Security Awareness Training in 2021: The Definitive Guide
Contents

3 What Is Security Awareness Training?

4 A Brief History of Security Awareness Training

5 Who Needs Security Awareness Training?

6 How Is Security Awareness Training Different from a Security Awareness Program?

7 How Is Security Awareness Training Delivered?

11 What Are Common Security Awareness Training Pitfalls?

12 How Can You Make Your Security Awareness Training Effective?

16 What Topics Should Security Awareness Training Cover?

17 Should Security Awareness Training Be Mandatory?

18 Is Phishing Training Enough?

20 How Should You Evaluate Security Awareness Training Vendors?

22 COVID-19 Pandemic Impact

23 Final Thoughts

24 About The Security Awareness Training Platform From Security Mentor

25 Resources

26 Contact Us
What is Security Awareness Training?

Security awareness training at its core is teaching people how to keep information and information technology systems secure.

Effective training makes people aware of their responsibilities to protect their organization from risks by being aware of and vigilant about threats and vulnerabilities, and to learn the techniques of cyber-hygiene. Security awareness training can be delivered online, over mobile devices, through software, or in person. Online security awareness training has become the predominant delivery method in recent years due to its ability to handle large or distributed workforces, provide access 24x7, as well as not require in-house training experts.

Security awareness training is often referred to by other names, including information security training, information security awareness training, cybersecurity awareness training, and information technology security awareness and training program. These names are used interchangeably, causing some confusion about what security awareness training is. Another variation is information assurance training which is the term used by the United States Department of Defense. The one type of end user security training that is different is Information Technology security training which is security training designed for technical staff such as systems administrations or software developers.
A Brief History of Security Awareness Training

Security awareness training predates the Internet. Early security awareness training focused on protecting information and data stored in paper documents and physical offices spaces, as well as safe transmission through the postal mail, telephone or in direct communications. Then as computers became widespread, information moved to digital files and devices, and security awareness training expanded to cover the new electronic universe. In the mid-90s, the Internet began its explosive growth, and it became clear that security awareness training had to evolve to address new online digital risks. But that was only the beginning, next was the mobile revolution, then the Cloud, and most recently the Internet of Things (IoT), which exploded to more than 20 billion Internet-connected devices in 2020. With the fast pace at which technology is evolving, we fully expect to see security awareness training needing to evolve equally rapidly.

Not that long ago, a debate raged about whether security awareness training was worthwhile – could people even be trained about security?

One of the flash points of the debate was an article written by cybersecurity luminary Bruce Schneier who voiced the opinion “I personally believe that training users in security is generally a waste of time and that money can be spent better elsewhere.” But that opinion gave way to a widespread acceptance of the need for security awareness training as the risks related to employees increased dramatically. Hacking evolved from initially defacing websites to hacking-for-profit with a focus on targeting the weakest link – employees.

Concurrently, the multitude of ways people interact with technology exploded, and therefore made their organization vulnerable. The use of websites, email, mobile devices, social media, cloud services and the Internet of Things, not only became commonplace, but often was required. It became clear that security hardware and software alone were not sufficient to protect against all the external security threats, as well as the self-inflicted mistakes that users made. Users had to learn how to protect themselves and their organizations – whether at the office, at home, or using mobile devices.
In the United States, security awareness training is mandated by the following laws and regulations:

- Health Insurance Portability and Accountability Act (HIPAA) §164.308.(a),(5)
- Graham Leach Bliley Act (GLBA) Safeguards Rule
- North American Electric Reliability Corporation Critical Information Standard (NERC CIP) CIP-004-6 R1
- Federal Information Security Modernization Act of 2014 (FISMA) Section 3554.(b).(4).(A).(B)
- FTC Red Flags Rule 16 CFR §681.1(e)(3)

Many state governments in the United States have laws that require security awareness training or other forms of training related to information security and privacy. Two key state laws are:

- Massachusetts’s Data Security Law 201 CMR 17.03
- State of Texas Security Awareness Training Certification HB 3834 (86R)

Furthermore, standards dictate security awareness training, either in general or under particular conditions, including the following:

- Payment Card Industry Data Security Standard (PCI DSS) Requirement 12.6
- NIST Special Publication 800-53 (Rev. 4)
- Information Security Auditor’s Certification Association (ISACA) Control Objectives for Information (CobiT) §DS7

Security awareness training is also mandated by many international laws, a few major ones include:

- Article 39
- Australian Government Information Security Manual (ISM)
How Is Security Awareness Training Different from a Security Awareness Program?

Security awareness programs often include multiple forms of security awareness outreach to employees, with security awareness training serving as the cornerstone of the program. The goal of security awareness is to make users aware of, or cognizant about, specific topics such as cyber security or cyber threats. Security awareness training differs from security awareness in several critical ways: 1) training is presented in far greater depth and provides greater understanding than awareness, 2) security awareness training teaches skills, can provide interactive experiences, and can assess knowledge retention, and 3) training provides an organized presentation of topics that build on each other.

Security awareness is an important, supporting tool to reinforce training, as well as create a general awareness about information security risks and cyber security best practices. A great example of awareness campaigns for the general public are public service advertising (PSA) campaigns, which focus on either raising awareness or changing behavior.

The components of a robust security awareness program include: security awareness training, and other forms of employee outreach such as emails, newsletters, posters, lunch & learns, webinars, and even dedicated events such as during National Cybersecurity Awareness Month in October each year. By using different training modalities, not only do you reach more of your employees with alternate learning approaches, but you reinforce important cybersecurity messages. Newsletters and emails are effective for organizations to communicate targeted organization-specific content to employees. Webinars and lunch-and-learns offer the ability for employees to interact with each other and the speaker in live situation, whether remote or in-person. Posters displayed in communal spaces provide visual awareness reminders and can be used to reinforce important cybersecurity training.
How Is Security Awareness Training Delivered?

Key to a successful security awareness training program is making training accessible to all employees.

Security awareness training can be delivered in multiple ways; here we discuss two of the most common training delivery methods – online and live – and the pros and cons of each.

Other delivery considerations also discussed are accessibility for users with disabilities and the advantages of localized training.
With distributed workforces, limited time, and varying schedules, many organizations have chosen to deliver security awareness training online. For mid-size to large global organizations, the challenge of training employees at geographically-distributed locations, often with multiple languages, and in different time zones, has made online security awareness training the strongly preferred choice. COVID-19 has accelerated this trend as significant portions of all employees were required to work from home.

The quickest and easiest way for an organization to deliver online security awareness training is to use a cloud-based service provided by a trusted vendor (see "How to Evaluate Security Awareness Training Vendors" section below). Such services will include both the training and a management portal. Authentication can be either using username/password or federated single sign-on (SSO). Alternately, if your organization delivers training through its corporate Learning Management System (LMS), either on premise or using a third party’s LMS in the cloud, you can either create your own SCORM modules or license them from a security awareness training provider.

Online security awareness training can vary greatly in its quality, and how it is presented from interactive training (most effective) to videos and even PowerPoint presentations.

**Pros**

- Training can reach all employees with Internet connections, it is available 24x7, is self-paced, can be bookmarked to restart again later.
- Online training should track trainee metrics and provides administrative compliance reports.
- Gamification and interactive exercises can be used to make training fun and sticky.

**Cons**

- No live or group interaction.
- Training effectiveness is highly dependent on the quality of the content and how it is delivered.
- Organization-specific content, especially critical for larger organizations, may be omitted.
In-person training used to be the most common form of training and is still widely used, especially in smaller organizations or for targeted topics. A presenter, or series of presenters, speak to an audience of employees either in a large conference room or virtually over the Internet. Often a PowerPoint presentation is given. At the end of the presentation, questions are taken from the audience directly or virtually using the web conference or collaboration service.

**Pros**

- Training can be presented organization wide or targeted to specific groups.
- Live interactions allow greater participation by users.
- Live virtual training can be recorded and viewed at a later time (i.e., on-demand), providing employees with greater flexibility.
- When followed by time for questions and answers, these sessions can be helpful at addressing areas where staff need assistance.
- When done effectively, live training can also help build the security culture between employees and the organization.

**Cons**

- Training effectiveness is highly dependent on the knowledge, preparation, and presentation skills of the instructor.
- Most organizations don’t have the time, or expertise, to design, develop, and maintain high quality training presentations that cover important cyber topics in a compelling, user-focused format, as well as find speakers who are both trained in cyber security and are gifted presenters.
- If the training fails in any of these areas, sessions can become very tedious with little learning. Also, due to the format, the number and depth of topics are limited.
- Another issue is that organizations with distributed staff may find it difficult or very costly to do in-person training.
- Finally, it can be difficult to track who participated and measure what they have learned.
Another important aspect of training delivery is ensuring training is accessible to all users, including those with disabilities. Various guidelines are available to assist with making training accessible. Section 508 of the Rehabilitation Act of 1973 requires United States federal government agencies, and companies that do business with them, to provide training that is accessible to people with disabilities. Many other public sector entities also require Section 508 compliance. The Web Content Accessibility Guidelines (WCAG), published by the World Wide Web Consortium (W3C), provides guidelines for making web content accessible to those with disabilities.

For organizations delivering training to staff in multiple countries, a final factor to consider is localization of training. Localization is not only the translation of training content into another language, but adapting it for a specific region culturally. Offering training localized in a person's native language increases the likelihood not only that they will take training, but increases their productivity and learning.
What Are Common Security Awareness Training Pitfalls?

When employees fail to change their behavior after taking training, it’s easy to blame the employees – they don’t care about security, don’t complete training and keep making the same mistakes. And certainly, this can be true for a small percentage of users. But most people want to learn and be secure, and the problem is with the training program itself.

Security awareness training most often fails because it’s poorly designed or executed. Some common security awareness training pitfalls are:

- Content is dry, too technical, or difficult to understand
- Content is written by individuals without cyber security expertise
- Training sessions are too long or delivered too infrequently
- Employee participation is low due to low engagement
- Training only raises awareness about security threats, but doesn’t provide deeper knowledge or teach the actionable skills employees need to be cyber secure

Alone, or in combination, the above training pitfalls are why employee behavior doesn’t change. The answer is to provide security awareness training that is effective and that people actually want to take.
How Can You Make Your Security Awareness Training Effective?

To be effective, security awareness training needs to be equally about the security content and about how people best learn. This sounds simple but in actuality is quite complex. In general, effective training needs to incorporate approaches from a broad range of subjects, each playing a key role.

Seven disciplines that you should incorporate into your security awareness training today are:

1. **E-LEARNING**
   A learning experience that occurs using a digital device. e-Learning, also referred to as eLearning, accounted for 40% of all training done by organizations (2018 State of the Industry Report, ATD). We are strong proponents of the learn-by-doing model that has been developed and championed by Dr. Michael Allen.

2. **INSTRUCTIONAL DESIGN**
   The creation of learning experiences that result in the acquisition and application of knowledge and skills. Instructional designers are skilled at both Computer Based Training (CBT) as well as adult learning theory.

3. **GRAPHIC & MULTIMEDIA DESIGN**
   As defined on Wikipedia, graphic design is the process of visual communications through the use of typography, photography, iconography and illustration. While multimedia design incorporates multiple types of media and is used in interactive learning applications. Utilizing graphic and multimedia design is one of the best ways to engage users, as well as convey more-complex learning experiences, such as skills-based learning.
Building security awareness training that is based on sound principles provides direct benefits to the organization as well. The greatest cost in security awareness training is the employees’ time. If training isn’t effective, employees’ time is wasted, and so is the business investment. And from a bottom-line perspective, organizations with either ineffective security awareness training, or gulp – none at all, will be at greater risk of security incidents and the business cost it entails. The average cost of a data breach in 2020 was $3.86 million.
By making security awareness training that is fun, informative, understandable and relevant, employees will actually WANT to take training, not just see it as a burdensome requirement.
Follow these 10 guidelines to make effective security awareness training that will transform your employees into being cyber savvy:

1. **Make security awareness training a positive experience**
2. Ensure information security content is robust, yet approachable and easy to understand
3. Use high quality graphics, animations and interesting colors for visual engagement
4. Incorporate interactions and games that are both fun and teach real skills
5. **Enhance participation** using gamification, giveaways, and other incentives
6. Make training relevant for employees at work and at home
7. Include storytelling and real-world events to establish credibility and interest
8. **Keep training sessions brief**
9. Provide training frequently throughout the year
10. Focus lessons on a single topic

By following the above recommendations, your security awareness training will be truly effective, not only engaging users, but sticky and resulting in a real behavior and culture change.
What Topics Should Security Awareness Training Cover?

Security awareness training must cast a wide net, covering all topics where end users interact with information, could put information at risk by their actions, or where the employee or their equipment may be the target of cyber attacks.

Security awareness training curricula should include basics like phishing, malware, email security, clean desk policies and office security, computer security, mobile device security, passwords and password management, remote work, privacy, social engineering, social media, and many more. Depending on organization size and employee roles, it is often a good idea to provide different training for different employees.

If you use a security awareness training vendor, part of the value they should bring is expertise on recommended training topics, or curricula, for your employees. Recently, some vendors have taken the approach that more is better. This approach is often the result of acquisition of other vendors, yielding training that is inconsistent, as well as varying markedly in quality or substance. The end result is rarely effective or engaging for the users, and often can be overwhelming and time consuming for administrators.

An alternate approach is the one Security Mentor uses. We separate our security awareness training into specific, targeted curricula to make it easier for organizations to roll out training and for employees to learn.
Should Security Awareness Training Be Mandatory?

The question of whether security awareness training should be mandatory is dependent on both on organization and the role of the individual. For certain businesses or entities, security awareness training is required by regulation as previously discussed. These organizations must provide training either to all staff, or those in specific roles, and document that the training has been completed.

For those organizations, where training is not mandated by compliance regulations, the decision whether to require all staff to take security awareness training often sparks debate. Certain groups or individuals may want to opt out, or the organizations themselves may look to limit training to save money or time. Below we discuss several common reasons used to opt out of training, and the associated risks with each.

Poor Reasons to Not Require Training:

Pass a quiz, skip training. This argument sounds great on the surface, save staff time by not requiring them to take training if they have some knowledge about a topic. However, it is a false assumption that if you can answer a few quiz questions, you know all that you need to about a cybersecurity topic and you won't benefit from training. In fact, effective security awareness training has something in it for everyone to learn.

Management is too busy. Executives handle the most valuable and critical business information and thus, need to know how to protect it and prevent security incidents. They are also the most frequent target of cyber attackers. Finally, executive management is the role model for the rest of the staff. For a security awareness program to be successful, not only is management buy-in essential, but management also needs to be active champions of the program.

Training is too elementary for IT and security staff. Depending on their level of experience, IT and security staff may know the tenets of security awareness training, but that doesn't mean it isn't worthwhile. Going through training provides valuable reminders. Furthermore, well-crafted security awareness training will contain content that is informative for all employees, including IT and security staff.

In light of the potential cyber risks, the best approach remains to provide organization-wide security awareness training. While all staff will benefit from a comprehensive security awareness program that covers a broad range of security topics, select types of staff may also need more targeted or role based training related to their work. For example, targeted training may focus on position (e.g., executives, managers), responsibilities (e.g., system administration), compliance (e.g., HIPAA, PCI), or whether it is a public entity (e.g., FISMA). If your organization has a need for multiple types of targeted security awareness training, it may require using multiple sources, as a single source may not have the breadth of expertise and quality that is needed.
Phishing, like its namesake “fishing”, uses bait to lure a target into getting hooked. In phishing, you are the target, and the bait is a clever but fraudulent message that appears to be from a legitimate person or organization. The phisher’s goal is to steal your private or sensitive information and exploit it, most commonly for financial gain or other criminal activities. Phishers are using increasing more complex phishing attacks, and employing techniques like spear phishing, whaling, and BEC attacks. In fact, phishing remains the top cause of data incidents.
With phishing one of the leading cyberattacks against organizations, phishing training, or phishing awareness training, has become essential. However, despite its important role, phishing training is only a part of a robust security awareness program, and not a replacement for general security awareness training.

Most phishing training is done by conducting simulated phishing attacks using a phishing simulator, such as Security Mentor PhishDefense. Employees are sent a simulated phishing email. Those who click, or otherwise take the bait are tracked by the phishing simulation service. Often, these at-risk or vulnerable employees are shown a notice alerting them that they fell for a simulated phishing message or directed to a lesson on how to identify and resist phishing attacks. The goal is that employees learn to identify and resist phishing attacks. Another important feature in phishing simulators is that they provide a dashboard for training administrators to look at metrics of their employee susceptibility, vulnerability over time and overall risk level.

Comprehensive security awareness training teaches employees about a multitude of essential security topics such as office security, mobile security, use of the cloud, password creation and management, phishing and email security, incident response, and protecting sensitive information, to name just a few. Employee mistakes in any of these areas can lead to hacking, data breaches, and other security incidents. That's why comprehensive security awareness training is critical for all employees.
How Should You Evaluate Security Awareness Training Vendors?

As the need for security awareness training has become recognized as a critical part of an organization’s security, the field of vendors has become crowded. The quality and breadth of these vendor offerings varies widely. Trying to select the best provider for your organization can feel overwhelming.

We provide 12 guidelines to help you evaluate security awareness training vendors.

1. **Analyze your needs.**
Begin by understanding the security awareness training needs of your organization such as compliance and any weaknesses or gaps that you need to address. Also, determine if you have special requirements such as training delivery using SSO or through your Learning Management System (LMS) with SCORM, localization of the training in specific languages, or accessibility support for people with disabilities.

2. **Choose an established vendor.**
Select an organization that has a record of successfully providing security awareness training for at least three years and ideally five or more years.

3. **See a demo.**
Vendors should be motivated to showcase their training in a demo. Look for them to explain the training features, options, and what makes it unique, as well as how it is effective. If a vendor either doesn’t want to demo their security awareness training, that’s a red flag.

4. **Choose quality over quantity.**
Vendors may try to impress you with the quantity of their materials. However, a large catalog of low quality, disjointed lessons may do more harm than good. Employees will tune out after the first lesson if the training is poor. In addition, it can add a significant burden on the security or training team to review and select training from a large catalog.

5. **Evaluate the information security content.** Have an information security expert from your team review and evaluate the thoroughness of the topic coverage and accuracy of the content. A good time to do this is during the vendor-provided demo so that more in depth questions can be asked.
Ask how they make training effective.
Look for training that integrates e-learning, instructional design, psychology, media, and information technology. Ask the vendor to explain in their demo how they develop their training and what instructional design methods they use. Remember, the greatest cost in training is your employees’ time, you want it to be well spent and see real behavior change.

Don’t just check the box.
Choose a vendor that emphasizes both security and learning equally. Training should be interactive, engaging, informative, easy to understand, brief, and effective at changing behavior. For more advanced lessons, determine if the training adequately covers the topic. For example, a three-minute lesson on security awareness for system administrators will have very little value. Finally, look for a security awareness training program that rewards employees for desired behavior and positively incents them.

Review the administrative portal.
Does the security awareness training program offer metrics including tracking training completion and employee engagement, measuring knowledge retention and evaluating vulnerability? How do they measure the change in trainees’ security knowledge after completion of training?

Review the phishing simulator.
Talk with the vendor about whether they do phishing simulation and is it included in their training program. However, don’t view phishing training as equivalent to security awareness training. It is an important component, but there are many other critical topics that need to be covered.

Assess other awareness materials.
Does the vendor offer other types of employee security awareness services or materials? For example, integrating security policies like the Security Mentor Policy Tracking and Compliance service, or offering posters, newsletters, cartoons and other awareness materials. Security awareness materials, like those offered by Security Mentor, are valuable in reaching employees in different ways, but also reinforcing security awareness training messages.

Determine the options available.
Ideally the vendor will provide different training programs with different options to meet a variety of needs. The options in security awareness training can be extensive. Look for the right option set that fits your company requirements (#1 above). Security Mentor offers different training packages which both have different security awareness training lessons in the curriculum, as well as features and options.

Look for a great partner.
The relationship that you develop with your security awareness provider will be important in the success of your training program. When buying security awareness training, look for a vendor with sales representatives who are knowledgeable, helpful, and most of all interested in your success, not just in making a sale.
The COVID-19 pandemic is no exception.

Cyber criminals immediately began monetizing the pandemic, not caring about the pain or havoc they caused. At a time when no business could afford to lose time or money, phishing attacks reached stratospheric levels, with the most frequent targets being the public sector, healthcare organizations, and remote workers.

Phishing attacks spiked 667% in the spring of 2020, and Google detected 18 million malware and phishing Gmail messages a day related to COVID-19. Even worse, ransomware attacks rose dramatically during the main thrust of the pandemic. This trend has continued with the 1st half of 2021 showing 102% increase over the 1st half of 2020.

Increased phishing attacks and ransomware are not the only pandemic-related risks organizations face. Remote work brings a new set of risks. With greater access to technology, cloud services, and online business – and with less access to IT support – the odds of employees causing security incidents are greater than ever before, making a robust security awareness training program a must for all organizations. Now is a critical time to assess if your employees are truly secure enough, and if not, how can you help them be more secure? In your evaluation, be sure to include remote work. Twenty percent of organizations faced a security breach related to remote workers. Remote workers need targeted security awareness training focused on remote work, such as the Remote Work Training Program offered by Security Mentor.
Security awareness training is more critical than ever.

New technologies, as well as technological transformation, continue to accelerate. Just over ten years ago, cloud services, mobile computing and IOT, were just beginning to take hold. Today they are seen as commonplace and essential. Technology will continue to rapidly evolve in the future, likely at an even faster pace. Employees will either be the strongest cyber defense or weakest link an organization has.

Most employees want to do the right thing, but of course, that doesn’t always happen. Why? Sometimes mistakes happen because of a lack of knowledge about either cybersecurity or organizational policies. Other times, competing factors influence learning such as job requirements, lack of time, or even remote work. But the underlying cause is usually the training itself. Security awareness training must be brief, engaging, and relevant to be effective.

By following the information presented in this eBook, you will be able to ensure your security awareness training program will be one that employees will want to take, and that will keep your organization secure.
About The Security Awareness Training Platform from Security Mentor

Security Mentor is helping organizations worldwide create cyber savvy employees with our transformative Security Awareness Training Platform.

The Security Awareness Training Platform is a comprehensive suite of services that addresses all your security awareness training and education needs.

**Security Awareness Training** — teach critical security skills in an easy to understand, fun format that drives real behavior change.

**PhishDefense Phishing Simulator** — run simulated phishing tests to identify vulnerable employees and train them to be phish resistant.

**Policy Tracking & Compliance Service** — easily communicate, track and report on your security policy from within our training platform.

**Security Awareness Materials** — provide high quality awareness materials with consistent messaging that reinforces knowledge and increase retention.

To learn more about how Security Mentor can help you protect your organization by creating cyber aware employees, [click here](#) to schedule a personalized, live demo.
What Is Missing From Your Security Awareness Program?
Explore the components a security awareness program must have to ensure employee success and organizational security.

Cybersecurity for Remote Workers
Read our whitepaper on the six key areas every organization should address for remote workforce security.

PhishDefense Phishing Simulation
Learn how phishing simulation enables organizations to effectively test and train employees against cyberattacks and build cyber resilience.

About Security Mentor
Security Mentor is the industry pioneer and expert in security awareness training and education services. Since 2008, Security Mentor has continually redefined how security awareness training is created, delivered, experienced and embraced by combining expertise and creativity in security, technology, media and e-learning. Trusted by customers and celebrated by users, its comprehensive training platform offers on-demand, easy-to-use, and effective solutions including security awareness training, phishing simulation and policy tracking & compliance services. Its training employs instructional design best practices, interactive content, and gamification to engage learners and deliver enduring knowledge acquisition and real behavioral and cultural change.