Targeted Security Awareness Training Delivers Large Return on Cybersecurity Investment

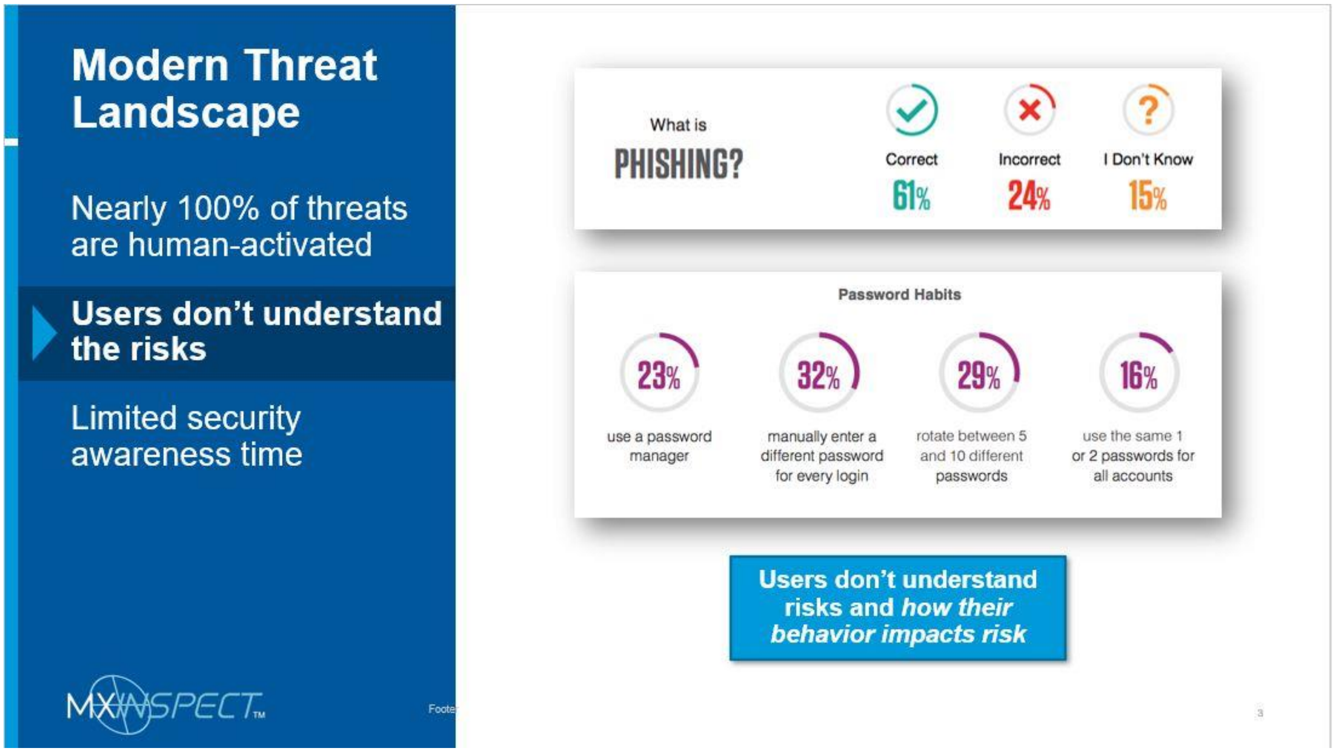
McAfee recently estimated the global cost of cybercrime at nearly $1 trillion. In response, companies have increased security spending while strengthening cloud security, network monitoring and threat detection. But to truly combat cyber threats, a comprehensive cybersecurity solution must include targeted security awareness training.

The People Challenge

Despite millions spent securing networks and deploying state-of-the-art cybersecurity tools, the biggest threat to an organization remains the human factor. When employees re-use passwords, click unsafe links or browse the internet, they introduce vulnerabilities. In fact, over 90 percent of cyberattacks occur because users click malicious links or share information.

Hackers know these human weaknesses, and they exploit them with great success. For example, using artificial intelligence, criminals can determine how best to manipulate human behavior. They then use that knowledge to bypass security measures and infiltrate organizations.

Common strategies involve luring employees through scare tactics or appealing to their greed. One employee may see a banner warning them that their computer has been infected by spyware, for instance. Another employee might receive an email with a tempting offer for a free product that seems to come from a legitimate source.



Modern Threat Landscape

Nearly 100% of threats are human-activated

Users don't understand the risks

Limited security awareness time

What is PHISHING?

Correct	Incorrect	I Don't Know
61%	24%	15%

Password Habits

23%	32%	29%	16%
use a password manager	manually enter a different password for every login	rotate between 5 and 10 different passwords	use the same 1 or 2 passwords for all accounts

Users don't understand risks and *how their behavior impacts risk*

Effective Security Awareness Training Offers Greatest ROI

Because employees represent the weakest link, investing in security awareness offers the greatest opportunity for significant return on investment. Relative to other cybersecurity measures, employee training costs very little. But it can reduce successful malware infections and phishing attacks by as much as 90 percent.

To achieve that success rate, security awareness training must reach end users at the right time and engage them in the right ways. The training approach must also ensure that users retain the information they learn. This involves revisiting the typical approach to security training.

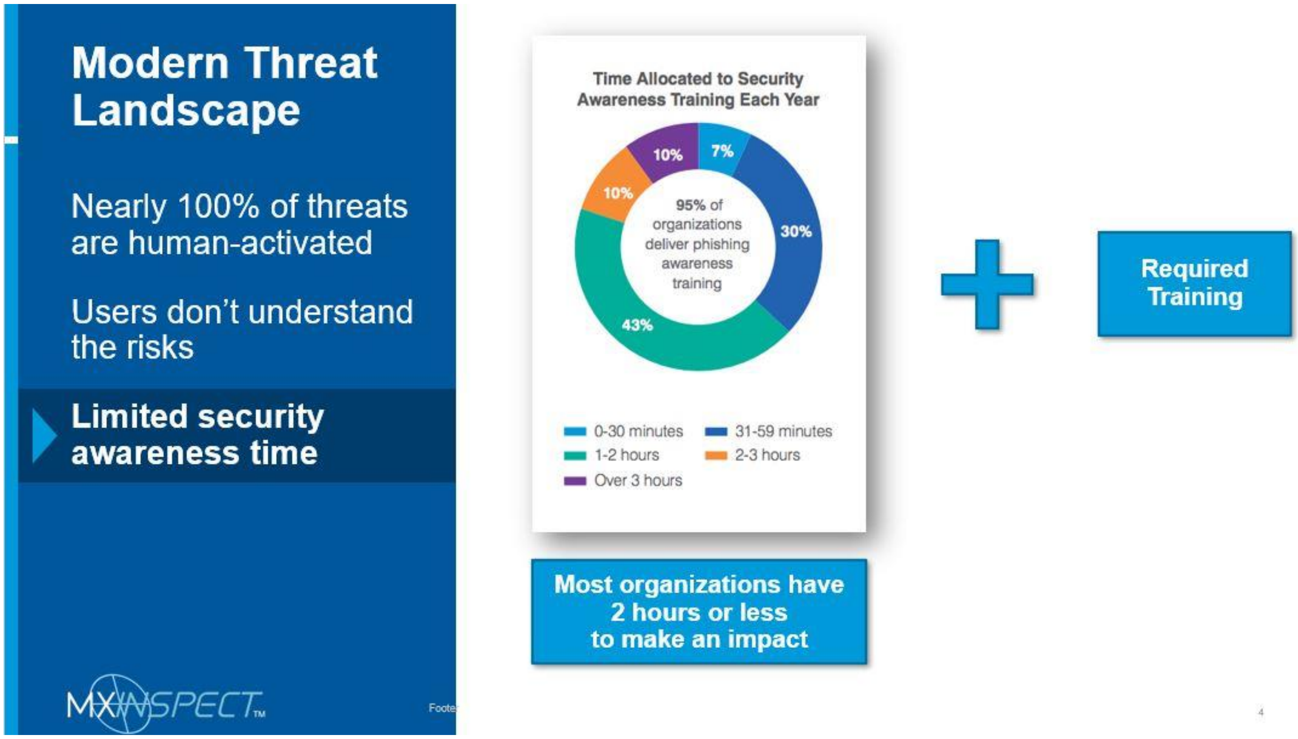
Training Built on Proven Learning Science Principles

Cybersecurity training programs typically fail for a couple of key reasons. In the first place, most organizations and their employees have a limited time to devote to developing security awareness. Consequently, users listen half-heartedly to annual training and quickly forget what they have learned.

eMazzanti takes a more targeted approach with MXINSPECT training. First, phishing simulations help identify the employees who most need the training. Then, content tailored to specific groups of users ensures that the right people get the right training at the right time. Finally, short, interactive training modules keep users engaged and increase retention.

Assess User Training Need with Phishing Simulations

To determine the users most in need of security awareness training, eMazzanti offers ThreatSim® phishing simulations. With thousands of simulation templates covering current attack trends, an organization can assess users relative to a variety of threat types. Users that fall for a simulated attack then receive targeted training.



Modern Threat Landscape

Nearly 100% of threats are human-activated

Users don't understand the risks

Limited security awareness time

MXINSPECT™

Foote

Time Allocated to Security Awareness Training Each Year

Required Training

Most organizations have 2 hours or less to make an impact

4

Interactive Training Modules Change Behavior

The MXINSPECT Security Awareness training modules employee a unique, game-based format to address multiple learning styles. Each lesson takes just five to fifteen minutes, and users can complete the training on any connected device. Available in 35 languages, the training modules stay relevant with continuous updates to a wide range of topics.

For example, available training includes a fundamental series of modules to educate users to recognize and protect against email threats. Another series of modules addresses password protection and multi-factor authentication. Additional training modules cover mobile device security, social networking, safe web browsing and more.

User Education Essential to Effective Cybersecurity

For over two decades, the cybersecurity experts at eMazzanti have helped thousands of organizations secure critical intellectual assets. Knowing that no security program will succeed without exceptional security awareness education, eMazzanti includes engaging, effective training as an integral part of its MXINSPECT solution.