opentext™ | Cybersecurity

DATASHEET

Webroot® Security Awareness Training

Reduce risk exposure through internal users

Phishing is the most popular choice for hackers because it can be easily deployed and 74% of these phishing attacks targeted onto US businesses are successfull.[1] 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 that want to transform end users from the weakest link in the security chain into a truly resilient first line of cyber defense.

The best security in the world can't prevent an unwitting employee, working on-site or remotely, from accidentally leaving the front door to the network wide open. Webroot® Security Awareness Training helps businesses empower end users to identify and report scams, avoid risks, fulfill regulatory compliance requirements and help prevent modern cyberattacks with regular training as part of the layered defense approach to become cyber resilient.

Reducing Risk with Security Awareness Training

Keep up with evolving threats and new attack vectors

Webroot® Security Awareness Training provides continuous, relevant and measurable education and testing that businesses need to help minimize risky user behaviors and achieve cyber resilience. 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.

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. Well-trained users will reduce the number of security incidents a business will face, which, in turn, reduces the costs as well as losses in terms of productivity and business downtime. According to our observations from real-world customers, businesses that use Webroot® Security Awareness Training alongside our endpoint security encounter 20% less malware than those who only deploy our endpoint protection and have no training.

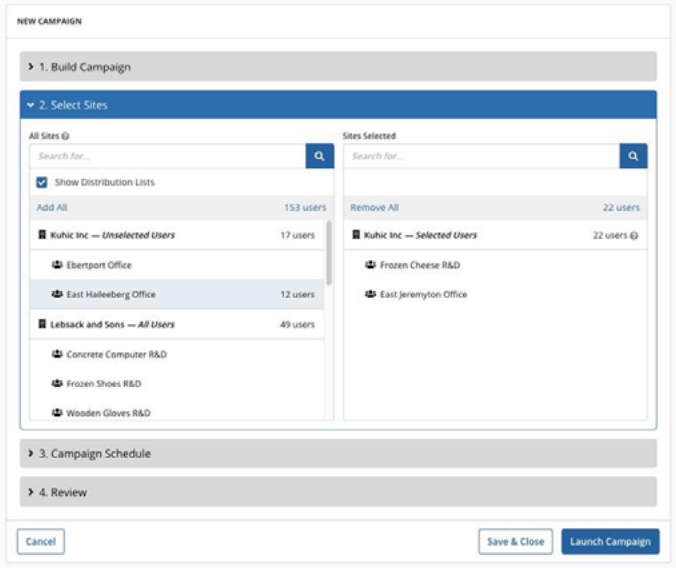
Key Benefits

- 20% less malware compared to customers with Webroot endpoint protection alone
- Simple administration and campaign management
- High relevancy and frequency of training updates featuring useful, interactive and effective content
- Integrated solution for MSPs and SMBs with multi-tenant management
- Automated training management and compliance reporting at an individual, group and company level

Single and multi-client console option that lets you run training easily across a single site or across multiple sites

How it works

Webroot® Security Awareness Training includes a highly automated Learning Management System (LMS) to make training management easy and efficient. 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 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.



Webroot Security Awareness Training console

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. The built-in LMS keeps track of every user's participation, making all cybersecurity education accountable and measurable. Our campaign executive summary report highlights the campaign data and results of the training. 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.

Webroot SAT now includes Autopilot, a turnkey security awareness program in which you manage the list of users; we send them training and phishing campaigns monthly.

Transform end users from the weakest link in the security chain, into a truly resilient first line of cyber defense

Continuous, relevant and measurable education to minimize risky user behaviors and achieve cyber resilience

OpenText Security Solutions brings together best-in-class solutions to help your business remain cyber resilient. Carbonite and Webroot can help you prevent and protect from threats happening in the first place, minimize the impact by quickly detecting and responding, recover the data seamlessly to reduce the impact, and help you adapt and comply with changing regulations.

Webroot® Security Awareness Training's expansive training catalog is updated monthly to cover a wide variety of security and business-related topics in a range of formats. You can receive phishing campaign statistics and generate per-user action and other reports to measure progress and ROI. In a recent customer snapshot of phishing simulations, 11% of users clicked on the first phishing email. By the time they had run their 6th simulation, the click rate had dropped to 6%; by their 18th simulation, this dropped to 4%. Webroot® Security Awareness training can help build cyber resilience among users with topics recommended by NIST Cybersecurity Framework.

[1] Venure Beat 2021, Phishing attacks get smarter as targets struggle to keep up

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. DS_020723