

Human error remains one of the most exploited entry points for attackers.

We help organizations proactively identify user vulnerabilities by simulating real-world phishing attacks, providing clear, actionable data that supports leadership in strengthening their security posture while building a more vigilant workforce.

Expose the Risk. Change Behavior. Build Resilience.



Campaign Design & Threat Simulation:

Collaboratively build scenarios that reflect business context and mimic real-world attacker tactics: social engineering, deceptive links, and credential harvesting.

Controlled Phishing Execution:

Deliver simulated phishing emails to targeted users across departments, using varied techniques and difficulty levels to accurately measure susceptibility.

User Interaction Monitoring & Data Collection:

Capture detailed engagement metrics such as opens, clicks, credential submissions, and user reporting behavior to build a clear risk profile.

Results Analysis & Improvement Planning:

Provide comprehensive reporting with executive summaries, risk analysis, and targeted recommendations for user training, policy updates, and future awareness efforts.

WHY CHOOSE US?

Threat-Realistic Scenarios:

Simulations are crafted to reflect current attack trends and threat actor tactics, not generic templates.

Measurable Progress Tracking:

Clear reporting shows improvement over time and pinpoints where additional focus is needed.

Fully Managed Delivery:

We handle planning, deployment, monitoring, and reporting, freeing internal teams from the operational lift.

Seamless Integration:

Delivered as a standalone service or fully integrated into our Security Awareness Training & MSSP offerings.

OUTCOMES YOU CAN EXPECT

- Visibility into real-world user susceptibility to phishing
- Actionable data to drive targeted security awareness efforts
- Measurable improvement in phishing resilience over time
- Compliance support for industries requiring user security testing
- Executive insight into organizational human risk factors

EMPOWERING USER AWARENESS

Our service produces transparent, actionable outputs that leadership and technical teams can use to reduce phishing risk and demonstrate security improvement.

It's a measurable way to reduce your exposure and improve organizational resilience with:

- ✓ Engagement Metrics
- ✓ Executive Summary & Risk Analysis Report
- ✓ Training & Remediation Recommendations

WHY IT MATTERS

Technology alone can't stop phishing. DigitalEra helps you expose vulnerabilities that technology misses, giving leadership the insight and confidence to reduce human-driven risks before attackers exploit them.