WEBROOT®

Security Awareness Training Best Practices Guide

Copyright

Security Awareness Training Best Practices Guide

Table of Contents

Chapter 1: Getting the Best Out Of Security Awareness Training

To get started using the Getting the Best Out of Security Awareness Training guide, see the following topics:

Security Awareness Training Overview

Cybersecurity awareness has become key in reducing the number, frequency, and impact of IT Users being the conduit for IT Security breaches. Cybercriminals today auto-research and target individuals in bulk as an easy entry point into organizations' systems, which is far easier than writing a software exploit or finding ways to bypass IT Security defenses.

User education via cybersecurity awareness training is, if conducted and managed properly, a highly effective way of arming users against the would-be social engineering hackers. At the same, time it helps foster good IT habits like password management, locking work stations, and other IT security habits and practices that make IT a lot safer.

This document looks at the best practices and procedures when introducing security awareness training to an organization and, in particular, the types of campaigns and ongoing user education needed to ensure the desired changes in user behavior to ensure long term effectiveness.

Core Principle Behind Effective Security Awareness Training

The effectiveness of any user education training is based on it being something you can measure over time. To achieve this, it needs to be run continuously so the results from individual users can be compared over the entirety of a program. This then allows the organization to see if the desired changes in behavior are being achieved, or other courses of action are needed to reinforce or accelerate that change.

The risks and desired behaviors may also change over time. This is especially true in cybersecurity where new threats are occurring all the time. The need to keep IT users aware of these new risks is also important and lends topicality and relevance to their education. Education training is always more effective when the IT user can see a direct relevance to their work role, or a clear relationship with their lifestyle and day-to-day IT activities.

Another key goal is to foster interactivity from within the computer-based training. This interactivity can take many forms, but is essential, as it allows the user to become more involved in what is being communicated, and it often takes the form of tests and quizzes to determine how much individual participants are absorbing from the education courses.

Webroot brings all of these to bear in its Security Awareness Training campaigns and ongoing user education programs — continuous, relevant, and involving education campaigns that together create an education program tailored to the IT users' role.


security
program
importance
password
training
information
awareness
organization
policies
threats
employees
firm
implement
company
education
business
Social
Security
resources
users
including
focus
time
take
safe
also
types
goal
buy-in
get
minor

Security Awareness Training Elements

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

- Phishing Simulator with expanding real world template library.
- Training Course Library with over 25 courses.
- Learning Management Console.

How Security Awareness Training Is Used

- Security Awareness Training:
  - Reduces Risk
  - Measures and improves employee behavior
  - Engage 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

Key Features of Security Awareness Training

Webroot's Security Awareness Training contains a complete learning management system (LMS), so running courses and programs is as easy as possible.

The five-step wizard set-up system greatly increases the ease and lowers the man-time costs of running any of the phishing, cyber-awareness and compliance education programs. Plus, the automated campaign scheduler means organizing ongoing continuous user education programs and reporting only takes minutes too.

Fully Featured Phishing Simulator

Phishing is the primary way users are socially engineered. Our ever-expanding and topical phishing template library is regionalized for effectiveness and relevance, while allowing realistic engagement with IT users in real-world phishing scenarios.

Launching realistic phishing attack simulations lets you accurately monitor normal user responses and then direct appropriate awareness programs to users accordingly.

Engaging, Succinct, and Effective Interactive Training — Anywhere

Offering engaging, easily consumed, interactive courses increases IT users' attentiveness and greatly increases the effectiveness of cybersecurity education programs.

All of Webroot's high quality cybersecurity courses can be sent on a scheduled or ad hoc 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 lets you direct relevant awareness training of different levels and types to users who need it most. The built-in Learning Management System keeps track of user participation and making all education accountable and measureable.

Campaign and Contact Management

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

Contacts are easily imported via CSV files, or our web-based form. Tags allow multiple metadata items to be added to each user to help group users by location, department, and 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 new Campaign Executive Summary Report highlights the campaign data and results of the training so accountability and value is always clear.

Chapter 2: Starting Off Your Security Awareness Training

To get started with Security Awareness Training, see the following topics:

Starting Off Your Security Awareness Training Overview

This section describes good principles to follow when you are starting out with Security Awareness Training to educate your users.

This diagram visually represents an approach to introducing and gaining buy-in and ongoing development of a user education program. The principal take away, however, is that user education and cybersecurity training is an ongoing process rather than a one-off event, especially if you are seeking real success from its operation. (Source: © Gartner Critical Elements for Your Security Program's Success- May 2017).

Engaging Your Management Team

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 share details around your first phishing and training campaigns. Webroot also has a white paper on this 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 too. If you are not sure how to craft that first email then we can help with that too. Sample stake holder email copy templates are available within the Webroot Security Awareness Training (SAT) learning management console. You can use these as is, or edit to suit your needs before sending.

Sending Your First Phishing Campaign

Consider starting your Security Awareness program with a phishing campaign. Your first phishing campaign will be used to establish a baseline and gauge how susceptible your end users are to phishing and their general level of security awareness.

There are many template options within the Webroot Security Awareness Training console for your first campaign. We recommend utilizing a template that mimics an internal communication from HR or the IT department to get the most eyes on the email.

It is also a good idea to consider using Webroot's 404 broken link template so that users who fall for the fake phish are unaware of being tested. Using Error 404 will also keep water cooler talk down and allow you to gain a more accurate susceptibility baseline.

Thereafter be sure to link your phishing campaigns to training pages and courses to maximize the training opportunity and consider changing phishing templates by job role to create an effective phishing program.

Note: Many of our phishing templates are regionalized to a particular region, and therefore effective at simulating a phishing attack.

Sending Communications To End Users

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 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 opens 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 roll out and introduce the security awareness training program that will be run throughout the coming weeks and months. Try using one of Webroot Security Awareness Training campaign summary reports and customize 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.

Setting Up Your Continuous Phishing And Training Program

Now that end-users are engaged and understand the value it's time to setup your training program. While there is no one size fits all user education program, however, Webroot recommends the following:

- Running at least one to two phishing campaigns per month
- Running a minimum of one to three training courses per quarter
- Running 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 defanged versions we have seen in the wild. We also include professionally developed and engaging topical training courses that you will be proud to share within your company. Popular topics covered include:

- Cybersecurity best practices
- Phishing
- Topical cybersecurity 5 minute micro-learning courses
- In-depth compliance courses that are related to PCI, HIPAA, GDPR, SEC/FINRA, and more

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.

Measuring Effectiveness And Refining The Training

Campaign reports are there to do two things:

- Show the value of the training by seeing the results achieved from each campaign over time.
- Letting you identify IT Users that are not responding at the desired level.

As with any educational approach not all people learn or absorb information in the same way. For users not responding, you might consider increasing the training frequency, or look at offering a different approach outside computer based training, for example, a classroom setting.

It is important to regularly use Campaign Reports to demonstrate the value to Management and quantify the return on investment, where practical, on the awareness you are both maintaining and achieving.

Summary of Security Awareness Training

This brief guide can help you plan out the campaign activities and ongoing user education training programs that are suitable for you or, if you are an MSP, for your clients.

Cybersecurity awareness training is not a one-size fits all solution, so you will need to look at your sector to determine what is relevant, if anything, in compliance terms and break your users into logical training groups, so the security awareness content they are receiving is useful.

To paraphrase a well-known proverb “In the land of the blind, the one-eyed man is king” and investing in cybersecurity awareness training lets your IT users more fully navigate the many risks and costs cybercrime can impose on any business.

Chapter 3: Security Awareness Training Support

For information about support, see the following topic:

Accessing Technical Support

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

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

Index

K

M

O

P

R

S

T