WEBROOT®

an opentext™ company

Security Awareness Training Best Practices Guide

Copyright

Security Awareness Training Best Practices Guide

Table of Contents

Security Awareness Best Practices Guide

To get the best out of using Webroot Security Awareness Training, see the following topics:

Benefits of Security Awareness Training

There are a variety of benefits to a cybersecurity awareness training program for end users, both for small and medium-sized businesses and managed service providers (MSPs). To begin with, signing your team up for cybersecurity training will ensure that everyone is on the same page as far as understanding and complying with any regulations applicable to your industry. Second, it ensures end users are aware of online risks and the types of web content and behaviors to avoid, helping to reduce the likelihood of a breach. Additionally, it streamlines operation procedures and courses of action if a breach is successful.

As an example, email phishing scams continue to be effective, and are one of the preferred methods hackers use to gain access credentials, infiltrate networks, steal sensitive data, and launch malware or ransomware. Today's phishing emails are much more sophisticated than the "Nigerian Prince" scams of old and are designed to take advantage of end users' trust, gullibility, and even their desire to perform well at work.

If your employees have been taught how to identify suspicious emails, both within the work environment and in personal settings, the company will be much less likely to fall victim to this type of attack.

Cybersecurity training can also help to save you money, since it helps you reduce the number of breaches that need to be remediated, the amount of downtime and man-hours spent on post-infection recovery, and even the number of ransoms you must pay hackers to get ransomed data back.

Additionally, if a breach does occur, customer trust can be very difficult to recover. The right cybersecurity awareness training can help you better ensure the security of your customers' data, which, in turn, helps to protect your company's reputation.

Achieving Success with Security Awareness Training

To really achieve success with your security awareness training program, there are a few things you need to focus on such as:

1. **Put Your People First**

- Security awareness is about people. It needs to be interesting, accessible, relevant, and meaningful; and the program you choose needs to put people first. To achieve these goals, you need to understand what you want to get out of the program. For example, different employees might need to focus on different issues, such as Business Email Compromise. Mapping out your security awareness expectations across your organization is a good place to start, so you can begin to prioritize the types of training your organization requires.
- Once you understand the scope of your security awareness program, you should look at how to convey the training. Make sure the program is fun. No one wants to sit through mind-numbing security content. They will simply check out, or worse, refuse to do the training.

2. **Emphasize a security-aware culture**

- Security awareness training is a top-down effort that affects all parts and departments in every organization. You need to "sell it" on the concept of shared responsibility. You're all in it together, you're all putting in the same amount of effort, and you're all benefiting from the results of your mutual work toward this security goal.
- Additionally, you need to make sure you get executive buy-in on the need for security awareness training. Presenting the case for funding a security awareness training program is part of making your program of security awareness successful. By running phishing simulations and reporting on the results, you can tell a compelling story to executive stakeholders that will demonstrate the value of a security awareness program, as well as its return on investment (ROI).

3. **Align your program to your security policies and regulations**

- You can add weight to your awareness training by including it in your security policy. Prevention of security exposure is not a point solution anymore. Keeping an organization safe is about the entire business, including its people. Make sure that the policy reflects this and includes awareness training as a fundamental part of your security strategy.
- As part of this step, you should also align the security awareness program to relevant business/industry issues, such as data security and privacy. Depending on your industry and location, your business may be subject to certain regulations (e.g. GDPR, HIPAA, PCI DSS, etc.), some of which include security awareness training as a requirement for compliance.

4. **Make training ongoing**

- Threats are constantly evolving, which means you're never really done training. Additionally, as employees change positions or leave the company, training requirements and frequency may change. It's important that everyone understands training as an ongoing process. Finally, as in all educational pursuits, the key to lasting results is repetition.

5. Encourage and welcome feedback

- If your staff finds particular training efforts useful, that's important to know. It's also important to know what they don't like, so you can find alternatives that can achieve the same result. Institute an open-door policy that allows staff to openly discuss the merits or problems within the training, and make sure they know how and where to report their feedback. Then, use these insights to tailor your programs and make them more effective.

How to Implement Security Awareness Training

The following tips will help you to implement a continuous security awareness training program:

1. **Tailor training exercises**

- Perform regular phishing tests, in which you send out a fake phishing email to all employees across the organization and determine how many people click on it. Then, break that data down by groups and types of messages, to tailor training to problem areas. This data also allows you to show progress.

2. **Include security awareness training as part of your organization's onboarding process**

- Start building the mindset as all new hires go through security awareness training from day one.

3. **Never stop evaluating**

- Perform regular vulnerability assessments to evaluate how susceptible your organization is to an attack.

4. **Communicate results**

- Communicate cybersecurity information to all employees to get all employees on board with training and learning best practices. Then, be sure to share successes and metrics that show improvement.

5. **Offer continuous training**

- Cybersecurity training should continue throughout the year, at all levels of the organization, specific to each employee's job.

6. **Acknowledge employees**

- Acknowledge users that find malicious emails and share stories about how these users helped the company avoid a security breach.

Efficacy and Metrics of Security Awareness Training

Untrained employees can present a huge security risk for businesses of all types and sizes.

Your organization needs to have the actual data to measure the level of understanding and awareness, and, thereby, the level of risk. As security awareness training is implemented and evaluated over time, it's possible to draw a correlation between effective training and reduced security incidents.

Efficacy Stats: Key Findings

#1: Clients who use training courses have less risk / more educated users

- Phishing Simulations Only = 26.47% click-through rate
- Phishing Simulations with Training = 12.32% click-through rate

#2: Risk is reduced with more Security Awareness Training

- 1 to 5 campaigns = (months 1-2): 37% click-through rate
- 6 to 10 campaigns = (months 3-4): 28% click-through rate
- 11+ campaigns = (months 4+): 13% click-through rate

These trends show that after a year of ongoing training, the average click-through rate on a phishing simulation will dip below 5% which is approximately a 70% reduction.

Awareness Metrics

To measure the impact of your awareness program and effectively change behavior, we recommend you run phishing simulations monthly, or close to this level of frequency.

Phishing simulations:

- Measure human risk
- Are easy to implement and automate at a low cost
- Offer repeatable and quantifiable measurements
- Give you actionable data

Click Results measure the number of people who fall victim to a phishing simulation. This number should decrease over time as end users become more aware of how to handle these types of messages.

Phishing Reporting measures the number of people who detect and report a phishing email. This number should increase over time as behaviors change.

Phishing Repeat Offenders measures the number of individuals that represent a high risk to an organization and must be addressed with additional and more frequent testing.

Compliance Metrics

We recommend you also run training courses regularly, on a monthly, bi-monthly, or quarterly basis.

Training courses:

- Measure level of understanding
- Are easy to implement and automate at a low cost
- Offer repeatable and quantifiable measurements
- Actionable

Training Completion measures the number of people who took the training and completed it.

Quiz Passing Rates measure the number of people who took the training and passed the quiz.

Security Awareness Training Solution Overview

Security Awareness Training Elements

These are the tools currently provided by Webroot® Security Awareness Training:

- Phishing simulator with expanding real-world template library
- Comprehensive training course library
- Learning management console
- Reporting

How Security Awareness Training Is Used

- Reduces risk
- Measures and improves employee behavior
- Engages end users

Penetration Testing

- Risk assessment
- White hat testing

Compliance

- Financial Services / SEC + FINRA + SOX
- Privacy / GDPR
- Healthcare / HIPAA
- Retail / PCI
- Energy / NERC
- Government / State + Local + Edu

Engaging, Succinct, and Effective Interactive Training

Offering engaging, interactive courses that can be consumed anywhere and on-the-go increases end users' attentiveness. This subsequently increases the effectiveness of cybersecurity education programs.

All of Webroot's high-quality cybersecurity courses can be sent on a scheduled or as needed basis directly to end users, who can then launch them in one click from any browser on their computer or mobile device.

Easily Tracked and Customized Campaigns

Measuring success generically and at an individual level is key, and enables you direct, relevant security awareness training of different levels and types for users who need it most. The built-in Learning Management System (LMS) keeps track of user participation—making all education accountable and measurable.

Campaign and Contact Management

Our training campaign management wizard, contact manager, training email templates, comprehensive course library, and reporting center give you the ability to schedule and assign training efficiently and get results.

Contacts are easy to import via CSV files or our web-based form. Tags allow multiple meta-data items to be added to each user to help group users by location, department, business unit, etc. The tags are then used to easily schedule and send relevant training by individual or group.

Reporting Center

Get phishing campaign statistics and generate per-user action reports and others to measure progress and ROI. Our Campaign Executive Summary Report highlights the campaign data and results of the training, so accountability and value is always clear.

Engaging Management Teams

While you may have implemented a holistic security perimeter, including endpoint protection, DNS filtering, and anti-spam measures, over 90% of successful security breaches involve a human element such as a social engineering attempt or a spear-phishing attack. Ensuring that your stakeholders understand the threats is the first step to initiating and then running a successful Security Awareness Training Program.

Send an email introducing Security Awareness to management, explaining the value of the service, and be sure to share details around your first phishing and training campaigns. Webroot also has a white paper called, "Why Businesses Need Security Awareness Training Now," which lays out the reasons why so many organizations are providing cybersecurity user education.

If applicable, loop in your local IT support so they are aware of the service and training schedule as well. If you are not sure how to craft that first email, we have provided sample stakeholder email templates within the Webroot Security Awareness Training learning management console. You can use these as is, or edit them to suit your needs.

Communicating Security Awareness Training Results

A key objective of Security Awareness Training is engaging end users by raising the level of cybersecurity awareness. A great way to accomplish that is to share the results of your phishing campaigns across the organization.

Even though Webroot Security Awareness Training does let you see who clicked what, the point of sharing results is not to call out individuals, but instead use this data to capitalize on everyone's engagement by sharing a statistical report. People will instantly recognize if they clicked or caught the phish and—more importantly—seeing the statistics of where the organization stands can open the door for further engagement and continuous Security Awareness Training.

After the initial phishing simulation, consider sending out a communication to all employees, letting them know the reasoning behind the campaign. This is also an opportunity to roll out and introduce the training program that will be run throughout the coming weeks and months. Try using one of the Security Awareness Training campaign summary reports and customizing the content to meet your organization's needs. Webroot can also supply a phishing infographic to send to your employees or use as a poster during the phishing campaign.

Security Awareness Training Setup Tips

Once end-users are engaged and your stakeholders understand the value of Security Awareness Training, it's time to setup your training program. While there is no one size fits all user education program, we recommend the following:

- Run at least one to two phishing campaigns per month
- Run a minimum of one to three training courses per quarter
- Run compliance courses at time of need (usually driven by audits)

> **Note:** Depending on the needs of each organization, you may want to increase the frequency and adjust intervals throughout the year.

Webroot Security Awareness training includes numerous pre-built phishing templates you can use, including real-world phishing scenarios that are, essentially, harmless versions we have seen in the real-world.

We also include professionally developed and engaging topical training courses that you will be proud to share within your company. Popular topics covered in the training courses include:

- Cybersecurity best practices
- Phishing
- Topical cybersecurity
- 5-minute micro-learning courses
- In-depth compliance courses (PCI, HIPAA, GDPR, SEC/FINRA, etc.)

We recommend using the Webroot Security Awareness Training Program Scheduling feature to combine and schedule campaign training sessions to set up a continuous cybersecurity training program.

With the program scheduling feature, you are able to choose to schedule one or many Welcome Email, Phishing Simulations, and Training Courses. Plus, add in a follow-up campaign summary report to automate your entire training program.

Return on Security Investment (ROSI)

After 12 months of training, our data shows that end users are 70% less likely to fall for a phishing attempt.

Use the ROSI calculation for cost benefit analysis during your first annual review to demonstrate the real savings to management teams or, if you are an MSP, to clients using Webroot Security Awareness Training.

$$\textbf{ROSI (\%)} = \frac{\text{(ALE x Mitigation Ratio) – Cost of Security Solution}}{\text{Cost of the Security Solution}}$$

ALE = Average Loss Expectancy = Cost per incident times the # of incidents

Mitigation Ratio = Efficacy of solution at stopping attacks as a percentage

Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Look for the answer in our knowledge base.
- Look for the answer in our online documentation.
- Enter a help ticket .
- Connect to the Webroot Online Business Forum.

Index

S

T