WEBROOT
Smarter Cybersecurity®

Webroot® Security Awareness Training

Why Businesses Need Security Awareness Training

Introduction: Why now?

When someone is in need, our initial reactions are usually to help however we can. But in the modern cybersecurity landscape, this trusting nature is routinely exploited by criminals looking to take advantage of end users. They utilize tactics like misinformation and partial truths, mimicking of trustworthy sources, and fake social media profiles, among many others, to prey on their victims. We are constantly being socially engineered by those who want to harm, undermine, and steal from us.

Today, every form of communication can be compromised for someone else's gain, which means you need to be aware of all the ways you can be manipulated. Additionally, you should question the motives behind every communication you receive. Unfortunately, a certain degree of conscious paranoia is necessary to protect yourself from modern cyber threats.

This is not just an issue off-the-clock. When we're at work, we often feel as though we're in a secured environment, which can lead us to let our guard down. But the reality is that employees must remain aware that they are their organization's first line of defense against cyberattacks.

Perhaps the greatest proof of this has been the growth in ransomware over the past three years. More than 90 percent of ransomware attacks use social engineering tactics like phishing emails to get their foot in the door. For more information click here.

That's why cybersecurity awareness training is a necessity. Training and educating users on security threats and best practices, then ensuring that they understand and follow the behavioral requirements they are taught, is a vital component of any business's security strategy.

Forewarned is Forearmed

Large enterprise organizations and those working in heavily regulated industries like Finance have been targeted by hackers for years, which has required them to implement IT security strategies that expand far beyond basic technology and policies. They've had to view IT security as a multi-layered strategy.

There are three main building blocks of a layered IT security strategy: people, processes, and technology. The human element, however, is not limited to the technical IT staff; rather, it consists of every end user in the organization. This is an important security layer often dubbed the "human firewall".

For these reasons, security awareness training has been a tool employed by large organizations for years. But due to the cost, it hasn't been as commonly used among small- to medium-sized businesses (SMBs). But as we've seen, the need for continuous workforce security training has grown exponentially due to the rise in frequency and impact of phishing and ransomware attacks. IT security truly is a shared responsibility in every organization, but it isn't always treated as such. That's part of the reason that some security practices and technology are no longer a nicety, but a necessity. Security awareness training—particularly short, relevant, computer-based training—is a proven way to arm users with knowledge.

What makes security awareness training effective?

In 2011, the ISACA.org Journal[1] published a study on the results of security awareness training. They found that:

- Continuous training is more effective than one-off training
- The methods and content used in the training were the biggest contributors to effectiveness
- Training that focused on compliance was successful
- Measuring and monitoring compliance (and non-compliance) was important to customers

The continuous monitoring and training capabilities are paramount. "Some public-sector studies have shown that more than 80 percent of breaches occur not because of malicious intent, but because employees claim not to know about a policy or because they simply ignored it."[2]

From a user perspective, relevance was the key contributor to the effectiveness of the training. Relating training to real-life experiences was a powerful teaching tool. Conversely, there is research indicating that stale, lengthy, or unengaging content can reduce the efficacy of training courses. Ineffective training fails to offer interactive elements or user involvement. Training content also fails when it panders to fear or is too trite for its users.

For security awareness training to be effective, the content needs to be relevant to the user, engaging, and as brief as possible. Users should be measured on their retention with measureable interactions. Phishing simulations that reflect course content need to produce the real-life scenarios users will face both in their business and personal lives. These learning experiences need to be useful on all levels, and should incorporate the cues that we all use to learn and retain valuable information.

As stated in the ABCs of a Persuasive Security Awareness Program[3], information security, like everything else, is a human enterprise and is influenced by factors that impact the individual. It's well recognized that the greatest cybersecurity danger to any organization is not a particular process, technology, or piece of equipment. It is the people working within the system who hide the inherent danger. Using psychological principles that social scientists and psychologists have discovered over the past 50 years, we can produce security awareness programs that are more personal, relevant, and persuasive.

[1] ISACA Journal. "Impact of Security Awareness Training Components on Perceived Security Effectiveness." (April 2011)
[2] Government Security. "Study Shows Fed Workers in Dark About Security." (May 2007)
[3] Samuel Chun, CISSP. "The ABCs of a Persuasive Security Awareness Program."

Phishing ransomware is low-hanging fruit

It has become increasingly clear that phishing plays a significant role in user-error security breaches. The 2017 Verizon Data Breach Investigations Report found that a staggering 90 percent of successful breaches were the direct result of a phishing attack.[4]

According to the report:

"Eagerness. Distraction. Curiosity. Uncertainty. All of these are drivers of human behavior, and one or more can be leveraged to influence someone to disclose information, click a link or wire money to a 'vendor' account...

"First, let's take a step back and examine the picture as a whole. There were a little over 1,600 incidents and more than 800 breaches featuring social actions in this year's corpus (all external actor driven). Phishing was again the top variety, found in over 90% of both incidents and breaches.

"Our non-incident phishing data is comprised of 7.3 million records (campaign data down to user level), over 14,000 campaigns, and over three million unique users across 2,280 different organizations. 7.3% of users across multiple data contributors were successfully phished—whether via a link or an opened attachment. That begged the question, "How many users fell victim more than once over the course of a year?" The answer is, in a typical company (with 30 or more employees), about 15% of all unique users who fell victim once, also took the bait a second time. 3% of all unique users clicked more than twice, and finally less than 1% clicked more than three times."

Given the Verizon Report's access to such large datasets for accuracy, their conclusions as they relate to security awareness training were equally interesting:

"The data shows simulated phishing makes a difference, but someone will always click. Focus on detection and reporting of clicks rather than just prevention. Implement and test a phishing response plan that:

- *Empowers users to alert on "phishy" emails*
- *Identifies phishing recipients and recalls the email*
- *Identifies phishing recipients who clicked the link or opened the attached file..."*

Results like these, combined with the fact that phishing is so highly associated with the spread of ransomware and other malware, should be alarming to small- and medium-sized businesses. Investing in phishing education ensures that all users are aware of different phishing tactics, which enables organizations to perform phishing simulations that are relevant to specific departments, significantly reducing risk.

Why is effective learning management software important?

Effective security awareness training starts with learning management software (LMS) that allows administrators to easily select, set up, run, manage, track, and report on their security awareness initiatives. The LMS lies at the heart of any security awareness solution, because its ease of use is paramount in getting the maximum benefit out of the content provided. Given that security awareness education is a continuous process and not a series of one-off activities it is essential that the LMS makes the repetitive processes straightforward and tracks each user's training and results. This way, future activities remain relevant and training sessions are not unnecessarily repeated.

What should I look for in security awareness training LMS?

Ease of use is the most critical feature. Given the modern trend toward highly mobile workplaces, it's important that employees can access courses anytime, anywhere, from any device. But ease of use doesn't just extend to end users. If the administrator has to struggle with the LMS application, it can hinder the value of the training.

Security awareness training should also be easy to integrate. The admins responsible for managing it should be able to use a single console to oversee successful completion of the training courses. Integration is also key from a security perspective, as it can facilitate training programs that are tailored to each individual user's risk profile and behaviors. An ability to leverage APIs is also essential so the LMS can export data and communicate with other applications (HR systems, for example) as needed.

Whether you're a managed service provider (MSP) or just a business that focuses on branding its internal content, the ability to customize and brand security training is important and can greatly increase the credibility of the training over anonymous content.

Full content management within the LMS is essential as well. The ability to upload existing courses, videos, and tests, as well as link content and users to other hosted content can provide flexibility. For instance, many businesses benefit from the ability to manage both pre-test and post-test content, as well as the capability to randomize content, create multiple choices, or have test results scored and weighted.

Furthermore, tracking and reporting are essential for proving the worth of security awareness training. You will need to show user progress and assess the effectiveness of content to ensure that every aspect of the training is measureable and accountable.

Finally, it may go without saying, but the LMS needs to be secure. Ideally, very little user data (if any) should be gathered or stored within the LMS, and while departmental and user reporting should be available, so too should anonymized reports and aggregations. Content needs to be protected and use of the system to launch phishing simulations or other social engineering attacks should be limited to only legitimate use.

As you can see, an effective and secure LMS for security awareness training is extremely important, as these capabilities help to realize the full value of security awareness training.

[4] Verizon. "2017 Data Breach Investigations Report." (April 2017)

In Summary

Security awareness training is rapidly increasing in popularity because it's becoming a necessity to ensure businesses of all sizes are secure. The type and depth of training may vary, but all offerings should incorporate basic phishing simulations and relevant data-compliance and security courses that educate users on the dangers they face both at work and at home.

As these training offerings increase in sophistication, you can expect to see not only highly customized content by industry sector, but also content geared to the actual real-life security incidents and behaviors of individual users.

Security awareness training is a layer of defense that has often been treated as a burden, but is now seeing serious advances—particularly as it sheds its standalone nature and is embraced by organizations small and large as an essential form of protection.

Of course, security awareness training is only one layer of defense. As such, it cannot deliver 100 percent protection, but it does help minimize an increasingly dangerous IT security issue—user error—and it educates users to make wiser decisions online, whether in the office, working remotely, or on their home networks.

GETTING STARTED

To learn more or try the Webroot Unity API for yourself, please contact us directly on 02087337103, or use the button below to drop us a line.

CONTACT US