login credentials, also up substantially from 2019, when just 2% submitted their credentials.
- The Public Sector and Transportation sectors struggled the most, posting a click rate of 28.4%.
- The Education and Finance & Insurance sectors performed considerably better than others, with click rates of 11.3% and 14.2%, respectively.
- Users in North America struggled the most with the phishing simulation, posting a 25.5% click rate and an 18% overall credential submission rate. This means that a little over 7 out of every 10 clickers willingly compromised their login data.

A little over 95% of IT professionals who responded to a survey said that their organizations have security awareness and phishing resistance training programs. Those programs can range from high-quality ongoing classes to occasional ad hoc meetings. But a much smaller percentage of those companies are invested in making sure their employees complete their security awareness training. Only 30% of the surveyed pros could say that 80% or more of their company's employees had completed any formal security awareness training courses. That means that companies understand the benefits of security awareness training but are often challenged in running and delivering it, wasting time and money.

But just running a few training courses for your staffers isn't enough to foster strong cybersecurity awareness. Making sure that every staffer from the C-Suite to the interns is taking and refreshing training courses regularly is vital to gaining and keeping awareness high and cybersecurity incidents caused by phishing low. In a report from consulting giant Accenture detailing the characteristics of a cyber resilient organization, researchers placed the ideal number of training courses for employees each year at 11, or just a little under one per month. This prevents courses from becoming rote but still keeps the topic fresh in employees' minds. The bottom line is cybersecurity awareness is a necessary operational cost of business and should not be overlooked. Don't make a cybercriminal's job easier.