CARBONITE an opentext company | WEBROOT an opentext company

# Webroot®
# Security Awareness Training

## Improve Cyber Resilience to Minimize Security Incidents and Unforeseen Costs

### Overview

No matter how large or small a business is, it's a target for cybercriminals. That's because it only takes a single unwitting click on a phishing link to grant criminals access to everything on a given network and, in some cases, beyond. It's also why security awareness training and phishing simulations are essential for businesses who want to transform end users from the weakest link in the security chain, into a truly resilient first line of cyber defense.

*A small business with under 50 employees faces nearly the same level of risk as a 20,000-employee enterprise.*[1]

Criminals target organizations for a variety of reasons. They might aim for long-term network infiltration and data theft, attempt to scam users or businesses out of data or money, or try steal user credentials to access different parts of the network. They might also attempt to turn an end user's machine into a 'zombie' as part of a botnet or spam relay, or to mine cryptocurrency by hijacking its CPU. There are numerous possibilities.

The bottom line is that end users need regular and consistent cyber-awareness education. With regular training, businesses can empower end users to identify and report scams, avoid risks, fulfil regulatory compliance requirements, and help prevent modern cyberattacks.

### The Webroot Approach

Webroot® Security Awareness Training provides continuous, relevant, and measurable education and testing that businesses need to minimize risky user behaviors and achieve cyber resilience. The system is easy to set up and administer because it is integrated into the Webroot management console and purpose-built for small to medium-sized business (SMBs) and managed service providers (MSPs).

And, because all Webroot products are backed by Webroot threat intelligence, customers can rest assured that all courses are up to date and relevant.

#### MSP and SMB-Friendly Training and Management

Webroot Security Awareness Training is a fully cloud-based software-as-a-service (SaaS) offering. Admins can manage training and phishing simulations via the same console as Webroot® Business Endpoint Protection and Webroot® DNS Protection, providing a single-pane-of-glass experience with low management overhead.

Unlike other training providers, Webroot focuses on the needs of MSPs and SMBs, who don't always have the resources to administer security and compliance training. Affordability is another important factor, which is why Webroot Security Awareness Training is designed to be easy to administer and automate, and it won't break the bank.

#### Microsoft® Azure AD Integration and Simple Management

With its Microsoft® Azure Active Directory integration, Webroot® Security Awareness Training lets admins automate the import of target users and keep them in sync. The simple five-step setup wizard makes it easy to create phishing simulations and training campaigns. In just a few minutes, you can name a campaign, choose the desired recipients, select the content, and launch.

Admins can schedule a sequence of multiple trainings and phishing simulations over a specific time period. Additionally, admins who manage multiple clients or sites, such as MSPs, can implement and manage these programs across multiple clients at a global level. Features for scheduling, delivery time randomization, automated reminders, and reporting, make it simple and straightforward to run fully accountable and continuous security awareness campaigns that effectively improve user behavior over time.

## What Results to Expect

Since introducing Webroot® Security Awareness Training several years ago, Webroot data has shown consistent, measurable improvements to end user click- through rates in phishing simulations. In fact:

- One in 10 users (11%) click on the first phishing email as part of a baseline campaign.
- Companies see an immediate improvement by the time their run a second phishing simulation, with the average click rate dropping to 8%.
- The click rate drops to one in 20 (5%) with monthly anti-phishing training with simulation emails after a year.

If the click-through rate on phishing simulations drops from 11% to 5%, that's a 55% reduction in clicks that could have compromised the organization.[2]

Consider the number of user errors that result security incidents each year. Then think about the subsequent productivity losses and hours of labor required for recovery. Now factor in any regulatory fines and the loss of customer trust and business reputation. That 55% reduction could easily mean the difference between thriving and struggling as a business.

## Security Awareness Training at a Glance

### Intuitive Learning Management System (LMS)

Webroot® Security Awareness Training includes a highly automated LMS to make training management easy and efficient.

### Microsoft® Azure Active Directory integration and 5-Step Wizard

The Azure AD integration makes managing user training straightforward, while the campaign wizard reduces the amount of time and cost of administering cybersecurity education programs.

### Dark Web Breach Report

Webroot provides an easy-to-use Dark Web Breach Report to help demonstrate the need for training, as well as any compromises affecting an email domain.

### Phishing Simulator

The full-featured phishing simulator provides an ever- expanding template library based on real-world scenarios. Templates are categorized and regionalized for ease of use, while schedule randomization enables staggered delivery to maximize campaign impact.

### Engaging, Interactive Training

Cybersecurity training must be engaging, interactive, and easy to consume to hold users' attention and achieve lasting results. All of Webroot's high-quality courses fit these criteria and can be sent directly to end users on a scheduled or ad hoc basis, as many times as necessary. Users can access and launch all courses in one click from any browser on any computer or mobile device. Automated reminders ensure users know about any outstanding coursework.

### Trackable, Fully Customizable Training Campaigns

The built-in LMS keeps track of every user's participation, making all cybersecurity education accountable and measurable.

### Full Course, Campaign, and Contact Management

The fully integrated course management wizard, contact manager, training email templates, course library, and reporting center enable you to quickly and efficiently schedule and assign training. Users can be imported via Azure AD, Active Directory LDIF, CSV files, or web-based form. Tags allow easy grouping of users by location, department, or category to streamline training.

### Global Campaign Management and Dashboard

A single-pane-of-glass training dashboard shows all the campaigns in progress or completed, while an intuitive campaign management workflow allows admins to compose and launch multi-client training quickly and easily.

### Scheduled Reporting Center

Receive phishing campaign statistics and generate per- user action and other reports to measure progress and ROI. Our Campaign Executive Summary Report highlights the campaign data and results of the training.

## 90+ Training Courses, Including:

### Featured Cybersecurity Courses

- Phishing - Understanding Phishing, Full Length
- Email - Cybersecurity Essentials
- Passwords - Cybersecurity Essentials
- Remote Work - Stay Cyber Resilient while WFH
- Malware - Understanding Malware
- Physical Security - Cybersecurity Essentials
- Cybersecurity - Overview
- Phishing - Understanding Phishing, Abbreviated
- Remote Work - IT Security for the Remote Worker and Business Traveler
- Websites and Software - Cybersecurity Essentials

1 Hiscox. "2019 Cyber Readiness Report." (April 2019)
2 Webroot Inc. "2020 Webroot Threat Report." (February 2020)

### Compliance Courses

- Bribery Act (UK)
- CCPA - Fired Up About CCPA
- Challenge 25 (UK)
- Consumer Rights (UK)
- Data Breach Notification Law (AU)
- Data Protection Act 2017 (UK)
- Equality and Diversity in the Workplace
- EU Competition Law (EU)
- FCPA - What is FCPA
- Freedom of Information (UK)
- GDPR Express
- Harassment and Bullying at Work (UK)
- HIPAA Privacy and Security 101
- Money Laundering (UK)
- PCI-DSS Overview
- Whistleblowing (UK)

## Trial and next steps

For more information, contact your Webroot Account Manager or our sales department. Visit webroot.com to initiate a FREE 30-day trial. Existing Webroot customers can also start trials directly via the Webroot management console.

**Contact us to learn more – Webroot US**

Email: wr-enterprise@opentext.com

Phone: +1 800 772 9383

**About Carbonite and Webroot**

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.