TERRANOVA
SECURITY

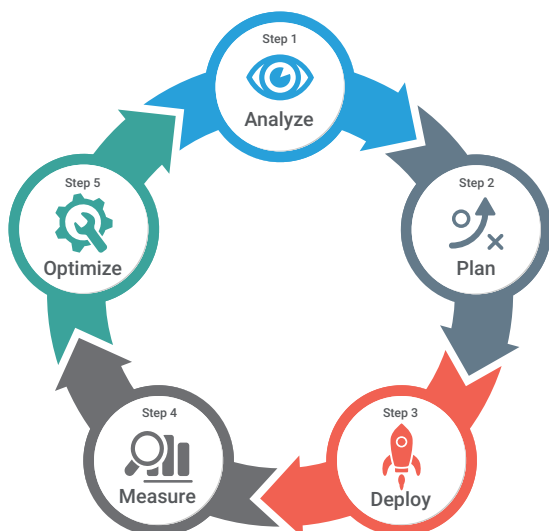## REDUCE HUMAN RISK WITH LONG-TERM BEHAVIORAL CHANGE

Security Awareness Training

Phishing Simulation Platform

GDPR Training

BUILD IMPACTFUL PROGRAMS BASED ON THE PROVEN SECURITY AWARENESS 5-STEP FRAMEWORK

Step 1: Step 1 · Analyze

Step 2: Step 2 · Plan

Step 3: Step 3 · Deploy

Step 4: Step 4 · Measure

Step 5: Step 5 · Optimize

Step 1: Analyze your organization's needs and objectives and develop a cyber security awareness program that generates results.

Step 2: Plan your program to stay on track and engage your workforce as well as your stakeholders.

Step 3: Deploy an effective training initiative and witness behavior change as it happens.

Step 4: Measure the performance of your program against your objectives and demonstrate progress to stakeholders.

Step 5: Optimize campaigns accordingly and update your program to incorporate new insight.

Design security awareness programs that deliver measurable improvements in security, drastically reduce breaches and protect from data loss.

SECURITY AWARENESS TRAINING

Security Awareness (28 topics)

- Introduction to Information Security
- Passwords
- Email
- Malware
- Phishing
- Identity Theft
- Social Engineering
- Social Networks
- Confidentiality on the Web
- Protecting Your Home Computer
- Working Remotely (Mobile Users)
- Mobile Devices
- Traveling Securely
- Cloud Computing
- The Clean Desk Principle
- Physical Security
- Access Control
- The Bring Your Own Device (BYOD) Trend
- Privacy
- Information Classification
- Information Lifecycle
- Intellectual Property
- Protecting Payment Card Data
- Ransomware
- Data Leakage
- Incident Reporting
- Business Email Compromised
- Unintentional Insider Threat

Microlearning (3 minutes)

- Vishing
- Web Phishing Through Search Engines
- Mass Market Phishing
- Phishing via SMS
- Spear Phishing
- Top Executive Phishing
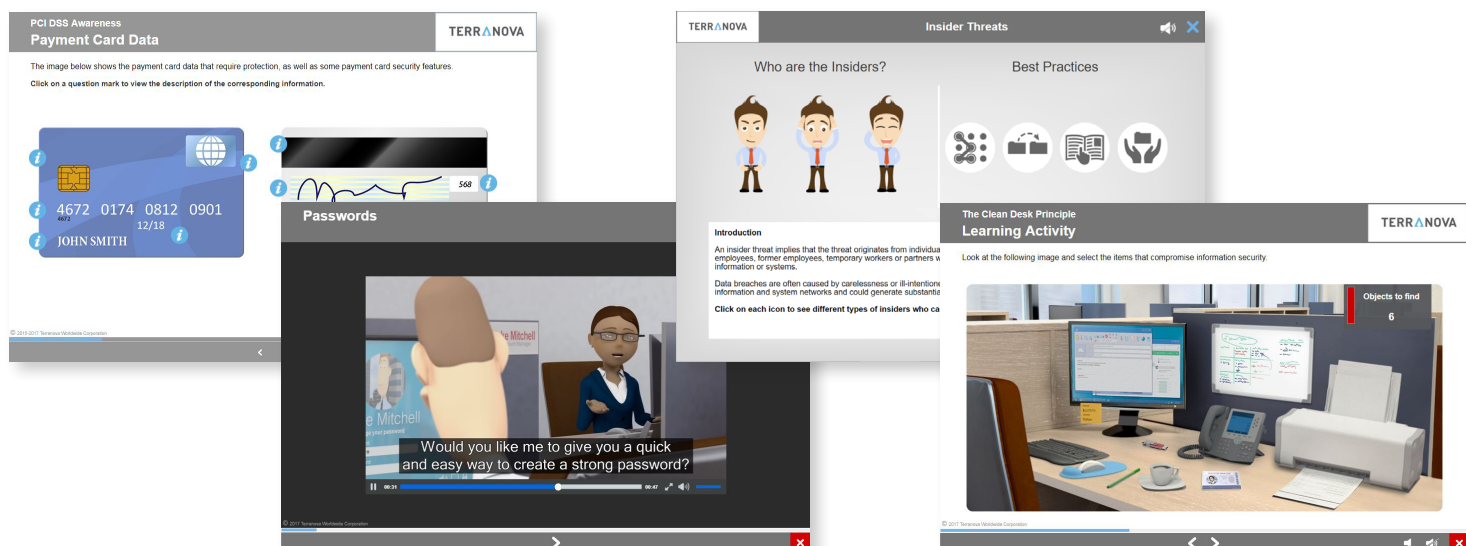- C-Level Email Impersonation

Nanolearning (1 minute)

- Being Security Aware
- Cyber Attack Detection
- Identity Theft
- Phishing - 6 clues
- Preventing Security Breaches
- Protecting Sensitive Information
- Ransomware
- Social Engineering
- Social Network
- Wi-Fi Security

GDPR and Privacy

- Privacy Awareness
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- GLBA
- HIPAA/HITECH
- General Data Protection Regulation (GDPR)
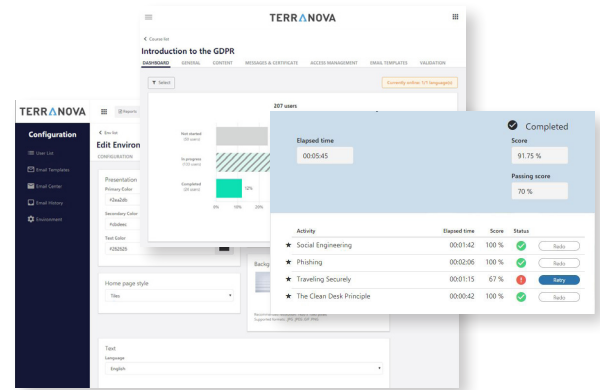- Privacy Shield

Compliance and Governance

- PCI DSS
- Business Continuity Awareness
- Code of Ethics and Business Conduct
- Records Management
- Sustainable Development Awareness
- Fraud Risk Management (FRM)
- Occupational Health and Safety (OHS)
- Workplace Violence Prevention (WVP)
- Defensive Security Brief (DSB)
- Building Emergency Evacuation Plans (BEEP)
- Fundamental and Privacy Breach (ATIP)
- Values and Ethics (VE)

SECURITY AWARENESS MANAGEMENT PLATFORM

Security awareness professionals leverage the Security Awareness Management Platform to:

- **Enroll, manage, and monitor** participation and performance.

- **Track, monitor, and record** employee progress and performance in real time.

- **Observe** elapsed time, modules completed, date, time, status of completion, evaluation results, scores, and much more.

PHISHING SIMULATION PLATFORM

Phishing simulations efficiently measure user vulnerability increasing alertness to all phishing attacks including malware, ransomware, spear phishing, whaling, CEO fraud and BEC. The Terranova Security phishing simulation platforms strengthens detection skills and empowers users to identify and report phishing attacks in real time.
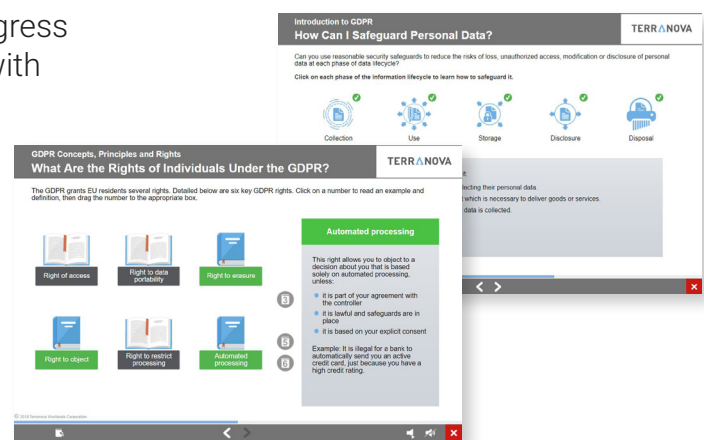
Social Engineering Tests

In addition to the reporting features of the platform, different methods for measuring campaign effectiveness are available.

- Phone vishing
- USB drop
- SMS-based phishing

GDPR TRAINING

Our interactive solution centers around the learning progress of each employee, ensuring that each one is equipped with core knowledge, mindset, and best practices.

- GDPR Key Concepts, Principles, and Rights
- GDPR for Managers
- GDPR for Human Resources Employees
- GDPR for Call Center Agents
- GDPR for IT Development
- GDPR for Procurement Employees
- GDPR for Retail, Sales & Marketing

BUILD YOUR SECURITY AWARENESS PROGRAM COMMUNICATION PLAN

Communication plays a critical role in instilling a security awareness culture and best practices:

- Engage employees
- Increase user participation rates
- Reinforce ongoing training and performance

Use **posters, 3D videos, one-page refreshers, wallpapers, screen savers, web banners, and promotional material** to increase user participation and knowledge retention rates in order to change long-term behavior.

FLEXIBLE DELIVERY MODEL TO SUPPORT YOUR ORGANIZATION'S UNIQUE OBJECTIVES AND RESOURCES

Terranova Security is a trusted advisor and partner with extensive security awareness, compliance training and phishing simulation expertise allowing your organization to focus on core business. All delivery models are supported by CISO coaching, a dedicated project manager and personalized training delivering measurable security awareness results.

CISO Coaching

Our team of CISO coaches work closely with our customer and provide insight into analyzing requirements, content creation, program planning, metrics definition, and effective measurement. Regardless the size of your organization, the different languages, countries or the complexity of your requirements - a CISO coach will ensure that your security awareness program is customized to meet your specific needs.

Managed Services

Managed security services provide a holistic approach to security awareness generating measurable results. This option offers ongoing project management, seamless campaign launches and continuous optimization. It also ensure your program is aligned to your security objectives by defining and tracking KPIs, and reporting on results and progress.

Top notch company to partner with. Terranova Security has exceeded our expectations. They actively anticipate our needs and reliably deliver on time. Fantastic partner.