



CMMC

# AWARENESS & TRAINING

**Your People. Your Strongest Defense.**

Hackers don't need to break your firewalls if they can trick one of your people. A single careless click can hand over your contracts, your data, and your reputation. The Awareness & Training family ensures your employees aren't your weakest link, they're your first line of defense.

## Proof of Practice

Examples

- ✓ **Security Awareness & Training Policy**  
Defines who must complete training, how often, acceptable delivery methods, and includes a role-to-training mapping table.
- ✓ **Training Content**  
Copies or samples of the materials used for awareness and role-based training (e-learning modules, slides, videos, newsletters, phishing simulations).
- ✓ **Training Records**  
Proof of completion showing participant names, dates, and training types. Can be an LMS report or a spreadsheet.


## The Business Impact

A phishing email doesn't just cost money, it can expose CUI, trigger reporting, and jeopardize DoD contracts. Regulators and primes now require proof of training. Done right, awareness programs protect contracts, cut downtime, and prove your business is a trusted partner in the defense supply chain.

## Available Resources

-  **DoD Cyber Awareness Challenge**  
<https://www.cyber.mil/cyber-awareness-challenge>
-  **DoD Insider Threat Training**  
<https://securityawareness.dcsa.mil/itawareness/index.htm>
-  **CISA Cybersecurity Awareness Resources**  
<https://www.cisa.gov/resources-tools/all-resources-tools>
-  **Ninjio Security Awareness Training**  
<https://ninjio.com/>
-  **KnowBe4 Security Awareness & Phishing Platform**  
<https://www.knowbe4.com/>

## Quick Wins

-  1. Publish a Security Awareness & Training Policy
-  2. Establish company-wide security training program for all employees
-  3. Establish specialized training for privileged users
-  4. Launch a centralized training tracker
-  5. Conduct simulated phishing attack to measure current risk