TERRANOVA
SECURITY

The Definitive Guide to Security Awareness Training

The 4 Pillars of Successful Security Awareness Training

TABLE OF CONTENTS

What is Security Awareness?

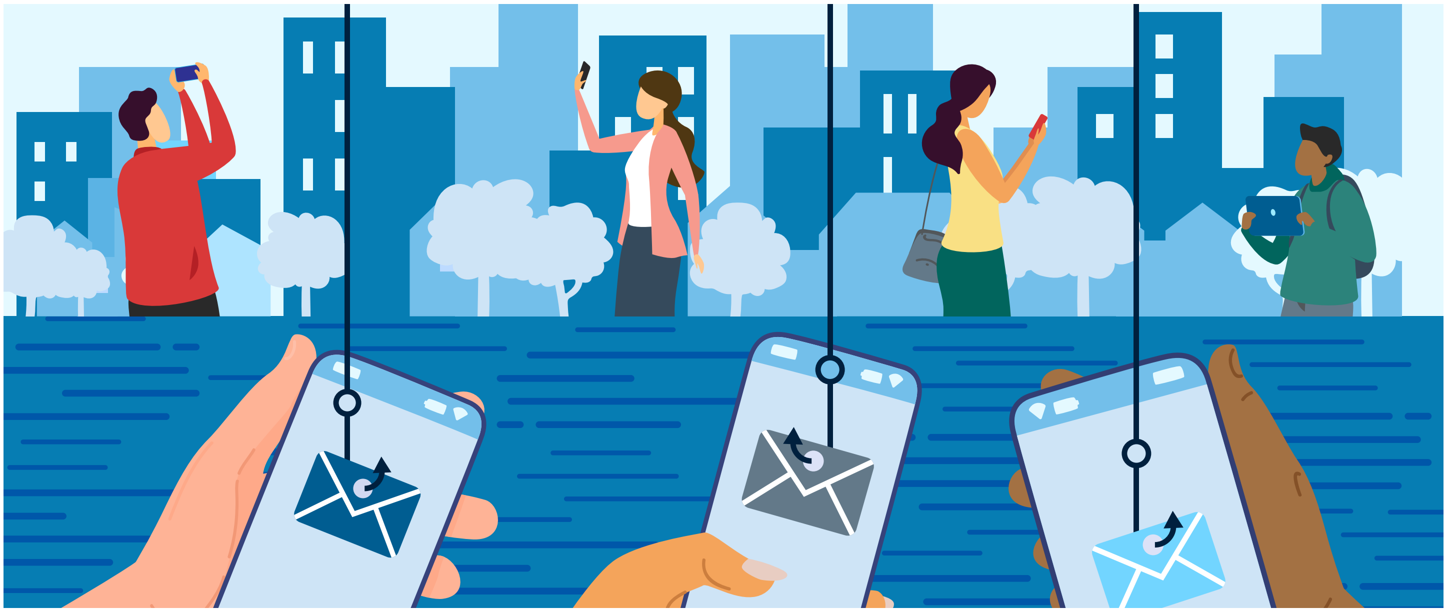
Security awareness training is an eLearning campaign or program that gives an organization’s end users the knowledge required to protect confidential information from cyber criminals. In this case, the term “end users” can encompass both full- and part-time employees, freelance contractors, and any other individuals who access, share, store, or edit organizational data.

Security awareness training courses and topics must support an organization’s overall cyber security objectives by modifying specific user behaviors that may amplify risk. These behaviors can include clicking on a link, reusing passwords, or entering sensitive information in a suspicious webpage form.

The best security awareness training programs leverage real-world phishing simulations and other web-based communication and reinforcement tools. The main goal of these campaigns is to reduce costs associated with potential breaches and mitigate the risk of mistakenly disclosed customer information.

Mitigating the Human Risk Factor

The Hollywood image of a hacker surrounded by screens, typing away lines to break into your system is not only uncommon, but it distracts from the most significant vulnerability in most organizations: The human risk factor. Over 3.4 billion phishing emails are sent every day, and if users are not adequately trained to detect them, it's only a matter of them until one of your users falls victim to one.



Keeping an up-to-date firewall, having strong antiviruses, and maintaining a strict hardware policy are essential to cyber security. Still, at the end of the day, the people you work with will always be the most important element of information security. Your users must be given the correct tools and knowledge to be aware of cyber threats and anticipate them even when they are vulnerable.

Mitigating the human risk factor isn't about pointing the finger at users but empowering them to work safer and smarter. It's good to pitch cyber security awareness training as a worker benefit when obtaining executive-level buy-in. It's easy to see this type of training as a boring necessity, but it should be framed differently and positively: An example of caring and thoughtfulness by the employer towards its staff.

The training and education in a people-centric security awareness program is designed to reduce human risk by producing long-term employee behavior change and instilling a security-focused mindset in employees as well as a security-focused culture across the organization.

The 4 Pillars of Successful Security Awareness Training

Cyber security awareness might seem like a tall task, but it's a simple process once you break it down to its requirements. Categorize the training needs by role, make sure the content is engaging and adapted to the user's reality, and you'll be well on your way to making lasting behavioral changes within your organization.

1. High-Quality Content

High-quality, relevant content is central to any security awareness program to engage users and provide a fun training program that resonates with employees and changes their behavior for the better.

Here are the five key factors that influence the quality of content and, ultimately, the learning experience for the modern learner:

1. Content should be created by a team of domain experts

Experts should understand adult learning, the psychology of changing behavior long-term, knowledge transfer, the most current cyber security trends and breaches, and governance and privacy compliance requirements. Content should be created in-house by the vendor selected to provide a standardized look and feel across the content library and the ability to be agile and customize the content for a more personalized approach. Read more about campaign personalization on page 7.

2. Proven pedagogical approach and methodology for adult learning

Security awareness training must be developed with adult learners in mind to ensure it is perceived as a valuable knowledge transfer and not a chore. Such an approach is characterized by the following:

- Content is relevant and meaningful, focusing on the "why"
- Instruction is task-oriented instead of promoting memorization
- Self-directed learning for adult learners, with guidance provided when needed
- Locked, mostly linear navigation prevents the learner from "nexting" through the topic and requires interaction to move forward
- Content narrated and displayed on the screen using closed captions to accommodate both visual and auditory learning styles
- Courses customized to meet unique cultural requirements
- Teaser videos included at the beginning of each module to engage the learner and introduce the topic
- Customizable topic evaluations – number of questions, randomization, and scoring can be modified to suit each organization's requirements

3. Microlearning modules provide risk-specific content to reinforce security awareness behaviors

Microlearning content is the best format to help impart lasting behavioral changes to the audience. To make sure you achieve this, make sure your content is:

- Short 2D video with audio
- Focused on one risk, easily consumable bites of content
- Scenario-based branching design
- User decision making allows a learner to see the immediate impact of making the right or wrong security decision
- Up to three minutes in length

4. Gamification for increased user engagement and motivation

Gamification allows you to keep your users engaged with the content outside of the training parameters. To have a gamified approach conducive to cyber security improvements, your content should:

- Have a pedagogical approach to increase engagement and motivation
- Complement the course test and provide a positive learning experience
- Feature real-time points accumulation displayed on a leaderboard (peer ranking)
- Be part of a competitive strategy between countries, departments, roles
- Provide an opportunity for incentive-based initiatives

5. Role-based content

Learning activities are designed with what the audience's roles and responsibilities are within the organization, making the training significant and impactful. Roles within your organization that can benefit from role-based content due to the type and level of sensitive data they have access to include:

- Managers
- IT Administrators
- IT Developers
- Human Resources
- Marketing

2. Personalized vs. Pre-Built Training Options

There's no perfect answer when it comes to cyber security awareness training. Out-of-the-box and personalized options both have their benefits. Finding the best solution for your organization will depend on various factors.

Out-of-the-box is unmatched with it comes to the speed of deployment. If you face some common cyber security challenges, premade content that addresses security awareness fundamentals might be just what you need. Since this type of content takes minutes to configure and launch to your end users, your organization can be more agile and launch a campaign quickly and easily.

Keep in mind

An out-of-the-box solution must prioritize content quality. You will want to carefully vet the vendor and their experts to ensure that the subjects are well covered, especially that the content is engaging and current. Since the content itself won't be personalized, it must be very engaging to guarantee users will complete it.

If you are dealing with a large organization spread across several countries or if you have particular cyber security issues, a personalized campaign will most likely be the best solution. Whether you need to customize the visual look of the training, the content, or record in different languages, a personalized security awareness campaign gives you complete freedom.

This option provides you with ultimate flexibility regarding content and its distribution. It also allows you to refer to issues pertaining specifically to your company and keep the content as fresh as possible by updating it with the most recent cyber attack attempts.

3. Risk-Based and Role-Based Training Options

When you plan a cyber security awareness campaign, there are two ways of thinking. Targeting the content can be done via risk type or role. The first option aims to tackle specific issues your organization faces, like phishing or repeated passwords. The second focuses on the issues specific to a department, like fake invoices for accounting or social engineering for management.

While these two filters can be used to build an autonomous strategy, they are most efficient when combined. An issue like phishing is multifaceted and can mean opposite things to different departments or even authority levels. Combining these two differentiators give you the best understanding of the issues your organization is facing.

Here are the departments most likely to have specialized cyber security issues:

Managers

The risk of cyber security is highest at the point where money and people are managed. Social engineering is hazardous in this situation since users have access to company money and sensitive data. Users should go through a few phishing simulations and learn how to detect fake invoices, so they don't share credentials unwillingly.

IT development

Companies increasingly rely on IT developers to run crucial aspects of their business or build products. These employees are common targets because of their access to critical data. Their content should be angled towards threats like ransomware.

Marketing/HR

Hackers often target these departments because they use a variety of apps during their everyday work activities, which means risks of weak or repeated passwords. The risk of breaches can be devastating, especially with HR handling personal information like social security numbers. Teaching these departments about password hygiene is essential, and phishing attempts through a fake password reset request.

4. Real-World Phishing Simulations

Phishing simulations are an essential aspect of any cyber security awareness training campaign. It's one of the most prevalent types of cyber attack, and it comes in an alarming number of variants. Your users must be aware and ready to counter these attempts, from social engineering to full-blown fake websites.

Here are the essential elements of a successful phishing simulation:

Varied attempts

Don't limit yourself to the most common types of attacks or the ones your organization has experienced. You'll want to try social engineering attempts in plain text emails, a fake login website, and a malicious download to make sure you keep users on their toes and gather enough data on your needs.

Analytics

The phishing simulation platform you choose must come with built-in analytics. You'll be using these simulations to see what type of content you should follow up with and gauge success throughout the year. That's why granular data on the results is essential, from a specific user to company-wide trends.

Quality follow-up content

Once the attempts are made and the data is compiled, it's time for action. The content following a phishing simulation should be diversified and can be used for several desired outcomes. The most common types of content are a newsletter detailing how the company did on the test and video-based training detailing recent phishing trends.

Best Practices

Plan campaigns and build courses with automated results-based learning, including foundational training, microlearning, phishing simulations, and just-in-time training.

Define a tailored awareness strategy to help address the different learning needs per group (i.e., new joiners, champions, repeat clickers, etc.).

Identify the security awareness goals that will help your leadership approve and support your program.

Determine metrics and KPIs to help measure the success of your program and align objectives to support your corporate business strategy and mission.

Choose a Visionary Partner

A cyber security awareness training provider is not just a supplier but should be a visionary partner. Seek out a company that engages in a consultative approach and will take the time to understand your unique situation and anticipate your needs. The right partner has the experience and the subject matter expertise to help you plan and execute a security awareness program designed specifically for your organization.

By bringing in a partner, you have an expert team with the knowledge to assess and analyze the data to measure and optimize your security awareness program. Remember, you are not alone !

A visionary partner in security awareness will:

- Offer expert advice and coaching to plan and execute your security awareness program. A partner also will understand the potential roadblocks, anticipate challenges and be available to you throughout your campaigns.
- Provide expertise and knowledge transfer to optimize your programs to motivate users and drive behavior change.
- Work with you to take the data and assess results, pinpoint strengths, and successes, and identify areas for improvement.
- Apply a proven pedagogical approach and methodology for adult eLearning.

Conclusion

With over three billion fraudulent emails sent every day, security awareness training is most important than ever when it comes to securing sensitive data. The cyber security principles taught in a training program can significantly reduce risk, build threat resilience, and ensure your organization steers clear of any negative repercussions.

The core tenets of successful awareness training include:

Be engaging. Have solid, well-produced content to keep your users engaged.

Stay sharp. New phishing techniques and viruses are born every day, and the only answer is continually improved cyber security awareness training.

Make it fun. There's a reason why people remember everything about their favorite video games. It's because they had fun and were rewarded while playing it. Whether it's points, leaderboards, or badges, give your users additional reasons to care about their training.

Put yourself in their shoes. Everyone's reality is different, and so should their cyber security awareness training. Assess the needs of every user based on their role, or you'll end up with ineffective methods.

Make it a benefit, not a task. Cyber security awareness training is too easily dismissed as another task when it's an exciting career development. Computers are a core part of everyone's lives. Your users should be appropriately trained to understand their power and best practices.

Security awareness training is an important investment in your organization's progress, and if you follow these five simple statements, you'll be on the road to success.