

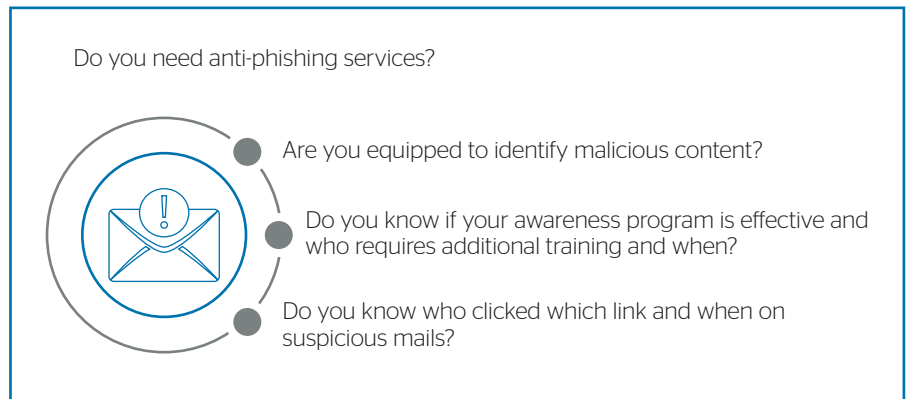
Defend against social engineering phishing campaigns

Differentiating legitimate content from fraudulent one is getting harder each day and phishing social engineering attack methods remain the single largest threat to organizations

Phishing techniques and their success rates to penetrate the internal IT are continuously evolving and improving. Hackers succeed to find new entry points to defraud by widening target base.

The operational and financial impacts to the organization are significant, especially when a privileged account is compromised and used to gain unauthorized access to the organization perimeter.

93% of IT security breaches are the direct result of some form of phishing



Phishing campaigns thrive on innovative techniques. Your cybersecurity program need to be able to detect and defend against sophisticated, persistent, global social engineering phishing campaigns and continuously assess and adapt, to keep pace with every changing and evolving methods and techniques.

What Atos can do for you



Data analytics & Phishing Readiness Score

Help organizations to assess, monitor, report and provide comprehensive phishing readiness



Multiple Simulation assessments

Assess constituent's ability to identify, prevent, detect, respond and effectively recover, from such threats



Security Awareness

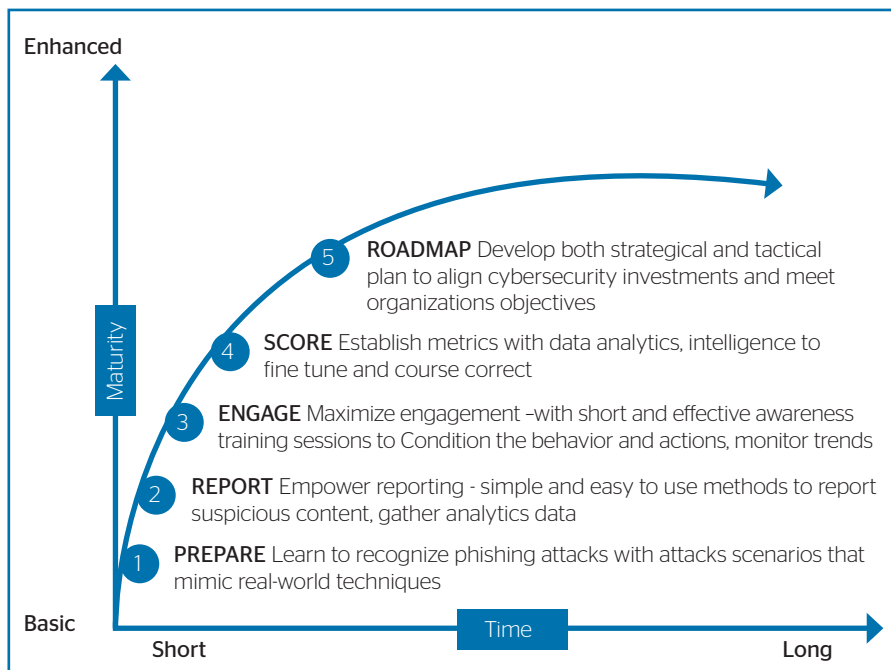
Deliver end to end solution to strengthen the cybersecurity security awareness program, with focus on social engineering phishing

A flexible and comprehensive approach to anti-phishing services

The anti-phishing services and solution is designed to aid in establishing a baseline for organizations to:

- identify the susceptibility score over a multi-year period,
- carry out multiple phishing simulation scenarios,
- integrate awareness training,
- strengthen visibility and transform deep insights into trends, activity and behavior patterns to finetune the delivery.

Anti-phishing services support organizations in their migration to a well-defined proactive risk-informed model from a general reactive-response model. With the flexibility to tailor security scenarios applicable to the organization's current setup, it is possible to measure the required outcomes so the risk-based approach can continuously evolve. Aligned with general security principles, potential threats, legal and regulatory requirements are evaluated and weighted to organizational constraints and business goals.



Awareness program with long term outlook yields greater benefit and strengthens the overall cybersecurity program maturity.

Key characteristics and deliverables

- Phishing readiness score to identify organization's readiness, its susceptibility to a potential social engineering phishing attempts at all levels (individual, department and enterprise scores)
- Unlimited and various simulation assessments
- Flexible and customizable templates (1000+)
- Time-of-click integrated user awareness training: when a user clicks on a malicious URL, it is detected in real-time. For active learning purposes, a pop-up window appears explaining the situation to the user providing immediate awareness impact.
- Data analytics and deep reporting with a prioritized and targeted plan of action based on the phishing susceptibility score
- Newsletters
- Real-time dashboard
- Executive summary and report

Sample dashboard

Click Rate Overview		Click Rate Score
Business Email Compromise	0%	
Drive by	8%	
Data Entry	15%	
Attachment	21%	
Department		Finance 0%

Re: Suspicious email submission

Dear Colleague,

Thank you for reporting this phishing mail and congratulations for staying vigilant! You have spotted a **phishing test** e-mail which has been sent by Group Security in the context of our ambition to improve your awareness about detection and handling of incoming phishing e-mails. You have demonstrated a good understanding and we count on your continued support to protect Atos and keep Atos and our Customer data secured.

Best regards,
Security Operations Center
BDS Cybersecurity

Atos added value on anti-phishing services

It takes an effective integration of good organization practices, awareness and training programs and continuous monitoring to establish a successful methodology to minimize the threats from social engineering and phishing and drastically reduce the occurrence of such attempts. Atos will partner with you to help drive security decisions to protect your valuable assets, to provide situational awareness and to justify the security spend.

For more information: atos.net/en/solutions/cyber-security-products/data-protection-governance/anti-phishing-services

Atos, the Atos logo, Atos | Syntel, and Unify are registered trademarks of the Atos group. June 2020. © 2020 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.