WEBROOT
Smarter Cybersecurity™

5 TIPS TO HELP MSPs MAKE MONEY WITH SECURITY AWARENESS TRAINING

"After 12 months of training, end users are 70% less likely to fall for a phishing attempt."

- 2019 Webroot Threat Report

Faced with today's threats, endpoint protection is a pretty obvious necessity for your clients. But even organizations with phenomenal endpoint protection are being compromised, because criminals prey on the naiveté and ignorance of your clients' end users. Ultimately, the best security in the world can't prevent an unwitting user from accidentally leaving the front door to the network wide open.

To augment the cybersecurity you provide your clients, you need cyber-savvy end users who know how to spot phishing emails and avoid risks online. Here 5 simple tips to help MSPs like you add security awareness training to your portfolio—and do it profitably.

Sell on the concept of "shared responsibility."

Well-trained users will reduce the number of security incidents a business will face, which reduces the costs associated with infections caused by unwitting user error, as well as losses in terms of user productivity and business downtime.

Once clients understand this 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 shared responsibility virtually sells itself.

Pro tip from our MSP partners: *Build training into your standard IT security services stack. 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.*

Run phishing simulations.

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.

Note: *93% of all successful security breaches start with phishing attacks.*

Verizon. 2018 Data Breach Investigations Report. (Apr 2018)

Make sure clients understand regulatory compliance requirements.

Many business sectors have specific compliance requirements. Identify whether your clients already conduct compliance training, or whether they're aware they need it, and then position yourself to provide it. You might be surprised at how many of your clients are subject to regulations.

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.

Did you know: *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.*

Don't overpromise.

Adding user education training won't make your clients' security bulletproof, but it will produce measureable user behavior changes over time that significantly reduce security risks and costs.

Keep in mind: *Your clients may expect to see results right away, but changing end users' behaviors takes time. Reassure them 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.*

Encourage clients to protect their security investment.

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 if an end user mistakenly (or unknowingly) 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.

Remember: *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.*