



Avoid Sophisticated Cyberattacks with Omega Systems' CAT+

Maintaining appropriate organizational-enforced security against cyber threats is a must! With each new threat, cyber criminals level-up their execution, targeting specific industries, organizations and even individuals. Keep your staff on their toes and armed with always-fresh cybersecurity training, presented in a way that is sure to stick!

●●● **90% of cyberattacks are caused by human error; Therefore, many cybersecurity defenses and investments can be undermined by a single absent-minded click.**

Fortify your Human Firewall.

Omega Systems' CAT+ gives you access to the world's largest cybersecurity awareness training library, with always-fresh and engaging content. Business-centric features like targeted training, smart groups, automated awareness, advanced reporting and active directory integration create a solution that checks all the boxes of your fully-mature and up-to-date cybersecurity training strategy.

Assess, Evaluate, Educate

- ✓ **Automated Security Awareness Program (ASAP)**
Customized, fully-mature security awareness training program.
- ✓ **Assessments**
Measures user security knowledge to determine baseline and forward-moving awareness metrics.
- ✓ **Training Access Levels I - III**
Access to 950+ user compliance and security training content - live-action videos, games, micro-modules, quick-reference posters, and newsletters.
- ✓ **Automated Training Campaigns**
Training roll-out automation with reminder emails for all users.
- ✓ **Security 'Hints & Tips**
Library of threat emails for employee reference and on-going compliance training.

Beyond other training platforms, Omega Systems CAT+ includes "Simulated Phishing Attacks" and the "Phish Button," both leveraged for your employees to actively practice the human firewall exercise. These features train your team to effectively detect and report suspected threats, and provide the tools to strengthen the whole of your company-wide defenses. When a phony email is spotted (real or simulated), your team can click the phish button to automatically send the suspicious email directly to Omega-badged SOC Experts for professional review. A caught phishing attack will be professionally handled and the forensic knowledge will be applied to your entire network.

CAT + is an optional service that can be added to a Smart Secure (Managed Cybersecurity) service contract. For more information regarding Smart Secure visit: <https://omegapa.com/managed-cybersecurity/>
Call to request this service. **610.678.7002**

Omega Systems eases the burden of integration

Integration involves the resources of time, bandwidth and attention. No need to wait for a window of available time; CAT+ affords you the benefit of professionally managed integration, setup and maintenance from Omega's SOC Team, while you remain focused on your daily responsibilities and workload. Once integrated, our technicians help you zero in on your ideal training strategy, making campaign recommendations that align with your market, specific business composition and most importantly, your employees' varying levels of proficiency.

Combat Social Engineering

- ✓ **Unlimited Phishing Security Tests**
Year-round, unlimited phishing attack simulations.
- ✓ **Vishing Security Test**
Simulated voice phishing calls to your employees.
- ✓ **USB Drive Test**
Tests users' reactions to unknown USBs found in and near their workspace.
- ✓ **Social Engineering Indicators (SEI)**
Dynamically trains users with instant-view report cards and wrong answer red flags.
- ✓ **AI-Driven Phishing**
Uses AI to automatically personalize a user's experience that adapts to their current level of knowledge.
- ✓ **AIDA™ Artificial Intelligence-driven Agent BETA**
Uses AI to simulate various attack vectors of social engineering (phishing, smishing and vishing)
- ✓ **Phishing Reply Tracking**
Tracks simulated phishing email replies to ID where training reinforcement is needed

Customize Your Training

- ✓ **Active Directory Integration (ADI)**
Automatically synchronizes your AD user information with the training platform.
- ✓ **Virtual Risk Officer™**
IDs at-risk users or groups for future data-driven decision making.
- ✓ **User Event APIs**
Customizable security event activities (per user) reinforce awareness on an individual basis.
- ✓ **Smart Groups**
Create dynamic training groups to train users based on risk-level (department, behavior, location, etc.).

Restrict, Monitor & Report

- ✓ **Industry Benchmarking**
Monitor and Compare your business' Phish-prone percentage with competitors.
- ✓ **Monthly Email Exposure Check**
Deep web search crawling that hunts for data resembling any of your organization's email addresses or at-risk end users.
- ✓ **Advanced Reporting**
Reports your organization's specific security awareness performance with insights and metrics pulled from any period of time.
- ✓ **Reporting APIs**
Customizable reports and dashboards.
- ✓ **Security Roles**
Delegates and restricts employee access to security training data metrics.