800.956.6065
www.social-engineer.com

The Business Value of the Social-Engineer Phishing Service

Phishing attacks continue to plague organizations across the globe with great success, but why?

Cybercriminals are targeting the human element of organizations. Additionally, they are developing techniques to use an organization's employees as the first point of entry. According to the 2021 Verizon DBIR report, of the 3,841 security breaches reported using social engineering, phishing was the key vector for over 80% of them. The 2021 Proof Point State of the Phish report states that 66%] of organizations saw targeted phishing attempts in 2020, showing that no corporation is immune to phishing attacks. For example, the SANS Institute, a provider of cybersecurity training and certification services, lost over 28,000 items of personally identifiable information (PII) in a data breach that occurred after a staff member fell victim to a phishing attack. We share these statistics to highlight the business value of the Social-Engineer Phishing Service (SEPS). The goal of this service is to train your employees to become the first line of defense.

Phishing Attacks - Sophisticated and Targeted

Gone are the days when phishing emails consisted of broken English and poor grammar. And it's no longer a simple "click now" to win these outrageous prize offerings. In fact, skilled phishers now send highly sophisticated emails that appear to be from a legitimate source. For example, the most effective phishing emails are sent from a "fellow employee," a specific department such as HR, or a third-party partner. They leverage everything from an organization's logo and layout to internal lingo. Highly targeted spear- phishing attacks go after a specific individual's personal interests. These days, phishing emails are so good that they establish immediate credibility, and users don't think twice before acting. One of our clients told us how they were duped by the attackers sending emails from their very own domain! By then it's too late.

Train the Way You Fight Because You Will Fight the Way You Have Trained

It's time for businesses to take a page from martial arts when it comes to training for security breaches. By putting effort into the way employees are trained, organizations equip their employees with the skills to help defend the organization's intangible assets. In martial arts, sparring is a mechanism for testing techniques learned in the studio. A martial arts practitioner may master a technique while standing still. But find the technique much more difficult to execute when facing a moving opponent. When an individual experiences a real-world attack, they go into fight or flight mode. Someone who masters martial arts practices, but has never executed against a determined aggressor, may find those skills difficult to apply in the heat of the moment. This can be likened to a

well-crafted phishing email. An employee may know better. But what will the employee do if faced with an authentic-looking email sent from an internal source that confirms submission of incorrect information? The individual's initial reaction may be to respond and hand over the "correct" data.

In sparring, some techniques work well when combating tall people. However, those same techniques aren't as effective when combating a compact and robust individual. Martial artists must learn to continually adapt. Sparring enables martial artists to become confident with learned techniques. In addition, it affords them the opportunity to grow from actual mistakes. An organization may effectively stress the importance of security. However, until employees face a believable attack vector, they will not learn how to adequately respond.

The Social-Engineer Phishing Service (SEPS) Helps Organizations Combat

Sophisticated, Targeted Threats.

Military experts train their soldiers to fight in a worst-case scenario. Similarly, organizations should train and educate staff to detect social engineering attacks to improve overall security. The concept of phishing your own employees has been around for years, However, the concept of a customized and continuous Phishing Service is unique.

From start to finish, Social-Engineer helps an organization's most unpredictable asset (their people) become the first line of defense. If an employee understands the value of reporting suspicious activity to their internal security department, they will likely react to real-world scenarios the same way. Rather than simply training staff to look for suspicious activity, the Social-Engineer team teaches users to apply critical thinking, to recognize phishing emails, and how to properly report and respond to them. It's important for employees to understand the assets they are responsible for protecting and how they can better protect them. Security starts with each individual user.

By sending an initial wave of well-crafted phishing emails, Social-Engineer creates a baseline for an organization's susceptibility to these types of attacks. From there, our team conducts a thorough debrief, focusing on remediation and education. We repeat this process with increasingly sophisticated phishing awareness education. By conducting ongoing and regular phishing campaigns, organizations can quickly develop a culture of phishing awareness and education. Our service can also provide advanced metrics, such as click and reporting rates, repeat offenders, and trend data in order to identify specific areas of improvement and, eventually, ROI.

Securing Your Organization with Social-Engineer's Phishing Service

When it comes down to it, employees who know they are being tested are more apt to report and respond appropriately to questionable emails and activity. By keeping employees on their toes, organizations vastly improve their overall security posture.

Organizations who have implemented our SEPS program have experienced:

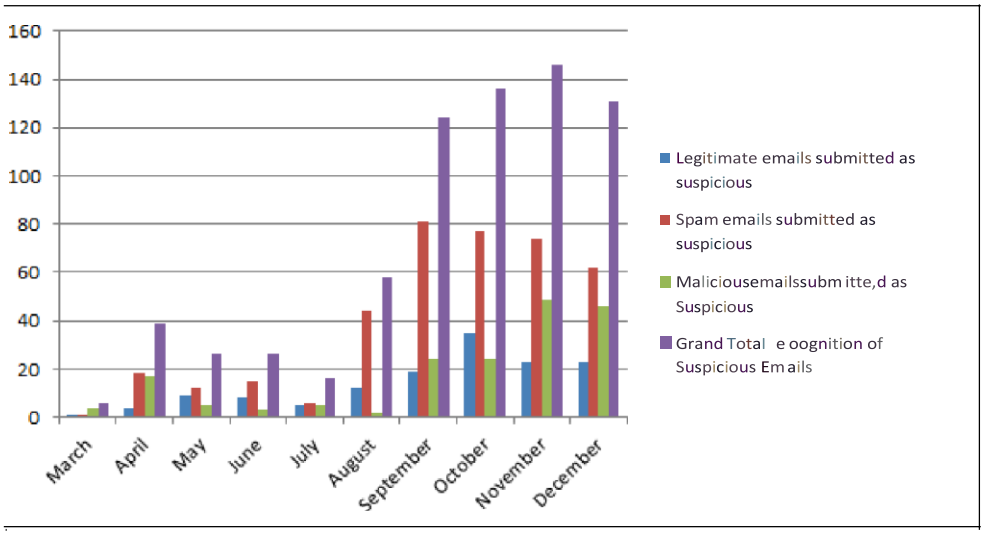
- Increased positive dialogue between employees and IT teams.
- A dramatic decrease in known malware incidents and malware infection rates (one client experienced a 70% reduction).
- Decreased frequency of computer re-imaging.
- A reduction in drive-by downloads and adware; and
- Less disruption to the corporate network.

The Results Are Real, But Don't Just Take Our Word For It

The chart below illustrates data from one of our clients who implemented SEPS. Prior to working with Social-Engineer, this organization was running a phishing education program on their own, using a popular phishing tool. They were sending out regular emails and testing their whole population. On the surface, everything was the way it should be for a phishing program. However, despite their efforts, the organization simply did not experience the results they thought they would. After one year of trudging through it on their own, they contacted Social-Engineer to offer assistance in enhancing their program. After 6 months in the SEPS program, the organization continued to experience tremendous results.

The below chart demonstrates the tremendous value of the Social-Engineer phishing service even after just one month's time. Most noticeable was an increase in recognition of suspicious emails over the entire population.

What were the results?



More than a 370% increase in recognizing phishing emails.

Businesses spend hundreds of thousands of dollars on IDS systems, firewalls, and other protection mechanisms to monitor the network, but one skilled phishing attack can lead to total devastation
without the attacker having to hack one thing. It's a matter of when, not if, your organization will be targeted. Implementing a well-managed phishing and education program is a cost-effective mechanism for preparing your employees for real-world situations and keeping your business out of the
headlines. The business value of the Social-Engineer Phishing Service is worth investigating. For more information please visit: Managed Phishing Service - Social-Engineer, LLC