

Irish MSP helps clients defend against cyberattacks with security awareness training



At a glance

Products

Webroot® Business
Endpoint Protection

Webroot® Security
Awareness Training

Website

<https://www.ortus.ie/>

Key Findings

Efficacy

38% increase in ticket volume after completing training

Clients increasingly aware of potential threats

89% fewer cases of phishing attacks

92% of clients have completed training

There's no doubt that Webroot® Security Awareness Training has had a hugely beneficial effect. Clients are becoming more wary of suspicious emails and, as a result, are logging more support calls with us."

- Bryan Fitzpatrick

Background

For over six years, Bryan Fitzpatrick has worked in the Department of Professional Services for Irish MSP Ortus. The company helps clients get the most out of technology by implementing, managing and supporting secure IT solutions.

With security breaches at an all-time high and the recent attack on the HSE, security has become a key concern for many of the company's clients. To help provide a robust defence against cyber threats, Ortus regularly meets with customers to review their IT infrastructure, advise on cyber security and ensure that the right systems are in place to protect their business.

GDPR compliance has also become a top priority as Fitzpatrick notes, "The GDPR has placed an extra onus on clients to demonstrate that they take data protection seriously. In the event of a breach, one of the first things the Irish Data Protection Commissioner will do is investigate what steps a company has taken to safeguard data."

"In addition to the more obvious technological defences such as encryption and anti-virus, they will also be asked if they've provided security awareness training for staff. If they are unable to tick all the boxes, they could face crippling fines, damage to reputation and an increased risk of cyberattacks. With such high stakes, it's just too risky to leave anything to chance."

To help clients comply with the regulation, Ortus regularly reviews any gaps in coverage and advises clients to implement Security Awareness Training to bolster their defences.

Before Webroot® Security Awareness Training

Prior to implementing Webroot® Security Awareness Training, Ortus could see a trend emerging and the real-world damage that could result from a phishing attack. The company understood the importance of a holistic approach to cyber security rather than just focusing solely on the technological side of things.

Fitzpatrick explains, "Part of our job is to make sure we have all our clients' bases covered. Security software is obviously an important part of this but it's only one line of defence. Human error remains the number one cause of all cyberattacks so, it's crucial that staff receive regular security awareness training to educate them on evolving threats."

"Without this training, all it takes is one employee to click on a link or download a malicious attachment and a company's data could be compromised within a matter of minutes."

Fitzpatrick believes that from a business owner's point of view, one of the biggest moments of trust in any organisation is giving new or existing employees access to company data. "This data needs to be protected and used responsibly. Many employees are simply unaware of the value of this data and the damage that could ensue if it fell into the wrong hands. Educating staff on the risks is key in creating a shared responsibility for the everyday data they work with."

"Security awareness training shouldn't be an afterthought; it should start on day 1. If the correct behaviour is ingrained from the get-go, staff will act responsibly and gain a better understanding of how their actions contribute to the overall security of the company."

After Webroot® Security Awareness Training

Since implementing the training, Ortus has noticed a significant improvement in security awareness amongst its clients. Fitzpatrick explains, "There's no doubt that the security awareness training has had a hugely beneficial effect. Clients are becoming more wary of suspicious emails, and as a result, are logging more support calls with our team. This demonstrates that the training is really making an impact and the message is hitting home. We would rather customers log a million tickets about potential phishing emails than make the mistake of clicking on one."

For most clients, the alternative to being careful is two weeks of expensive downtime wondering how they got hacked. "It takes about 10 minutes for us to check an email versus two weeks of hell. The training itself takes between 8-10 minutes so clearly, it's a no-brainer."

Protecting business owners is Ortus' top priority. When Fitzpatrick explains the benefits of Webroot® Security Awareness Training to his clients, he often asks "What's two weeks of your time worth? What do you turn over in a day? I would multiply that by two weeks or possibly a month. If you fell victim to a ransomware attack, it could be weeks before your business is back up and running again, and that's if you're lucky. Are you willing to take the risk?"

Conclusion

In addition to reducing risk, Fitzpatrick believes Webroot® Security Awareness training is effective for a number of reasons, "The training can be customised with company branding, it provides business owners with detailed reports and lastly, it ticks the compliance box by evidencing data protection responsibilities."

Security awareness training is one of the most effective and cost-efficient ways to prevent cyberattacks. Well-trained employees know the best ways to identify, respond to and recover from an attack.

"Ultimately, our clients appreciate that as their IT partner, we want to keep them protected and help them make the most out of their IT security budget."

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.