opentext™

Survey says...

MSPs (and their clients) benefit from offering security awareness training

We surveyed hundreds of MSPs around the world about their cybersecurity training offerings.

Here's what we learned.

OpenText recently surveyed more than 200 MSPs around the world to gauge their phishing awareness and learn about their clicking habits. We thought this was important to do because of the pervasive misconception that endpoint security and a firewall are sufficient protection from online threats. But cyberattacks are increasingly interpersonal affairs, and hacking the human is often a more surefire path to success for cybercriminals.

The results of our study show that, while there's still a need for awareness of that fact, many organizations are catching on. Here's what the data tell us about the problem and how it could be solved.

Phishing is a big problem and users aren't exactly helping.

Types of attacks experienced by SMBs[1]

In our survey, **29% of workers worldwide** admitted clicking at least one phishing link in the past year.

In the United States, it rose to **1 in 3 workers.**

The #1 barrier to adopting security training? **Their clients.**

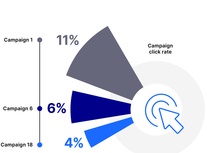
#1

Only 45% of MSPs surveyed offer security awareness training, but MSPs often aren't the problem.

Is there anything preventing you from delivering more SAT?

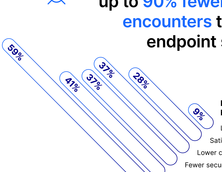
When adopted, training works.

OpenText data show click-rates on phishing emails drop drastically with ongoing training.



In fact, businesses that use OpenText Core Security Awareness Training experience

up to 90% fewer malware encounters than those with endpoint security alone.[2]



Here are some of the other benefits they're reporting:

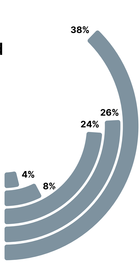
- Lower support costs
- Satisfied compliance requirements
- Lower click rate on simulations
- Fewer security incidents in general
- Fewer phishing incidents
- More suspicious emails being reported

In all, a whopping

97% of the MSPs surveyed

who conduct training reported seeing some benefit. But many are still unsure how it fits into their offerings.

How MSPs package SAT?



How do businesses use OpenText Core Security Awareness Training?

These are some of the main reasons, according to real user reviews on G2 Crowd:

To achieve compliance
We need to comply with PCI and GDPR, and awareness training is a requirement."

To identify high-risk users
Helps us identify end users that easily fall for phishing schemes."

To onboard clients
Using this as a hook for potential clients is a great way to get a foot in the door at very low cost."

To stop risky behavior
Drastically lowered the number of users who have given their email credentials out."

Now, we'd like to hear from you.

Do you offer cybersecurity training to your clients? Why or why not? Let us know in the comments!

For more about the study and how you can approach the topic with skeptical clients, check out this guide.

About OpenText Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

1 Ponemon Institute, *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses*. (October 2019)

2 Based on internal Webroot data from April-September, 2020

opentext™