

Addressing Human Risk The *A*daptive Way

Mitigating Human Risk through AI-Powered Integrated Security Behaviour Monitoring, Security Awareness, Phishing Readiness & Policy Compliance

Artificial Intelligence is a core pillar of digital transformation across organisations, and cybersecurity is no exception. As threat actors increasingly leverage AI to enhance the scale and sophistication of attacks, AI-powered Human Risk Management enables organisations to identify, assess, and mitigate human-centric risks by correlating behavioural data across functions and predicting vulnerable user behaviour for proactive risk reduction.

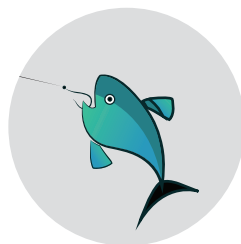
PhishRod is a market leader in AI-Powered Human Risk Management helping organisations in mitigating cyber threats relating to vulnerable end user behaviour. By leveraging advanced adaptive analytics, end user behaviour monitoring, personalised training interventions, policy compliance and continuous profiling through phishing simulations, PhishRod helps organisations reduce human-related security breaches, foster a culture of security consciousness, and improve overall resilience against cyber threats.

“ 95% of cybersecurity incidents occur due to human error or negligence.* ”

* Source World Economic Forum

Unified framework for behavioural analytics, security awareness, compliance, and phishing readiness to address human risk holistically leveraging AI.

A'daptive Risk Agent



Built-in use cases for end-user behaviour monitoring & human risk management.

Behaviour Insights

Automated Phishing Incident Response with **130+ built-in threat intelligence** feeds to analyze, quarantine & delete suspicious emails.

PhishScout

Security Awareness Manager

Cybersecurity-focused LMS with **500+ SCORM-compliant** training modules, videos, games, & infographics for end user awareness.

Assess the end user behavior against phishing attacks using **2000+ proven phishing templates**.

Phishing Simulator

Policy Compliance Manager

Ensure **compliance of IT Security & Governance** projects by assigning corporate policies to end users