TraceVishing

Emails Aren't The Only Problem

For many organizations, phishing is a large problem due to the fact that attackers can mass email these phishing attempts out to thousands of targets at once. What happens, however, when someone decides to really target your organization? What other avenues could they use to take sensitive data and compromise the organization?

People are one of the largest vulnerabilities of an organization, and that doesn't stop with emails. Vishing or 'voice phishing' is when someone decides to target your employees and call them individually, posing as someone legitimate, to try and get sensitive information. These calls, while less frequent than phishing attempts, can be far more effective for attackers to get sensitive information, especially when employees don't know what to look for.

Recognizing The Threat

As a part of a greater Security Awareness program, TraceVishing can be a critical component to assessing the effectiveness of a program. By having Trace simulate what an attacker could actually do via vishing, an organization can be more aware of these types of attacks and be better prepared if something does occur. Combined with TraceEDU and TracePhishing, you get a comprehensive security awareness program that covers employee education, and assessments via phone and email.

Process For Prevention

During our TraceVishing engagement, our cybersecurity experts will work with you to identify which employees to test along with a convincing cover story. We then call and see if we can extract any sensitive information from the individual. This can be done utilizing no inside information, or you can upgrade to Premium, where you give us fake customer data so that we can do an even more thorough test of your organization.
Once all of the calls have been made, we provide a comprehensive report. This report also includes recommendations on the best next steps to take to make sure your organization stays secure.

TraceVishing Provides:

- **Scripts based on our expertise, with your input**
- **Targeted or randomized employee testing**
- **Comprehensive reporting on all phone calls along with recommendations on how to improve training**

Frequently Asked Questions

What data will you need from me or my team for vishing?
All of the information required for vishing engagements is covered during the scoping call/email that you will receive before the engagement begins. The analyst conducting the vishing engagement will gather information such as: the names, positions and direct lines (or extensions) of the employees to be tested, whether or not your company uses a call center or a receptionist, and your company's hours of operation or the hours during which employees should be contacted.

Will you Vish employees year-round or is it a set engagement with a limited number of vishing attempts?
This will depend on the stipulations of the contract that you agree to with TraceSecurity, but you will be able to control the duration of the engagement as well as the number of vishing attempts that our analyst will conduct.

Explain how TraceVishing and TracePhishing complement each other. Should I get both?
Yes, because vishing and phishing are both commonly used social engineering strategies, it is best practice to test your employees against both methods to truly determine how your employees respond to various forms of attacks.

What sort of scripts do you use when you call? Do I have input on the types of scripts you will be using?
Our analysts use strategies that have proven to be most effective in the past when conducting calls. Because real-world vishing attempts are ever-evolving, our methods are constantly changing, too. No two employees of your organization will be tested on the exact same script. However, if you wish to use a custom script or strategy that you know to be effective for testing your employees, our analyst will work with you and deliver the script(s) that you choose to use.

How do you decide which employees to target? Can I target specific departments?
You are in complete control of the employees to be included in the vishing engagement by providing a specific list of employees. If you prefer, you can provide a list of all employees of a department or departments so the analyst can select employees at random.

What happens if you can't get in touch with an employee?
Each employee that we attempt to contact will be called up to three times (on three different days). If, after three attempts, the employee does not answer, he or she will be recorded as such and reported to you as a "No Answer."

What is included in the report you provide?
The report includes statistics on the pass/fail rate of each user contacted as well as a detailed description of each call.