Steer Clear of Today's Sophisticated Cyber Attacks with Actionable Techniques

Maintaining appropriate organizational-enforced security against cyber threats has become a unique challenge. With each new threat, cyber criminals level-up their execution, targeting specific industries, organizations and even individuals and widespread effects are felt regardless of a business' type, size or locale. Understanding the current state of cyber security awareness and implementing a robust, preventative awareness training program for employees can go a long way in overcoming a threatening cyber landscape.

Omega's Advanced Security Awareness Training includes:

- **Unlimited Phishing Security Tests**
  Year-round unlimited simulated phishing attacks with use of all phishing templates.
- **Training Access Level I**
  Segmented training modules with Phish Alert Button training and quick reference awareness posters.
- **Training Access Level II**
  Access to 100+ training, video and micro-modules regarding end user compliance and security.
- **Automated Security Awareness Program**
  Quickly create a customized, fully-mature security awareness training program.
- **Smart Groups**
  Create dynamic training groups to train users based on risk-level (department, behavior, location, etc.).
- **Assessments**
  Measured user security knowledge to determine baseline and forward-moving awareness metrics.
- **Virtual Risk Officer**
  Leverage the latest functionality to ID at-risk users or groups for future data-driven decision making.
- **Priority Level Support**
  Top-of-queue placement of support tickets.
- **Phish Alert Button**
  One-click add-in button that gives users a safe way to report email threats.
- **Phishing Reply Tracking**
  Track simulated phishing email replies to ID where training reinforcement is needed.
- **Active Directory Integration (ADI)**
  Automatically synchronizes your AD user information with the training platform.
- **Industry Benchmarking**
  Monitor and Compare your business' Phish-prone percentage with competitors.
- **Advanced Reporting**
  Report your organization's specific security awareness performance with insights and metrics pulled from any period of time.
- **Crypto-Ransom Guarantee**
  Ransom payments made on your behalf* if you are infected with ransomware.
  *Terms and conditions apply.
- **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.
- **Vishing Security Test**
  Simulated voice phishing calls to your employees.
- **Automated Training Campaigns**
  Training roll-out automation with reminder emails for all users.
- **Reporting APIs**
  Customize reports and dashboards using your organizations user and group data.
- **User Event API**
  Send custom security events to users to advance awareness on an individual basis.
- **Security Roles**
  Delegate and restrict employee access to security training data metrics.
- **Social Engineering Indicators (SEI)**
  Dynamically train users with instant-view report cards and wrong answer red flags.
- **USB Drive Test**
  Test users' reactions to unknown USBs found in and near their workspace.
- **Security "Hints & Tips"**
  Library of threat emails for employee reference and on-going compliance training.