SATILOR

PHISHING SIMULATION

ADDRESS

67 Zlatovrah Str., Office 2
1231 Sofia
Bulgaria

PERSONAL CONTACTS

e-mail : gg@satilor.com
e-mail : vm@satilor.com

www.satilor.com | info@satilor.com

SATILOR

PHISHING SIMULATION SOLUTION BRIEF

Phishing, by definition, is type of social engineering attack, which attempts to obtain sensitive information or resources. It is commonly used by adversaries to bypass technical security controls. It is designed to exploit the most vulnerable asset in the organization, the human factor. Psychological manipulation of people through electronic communication is still one of the most effective attack method and main reason for significant amount of cyber security breaches.

Our Phishing Simulation services are always tailored to your organization's specifics and business priorities. We use advanced psychological techniques to thoroughly assess how susceptible the employees are towards fraudulent data access or exfiltration attempts. Our follow-up assessment report and awareness training provide the means for human behavior manipulation resilience and efficient measures to mitigate those types of attacks.

Why SATILOR?

01 **We invest in services**, that help you stay on the verge or ever-changing regulations and standards for cybersecurity resilience.

02 **We help solve complex** challenges in alignment with business goal.

03 **Our innovative approach** provides resilience during corporate transformation in constantly evolving digital environment.

04 **Led by the industry best practices** we develop easy to follow processes, practical solutions, products and services.

SATILOR

Package Deliverables

- Phishing E-mail tailored content
- Landing Pages tailored content
- Technical preparation
- Simulation delivery
- Detailed report delivery
- Customized tailored training content
- Training technical delivery
- Training report

Business Benefits

- Gain extensive visibility of how susceptible your employees are to social manipulation.
- Reduced fraudulent activities due to faster and more accurate detection and reporting of cyber threats by your workforce.
- Help effectively shape the awareness training required by standards and regulation like PCI-DSS and GDPR.
- Verify the capabilities of your organization's cyber security controls to ensure effective mitigation of social engineering attacks.