Sword&Shield
ENTERPRISE SECURITY

Phishing Services

Realistic simulated cyber attacks to put your security to the test.

Phishing uses simulated real-world email-based scenarios to test and train your team members regarding this dangerous type of social engineering. These exercises are conducted in a safe and controlled environment, then used to increase awareness to proactively head off falling prey to a real attack.

Sword & Shield *partners with you* with our phishing services to assist you in both understanding your employees' knowledge in relation to cyberthreats and training those employees to improve their cyber awareness.

Phishing as a Service

Phishing as a Service (PHaaS), a component of Sword & Shield's Security Awareness Program, is offered through our comprehensive Managed Security Services platform. PHaaS is subscription-based, and provides consistent and ongoing phishing campaigns and analysis.

Our experts get to know your company and how you do business. Then, they apply their depth and breadth of cybersecurity knowledge to help you select the right campaigns and cadence to run them; and to determine who in your organization should be targeted based on their role and responsibilities.

PHaaS Process

Sword & Shield implements the following to create an effective phishing program tailored to your organization:

Test

Sword & Shield runs variations of realistic phishing, SMiShing, malware and portable media attack simulations regularly throughout your subscription, including a customized annual campaign based on your company's specific requirements.

Train

We provide an interactive eLearning module for corrective training for team members who fall victim to our simulated attacks. This flexible tool can be used following each campaign or at certain more strategic times.

Detect

This service includes detection of malware-related risks at every level of your IT infrastructure from your network and systems to individual applications without having to involve other employees.

Measure

Sword & Shield measures progress with user-friendly reports following each campaign and a trend analysis to provide insight over time. We can track vulnerability to phishing attacks by employee, department, region, or the company as a whole.

Executive Level Insight

In addition to working with our expert security analysts on a regular basis, our PHaaS includes a semi-annual review of testing results with a virtual chief information security officer (vCISO). This executive-level guidance and leadership allows you to strategically plan how to move forward to uphold the integrity of the program.

About Us

Securing business for more than 20 years, Sword & Shield Enterprise Security, Inc. partners with our customers to meet the needs of their dynamic cybersecurity and compliance landscape.

We work closely with companies to become tightly integrated with their enterprise operations in the areas of managed security, risk and compliance, enterprise security consulting, security incident response and forensics, and security training.

Recognized nationally and headquartered in Knoxville, Tennessee, Sword & Shield has offices throughout the US. Sword & Shield services a broad spectrum of industries, including healthcare, retail, media, banking and finance, legal and manufacturing.

Just Ask

Sword & Shield has vast experience in virtually every area of information security and compliance. If you need a service in these areas not specifically named in a description, the chances are we do it, and we do it well. So, just ask.

Our Phishing as a Social Engineering Service

Sword & Shield's phishing as part of our social engineering services is generally a one-time engagement. This be conducted along with other associated exercises designed to trick employees into divulging confidential company information.

Sword & Shield analysts work with you to create a targeted phishing email message from a supposedly trusted source, track the open and click through rate, and follow up with training for employees who inadvertently reveal information.

Phishing as a social engineering service can be conducted in conjunction with the following:

- Pre-Texting: Phone calls impersonating someone with perceived authority or privilege in order to gather key information.
- Baiting: USB flash drive or other form of mobile storage media left in an open area in order to identify employees who attempt to use the device.
- Tailgating (or Piggy-Backing): Attempt to bypass physical security at client sites in order to roam unescorted.

Why Sword & Shield Enterprise Security

Technology firms that dabble in security tell you what you're doing wrong (or not doing at all) and walk away, leaving you without a plan of action. Sword & Shield partners with you to become an integral part of your cybersecurity and compliance program by not only identifying gaps and vulnerabilities, but also continuing to work with you to achieve and maintain a secure and compliant environment.

In short, Sword & Shield's depth and breadth of expertise in every aspect of our comprehensive portfolio of security services, coupled with our customer-first approach, empowers us to provide tailored solutions and personalized support for small to enterprise level companies. We strive to make your security and compliance initiatives as easy as possible on you.

This is what sets us apart from other information security and compliance firms.

Knoxville, Tennessee
1431 Centerpoint Boulevard
Suite 150
Knoxville, TN 37932
Phone: 800.810.1855

Nashville, Tennessee
131 Maple Row Boulevard
e500
Hendersonville, TN 37075
Phone: 615.928.1990

Portland, Oregon
1220 Main Street
Suite 400
Vancouver, WA 98660
Phone: 360.567.2587

Washington, DC
1655 N. Fort Myer Drive
Suite 700
Arlington, VA 22209
Phone: 703.382.6316

www.swordshield.com
sales@swordshield.com

Sword&Shield
ENTERPRISE SECURITY