WEBROOT
Smarter Cybersecurity™

FAQ | Webroot® Security Awareness Training

What is Webroot® Security Awareness Training?

In July 2017, Webroot acquired the assets of Securecast, an innovative startup that has developed cloud-based, multi-layered end user security awareness training. Currently, we are working to integrate Securecast IT security simulation, training, and user education courses into the Webroot® Global Site Manager console. During this time, existing managed service provider (MSP) partners can begin BETA testing an early version of the upcoming Webroot Security Awareness Training. The BETA will be limited to 20 users per MSP for 60 days, from mid-August until mid-October 2017. We plan to release the fully integrated Webroot Security Awareness Training to all Webroot customers in October.

During the Webroot Security Awareness Training BETA, MSPs will receive access to the existing Webroot/Securecast education and training software, including:

1. A sophisticated phishing simulator
2. The phishing avoidance training module
3. A forum to make comments or suggestions for usage, features, and additional training going forward

How do I start the Webroot Security Awareness Training BETA?

Webroot chose Securecast specifically for their very intuitive cloud-based console and easy five-step process for initiating security awareness trainings and user education programs. The software is very easy to use and the phishing simulator and education program are straightforward to test.

To request BETA access, click here and enter your details. We will then send you all the information you need to start your BETA.

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

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

1. IP Address: 167.89.85.54
2. Mail Server: o1.relay.mx-secure.com (o1.relay.mx-secure.com [167.89.85.54])
3. Sending domain(s): use the sending domain you set up

Why should I trust Webroot Security Awareness Training as a service?

Established in 1997, Webroot has a long track record of delivering high integrity IT security solutions to the global market. By bringing the Webroot and Securecast teams together, we're combining nearly 20 years' experience in cybersecurity and education technology.

Webroot Security Awareness Training will:

» Sanitize lure pages on the client side to ensure credentials (usernames/passwords) 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

How do Webroot Security Awareness Training simulations work?

As our client, you will be able to build your phishing simulations through our easy-to-use Simulation Wizard. In five easy steps, you will:

1. Import your 20 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 to ensure users cannot add custom scripts, links, or forms to emails or lure pages. This ensures only action statistics are collected.

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

We will not sell any of the email addresses you enter.

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 events does Webroot Security Awareness Training report?

The Email Activity Feed will show you data on the following types of email events:

- **Processed:** requests from your website, application, or mail client via SMTP Relay or the API that the emailer processed
- **Clicks:** when a recipient clicks one of the Click Tracked links in your email
- **Delivered:** an email that was delivered to a recipient
- **Opens:** whenever an email is opened by a recipient
- **Deferred:** the recipient mail server asked the emailer to stop sending emails so fast
- **Drops:** if the recipient email is in one of your suppression groups, the recipient email has previously bounced, or that recipient has marked your email as spam, the emailer will drop an email
- **Bounces:** when an email is rejected by the recipient mail server before it can be delivered
- **Spam Reports:** whenever a recipient marks your email as spam and their mail server reports the action to us

What other types of reporting are available?

Webroot Security Awareness Training tracks nearly all activity associated with a phishing campaign, including number of messages sent and delivered; number of messages opened and clicked; and number of individuals who post data. Reports are presented in easy-to-read charts directly within the Security Awareness Training solution. Reports can be exported simply by printing or saving as PDF via your browser.

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 MSP account to run a simulation.
3. For BETA evaluation purposes, you can send simulations to your own validated email. **If you intend to run simulations for one of your customers, you must inform us so we can validate their email domain.**

About Webroot
Webroot delivers next-generation network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and 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

©2017 Webroot Inc. All rights reserved. Webroot, CyberFlow Analytics, SecureAnywhere, Webroot SecureAnywhere, BrightCloud, FlowScape, and Smarter Cybersecurity are trademarks or registered trademarks of Webroot Inc. in the United States and other countries. All other trademarks are properties of their respective owners. FAQ _ 080817 _ US