CARBONITE® + WEBROOT®
opentext™ Business Solutions

10 Reasons MSPs Should Add Security Awareness Training to Their Offering

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.

Learn why training is a must in today's cyber-climate.

1 End users are the weakest security link.

Whether we like it or not our users are the most vulnerable and exploited link in being the reason behind successful cybersecurity breaches. The latest (2021) Verizon Data Breach report highlighted that 85% of successful breaches were down to phishing and pretexting (scams) that they class as social engineering. Bad actors know that preying on human curiosity, trust, negligence, good intentions and greed are all ways to compromise systems and networks[1]. The Webroot COVID-19 Clicks report that samples 7,000 respondents from around the world found an average of 29% or respondents had clicked on a phishing link in the past year and many didn't take appropriate pre-breach precautions or post-breach action to inform or even change passwords![2]

2 End users are ALSO the first 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 Training is a 'smart' investment.

According to the 2021 Verizon Data Breach Investigations Report this is what they said in the Control 14: Security Awareness and Skills Training section: "Considering the high prevalence of Errors and Social Engineering, it is obvious that awareness and technical training are probably a smart place to put some dollars to help support your team against a world full of cognitive hazards." Our own customer data shows that running training alongside endpoint sees customer experiencing 20% less infections that using endpoint security just on its own.[3]

4 It's time for 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.

5 No target is 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 The stakes are high.

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 abound.

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 It's always going to be a 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.

9 Training helps ensure regulatory 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 Embrace 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.

Become an MSP partner

Webroot offers a family of services and solutions that protect users and devices no matter how or where they connect, across all the stages of a cyberattack. Our multivector endpoint protection, mobile protection, DNS protection and security awareness training help make businesses their most secure, and MSPs their most profitable.

To learn more about how multivector protection from Webroot can help you keep clients safe and more profitable, visit www.webroot.com/MSPpartners.

[1] 2021 Verizon Data Breach Investigations Report (May 2021)
[2] Webroot Inc. "COVID-19 Clicks: How Phishing Capitalized on a Global Crisis" (September 2020)
[3] Webroot Inc. "2020 Webroot Threat Report." (February 2020)

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.