COMMUNICATING STRENGTHS, COMPLIANCE, AND PROTECTION BENEFITS OF A PREVENTATIVE CYBERSECURITY SYSTEM

2026

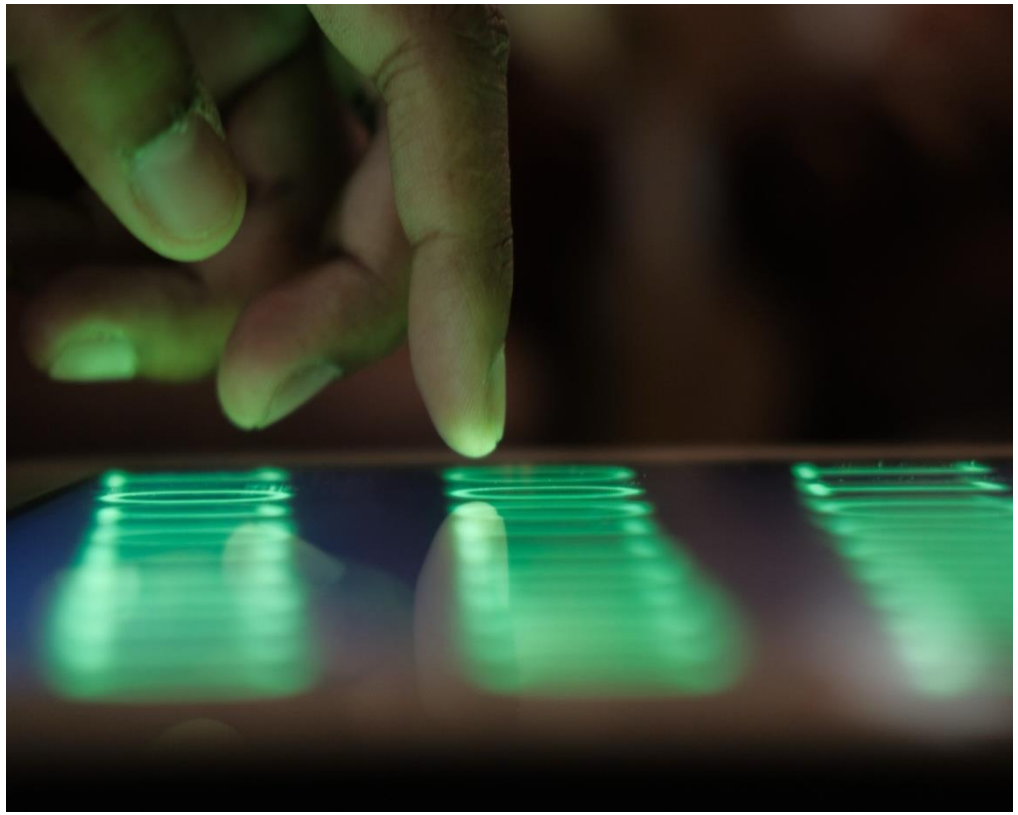
Highlighting security features and regulatory adherence advantages in meeting and exceeding regulatory requirements, and safeguarding Systems and Data.

Cybersecurity training is now part of the Port Security Management System Training (PSeMS)

Information – Physical – Cyber – Personnel

In Cooperation with the Morrone 9/11 Center for Counterterrorism and Security

PREVENTION MUST BE ADAPTIVE:



PSeMS: Addressing one of the greatest threats to our authorities worldwide.

INTERPORTPOLICE

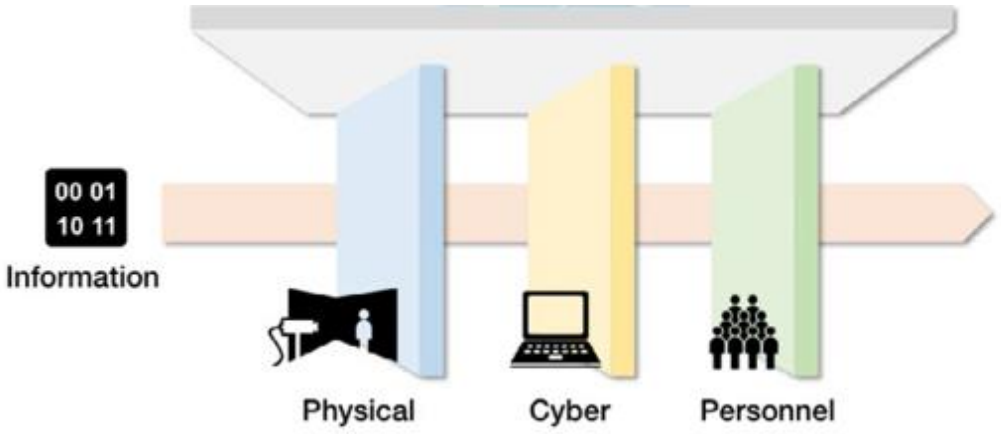
- In 1968, international law enforcement leaders from multiple countries came together to address international cooperation with an eye on terrorism and serious transnational crime.
- Initially, maritime authorities were involved, but soon after, in 1974, airport authorities were included, as they were often in the same jurisdiction. At that time, the name was changed to the International Association of Airport and Seaport Police (IAASP)*.
- In 2010, a new global charter was adopted to include transport and border jurisdictions whose activities are integral to public transportation security. INTERPORTPOLCE was adopted as a contraction of the International Organization of Airport and Seaport Police, patterned after INTERPOL, the International Crime Police Organization.

***INTERPORTPOLICE** – The International Organization of Airport and Seaport Police – (The International Association of Airport and Seaport Police is legally maintained). The Morrone 9/11 Center for Counterterrorism and Security was born out of the INTERPORTPOLICE's education programme. It was developed into a separate U.S. 501 (c) (3) education charity (also now listed in the UK.) The 37 Stars represent our leader, NYNJ Port Authority Police Superintendent and Director of Public Safety Fred V. Morrone, and the 36 other officers who perished in the World Trade Towers on September 11, 2001.

PREVENTION IS IN OUR DNA

An assurance for organizational security

About Port Security Management System (PSeMS)



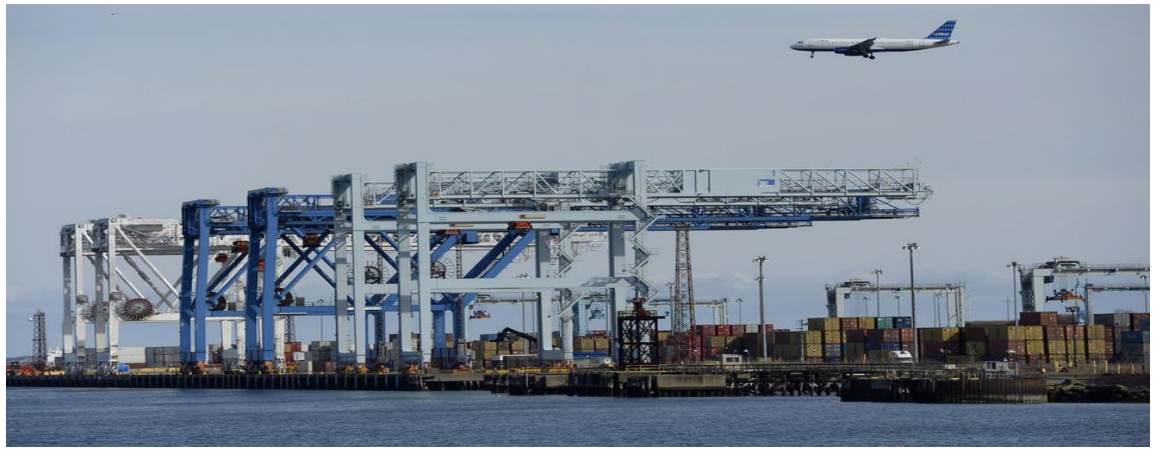
PSeMS is offered as a five-day training program focused on organizational security assurance.

- The PSeMS framework and approach helps coordinate processes and procedures covering governance, legal requirements, operating procedures, delivery, monitoring, review, and audit for security. In simple terms, it is a framework and methodology for your organization's security assurance.
- Together, It brings forth principles based on lessons learned, evidence-based practices, and assurance security systems, forming a methodology and approach that supports security resilience.

  Cyber disruption is the greatest day to day threat to maritime, aviation, and other transportation activity.

INTRODUCING A PREVENTATIVE PORT CYBERSECURITY PROGRAM OVERVIEW:

Building a partnership that provides an advanced automated phishing simulation and security platform



- ✓Advanced AI Simulation
- ✓Integrated Threat Intelligence
- ✓Holistic Training Academy
- ✓Compliance Alignment
- ✓Provide a collaborative quantum encrypted app for CySo/CTO staff

CYBERSECURITY PRIORITY OVERVIEW:

Behavioral Change Focus

Emphasizing behavioral change over compliance to effectively reduce organizational cybersecurity risk.

AI-Driven Adaptive Training

A platform that uses AI to deliver personalized phishing campaigns and training aligned with individual risk profiles.

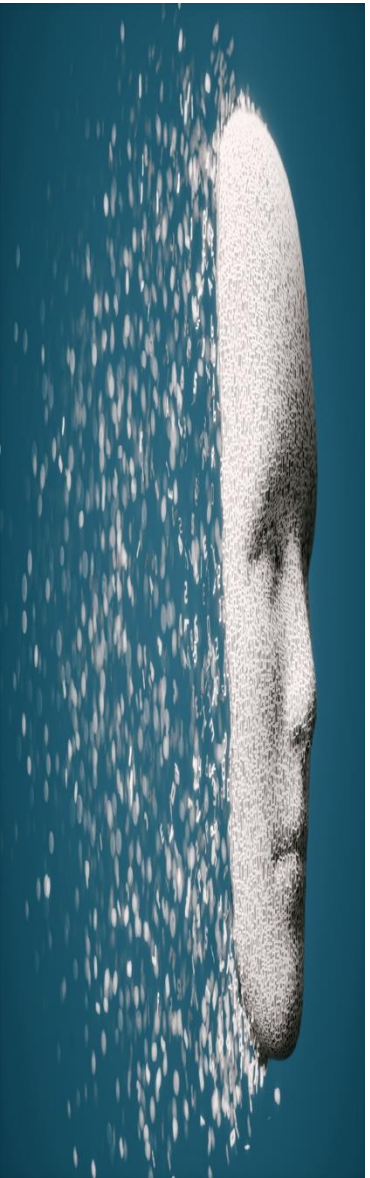
Automated Workflows and Insights

Having automated workflows and providing actionable insights through behavioral risk scoring minimizes IT workload.

Continuous Learning and Feedback

Integrating continuous learning and real-time feedback creates a dynamic defense against evolving cyber threats.

MANAGING CYBER RISK: EXCEEDING REGULATORY REQUIREMENTS



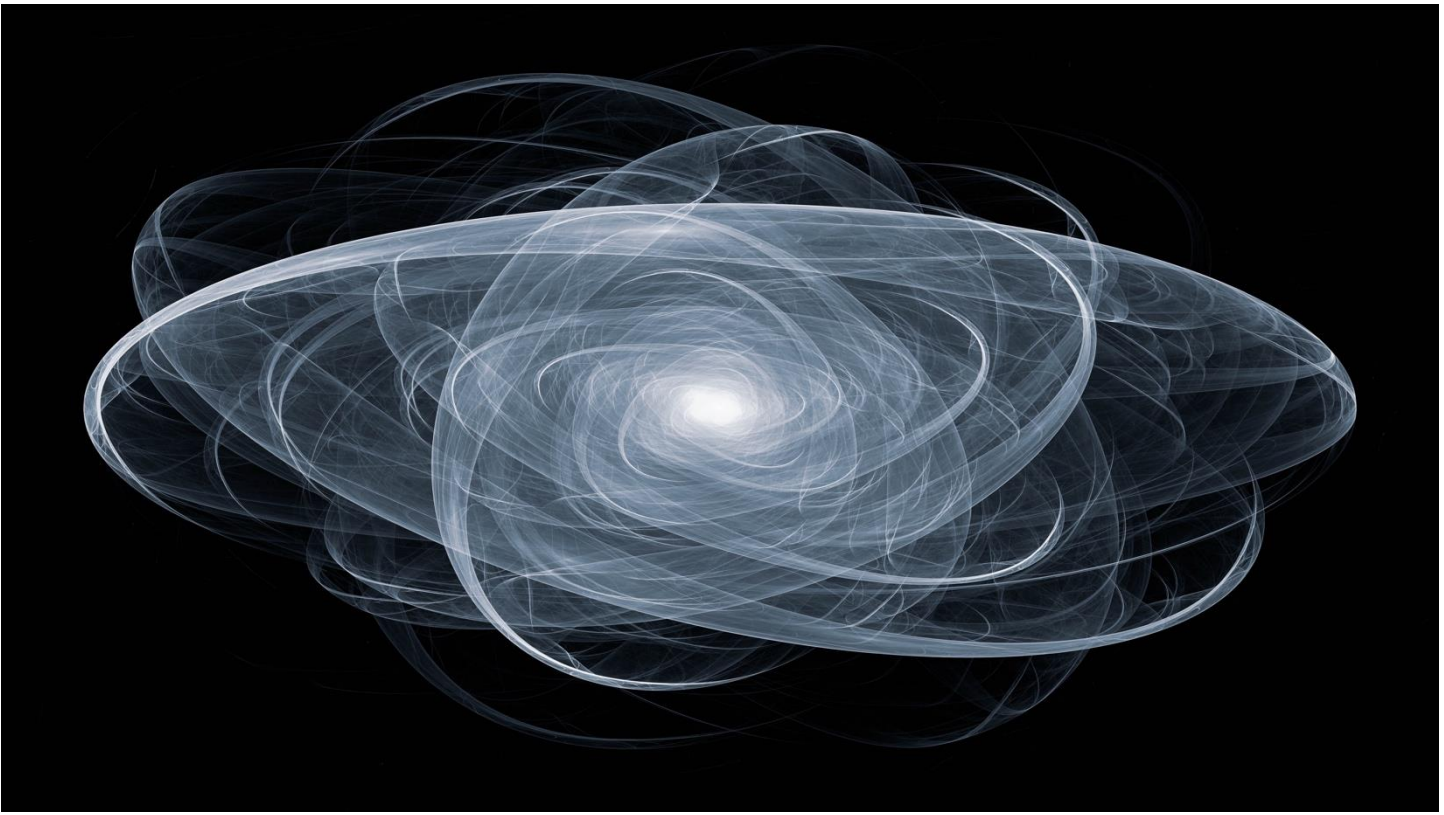
- US Coast Guard (USCG)
  - CFR 33 Part 101 Subpart F; Establish mandatory cybersecurity controls for U.S.-flagged vessels, MTSA facilities, and OCS operations- covering IT/OT systems with enforceable requirements
- International Maritime Organization (IMO)
  - ISM Code + MSC 428(98): mandates integration of cyber risk management into Safety Management Systems under ISM Code. MSC-FAL1/Circ.3 Rev3: Voluntary guidelines offering a structured approach to cyber risk management for ships.
- European Union – NUS3 & CRA
  - NUS2 Directive (effective 2024): Enhances cybersecurity across essential sectors, including maritime, and requires comprehensive risk and incident reporting, supply chain security alignment, and governance accountability. Cyber Resilience Act (CRA) makes security by design mandatory for maritime digital products; enforces continuous vulnerability management and supply chain protections.
- International Association of Classification Societies (IACS)
  - Unified Requirements apply to all new-build ships contracted after July 1, 2024, to strengthen cyber resilience standards. Proactive monitoring and mitigation strategies reduce phishing breaches and enforce zero-tolerance security policies.
- Canada – Maritime Transportation Security Regs (MTSR)
  - Under the Marine Transportation Security Act (MTSA) & MTSR, vessels and marine facilities are required to have security plans and incident reporting. While primarily focused on physical threats, evolving guidelines integrate cyber assessments, incident reporting, and governance responsibilities.
- Australia, UK & Singapore
  - **Australia:** Regulatory focus is embedded within maritime and national cybersecurity policies, with active guidance from the Transport Safety Bureau and ACSC, aligning with IMO/ISM
  - **UK:** Updated NIS Regulations align with IMO & NIS2, requiring reporting, board-level governance, and supply chain oversight.
  - **Singapore:** PSA & MPA issued voluntary cyber guidelines aligned with IMO and industry best practices, including reporting and resilience.

Comparison of international cybersecurity regulations relevant to maritime sectors: INTERPORTPOLICE (IAASP) is identified as a consultative body in the US-MTSA PL107-295 Sec. 109 (a) (2); and holds Consultative Statutes in the United Nations' International Maritime Organization (IMO)

ALIGNMENT WITH CYBERSECURITY REGULATORY REQUIREMENTS

USCG REQUIREMENTS	SYSTEM CAPABILITY
Comprehensive Cyber Training	On-going learning modules for all staff
Phishing Simulation & Reporting	AI-driven campaigns with real-time feedback and reporting workflows
Incident Response Readiness	Guided reporting prompts and audit-ready logs
Role-Based Training	Specialized modules for CySO, FSOs, and privileged users

INTRODUCING OUR CYBERSECURITY OUR TRAINING PARTNER: PHISHED.IO



AI-Powered Simulations

Uses AI to create adaptive phishing simulations based on user behavior for realistic testing.

Personalized Training Modules

Training is tailored to individual risk profiles, enhancing learning effectiveness and engagement.

Automation Reduces Burden

Automation features decrease administrative workload, allowing IT teams to focus on strategic tasks.

Behavioral Risk Analytics

Comprehensive analytics provide behavioral risk scores to identify vulnerabilities and prioritize actions.

WHY WE PARTNERED WITH PHISHED.IO

Regulatory Compliance

Aligns with USCG and most other regulatory mandates to ensure organizations are ready for inspections and maintain compliance.

Positive Training Approach

Comprehensive cybersecurity curriculum for all staff, with on-going year-round training.

AI-Driven Personalization

The platform uses AI for personalized, automated training that improves employee behavior and reduces phishing risks.

Phishing Prevention

Effectively prevents phishing attacks and safeguards sensitive organizational transactions from cyber threats.

Proactive Security Culture

Fostering a proactive security culture helps organizations thrive amid complex cyber threat landscapes.

CORE STRENGTHS

We are in the process of modeling CySO/CTO tabletop exercises

- Realistic Phishing Simulations
- Simulations mimic current threat tactics, providing employeesauthentic attack scenarios in a controlled setting.
- Advanced Threat Intelligence
- Platform integrates global threat feeds to keep phishing simulationsup-to-date with emerging attack trends.
- Interactive Awareness Training
- Adaptive training modules deliver targeted education based onindividual employee risk profiles.
- Zero Incident Mail (ZIM)
- Proactive monitoring and mitigation strategies reduce phishing breaches and enforce zero-tolerance security policies.

PHISHING:

PREVENT AND PROTECT

Phishing Risk Reduction

Phished.io lowers phishing click rates by up to 90%, reducing credential theft and ransomware risks significantly.

Secure Communication Promotion

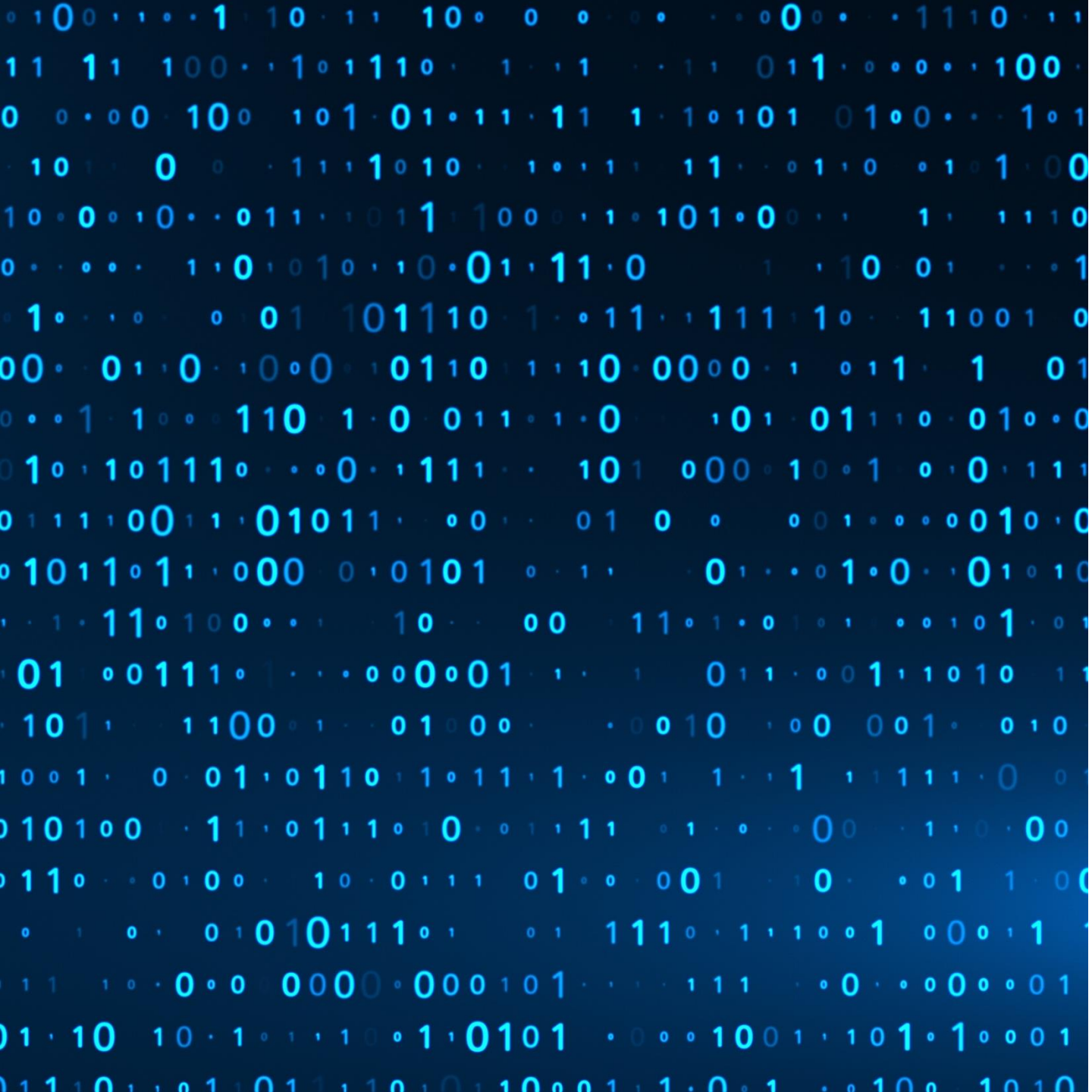
The platform promotes multi-factor authentication and secure communication to safeguard sensitive organizational data.

Continuous Employee Training

Real-time feedback during simulations trains employees to recognize threats and protect controlled information.

Enhanced Organizational Resilience

Continuous updates and preparedness help reduce financial exposure and maintain stakeholder trust effectively.



ZERO INCIDENT MAIL (ZIM)

Zim provides a 100% business Email Compromise protection, vital; critical to port/government authorizes

- Proactive Threat Detection
- ZIM continuously monitors interactions and alerts to detect earlysigns of phishing threats proactively.
- Automated Countermeasures
- Uses predictive analytics to initiate automated actions likequarantining suspicious emails instantly.
- Compliance Integration
- Integrates with frameworks like GDPR and MTSA to ensureregulatory compliance in phishing defense.
- Strategic Organizational Impact
- Fosters a zero tolerance culture, reinforces accountability, andsupports uninterrupted operations.

MEASURABLE OUTCOMES AND EXECUTIVE VISIBILITY

Phishing Risk Reduction

Phished.io significantly reduces phishing susceptibility by enhancing user awareness and reporting suspicious emails.

Executive Governance Visibility

Dashboards provide cybersecurity officers and executives with clear insights into compliance, training, and risk trends.

Informed Decision-Making

Actionable insights from data enable strategic resource allocation and continuous cybersecurity improvements.

Phished is the only platform to date where customers have not experienced breaches caused by human error, further emphasizing risk reduction.

FEATURE COMPARISON - PHISHED:

FEATURE	PHISHED	OTHERS – WE FOUND
Phishing Simulation	Advanced AI-driven, real-time updates	Basic templates, periodic updates
Awareness Training	Personalized modules	Static, generic content
Threat Intelligence	Integrated global feeds	Limited or manual updates
Reporting & Analytics	Granular dashboards, risk scoring	Basic metrics
Zero Incident Mail (ZIM)	Included – proactive mitigation	Not available

YOUR NEXT STEPS: ENGAGEMENT FOR CYBERSECURITY

Schedule Demo or Consultation

Organizations are encouraged to schedule a demo or consultation to explore phishing resilience capabilities.

AI-Driven Simulations

Phished IO leverages AI-driven simulations and adaptive training to provide comprehensive phishing risk mitigation.

Direct Engagement Channels

Customizable contact options including email, phone, and website enable direct engagement with Phished IO services.

Enhanced Cybersecurity Posture

Adopting Phished IO helps safeguard workforce, maintain compliance, and strengthen cybersecurity against phishing threats.

PROGRAM RECAP

- Compliant Resilience Standards
- Data Protection Alignment
- Audit Ready Reporting
- Physical & Cyber Security Committees
- Collaborative LE/Sec & CySo/CTO Quantum Encrypted Communications
- Discounted / Competitive Fee

WORKING TOGETHER WE ARE A GLOBAL FORCE

E:: info@interportpolice.org

W: https://interportpolice.org