Quorum Cyber

Service Description
Phishing Simulation
G Cloud 15

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Service Overview

Background

As email-based phishing attacks continue to grow in frequency, sophistication, and impact, organisations face an increasing risk from one of the most exploited attack vectors targeting users directly. Measuring human risk and demonstrating the effectiveness of security awareness initiatives has therefore become a critical component of a resilient cybersecurity strategy.

Quorum Cyber's Phishing Simulation service enables organisations to regularly and realistically assess their resilience to phishing threats by launching advanced, controlled phishing campaigns against users. The service provides clear insight into user behaviour, susceptibility, and response patterns, allowing organisations to quantify human risk and track the effectiveness of their cybersecurity awareness investment over time. This evidence-led approach supports continuous improvement, helping organisations strengthen their human defence layer and reduce exposure to phishing-driven compromise.

Quorum Cyber's Solution

Phishing Simulation is a Quorum Cyber service designed to provide a cost-effective, continuous approach to user education and awareness against phishing threats. Delivered as a fully cloud-based, Security-as-a-Service (SaaS) offering with no on-premises requirements, it enables organisations to strengthen their human security layer without operational complexity.

The service combines employee education and realistic phishing simulations within a single, per-user pricing model, helping organisations build long-term resilience to phishing attacks through ongoing testing, learning, and measurable improvement.

Differentiators

- **Business-Critical Asset-Led Design**: Phishing campaigns are designed around your business-critical assets, ensuring testing is aligned to what matters most and focused on the users and roles that present the highest risk.
- **Targeted, Controlled Campaign Execution**: Campaigns are precisely scoped and delivered using automated tooling, with predefined targets and tailored phishing templates to ensure consistency, accuracy, and realism.
- **Detailed Behavioural Analysis**: Results are analysed to provide insight into how users interact with phishing attempts, including engagement patterns and credential submission, enabling a deeper understanding of organisational risk.
- **Insight-Driven, Actionable Reporting**: Reporting highlights trends across departments, locations, and timeframes, identifying both strong performance and higher-risk behaviours to support evidence-based decision-making.
- **Anonymised Results with Clear Improvement Guidance**: Findings are presented anonymously to protect individuals while equipping management with clear recommendations to strengthen phishing awareness, detection, and overall security maturity.

Service Features

- Tailored phishing scenarios based on real-world threats
- Point-in-time phishing education
- A detailed report with the results of the test, trends, metrics, and recommendations
- Templates range from social media and High Street Banks impersonations as well as internally structured templates; we drive security awareness by providing constant tests and challenge knowledge reinforcements to users.

Service Benefits

- Snapshot of current awareness, risk and exposure level,
- Raise security awareness across the organisation,
- Prime staff for further awareness training.