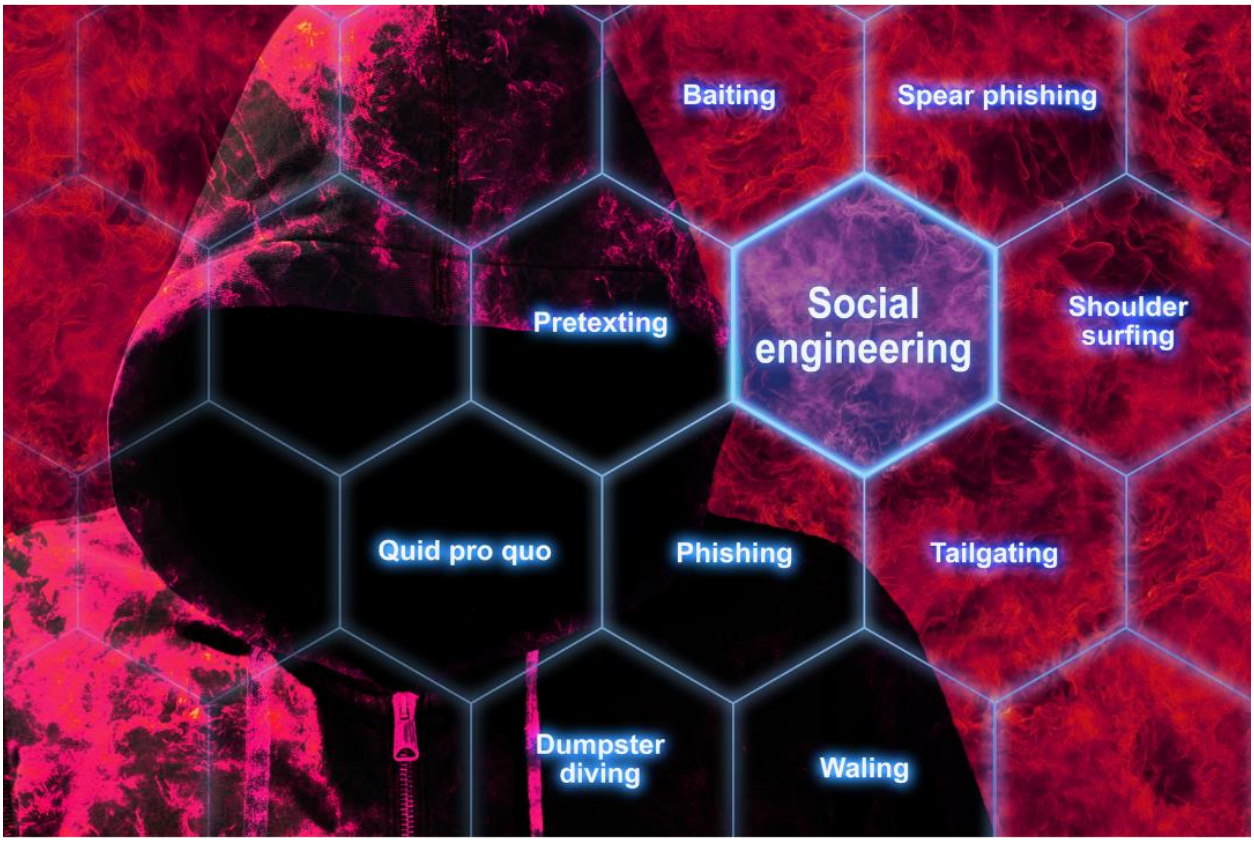
800.956.6065
www.social-engineer.com

Social-Engineer: What Makes Us Different

At Social-Engineer (SECOM), we pride ourselves on what we do and how we do it. We are a security services provider, focusing on the four primary attack vectors: vishing, phishing, SMiShing, and impersonation. Our testing, training, and simulated threat engagements are customized to our clients' specific needs. They seek us out for our expertise and for our ability to fully manage security awareness programs. We are not alone in the market. But what makes us different?



Our Core Ideal Drives Us

Our company ethic is: "*Leave them feeling better for having met us.*" This core ideal drives every employee at SECOM. We express it in all our work. In our industry some players are only in it for the win, to show how great they are at their job, and many of them are great, no doubt. That is just not our driving force. Let us be clear though, we certainly have our fair share of "winning," we just view it different from everyone else. One form of winning is

getting the compromise and leaving the target in a frame of mind that allows for maximizing the teachable moment. We also consider a shutdown or a user-reported attempt a win because it shows the client sponsors that they are educating their users effectively and getting the results they are looking for. We will never embarrass, victimize, or use intense fear to get the point across that your users are vulnerable and need training. We are able to make the same point by using influence, instead of manipulation, and leave the users feeling better for having met us.

Phishing the SECOM Way

We do not expect every target we test to pass, but we also find satisfaction when they do. Using our trained and certified social engineers to perform these tests ensures the quality of the testing. As you might expect, anyone can write a phishing email that will have a very low click rate. That is simple to do, but is it really testing your employees' ability to catch 'real world' phish and protect your network and data? What happens when your users get a highly sophisticated phish or SMiSh? Are they ready and trained to spot the red flags in those messages?

Perhaps some are, but only through verified testing will you know for sure. At SECOM we do not rely solely on the 'click rate' metric to demonstrate effectively trained user groups. Click rates will vary month to month, and a progression graph should look like a mountain range with lots of ups and downs.

That is a good thing. It shows true testing and educating (with your landing pages) on varying levels of sophistication. That is why we focus on the reporting rates of your users. This is where you see return on investment. The more you expose your users to trainable moments, the more they will absorb and use it outside of testing. That is the real goal. You want staff to perform as you expect in all situations, not just your test scenarios. Getting the graphical data to show your reporting rate is on a consistent upward trend is how you "win" in phishing testing. We work to change the perspective of everyone we meet by demonstrating the value of a varying click-rate and an upward-trending reporting rate.

Our Vishing Programs Stand Above the Rest

There are two things to keep in mind when you are setting up a consistent and effective vishing security awareness program: 1) Are the calls your users are getting realistic and a true test? 2) Are you able to perform this testing at a scale that you are not spending 15+ years to test each user in your organization? In this way, we are different from our competitors. There are some other providers that can perform testing at a similar quality that we can, but they do not scale.

Our clients shared that when they tried to find comparative services to ours, they found: "*The high-quality vendors maxed out at 10-50 calls per month to our users.*" If your organization has 50,000, 100,000, or 250,000 users you can see how long it will take to test your userbase. Some vendors try to address this problem and attempt to scale through the use of robots (automated IVR-based testing) or script-based call centers. These call centers

can make the number of calls necessary, but their staff are not trained like a real adversary to "bob n' weave" or pivot the conversation using science-based influence techniques. The choice becomes either high-quality calls at low scale, or high scale with untrained callers.

We believe you can have both with SECOM's testing methodology. Our team of vishers are all trained and certified social engineers and capable of making hundreds or thousands of calls per month. True quality and scale, that is what makes us different. Couple our managed vishing service with our Instant Vishing Education Service (IVES™) and consistently test and train users against the vishing attack vector. This is measurable and reliably shows return on investment.

Understanding Total Cost of Ownership

We perform all our testing in a manner that shows respect to your employees and retains their dignity and integrity. It also shows stakeholders real vulnerability and opportunities to remediate it. If you have read this far, we know you believe in the importance of quality security awareness training. We also know that one very real consideration, in choosing and running a program of the quality you believe in, is cost.

When setting up your own program or optimizing your existing program, think about the total cost of ownership for running it. It is not just the software you are licensing to send the phish or make the robocalls. You need staff, paid employees with benefits and other perks, to setup, execute, and analyze the results. Sometimes to get the quality you are looking for; those employees require specialized training. All of that comes at a cost, and that should be calculated into the total cost of ownership of the program.

When you leverage managed services like SECOM offers, many of those costs are baked into the price already, and in most cases at a substantial discount to an in-house option. Do not get us wrong here, we are not suggesting you fire your valuable employees and replace them with our services. We are suggesting you utilized the already trained and certified social engineers at SECOM to augment your security awareness staff and maximize their benefit to your company by empowering them to make decisions and changes to training without having to be overworked and personally manage and run the tests.

Ask the Right Questions

With the threat of social engineering attacks on the rise, it is important to think about the *what, how,* and *why* when building or enhancing your security awareness program.

- What level of quality and scale are you looking for in the testing and training?
- How is the testing performed and does it leave opportunity for training when testing completes?
- Why invest in this program? Is it for compliance purposes only or are you looking to really secure your users, network, and data from malicious actors?

After answering these questions, you will be on the path to choosing the right provider for your needs.

We would love to talk with you about Social-Engineer, LLC and how we can help you achieve your goals.

www.Social-Engineer.com