Phishing Awareness Training Turns User Liabilities into Assets

The statistics give an unmistakable message. Phishing attacks continue to succeed, and no amount of security technology provides 100 percent protection. To defend against hackers, organizations must strengthen cyber security by implementing effective phishing awareness training. While users can sometimes prove the weakest link, they can also become the strongest deterrent.

A successful phishing attack depends on humans taking the bait. And because attackers imitate trusted sources, they can appear quite convincing. For instance, using information easily obtained online, an attacker can pose as a trusted source with inside information. But when users know what to look for, they can stop attackers in their tracks.

Phishing Awareness as Part of Security Awareness

First, successful phishing awareness training must present the right information. Users need to know:

- What phishing attacks involve – Phishing involves using fraudulent emails or websites to trick users into acting in a certain way. This could involve clicking a malicious link, wiring funds or giving up privileged information. Hackers often strengthen their attack using spoofed email addresses and realistic-looking websites.

- Signs of a phishing attack – Teach users to recognize telltale signs of a phishing attempt. These can include a sense of urgency, slight errors in the sender email address or URL, poor grammar or spelling and unsolicited attachments.
- What to do when they spot a phishing attempt – Make sure users know how to report a phishing attempt (successful or not). This will help security personnel ensure that other users in the organization know to be prepared.

Train Users at All Levels

All users in the organization need to complete cyber security training, including phishing awareness. In fact, high-level employees with privileged access often prove the most likely targets for a targeted phishing attack. No one gets a free pass!

Leverage Multiple Channels for User Phishing Awareness Training

Each user learns in their own way and at their own pace. Consequently, one-size-fits-all training will not have the desired effect. Instead, utilize different teaching methods for phishing awareness training.

For example, an organization might offer monthly webinars, combined with online training modules that users complete within a given timeframe. Managers might include a short training segment as part of regular departmental meetings. Training format could consist of interactive games, quizzes, or classroom instruction.

Use Repetition to Cement Learning

Attackers continually up their game, employing more sophisticated techniques over time. To defend effectively against increasingly subtle attacks, organizations need to keep phishing awareness constantly on the radar. At a minimum, security experts suggest that companies conduct phishing awareness training quarterly.

Keep It Simple, Relatable

An overly technical training seminar will only leave end users bored and confused. Enlist presenters who deliver training in a way that is both relatable and understandable. In addition to substantial knowledge about cyber security, presenters need to be skilled in sharing that knowledge. Likewise, apps or other resources used in training must be easy to navigate.

Bring It Home with Phishing Simulations

Once users learn about the dangers and signs of a phishing attack, they need a chance to practice what they have learned. Simulated phishing campaigns provide that opportunity in a controlled environment. When users click on an attachment or link in a simulated phishing email, they receive just-in-time training.

Deliver Enterprise-Level Phishing Awareness Training with MXINSPECT

To help organizations get the most out of their training, eMazzanti offers targeted security awareness training as part of MXINSPECT. MXINSPECT uses a people-centric approach designed to change employee behavior, reducing the chance of breaches. Targeted, just-in-time training and phishing simulations teach users how to recognize and respond to phishing attacks.