CARBONITE an opentext company | WEBROOT an opentext company

MSP GUIDE

Making Money with Security Awareness Training

How addressing human error reduces risk and bolsters your profitability

Introduction

The volume and sophistication of cyberattacks that target your clients have skyrocketed in the past few years. And, in addition to the advancements in threat trends, your clients' cyber resilience needs have also changed.

In the past, most small and medium-sized businesses (SMBs) were safe and happy with nothing more than a basic firewall and endpoint antivirus protection. But, faced with today's threats, these same businesses must invest more heavily in cybersecurity. In turn, the variety of security-related services managed service providers (MSPs) offer is broadening to match demand.

Endpoint protection is only the beginning. Even organizations with phenomenal endpoint protection are being compromised as criminals prey on the naiveté and ignorance of your clients' end users. 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.

The majority of your clients know their employees are on the front lines of their cybersecurity defenses. They also understand that empowering employees with training on malware trends, regulatory compliance, cybersecurity best practices, and more, will strengthen the overall resilience of their business. In this guide, we'll discuss why you and your clients should choose Webroot® Security Awareness Training, and how you can turn your clients' cybersecurity concerns into a profitable opportunity for you both.

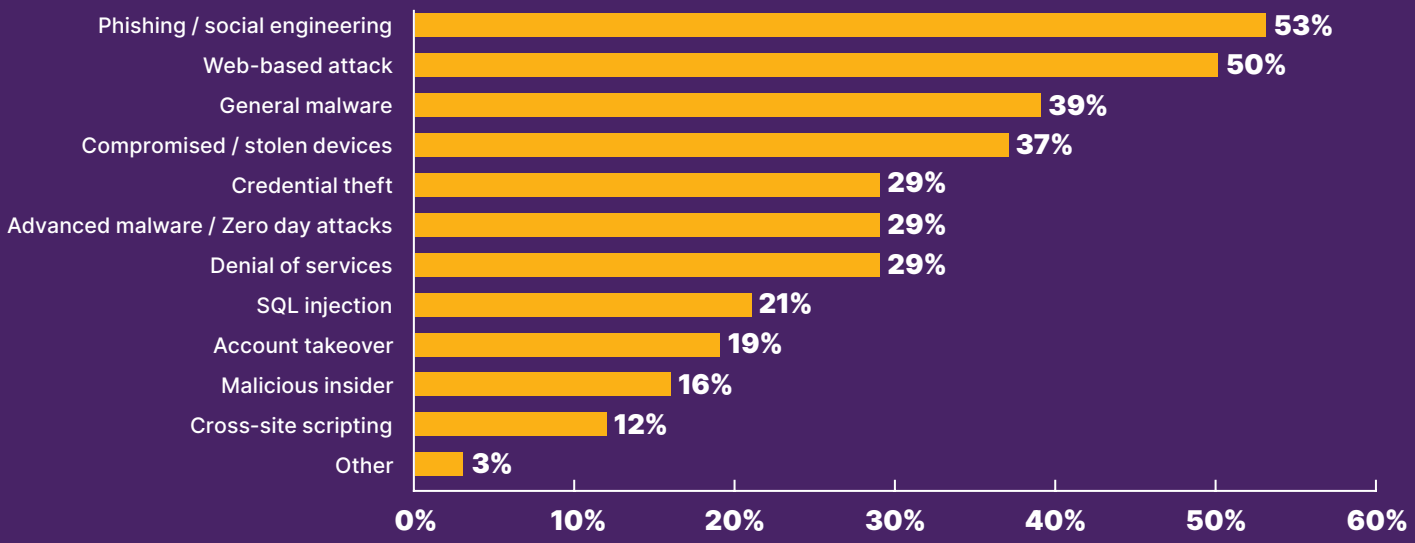
The importance of security layers for users, endpoints and networks

According to a recent report, in which we surveyed 7,000 office workers around the globe about their phishing risk and click habits, an average of 29% said they had clicked at least one phishing link in the past year. Among workers in the United States, that average was 33%. Because phishing and malicious spam ("malspam") campaigns continue to be primary ways businesses get breached, the need for layered security that includes cybersecurity education for employees is critical.

Webroot currently offers three distinct layers of cyber resilience solutions to MSPs, which include Endpoint Protection, DNS Protection, and Security Awareness Training. These three layers are designed to work together to reduce the impact of attacks and enhance your clients' overall resilience against threats. According to our observations from real-world customers, businesses that use Webroot® Security Awareness Training experience up to 90.2% fewer malware encounters than those who only employ endpoint antimalware without training. Additionally, adding Webroot® DNS Protection means you can prevent up to 74.7% of web-based malware from hitting endpoints in the first place. Paired alongside the web reputation and real-time anti-phishing intelligence that back Webroot® Business Endpoint Protection, this combination of solutions provides a strong defense for clients of all types.

To augment your cybersecurity offerings and enhance your clients' overall resilience against threats, you need cyber-savvy end users who know how to spot phishing emails and avoid risks online. Thankfully, while cybersecurity awareness training was once the costly purview of highly targeted organizations in the finance, government, pharmaceutical, and technology spheres, it is now a practical, affordable, and even necessary addition to your clients' overall security portfolio. Not only that, but if they haven't already, your clients are likely to start asking for it.

Types of attacks experienced by SMBs[2]



Reducing Risk with Security Awareness Training

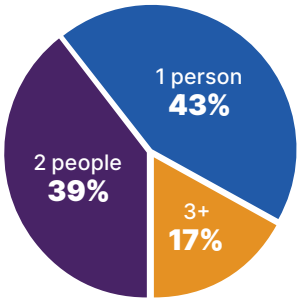
Webroot® Security Awareness Training is a highly automated, 100% computer-based training solution, so there's no need for MSPs to worry about becoming education experts on top of their other responsibilities. Not only is Security Awareness Training simple and straightforward to deploy, it's also efficient, effective, and easy to customize to your clients' unique needs; and it's priced competitively to help keep it affordable for clients and profitable for you. Finally, it produces very real, measurable results, which makes it easy for you to demonstrate its value to clients.

How Webroot MSPs Package Security Awareness Training

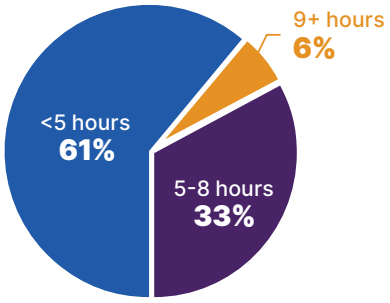
Per a recent survey of Webroot MSPs, there are typically two approaches to offering Security Awareness Training: either as a core offering or an additional one.[3] The core offering is either delivered through standardized training for all of a given MSP's clients or customized for individual clients, while the additional offering is typically customized. Both of these scenarios underscore the importance of training that includes a balance of standard training templates and customization.

How MSPs Package Security Awareness Training

Number of staff involved



Monthly hours spent on training

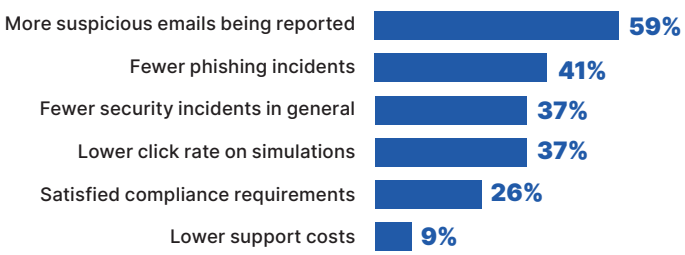


Additionally, our survey asked how much time and how many people were involved to run the training. On average, Webroot MSPs reported only requiring one or two staff members and less than 8 hours for administration per month. Clearly, the high automation and intuitive nature of Webroot Security Awareness Training help keep MSP operating costs low while still providing the flexibility you need to tune education to meet your clients' precise needs.

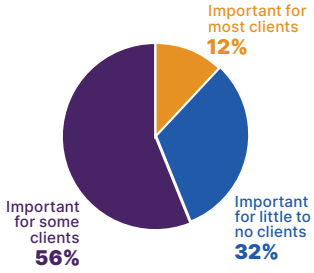
Real-World Benefits of Training

After implementing Security Awareness Training, respondents in our survey indicated that they had seen a variety of benefits. Some of these included significant reductions in phishing incidents (41%) and security incidents in general (37%), while 59% of Webroot MSPs saw an increase in the number of suspicious emails being reported to IT teams, rather than clicked on.

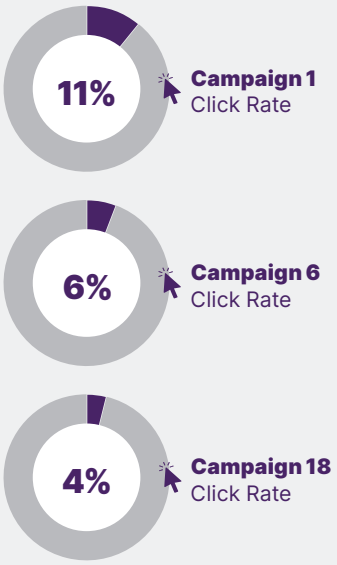
Have you or your clients experienced any benefits? (Select all that apply)



How important are compliance requirements to justify training



Running 18 campaigns reduces phishing click-through by nearly 64%.[4]

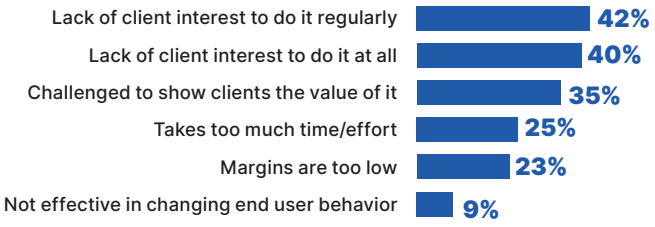


- Interest in the training campaigns remained high or increased.
- There's a direct correlation between the number of phishing simulations companies ran and the click-through rate on fake phishing emails. As you can see, the more training campaigns you run, the more the phishing email click-through rate drops.
- MSPs whose clients are using Security Awareness Training have reported their clients experience significantly fewer security incidents.

Barriers that Prevent Better Training Adoption

When asked to name barriers that prevent MSPs from delivering training to more clients, under 25% considered margins, time or effort to be significant obstacles. Instead, the most common roadblocks to overcome were that clients didn't want to have to conduct training regularly, had little interest in training on the whole, or simply didn't see the value of a training program.

Is anything preventing you from delivering more training? (Select all that apply)



How MSPs use Security Awareness Training

According to recent reviews from verified Webroot MSPs on G2, an independent software review platform, service providers leverage Security Awareness Training to achieve multiple types of business objectives. Quotes from these are listed below.[5]

Achieve Compliance

- "We need to comply with PCI and GDPR, and awareness training is a requirement."
- "Need to train staff as part of infosec policy outlined in ISO27001. Since implementing this and using phishing sims, click rates have dropped to 0%."

Identify High-Risk Users

- "The training highlighted members of our team that would put our network at risk and helped to train them."
- "Helps us identify end users that easily fall for phishing schemes."

Onboard Clients

- "Helps us determine the competency of our clients concerning cyber threats."
- "Using this as a hook for potential clients is a great way to get a foot in the door at very low cost."

Stop Risky Behavior

- "We are deploying to clients that have issues with phishing attacks."
- "Helped our customers to become more vigilant in their day to day tasks."
- "Customers with [training] experienced a marked decrease in successful phishing and malware attacks."
- "Drastically lowered the number of users who have given their email credentials out."

Selling Webroot® Security Awareness Training as a Service

There are several different ways to offer Security Awareness Training to your clients, but our MSP partners have expressed that the most profitable model is to build training into your standard IT security services stack. Of course, you can give clients the choice to opt out, but that decision must be factored in when you later have to charge for certain incident-related services. In a sense, you're selling on the notion of shared responsibility.

1. Shared Responsibility

Well-trained users will reduce the number of security incidents a business will face, which, in turn, reduces the costs associated with infections caused by unwitting user error, as well as losses in terms of user productivity and overall business downtime. For a minimal investment in high quality, highly affordable awareness training, the ROI for the client is considerable. (Use the Return on Security Investment calculation included in this guide, if possible.) Once clients fully understand the ROI vs. the cost of an incident, as well as the cost of your services to address the consequences of an incident, the concept of using training to promote shared responsibility virtually sells itself.

2. Regulatory Compliance

For some clients, the sectors in which they operate may have specific compliance requirements. In these cases, you need to identify whether they already conduct compliance training, or whether they're aware they need it, and then position yourself to provide it. Reviewing the relevant compliance requirements and the courses you offer, in addition to the benefits of ongoing phishing simulations and other cybersecurity training, should be enough to persuade the client that the need exists.

You might be surprised at how many of your clients are subject to regulations; Webroot MSPs have reported up to 68%. For instance, any business that takes credit card payments from customers must be PCI compliant, while any business offering healthcare services is subject to HIPAA, GDPR, and other regulations, depending on their geographic location. These are just a few of the cases that require accredited training; there are numerous others.

3. Phishing Simulation Assessment

If your clients aren't sold on the importance of end user awareness, offer them a free phishing simulation. Phishing simulations can look exactly like the real thing, which are designed to fool even the savviest user. Results from the simulation can provide the evidence you need to convince any skeptics. As we saw in the previous section, G2 reviewers have used Webroot Security Awareness Training both to identify high-risk users and convince skeptical clients of the need for training in the first place.

4. Investment Protection

By offering security awareness training alongside your other security offerings, you're protecting your clients' investment. After all, there's only so much security software can do—even phenomenal, best-in-class protection backed by leading threat intelligence—if an end user unwittingly hands over their access credentials for sensitive systems. When you include end user awareness training in your service offering, you're helping your clients make the most of their IT security budget.

5. Selling Considerations

When adding Security Awareness Training to your portfolio of offerings, there are a few tips to keep in mind.

- **Training must be ongoing.** End user education is also not a one-off exercise. Because humans usually need to repeat tasks to fully understand them and integrate their lessons; and compliance testing is often required at regular intervals; and cyberattack trends and tactics vary widely and change in an instant; your clients will need ongoing, regular phishing simulations, courses, etc.
- Results take time. Your clients may expect to see results right away but changing end users' behaviors takes time. Reassure your clients that the ROI is undeniable, even though they're unlikely to see drastic results until after training has been going on for at least a few months. Phishing simulations are a good way to measure those results over time, so we recommend doing these at least monthly to ensure you have good data to demonstrate improvement and value.
- **Don't overpromise.** Adding user education training won't make your clients' security bulletproof, but it will produce measurable user behavior changes over time that significantly reduce security risks and costs. Additionally, by offering Webroot Security Awareness Training, you're not promising to be your clients' personal security education guru. You're telling them the cybersecurity vendor who currently protects their devices is offering proven, professional, relevant, and measurable user education that will benefit their business.
- **Relevance is key.** End user education is not one-size-fits-all. Look at the courses we offer and relate the relevant ones to your client from a compliance or incident-related perspective.

How Webroot can help you sell Security Awareness Training

Many MSPs offer security awareness training as an add-on paid for and included service, since the proven value of security awareness as an additional layer of defense against breaches is so high. Others are including end user education as a standard component of their bundled security offerings, alongside endpoint security and patching services. In the latter pricing model, MSPs calculate that the savings from dealing with fewer incidents and service calls after customers have begun leveraging training courses and phishing simulations can improve the profitability of their offerings. In either model, both MSPs and their customers benefit.

Webroot MSP Client Models

- **All Inclusive**

  When the contract renews, or when the annual (or quarterly) review arrives, Security Awareness Training is automatically built into the monthly cost. The discussion moves to start dates for phishing simulations and the courses you'll be providing to minimize risk for both parties.

  Prior to that automatic inclusion, you'd send out a series of communications discussing the necessity and additional cost, as well as the amount of training and reporting provided. The timing should be such that your clients have time to contact you if they have any concerns.

- **Optional**

  This approach is similar to the above, except the conversation starts with details on why user education is important, why you're providing it, etc. Again, the client should have been informed about the option via numerous communications before any new services are added. Also, this is where the notion of shared responsibility may weigh more heavily.

- **Free Trial: Phishing Tests**

  If you need to prove the value of Security Awareness Training to your clients, you can initiate a free 30-day trial during which you can run unlimited phishing simulations to prove your clients' susceptibility to these threats.

- **Client Testimonials**

  If you send regular newsletters or updates to your clients, the best way to encourage sales is through the testimonials of other clients who've seen the positive results for themselves.

The Return on Security Investment (ROSI)

A relatively straightforward way to determine the return on security investment is through a ROSI calculation. In addition to helping you justify to your client why they should consider security awareness training, you can also use the ROSI calculation to show return based on real-world data at other times in the contract, since it can be applied to other cybersecurity purchases beyond training.

The ROSI Formula

When calculating the return on security investment; it can be difficult to determine realistic figures to use. Incident and breach costs vary, especially when you compare the cost of a malware attack (which is more limited) to a ransomware attack that has business-wide cost implications. For simplicity's sake, the calculation example below will use a median cost of $57,000 for a cyber event. This figure is based on costs experienced by Hiscox, a Lloyds of London cybersecurity insurance broker.[6]

The Equation:

$$\frac{\text{Average Loss Expected x Mitigation Ratio} - \text{Cost of Security Solution}}{\text{Cost of Security Solution}}$$

Doing Your Own Calculation

The equation above is fairly simple, once you have the following information:

- The average cost you incur per incident, where an incident is defined as a malware infection and the resulting clean-up, or some other type of cybersecurity breach. In this example, we'll use Hiscox' median cost of a data breach: $57,000. It's best to use your own figures, if possible, but don't forget to factor in the level of effort and productivity hours lost.
- The number of incidents caused by end user/employee error in the past 12 months. For our example, let's estimate that a company with 50 or fewer employees will experience two such incidents over 12 months.
- The average loss expectancy (ALE). In this case, it would be two incidents per year times $57,000, which equals $114,000 USD per year in employee-related incident costs.
- The mitigation ratio (impact) you expect. Using what we saw in our own training figures, employee security errors reduced from 11% to 4%. That's a 64% reduction.
- Your purchase price for the training over the year, as well as your selling price. For 50 users, we'll use a $9/user/year purchase price, or $450, and an $18/user/year ARR price, or $900 charged to a 50-seat client.

Running the ROSI calculation you get:

$$\frac{\$114{,}000 \times 64\% - \$450}{450} = \frac{72{,}510}{450} = 161.13$$

Now, here's what these numbers mean.

1. For an investment of $450 on your part, you'd save $72,510 in incident-related costs, which is a 161.13x return on your security investment.
2. For your clients' investment of $900, there is a $72,060 savings, which is an 80.06x return on their security investment.

In both cases, your return on the cost (investment) is significant.

This is, by no means, a comprehensive calculation, as there are a variety of other cost factors like operational overheads not included here. However, it is nonetheless a simple way to get a strong sense of the potential return on investment when deploying Security Awareness Training, or any other security technology.

Our Commitment to Success

Webroot focuses on the needs of MSPs and SMBs, enabling them to be their most profitable and secure. We have direct visibility into the latest threats facing users around the world, and our global machine learning threat intelligence approach ensures that all Webroot-protected devices are secured in real time. Our threat intelligence also allows us to proactively produce security awareness training that is always relevant, topical, and tailored to the real-world threats end users encounter. When your clients choose Security Awareness Training from Webroot, they can rest assured they're getting best-in-class training from a security leader.

We also regularly produce white papers, datasheets and FAQs to enable MSPs and SMBs to achieve maximum success implementing Webroot cyber resilience solutions. See our white paper, Recommendations for Successful Security Awareness Programs, for more details on implementing an effective training program.

Summary

As an MSP, adding Security Awareness Training to your portfolio considerably reduces the number of security incidents that occur as a result of user error. It also helps ensure shared responsibility with your clients and fosters an understanding that a security breach is not necessarily a reflection on you or your services; it is, instead, something that you and your clients must work together to prevent. After all, cybersecurity isn't just an IT issue anymore, it's a major issue for everyone involved in a business.

In the end, by offering a service SMBs need, you benefit from an additional revenue stream, and, more importantly, you'll save countless hours in terms of infection-related technical support and remediation. Not only that, but your clients will also benefit from fewer infections, reduced costs, and lower productivity losses, as well as a stronger reputation with their own customers. Additionally, they can use Security Awareness Training to fulfill compliance requirements, such as PCI or HIPAA.

Security awareness programs also teach employees about the obligations they have to keep the companies they represent safe, which they can easily accomplish simply by keeping themselves safe online. Employees who receive end user cybersecurity training learn to avoid risk not only during working hours – whether in-office or remote – but also during personal time and using personal devices.

Ultimately, Security Awareness Training benefits SMBs and the MSPs who serve them, as well as the employees who work for them and the customers who trust them. By adding phishing simulations and cybersecurity training to your portfolio, you can grow your profits, improve your clients' resilience against threats, and create a win-win scenario for all involved.

[1] Webroot Inc. "COVID-19 Clicks: How Phishing Capitalized on a Global Crisis." (October 2020)
[2] Ponemon Institute. "2019 Global State of Cybersecurity in Small and Medium-Sized Businesses." (October 2019)
[3] 2020 Webroot MSP Security Awareness Training Survey (November 2020)
[4] Based on Webroot customer campaigns run through June 2020, excluding campaigns sent to <10 users
[5] Real-world reviews from verified Webroot MSPs on G2.com (November 2020)
[6] Hiscox Ltd. "Hiscox Cyber Readiness Report 2020." (June 2020)

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.