WEBROOT
Smarter Cybersecurity™

FAQ | Webroot® Security Awareness Training

Overview

When it comes to business cybersecurity, end users are your first line of defense. Unfortunately, they are often also your weakest link. Today's cybercriminals target employees to infiltrate small to medium-sized businesses (SMBs), counting on their ability to exploit human curiosity, error, and even greed. Many employees are totally unprepared to identify suspicious or malicious web content, putting themselves and the companies they represent at risk. Plus, for higher-value hacks, criminals put in greater effort to socially engineer the employee and abuse their trust. Senior executives with higher-level corporate permissions and access are often targeted in these types of campaigns.

To strengthen their overall IT security strategy, businesses need effective, relevant, interactive content to educate employees on risks and modern malware tactics. When the Ponemon Institute looked at phishing awareness programs, even the least effective training program still resulted in a seven-fold ROI, and that includes lost productivity time. This is proof that security awareness training works and protects the bottom line.

Through regular security awareness training programs, SMBs improve their overall IT security strategy and reduce costs associated with remediation. Similarly, managed service providers (MSPs) also benefit from reduced remediation costs, as well as an additional revenue opportunity and a stronger trust relationship with their customers.

What is Webroot® Security Awareness Training?

Webroot® Security Awareness Training provides effective cybersecurity education that is both timely and relevant to the employee. Through a continuous training approach, our courses are designed to modify risky user behaviors that can put the network at risk.

Key Features

» ***Easy 5-step setup wizard and LMS***

Webroot Security Awareness Training is integrated into the Webroot Global Site Manager console and contains a complete learning management system (LMS), so running courses and programs is as easy as possible. The built-in five-step wizard increases the ease and reduces the man-time costs of running education programs. Plus, the automated campaign scheduler means you can organize ongoing user education programs and reports in minutes.

» ***A fully featured phishing simulator***

Phishing is the primary way users are currently socially engineered. Our ever-expanding and topical phishing template library is regionalized for effectiveness and relevance, while allowing realistic engagement with end users in real-world phishing scenarios. Launching realistic phishing attack simulations lets you accurately monitor actual user responses, then direct appropriate awareness programs to users accordingly.

» ***Engaging and effective interactive training courses***

Offering engaging, easily-consumed, interactive courses increases end users' attentiveness, as well as the overall 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.

» ***Trackable, customizable training campaigns***

Measuring individual and overall success is key so you can direct relevant awareness training of different levels and types to users who need them. The built-in LMS keeps track of user participation, 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. You can import contacts via CSV or web-based form; use tags to group contacts by location, department, business unit, etc.; and send training and phishing by individual or group.

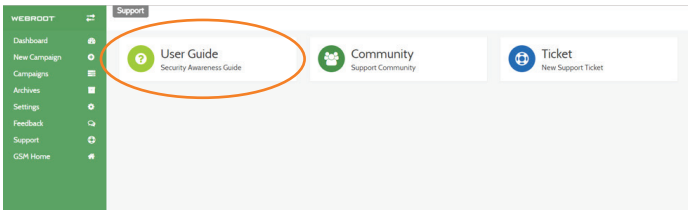
» ***Reporting Center***

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 are always clear.

Operation

Is there a Getting Started Guide or Admin Guide?

Yes. The guides are available at docs.webroot.com/us/en/business or within the GSM console.

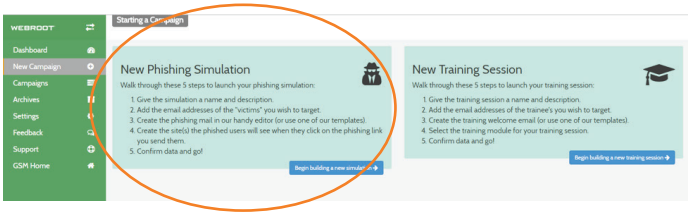


How do Webroot Security Awareness Training simulations work?

You'll be able to build your own phishing simulations through our easy-to-use Phishing Simulation Wizard and apply them by site, location, user group, or individual.

In five easy steps, you will:

1. Import your 50 user email target list
2. Add your bait email and lure page by using pre-configured templates or your own custom content
3. Send a test email to test the simulation
4. Schedule and launch your simulation against your targets
5. Watch simulation reporting in real time, including:
   - Email processing and delivery
   - Email opens and clicks
   - Data post attempts to the lure page



Isn't Phishing Dangerous?

Real-world phishing attacks can be devastating. Webroot Security Awareness Training only simulates a phishing attack, and can only collect action statistics on your users' interactions with the simulation—helping you identify education needs within your organization.

Webroot Security Awareness Training alters simulated emails and lure pages to ensure data such as user names, passwords, or any other sensitive data never leaves the user's device, and is never seen by our servers.

Simulation emails and lure page code are sanitized on the server, so users cannot add custom scripts, links, or forms to emails or lure pages. This ensures only action statistics are collected.

What stops me from Phishing anyone I want?

By default, phishing simulations are only available to launch against your authorized domains. You will not be able to target email addresses outside of your authorized domains list. These types of tests are generally run by your company IT or security team. Before running any simulations against your organization, you should consult with your company's IT and/or security staff to make them aware of the tests, and maximize the success of your simulation.

What email addresses should I import into Webroot Security Awareness Training?

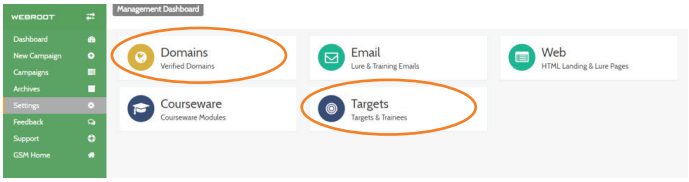
You will enter two types of email addresses into Security Awareness Training:

1. ***Authorized Domain Address***

   This is your own address on your organization's domain. When you add an Authorized Domain address, you will receive an email with a validation link. Click that link to verify that you can access that email box, and have an account on your organization's domain. This will allow you to import target email addresses on that domain.

2. ***Target Email Addresses***

   These are the email addresses belonging to your organization's employees/users which will be targeted in your simulation. These are necessary for the simulation to deliver bait emails.



What should I do if Webroot Security Awareness Training emails get caught in my spam filter?

Some spam filters may prevent emails from Webroot Security Awareness Training. You may need to whitelist emails from the Webroot send mail server by IP address or server name, or whitelist the sending domain. To do so, log into your email gateway or spam filter and whitelist any of the following:

» IP Address: 167.89.85.54

» Mail Server: o1.relay.mx-secure.com (o1.relay.mx-secure.com [167.89.85.54])

» Sending domain(s): use the sending domain you set up

What email events does Webroot Security Awareness Training report?
The Email Activity Feed shows data on the following types of email events:

» ***Processed:*** the emailer processed requests from your website, application, or mail client via SMTP relay or the API

» ***Clicks:*** the recipient clicked one of the Click Tracked links in your email

» ***Delivered:*** the email was delivered to a recipient

» ***Opens:*** the email was opened by a recipient

» ***Deferred:*** the recipient mail server asked the emailer to stop sending emails so fast

» ***Drops:*** the emailer dropped your email because the recipient email is in one of your suppression groups, the recipient email has previously bounced, or the recipient has marked your email as spam

» ***Bounces:*** the email was rejected by the recipient mail server before it can be delivered

» ***Spam Reports:*** the recipient marked your email as spam, and their mail server reported this action to us

What other types of reporting are available?
Webroot Security Awareness Training tracks nearly all activity associated with courses and phishing campaigns, including the number of messages sent and delivered; the number of messages opened and clicked; and the number of individuals who post data. Reports are available in easy-to-read charts within the Security Awareness Training console. You can also export reports by printing or saving as a PDF via your web browser.

We also offer a Campaign Executive Summary Report, which highlights the campaign data and training results, ensuring every campaign is accountable and its value is clear.

Why should I trust Webroot Security Awareness Training?
Established in 1997, Webroot has a long track record of delivering high integrity IT security solutions to the global market. With this new security service, Webroot customers can benefit from nearly 20 years' experience in cybersecurity education technology.

Webroot takes customer data security very seriously. As part of this service we:

» Sanitize lure pages on the client side to ensure credentials, such as usernames, passwords, or account numbers, are never sent to or seen by our servers.

» Ensure simulations can only be launched against targets on your validated domains

» Restrict launching simulations against public ISP domains

What is the Webroot's policy on data privacy?
Webroot will not sell or share email addresses in our system with any non-Webroot person or group, nor will we use any of your target addresses. You can easily purge your data from Webroot Security Awareness Training, should you feel it necessary.

Does Webroot provide support for Security Awareness Training?
Yes, Webroot provides full, inclusive 24x7 ticket-based support, as well as inclusive telephone support during the normal working week in your region.

Trial or Buy

How do I start a Webroot Security Awareness Training trial?
You can start a trial on webroot.com. If you're an existing Webroot customer, you can also contact your Webroot sales representative or Channel Account Manager to get started.

How do I buy a full subscription?
To purchase, contact your Webroot sales representative or Channel Account Manager.

Is the trial limited in any way?
We offer a standard free 30-day trial for Webroot Security Awareness Training, with the following requirements:

» Training is limited to 50 users per customer. (MSP trials are limited to 50 users per customer site.)

» Webroot SecureAnywhere Business customers must have the GSM console to implement Security Awareness Training.

» Training is limited to a single course: "Understanding Malware."

» Use of the Phishing Simulator and simulations is unlimited.

Important Notes

1. Email addresses on ISP or public domains (such as @gmail.com, @yahoo.com, etc.,) are restricted and cannot be used with this service.
2. User accounts and target email addresses must be valid company or organization addresses. After signing up, you will receive a welcome email with a validation link to enable your email account to run training and simulations.
3. For trial and evaluation purposes, you can send simulations to your own validated email.
4. When you run simulations for a customer, you must validate their email domain in the GSM console.

About Webroot
Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900