



In-use Cyber Resilience Portfolio

 Backup Train Block Protect Restore

At a Glance


Vertical
MSP

Shared Technical Services Manager
Anjali Godya

Users Targeted
3,945 for Webroot® Security
Awareness Training

Products Used
Webroot® Business Endpoint Protection
Webroot® DNS Protection
Webroot® Security Awareness Training

Website
<https://mytech.com/>



Webroot® Security Awareness Training has essentially helped close the security gaps that humans create, making our clients more resilient overall.

Anjali Godya, Shared Technical Services Manager,
Mytech Partners

Adding Webroot® Security Awareness Training helps Mytech Clients Close Gaps in Security

Background

In 2000, Mytech Partners was founded in the Twin Cities region of Minnesota with the mission of providing managed and co-managed IT services. In 2015, they expanded and began supporting clients in Colorado. Anjali Godya has worked for Mytech for the last five years and currently serves as its shared technology services manager. In that role, she has overseen Mytech's deployment of Webroot® Business Endpoint Protection and Webroot® DNS Protection to its customer base.

The Challenge

Mytech's clients serve numerous industries, including health care, manufacturing, financial services, and others that are subject to compliance regulations. And they work with businesses of all sizes, from small shops with a handful of employees to larger businesses with multiple branch offices.

"Phishing and business email compromise continue to be a big problem, and we wanted to raise our clients' awareness," Godya explains. "Many of our clients need security training for two reasons: first, to avoid phishing and other risks; second, to fulfill requirements for security compliance. Both of these are strong incentives."

Godya and the rest of the team at Mytech were already certain of the need for a security awareness training program with phishing simulations. The question was how best to demonstrate the value to clients and integrate it into their existing security offerings.

The Solution

Since Mytech already had endpoint and DNS protection from Webroot, adding Webroot® Security Awareness Training was a natural choice. All three are managed through the same admin interface and integrated with the remote monitoring and management (RMM) tool Mytech was already using, making it easy to bundle with other protection services.

As part of her commitment to proactive security, Godya has enrolled almost all of Mytech's customers in training and sends phishing simulations regularly. "Our users look forward to the training. We send a wide variety of topics and our clients appreciate that the training mimics real-world scenarios."

"The content and wide variety of phishing templates Webroot provides, especially their newest material, is just phenomenal. Our clients are extremely pleased with it. And the rate at which Webroot issues new content creation has really helped us ensure our clients are learning about the most relevant, most up-to-date threats they may face and how to avoid them."

– Anjali Godya, Shared Technical Services Manager, Mytech Partners

Godya has also found ways to optimize training administration. A few months ago, she activated the Microsoft® Azure Active Directory integration, which enables administrators to control which users and groups should be synced to serve as targets for campaigns, and keeps the list updated automatically as users are added, updated, or removed in Azure AD. "The Azure AD functionality has been extremely helpful," she reports. "We can easily see and manage who is supposed to get training."

Conclusion

Godya says administration time has been significantly reduced. Thanks to the Azure AD integration, additions and deletions take almost no time at all, and Mytech staff can easily ensure all users get the training, even as their clients onboard new employees and offboard departing ones. Additionally, the Global Campaigns Manager allows the team to send the same phishing simulations and training campaigns to thousands of end users across their sizeable client base.

"The trick is to find the right cadence. We know it has to be regular to be effective, but we don't want it to be too predictable, or else it could skew the results. I find it's best to switch up the schedule to keep end users on their toes, while still maintaining regular delivery."

– Anjali Godya, Shared Technical Services Manager, Mytech Partners

Not only has overall client awareness increased, but Godya says they've seen a subsequent decline in the number of threats those clients face. "They are much more cautious now about emails and the types of software they install. They understand better how to take care of their identities, as well as sensitive company information, and avoid social engineering scams. Webroot Security Awareness Training has essentially helped close the security gaps that humans create, making our clients more resilient overall."

Results

- Deployment for three security solutions integrated into a single console
- Cybersecurity threats declined since training implemented

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.