A Case Study in Vishing

Vishing (voice-based phishing) has been a problem for quite a long time. There are many vendors in the marketplace that offer vishing services. However, they tend to use robo-callers or call centers for large volume engagements. If they are using trained humans to make calls, it is likely in very low numbers. Frequently it’s not an on-going program, but merely a point-in-time assessment. Robo-callers present a very noticeable problem. Ask yourself a simple question: “*Do you answer questions once you realize you are talking to a robot?*" Assuming the answer is ‘no’ to that question, your users likely feel the same.

If seeking to train your users on combating malicious vishing attempts, train them to avoid disclosing information to a robot might not be the best use of your training budget. When it comes to using call centers to make vishing calls for your program, yes humans typically make the calls, but they tend to use a script with little deviation from their defined path.
What do the callers do when the target answers in a way they are not prepared for? Regardless of how that question is answered, if the call is mimicking fraudulence or is real, “red flags” tend to be raised and the caller’s pretext falls apart if they cannot successfully pivot the conversation.

This was the issue one future client with 60k-70k employees started to realize when planning for their on-going vishing training program. “*How do we simulate a real adversary in a safe and controlled manner, and provide actionable feedback to our internal testing department?*"

Live, Trained, Vishers

This company found **Social-Engineer, LLC (SECOM)**. We utilize live, trained, and certified professional vishers. Our service can be performed with over 1000 calls or more per month. They contracted us to run a small pilot program to get a baseline of their risk associated with this attack vector. We worked with this company to come up with relevant pretexts aligned specifically for their business, testing their employees' ability to follow the established policies and procedures when dealing with an unknown caller asking for sensitive information.

Year One Results

That initial test, using a very small sample size in their environment resulted in a 46.0% compromise rate and a 36.0% shutdown rate. This was a good starting point. They signed up for a full year of service using the entire company as possible targets, wanting to gge what type of effect a long-term engagement would have on their security posture. In the first year of testing, there was a high mark of 72.2% compromise rate, with a low mark of 12.2% shutdown rate. This worked out to a 54.5% average compromise rate and a 27.2% average shutdown rate for the year.
It was clear they had to adjust their internal training to make these numbers move in a desirable direction.

Adjust Training, Retest the Population

This company saw the value of this type testing and renewed for a second year. They updated their internal training using the data SECOM provided and were very interested in the results after the second year of testing. We again worked with them to come up with new pretexts that would resonate with the employee-base and year two data went in a negative direction for them. 61.1% of calls on average resulted in compromise (up 6.6%) and there was a 24.2% average shutdown rate (down 3.0%). Why were the numbers getting worse with on-going testing?

There are several reasons, we explained, why this might happen. First, our vishers were more familiar with the jargon of the company. Second, our vishers were now more familiar with the verification processes the employees were trying to use. Also, the pretexts changed from the first year using all this new knowledge. The tests got harder.

In the third year, it was evident that our new program was helping the in-house training initiative. We saw a notably dramatic shift in the numbers. The average overall compromise rate across the multiple tested levels of sophistication, dropped to 33.5% (down 27.6%) and the average shutdown rate jump to 66.4% (up 42.2%!!).

This huge shift, almost a 180-degree change was due to testing that was just difficult enough to give the users a chance to make the right decision, then progressively increase that difficulty as they learned more.

Incremental testing allowed the employees to learn the multiple techniques a malicious caller could us, while also re-enforcing the verification and reporting processes the company had established. The fourth year of the contract builds on that trend. We recorded an average compromise rate at 28.3% and the average shutdown rate at 71.6%.

The Takeaway

The main points:
- Test just beyond your user's current knowledge to make them think critically about the situation.
- Progressively increase difficulty to continue to test the users as they learn and become familiar with the policies and procedures.
- Test the entire user base to understand where vulnerability lies within your organization.
- Follow testing with training that reflects the previous tests, so it is relevant and timely.

Do you want to experience the same dramatic shift in your security awareness program?
Are you ready to secure your organization from the evolving threat of vishing?
We invite you to contact **Social-Engineer, LLC** about our **Managed Vishing Service** paired with our Instant **Vishing Education Service** (IVES™).