BISHOPFOX

DATA SHEET

Social Engineering

Bishop Fox Social Engineering goes beyond conventional phishing exercises to explore the depths of how hackers can exploit your users, empowering you with insights to improve your security awareness program and related controls like email and file security.

OUTPACE MODERN ADVERSARIES

Better Resilience to Social Engineering Attacks

Security awareness and user risk programs are losing their effectiveness. Most approaches are largely designed to satisfy lowest common denominator requirements as opposed to giving security leaders a realistic assessment of the risk that exists in their user base.

Bishop Fox's elite red team consultants emulate every stage of a social engineering attack, providing a clear understanding of execution methods and potential damage. Through vulnerability analysis and technical control assessment, we enable effective communication of user risks facilitating the evolution of your awareness program.

LEARN MORE

KEY OUTCOMES

Demonstrate the Potential Business Impact of Your User Risk

Pressure-tested Security Investments & Controls

Unique Insight Into How Your Users Could be "Hacked"

Augment Your Existing Approaches to User Testing & Risk Measurement

Improved Communication of User Risk to Key Stakeholders

Overall Improvement of Your User Risk & Awareness Program

HOW IT WORKS

Social Engineering Workflow

1

Pre-Assessment

- Engagement kickoff meeting & scope agreement
- Open-source intelligence gathering (OSINT)
- Pretext development
- Content & payload development
- Engagement Scheduling

2

Testing

- Domain allowlisting (if necessary/in-scope)
- Active testing
- Two-way communication during testing & "ride along" (optional)
- Preliminary results

3

Reporting

- Report
- Post-engagement meeting
- Recommendations

Impactful Insights to Evolve Your Strategy

Tailor-made to Your Objectives

Bishop Fox offers a “building block” approach to red team services that can include a Social Engineering Exercise and any combination of the following methodologies:

Assessment Knowledge Types:

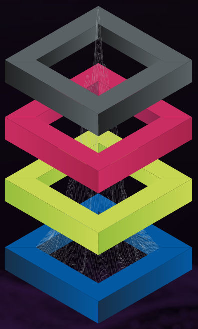
- Full Knowledge
- Partial Knowledge
- Zero Knowledge

Methodologies:

- External Breach Red Team
- Assumed Breach Red Team
- Ransomware Readiness
- Physical Breach Red Team
- Social Engineering
- Purple Team
- Continuous[1]
- Tabletop Exercise
- Red Team Program Build

[1] (Multi-phase Red Team, Purple Team, Ransomware Readiness)

Example:



CLIENT SATISFACTION

6000+
Offensive Security Projects Delivered

1000+
Global Customers Protected

81
Net Promoter Score

16+
Years of Experience

Trusted By Industry Leading Organizations

amazon
EQUIFAX
SONOS
august
CHANGE HEALTHCARE
Google

Recognized as a Leader in Offensive Security

- Best Workplaces for Innovators
- Attack Surface Management Market Leader
- Product Innovation, Thought Leadership, & Web Design
- Security Product for Large Enterprise
- Hot Company in ASM
- SC 2021 awards BEST EMERGING TECHNOLOGY

About Bishop Fox

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. We’ve worked with more than 25% of the Fortune 100, half of the Fortune 10, eight of the top 10 global technology companies, and all of the top global media companies to improve their security. Our Cosmos platform, service innovation, and culture of excellence continue to gather accolades from industry award programs including Fast Company, Inc., SC Media, and others, and our offerings are consistently ranked as “world class” in customer experience surveys. We’ve been actively contributing to and supporting the security community for almost two decades and have published more than 16 open-source tools and 50 security advisories in the last five years.

Learn more at bishopfox.com
Follow us on