# CRITICAL FAULT
## PROFESSIONALLY PARANOID

# SECURITY AWARENESS TRAINING

## In-Person Training Sessions

The first step toward securing your company's networks, systems, and data is ensuring your employees receive effective security awareness training. 95% of security breaches are caused by human error. These security breaches range from hacking attacks to accidental data exposure. Every employee has role to play in defending against security incidents.
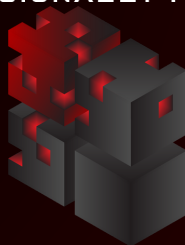
## Training Provided:

General Employee Training
Physical Security Training
IT Security Training
Administrative Training
Executive Training

*Employee training includes complimentary attendance and participation reports, plus follow-up security quizzes by email.*

# CRITICAL FAULT
## PROFESSIONALLY PARANOID

## In-Person Security Awareness Training

### GENERAL EMPLOYEE TRAINING

Teach your employees how to recognize social engineering attempts, how to properly protect data and prevent exposures, and how to recognize threats when they occur.

### PHYSICAL SECURITY TRAINING

Teach employees about how to prevent physical access to company buildings and hardware by securing access controls and recognizing social engineering tactics.

### IT SECURITY TRAINING

Refresh your IT team's security awareness with detailed cybersecurity training tailored to Information Technology Professionals. Train your IT team to be prepared for a possible cyber incidents with vulnerability management, key management, and supply chain management training, and more.

# CRITICAL FAULT
## PROFESSIONALLY PARANOID
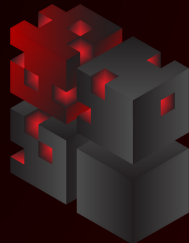
## In-Person Security Awareness Training

### ADMINISTRATIVE TRAINING

Teach your administrative team about information security regulatory compliance, such as PCI DSS, HIPAA, and CMMC. Understand the cybersecurity lifecycle and its effect on business operations and regulatory requirements.

### EXECUTIVE TRAINING

This training course is designed for C-Suite Members and Executives. Learn how to incorporate security awareness into leadership and understand the big picture when it comes to protecting your data, compliance and regulatory needs, incident response and business continuity planning, and more.

# CRITICAL FAULT
## PROFESSIONALLY PARANOID
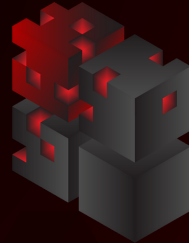
| | | |
|---|---|---|
| **General Employee**<br>Topics Included: | **90 Minutes**<br>Social Engineering, Data Handling/Exposures, Recognizing Incidents | **$750** |
| **Physical Security**<br>Topics Included: | **60 Minutes**<br>Access Controls, Physical Security Safety, Doors and Locks, Social Engineering | **$500** |
| **IT Security**<br>Topics Included: | **90 Minutes**<br>Cybersecurity Lifecycle, Hacker Prevention, SCADA, Wireless Security, Supply Chain Management, Ransomware | **$750** |
| **Administrative**<br>Topics Included: | **60 Minutes**<br>Audit, Regulatory Compliance, Supply Chain Management, Cybersecurity Lifecycle, Password Management | **$500** |
| **Executive**<br>Topics Included: | **60 Minutes**<br>Security Leadership, Regulatory Compliance, Audit, Risk Assessments, Gap Assessments, Security Frameworks | **$500** |

| | | |
|---|---|---|
| **Additional Training Options** | **Phishing Campaign**<br>Critical Fault puts your employees to the test by administering a phishing campaign, tracking click metrics and identifying areas of improvement | **$1500** |