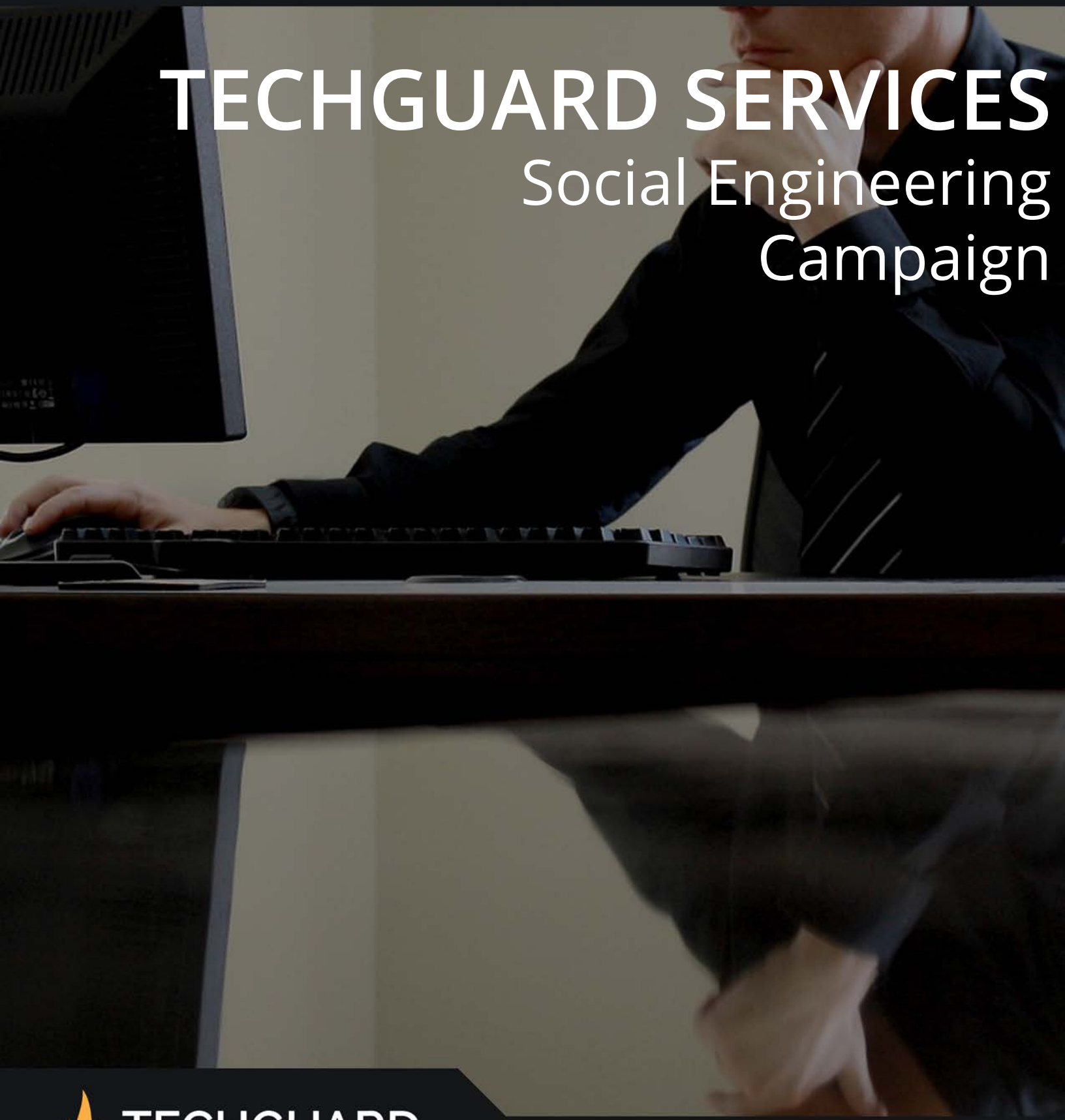


TECHGUARD SERVICES

Social Engineering Campaign

TECHGUARD SECURITY®

TechGuard Services
Social Engineering Campaign

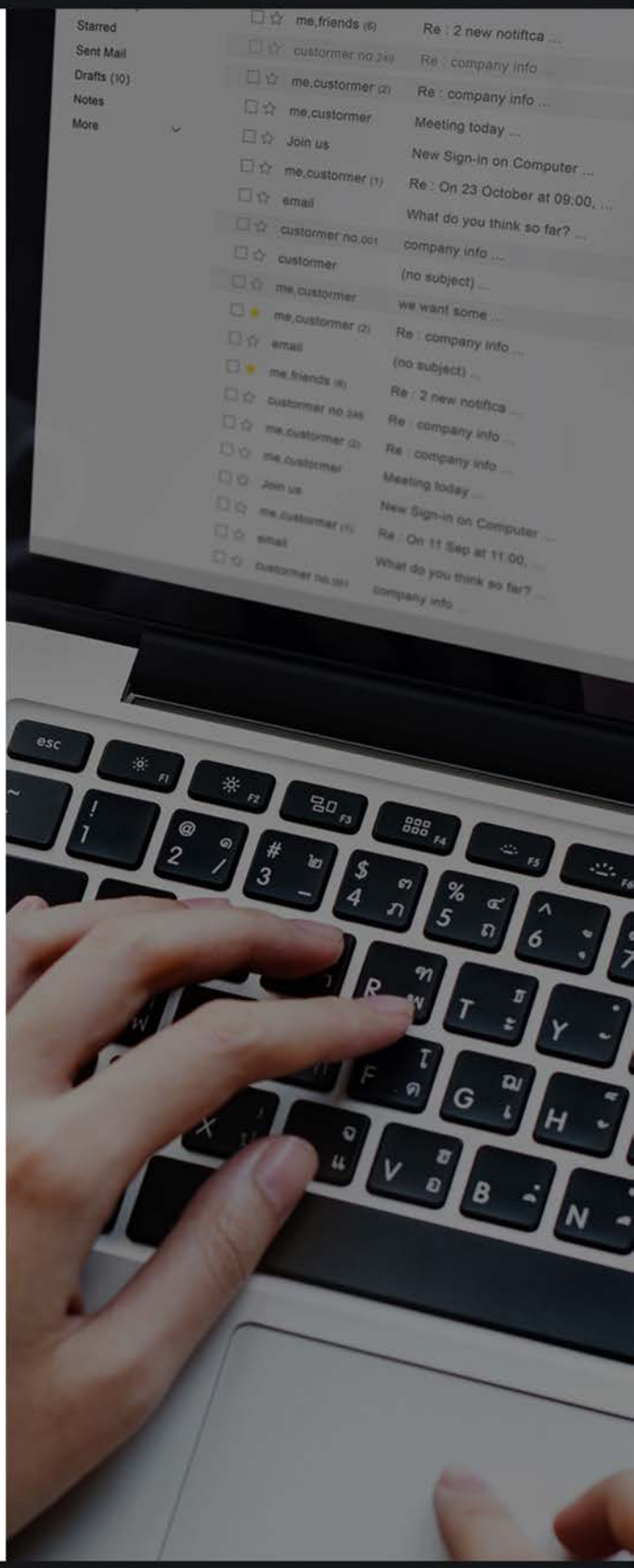
CONTENTS

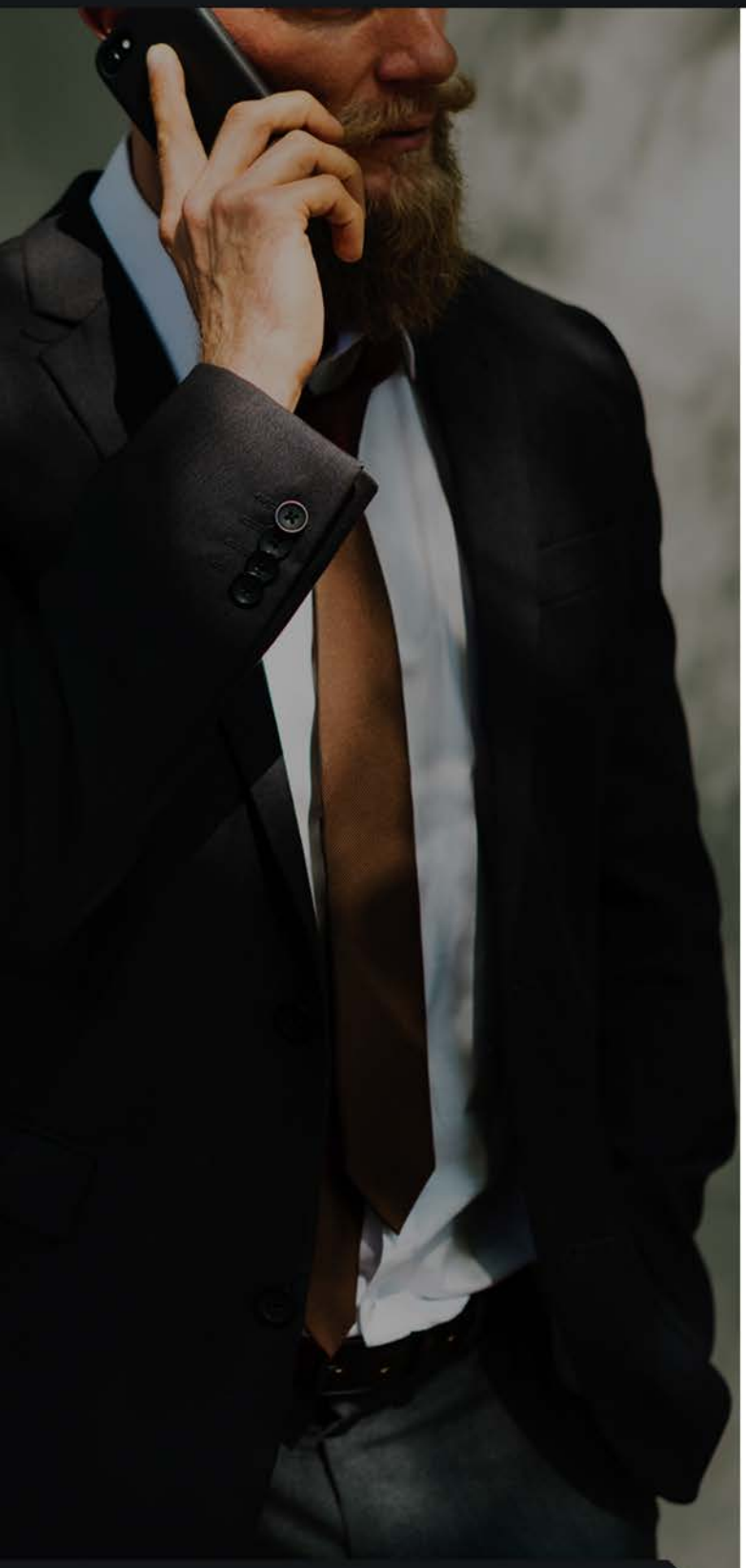
WHAT IS A SOCIAL ENGINEERING CAMPAIGN?

Social Engineering Campaigns use deception to manipulate people into divulging confidential or personal information that may be used for fraudulent purposes. Social Engineering Campaigns utilize a variety of methods such as phishing (spear phishing, whaling, pharming, etc.) and vishing.

Phishing attacks attempt to obtain personal or sensitive information through electronic communications and have become very sophisticated. In 2017, the average user received 16 malicious emails per month (Symantec Internet Security Threat Report, 2018). Phishing attacks are effective because they leverage curiosity, fear and urgency in employees.

Vishing is a technique used to elicit information or attempt to influence action through a phone conversation. This attack strategy has also become one of the hottest trends in social engineering attacks because the target is typically someone who has privileged information or access to privileged information at their fingertips.





WHY SHOULD A SOCIAL ENGINEERING CAMPAIGN BE PERFORMED?

Year after year, people remain at the top of the list of cybersecurity risks organizations face. The human element is one of the most unpredictable factors and because humans are subject to manipulation, they often become an organization's weakest link.

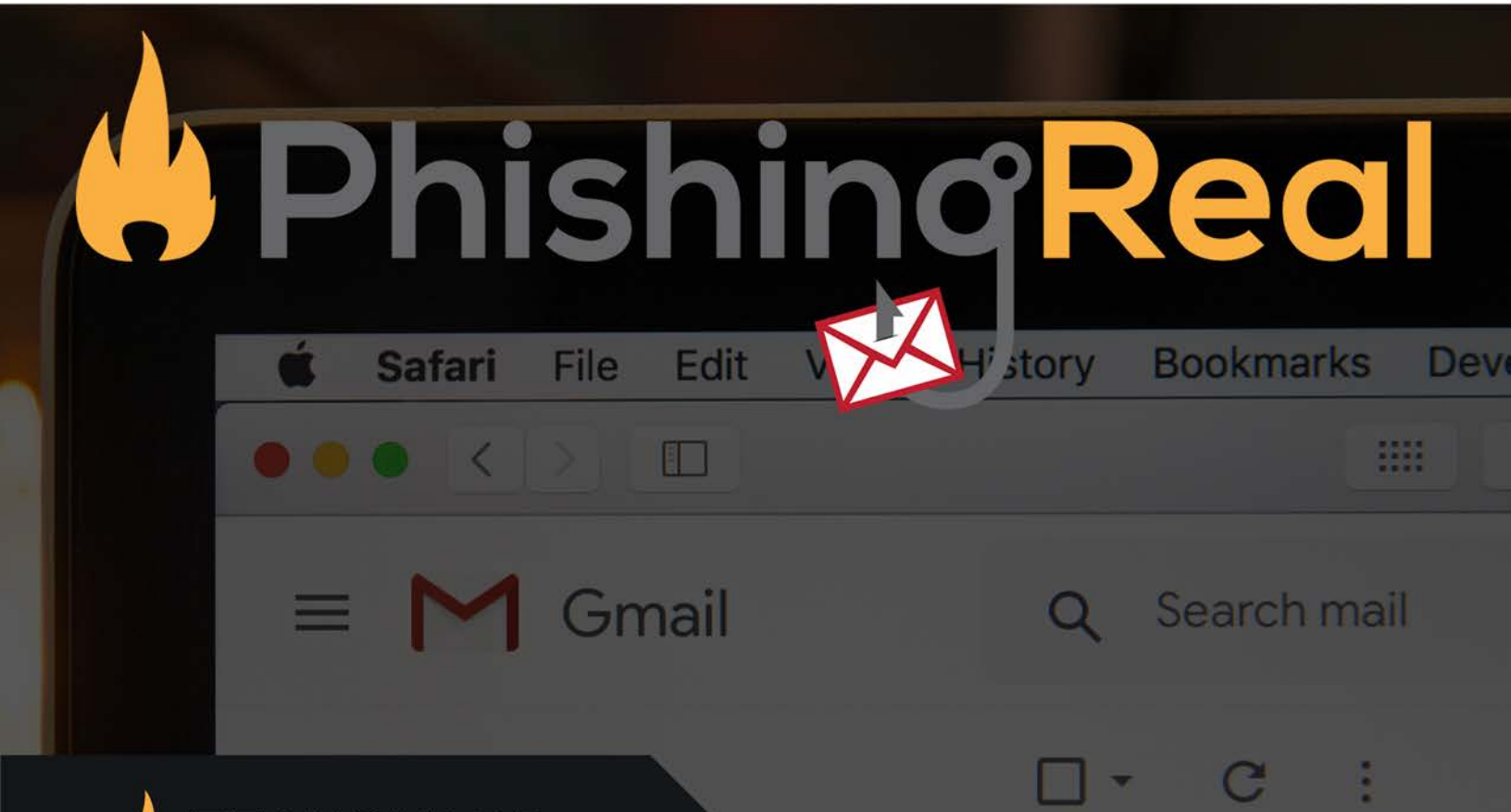
Each organization has data such as Personally Identifiable Information (PII), Protected Health Information (PHI), intellectual property, etc. that requires specific handling and/or protection. If this data ends up in the hands of an adversary, the effects can be devastating.

Attackers use social engineering tactics to "trick" employees into providing information that may allow an adversary to gain unauthorized access into systems in search of this sensitive data. Social Engineering campaigns provide an economical way to measure the effectiveness of the administrative controls that are in place to prevent unauthorized or accidental disclosure of data as a result of a social engineering attack. Performing routine social engineering campaigns also trains users to spot these types of attempts and reinforces content provided through the security awareness training program.

HOW DOES TECHGUARD APPROACH A SOCIAL ENGINEERING CAMPAIGN?

At TechGuard, we devise personalized Social Engineering Campaigns to fit each specific organization. Our scenarios are customized and simulate realistic situations employees are likely to encounter. Phishing and/or vishing techniques may be utilized. Our innovative Phishing attack simulator is used to launch an email campaign against employees. These emails can be crafted to mock social media notifications, package deliveries or even messages from a system administrator.

Vishing scenarios are devised to test employees' compliance with policies and procedures governing the sharing of sensitive information.



WHAT IS THE TECHGUARD DIFFERENCE?

We pride ourselves in building and maintaining long-term relationships with our clients. This ensures each client receives a tailored, customized service based on their unique organizational needs. From the initial kickoff meeting to delivery of the finalized Social Engineering Report, client satisfaction is our number one concern.

At TechGuard, we place the utmost value on the delivery of quality services. Every client is assigned a Project Lead who will serve as their single point of contact throughout the engagement.

In addition to the detailed written report provided at the end of the assessment, clients engage in a presentation with their Project Lead. Our report delivery presentation provides the opportunity to discuss details of important action items, next steps, and answer any questions related to remediation recommendations.

TechGuard has been dedicated to delivering high-end, professional cybersecurity solutions since 2000 - making us a trusted partner in both the government and private sectors.

TechGuard Security is an ISO 9001:2015-registered, certified SDB, DBE and Woman-Owned Business Enterprise. TechGuard Security was founded to address national cyber defense initiatives and US critical infrastructure security. We provide a comprehensive suite of cybersecurity solutions to help reduce your risk of cybersecurity-related incidents.