EXIGENT

Vigilant Awareness

Security Awareness Training

Your best line of defense against today's sophisticated cybercriminals is sitting right in your office.

Your employees get phishing emails every day. While cybersecurity tools capture and filter out many phishing emails, hackers are persistent and increasingly innovative, so it's only a matter of time before a threat lands in the inbox of one of your employees and they take the bait.

With Vigilant Awareness security awareness training, Exigent will educate your team on how to spot suspicious activity and create new, safer habits. Effective security awareness training improves your company's cybersecurity culture and reduces phishing email clicks by your employees by as much as 70%.

Unlike traditional security training, our approach is engaging, empowering, and personalized. When you treat your employees as an asset instead of creating anxiety and fear, you'll find they are more than willing to be part of the solution. By inspiring your employees to step into their critical role as key defenders in safeguarding your company, you create a culture of engagement that strengthens security across the entire organization. That is exactly what Exigent Vigilant Awareness does.

Protect Productivity and Your Reputation

Security awareness training significantly reduces the risk of downtime by avoiding its leading cause – a cyber attack triggered through email. With a heightened level of cybersecurity awareness, you are protecting not just your assets but your business reputation. When customers can't be serviced and your employees are sitting idle, your organization loses money and, potentially, clients. Don't let that happen.

Our training focuses on four main themes:

- **Train Everyone**
- **Expect Mistakes**
- **Set Goals**
- **Don't Punish Mistakes**

Compliance and Insurance Requirements

If your organization is one of the many governed by strict compliance standards, you'll find security awareness training provides additional support. More and more compliance programs require a security awareness program, including:

- SOX
- 23 NYCRR 500
- PCI DSS
- HIPAA
- ISO/IEC 27001
- ISO/IEC 27002
- FISMA
- GDPR and other privacy laws

Security awareness training is also typically required to get and maintain cyber liability insurance.

FAQ

What is phishing testing?
Phishing testing educates employees and reduces the risk of phishing attacks in your company through automated phishing emails periodically sent to members of your team. By using phishing simulations, we will test your employees in their own environment and train them at the point of infraction, creating best practices and good habits over time.

What happens if my employee clicks on a phishing test?
If employees click on one of our phishing tests, they are redirected to a landing page with a brief training experience, which includes a short, humorous, but educational video along with tips on how to spot and avoid phishing emails in the future.

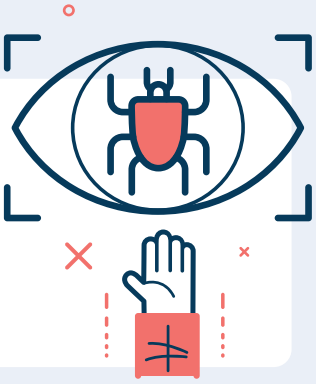
Does phishing testing really work?
Absolutely. In fact, after 12 months of consistent training, an employee is 70% less likely to click on a phishing email.

Who should receive phishing testing?
We believe all employees should receive phishing tests. No one, not even the C-suite or IT team, is above risk. In fact, those departments are targeted the most by phishing attacks. Plus, a security-aware culture comes from the leadership level down. If your leaders don't receive phishing tests and aren't modeling improved behavior, what does that say to the rest of the company? Train everyone.

BY THE NUMBERS

90% of cyber attacks start with a phishing email

287 days is the average amount of time it takes to identify and contain a data breach



The number of phishing attacks **doubled** between 2021 and 2022, and those numbers continue to rise