WEBROOT
Smarter Cybersecurity™

TOP 10 REASONS

SECURITY AWARENESS TRAINING IS A SMART MSP INVESTMENT

Cybersecurity breaches are expensive. Even if you provide industry-leading cybersecurity services, modern malware tactics are too sophisticated to guarantee 100% that your clients will stay safe. A single breach at a client site can spell countless man-hours lost to remediation and disaster recovery—not to mention the damage it does to the trust your clients place in you and your services. So what's an MSP to do?

It's not all gloom and doom. End users are on the front lines of your clients' defenses. Don't leave the future of their business (and your own) in untrained hands. Educate them.

By delivering continuous training to users at client sites, you not only improve their overall cybersecurity posture, you also protect your own business and add a new revenue stream.

Here are 10 reasons end user security awareness training is a must.

1 Weakest Link.

Let's be honest: users are the weakest link in the cybersecurity chain. Hackers prey on human curiosity, trust, negligence, and even greed to introduce malware into networks. There's a reason why phishing attacks were behind 90% of security incidents in 2016.[1] And why phishing accounts for at least 93 percent of ransomware attacks.

2 First and Last Line of Defense.

Users are generally an easy target for cybercriminals because they can be tricked into opening suspicious emails, downloading bad attachments, and visiting malicious URLs. With proper education about malware sources and training to avoid them, humans can become the first line of defense against cyberattacks. Trained properly, users learn to spot and report potential threats to security teams.

3 Wise Investment.

When the Ponemon Institute looked at phishing awareness programs, even the least effective training program still resulted in a 7-fold ROI, and that includes lost productivity time.[2] This is proof that security awareness training works and protects the bottom line.

4 Breaking Bad (Habits).

Technology alone cannot stop security incidents. But investments in security awareness help break bad habits by teaching end users about the critical role they play in keeping their organization safe. Companies that invest in training see user failure rates decline rapidly, from as much as 25 percent to 5 percent in a year.[3]

[1]Verizon. "2017 Data Breach Investigations Report." (April 2017)
[2]Ponemon Institute. "The Cost of Phishing & Value of Employee Training." (August 2015)
[3]CSOonline.com. "Does Security Awareness Training Even Work?" (September 2015)

5 No Target Too Small.

MSPs' SMB clients often assume hackers only target enterprise networks. In reality, SMBs face the same risk as large companies. Not only do SMBs handle the private and financial data hackers want, but they are also less likely to have the resources to invest in the types of security programs large enterprises can afford. In some cases, hackers even try to break into larger companies' networks through digital links with SMB partners.

6 High Stakes.

Preventing cyberattacks isn't just about avoiding malware infections. Depending on the extent of the damage, an attack can deliver financial and legal blows, erode customer loyalty and trust, and even threaten the survival of a business. For MSPs, an attack on a client is by extension an attack on their business, and poses similar threats.

7 Threats Aplenty.

From phishing to drive-by downloads, malvertising to ransomware, social engineering to code injection, threats are so numerous and varied that users can't keep up without education. Users not only need awareness training, they appreciate its benefits. With training, their own data is also less likely to be compromised, making it relevant to them on both a personal and professional level.

8 Work in Progress.

Cybersecurity training isn't a one-off. The threat landscape is always evolving, making user education an ongoing endeavor. Make sure clients understand their users need recurring high-quality, relevant, actionable training. Research shows that changing employee behavior through continuous security education can reduce the risk of a security breach by an average of 50 percent.[4]

9 Assured Compliance.

Many industries, such as financial services, healthcare, energy, and others, require end user awareness training at least annually. Depending on their industries, your clients could face stiff fines for neglecting compliance training.

10 The Trifecta.

Security awareness training is a win-win-win scenario. The user wins by becoming more aware and more secure. The company wins because its risks are measurably reduced and its compliance record stays in good standing. And the MSP wins by minimizing its remediation time and costs, providing relevant security service value to clients, and expanding its portfolio of revenue opportunities.

About Webroot

Webroot delivers 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.

[1]Aberdeen Group. "Security Awareness Training: Small Investment, Large Reduction in Risk." (July 2017)."