20
Aug

Cyber Security Awareness (/category/cyber-security-awareness) | **Phishing (/category/phishing)**

Why Is Phishing Awareness Training Important?

The reality is simple. Phishing (https://terranovasecurity.com/what-is-phishing/) is more prevalent than ever before.

An estimated three billion fraudulent emails (https://use.valimail.com/rs/936-SWF-978/images/Email%20fraud%20wave%20prompts%20shift%20to%20DMARC%20enforcement.pdf) are sent out every day as part of phishing schemes, resulting in the FBI’s Internet Crime

Complaint Center (IC3) (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf) receiving over 241,000 phishing-related complaints in 2020. Adjusted losses for affected organizations topped $54 million.

And, according to the most recent Gone Phishing Tournament results (https://terranovasecurity.com/gone-phishing-tournament-webcast/), one in every five individuals clicks on phishing email links.

As the threat landscape becomes increasingly complex, the inherent value of security awareness training (https://terranovasecurity.com/security-awareness-training/) continues to rise. However, information security courses can't guarantee that employees have the knowledge and skills they need to detect and avoid real-world phishing threats.

Practical training, including gamified content and simulated phishing attacks, is essential for effective information security.

This blog post will provide an in-depth look at phishing awareness training, its key components, and how you can easily launch these initiatives, regardless of your organization's industry, size, or region.

What is Phishing Awareness Training?

Phishing awareness training refers to a training campaign that educates end users on specific phishing threats they may encounter in their daily lives. Effective phishing awareness training typically leverages phishing simulations (https://terranovasecurity.com/phishing-simulation/) to deepen employee knowledge, allowing them to spot warning signs and report phishing threats in a safe environment.

Simulating phishing attacks on your workforce also allows you to assess your organization's maturity regarding its security awareness posture and optimize future iterations of campaign learning material and components. Testing your users and measuring where their security awareness knowledge and skills are at any given point strengthens data protection long-term.

To facilitate the overall behavior change process using free phishing simulation benchmarking data, download your copy of the 2021 Phishing Benchmark Global Report (https://terranovasecurity.com/gone-phishing-tournament/), co-sponsored by Microsoft.

The Importance of Phishing Awareness Training

Phishing threats are continuously evolving and are becoming much harder for the average person to detect. Many well-known organizations are targeted by cyber criminals and must navigate the negative fallout of successful data breaches.

But what does that mean for your employees? Are they really at risk of being targeted by a cyber criminal?

The following story reveals some of the devastating effects phishing attacks can inflict on the unsuspecting user. It also sheds some light on how phishing simulations can help build security resilience in your workforce.

***

Sam gets about 40 emails in her work account on a typical morning. She goes through the emails, deleting unwanted ones, reading ones of urgency, sending some out, scanning newsletters, opening shared documents, and checking her schedule for the day. All standard stuff.

These days, however, Sam faces her inbox with grim determination. Two weeks ago, she was under attack by a team of hackers whose goal was to phish Sam's company. Sam got an email with a link to another site that appeared almost identical to the company name, but the domain ended with ".org" when the site's URL should have been ".com."

Sam did not notice the subtle difference. After clicking on the link, she was directed to a page that looked like the original website, which asked her to input her username and password to exchange a downloadable document. Sam complied.

Our unfortunate employee's inbox was flooding with unrecognizable emails within three days. Sam's account was getting hit with unexpected messages. It became full of messages with subject lines like "Autoreply: Out of office" or "Delivery Failure" and messages from unknown senders asking her to stop emailing them.

After informing leadership of the suspicious activities, with a single glance, the CISO identified that Sam's email account was taken over and that the hacker used it to send phishing messages to other targets.

This event instilled paranoia in her. Every email from an unknown recipient could have been fake. Every shared link, a trap.

Does this scenario sound familiar to you?

If so, you are undoubtedly asking: How do I avoid this from happening again?

Phishing Awareness Training: 3 Phishing Simulation Essentials

Simulating phishing is an efficient way to test your employees' skills and measure their progress. A test provides data on which employees have been baited by the phishing email by clicking on the corresponding links. Your users can learn to identify suspicious emails and apply security awareness best practices by having the chance to experience a phishing attack.

So, how do you run an effective simulation?

1. Get Buy-In From Your Internal Leaders

The first step to any good phishing simulation is getting approval from management. Notify the few people and instruct them on handling calls from users who report the phishing message.

Don't forget, a user's reaction once he detects a phishing message, actual or simulated, should always be the same: Alert someone or contact the IT Service Desk. During simulations, you may not want to notify users that it is a test and inform them that the IT department is handling it.

2. Craft an Actionable Phishing Simulation Strategy

Next comes planning. Create a plan not to send tests too frequently, as your employees will come to expect them, and don't send them too infrequently since you need to gather statistics, draw reports, and always keep users sharp.

Don't send phishing emails to the entire company at once, which might spark suspicion. Instead, please send them to specific departments. For example, to the invoicing department, imbue your email with an urgent tone so that your employees act with haste. Hackers commonly use this technique to get people to click on links or download attachments.

Start thinking like a cyber criminal. What is going to get your employees clicking? Subject lines that include the terms 'unpaid invoice', 'free,' or 'exclusive offer' draw users' attention – greater the chances of falling prey to the attack.

3. Leverage Your Data-Driven Insights

During your phishing simulation campaign, track email open rates, attachment downloads, information disclosure, and clickthrough rates. Draw reports on the number of users who have fallen for the phishing attack and how many employees have reported the incident.

This phishing simulation data is essential to growing and optimizing your training program. It will give your leadership insight into the effectiveness of behavior change initiatives and take them to the next level. Your organization can use this intel to fine-tune its long-term strategy to align with larger business goals.

Recap

As you conduct your phishing awareness training, you add value to your overall security awareness initiative. By testing your employees' knowledge and skills, you contribute to behavior change at a more extensive scale. Users are encouraged to train and become more informed and alert in cyber security matters.

Do you have experience in simulating phishing attacks on your workforce? If so, were you successful in getting victims? What group did you target, and which type of phishing emails did you distribute? These are some of the many questions that will arise when deploying a phishing simulation campaign.

Free Phishing Benchmarking Data to Train Your Cyber Heroes

For more information on how your organization's click rates currently stack up against your peers, and for additional insight into how you can construct the best phishing awareness training program, download the latest Phishing Benchmark Global Report!

READ THE FULL REPORT (https://terranovasecurity.com/gone-phishing-tournament/)

Share:

Newer
How Security Leaders Can Use Multi-Factor Authentication to Protect Sensitive Data (/multi-factor-authentication-protect-sensitive-data)

(/blog/)

Older
How to Ensure Your Organization Enjoys a Cyber-Secure Summer (/why-summer-school-is-in-session-for-security-awareness-training)