Social Engineering

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Testing the Human Factor

The largest cybersecurity vulnerability at any company is its employees. Cyber breaches happen every day because someone clicked on a malicious link in an email or gave out a little too much information to a bad actor. Attackers have several ways they can use your employees to access sensitive company information – malicious phone calls, emails, and even walking through the front door of your business. You have policies in place to combat these threats, but you can't truly be sure how effective they are until you put them to the test. With so many attack avenues available, it's more important than ever to protect your business and your employees.

Our Social Engineering engagements are designed to simulate how a real attacker would attempt to deceive your employees into giving them access to sensitive company information. Security awareness training, while important, is simply not enough. By performing social engineering engagements, you'll have the ability to test your employees to see how effective your security awareness training really is and most likely find areas for improvement.

Types of Social Engineering

We offer Social Engineering in two forms - remote and onsite testing. For Remote Social Engineering, TracePhishing and TraceVishing are both great ways to test your employees on phone and email attacks. TracePhishing allows you to send simulated phishing emails to test who would click on a malicious link or attachment, while TraceVishing, or "voice phishing," involves simulated phone calls to your employees in an attempt to access company credentials. We have email templates and phone call scripts that we have found to be effective, but we give you the option to customize these if you'd prefer.

We also offer Onsite Social Engineering, which is a physical test of your employees to gauge adherence to visitor policies and to see if a malicious actor could access sensitive areas of your organization by posing as a vendor or other trusted agent. Our team of Information Security Analysts has a variety of disguises and cover stories that they can use to trick your employees into trusting him or her to be alone in sensitive areas of your organization.

What's Next?

Once you've testing your employees, you'll know how well they follow security awareness company policies and procedures. It's important to educate them on how to recognize these types of threats before there is a real attack, especially for the employees that may have fallen for a social engineering attempt. If there are any policies that you haven't implemented, like an escort policy for onsite visitors, this is the perfect time to implement them and train all employees on new procedures. This is also a great time to update or tweak your security awareness training to address any gaps in knowledge found during your Social Engineering engagements.

Key Takeaways:

- **Manual exploitation of vulnerabilities using real-world hacking techniques**
- **Understand any network security gaps and how to fix them**
- **Simulation of what an attacker could access through unsecured networks**
- **Verification of network security controls**

Frequently Asked Questions

Can you use more than one cover story between locations?
It is much easier for our Information Security Analyst if they don't have to bring along multiple costumes/disguises, but we can upon request.

Do you perform USB drops?
We will upon request but typically don't because we have a separate service that includes this.

What is the script you use for vishing phone calls?
We do not have just one script that we use. We are open to hearing your ideas, but we can also suggest some that we regularly use and have success with.

How often is the phishing platform updated? How often can I expect new phishing templates?
While there is no defined schedule for releasing new phishing templates, our team is continually searching for innovative methods for conducting phishing tests and will periodically release new templates. Additionally, our software provides the ability to create custom phishing templates which allows users to define their own content.

Will Trace phish my employees continuously or only on set intervals?
Depends on scope of the engagement - typically done in quarterly intervals but the emails are not all sent at once.

If an employee fails a phishing attempt, what happens?
Employees who fail phishing attempts are logged as such in our system and the details of the failure are reported to you. The details will include whether or not the phishing email was opened, whether or not the user clicked on the malicious link(s) included in the email, and exactly when the user failed the test (date and time). Additionally, there is an option to display a configurable web page with a message to notify users of their failure with tips to improve security awareness.

How much does support cost? What happens if I have an issue with the software?
Support is included at no additional cost.