Vishing and Phishing Must be Ongoing to be Effective

Most companies have a security awareness program in one form or another. If they don't, it should be on the short list of programs to start as soon as possible. In our experience, many of these programs take the form of computer-based training. This is usually done once a year to satisfy the compliance requirements set forth by auditors in varying industries. But is that really a security metric to gauge how your userbase responds to real world threats against your valuable data and resources? We believe that vishing and phishing must be ongoing to be effective. Sure, having users complete a standard collection of trainings with a "passing" grade is one component of a well-rounded security awareness program. However, what are some of the other successfully utilized components?

Testing, and Not the Multiple-Choice Variety

Real world testing is successful in building a culture of security among employees. Stakeholders can see value and return on investment when testing is done in a controlled and measurable manner. Our clients get data that, as they have told us, is very actionable. In addition, the data helps inform updates to the standard training they had been using.

The testing we employ with our clients attempts to mimic what they would typically see in real attack scenarios. We expect them to respond and react as if it were a real attack. This builds muscle memory. So, when they are not being tested, they respond and react in a manner the company expects. We work with our clients in a reinforcement framework to encourage the desired behavior over and over. As a result, the correct behavior is the first thing that comes to mind when presented with a possible attack. This builds the critical thinking that is necessary to properly defend an organization, from the lowest level of employees to the highest level.

How Often Should This Testing Occur?

That is a very common question when we pitch our services to prospective clients. The answer really depends on what your goal is. But we tend to lean toward a monthly test as we have seen the most positive feedback from clients on that frequency. Quarterly and annual tests can give you actionable data. However, the concepts we are trying to reinforce, which are your policies and procedures about data protection and system usage, can be forgotten fairly easily if they are not engaged often enough.

Testing that is too frequent can also deter the progress a program is trying to achieve. Over-testing may exhaust the userbase or even desensitize them, so you may want to avoid daily or weekly tests. Your users will tire of the process and find ways to complete the tasks that are not conducive to learning the lessons you want them to learn. Getting the most out of your security budget

Running a simulated full-scope attack against your company periodically will add a new form of testing to your security awareness program. We recommend coupling this with an ongoing phishing and/or vishing testing program. Doing so will help to identify security gaps and further promote a secure culture in your company. Indeed, having ongoing phishing and vishing programs running concurrently gives stakeholders a holistic view of the vulnerability present in the tested userbase. Combining those two data sets is a powerful tool in measuring the effectiveness of your company-wide security training.

Phishing and vishing are the most common types of social engineering attacks. Seeing where your company stands with respect to those attack vectors, specifically when the testing is being performed by the same entity, will provide a very clear picture on where your budget should be spent to get the most value.

Check out our services page to see how you can utilize industry experts in the field of social engineering. Maximize your security budget and secure your company with testing that uses the science of human nature to back up your technology.

www.social-engineer.com