

## Safeguard Your Business with Security Awareness Training

Today's cyber threats are smarter, faster, and more sophisticated than ever. Even the most advanced security technologies can't fully protect your business without one critical element: An educated, vigilant team.



## Introduction: Why Security Awareness Training Matters

Today's cyber threats are smarter, faster, and more sophisticated than ever. Even the most advanced security technologies can't fully protect your business without one critical element: An educated, vigilant team.

At Exigent Technologies, we believe that people are your strongest defense against cyber attacks—when armed with the right knowledge. Through The Exigent Method, we empower growth-oriented businesses to build a culture of cybersecurity that supports long-term success and resilience.

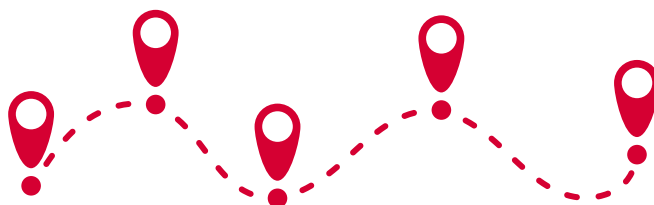
Security awareness training isn't just another box to check—it's a critical investment in protecting your assets, your reputation, and your future.



## The Exigent Method

At Exigent, we have a strategy that combines long-term vision with quarterly agility, ensuring we're always prepared to innovate and overcome challenges by aligning resources with our strategic vision. We apply that same strategy with clients: The Exigent Method.

We uncover your business aspirations, identify key tactical areas, and pinpoint potential obstacles. This collaborative process allows us to tailor a precise IT roadmap—one that uses the right solutions to empower your business with the exact technology stack it needs to execute on your long-term vision.



## What is Security Awareness Training?

Security awareness training is an ongoing education process that teaches your employees to recognize, respond to, and prevent cyber threats like phishing scams, malware, social engineering, and more.

A reputable security awareness training program integrates real-world simulations, positive reinforcement, and ongoing education to create a workforce that is truly security aware—laying the foundation for a security-first culture in your organization.

Key elements of any effective training include:

- Simulated phishing and cyberattack exercises
- Personalized learning paths
- Continuous reinforcement through microlearning
- Positive, non-punitive behavior coaching (PsySec approach)

When you select the right training program and partner, it can transform your employees into active participants in your cybersecurity strategy—turning your greatest risk into your strongest asset.

## How Does Security Awareness Training Work?



Rather than relying on annual sessions that quickly fade from memory, effective security awareness training should focus on building daily habits.



Training is woven seamlessly into the workday using:

- Phishing simulations in your employees' inboxes, followed by instant feedback
- Short, engaging videos are used to help keep employees focused on the message
- Interactive modules tailored to each employee's role and risk level
- Gamified experiences to boost engagement and reinforce learning



By reinforcing good security behaviors over time, security awareness training helps businesses make cybersecurity second nature—not a burden.

## What Does Security Awareness Training Cost?

Cost should never be a barrier to protecting your business. Many reputable, effective programs are highly affordable and scalable. Typically, companies can expect to invest between \$10 and \$40 per employee per year for training.

Additionally, the ROI on cybersecurity awareness training is high—**when done correctly, SAT can reduce phishing clicks as much as 70%**. Imagine what that could save your business when compared to the cost of a data breach or ransomware attack, which come with legal fees, fines, operational downtime, reputational damage, and more.

## Why Is Security Awareness Training Critical?



### Cyber Threats Are Evolving

AI-powered phishing, ransomware, and vishing attacks—modern threats require modern defenses. Ongoing training keeps your team ahead of evolving attack vectors.



### Compliance and Regulations

Security awareness training is a requirement under many major compliance frameworks, including:

- HIPAA (Healthcare)
- PCI DSS (Payment processing)
- SOX (Public companies)
- GDPR (Data protection for EU citizens)
- CMMC and ISO 27001 (Cybersecurity frameworks)

Failing to train employees can lead to fines, audits, and more.



### Cyber Insurance Demands

Today's cyber insurance policies increasingly require documented security awareness training as part of coverage conditions. Insurers know that educated employees are your best first line of defense.



### Remote Work Challenges

Remote and hybrid environments expand the threat surface exponentially. Security awareness training keeps remote workers vigilant and protected across unsecured networks, personal devices, and decentralized environments.

## Building a Security-First Culture

A true cybersecurity culture doesn't happen by accident. Rather, it is a thoughtful, layered approach to addressing cybersecurity throughout the business, at every layer. It often starts in the C-suite with leadership committed to protecting the organization, its data and assets, and its employees.



To start:

- Create security policies that employees understand and follow (simple is always best!)
- Conduct phishing simulations and real-world training exercises (remember, ongoing education is key)
- Reward and recognize good cybersecurity behaviors (find your SAT champions and utilize them to spread the word)
- Embed security education into every level of the organization—from the C-suite to the newest hire (no one is above training)

Wrap training around an integrated approach to cybersecurity technology, and you'll start seeing the entire organization shift toward a "defense at depth" security posture.

## Exigent's Approach: Vigilant Security Awareness Training

At Exigent Technologies, we deliver a Security Awareness Training solution designed to meet your business's unique needs, challenges, and goals.

- Tailored training plans aligned to your industry and compliance needs
- Ongoing reinforcement with updated threat intelligence
- Regular reporting and assessments to measure program success
- Expert consultative support to adapt and evolve your strategy

When integrated with our Assurance Managed Services, your organization gains a strategic partner focused on stability, integrity, and long-term success.

## Ready to Empower Your Team?

Schedule a consultation to learn more about Vigilant Security Awareness Training today.

