

Created By: mothered

<https://www.socialengineers.net>



Listen To Background Noise During Phone Conversations.

Inevitably so, calls will be generated (and received) from other departments of your organization throughout the duration of your company's business hours. It could be the accounts department at the head office requesting taxation details of a particular worker, or someone from sales asking for the latest update on a client's contract. Whatever the case may be, sensitive details will be distributed over the phone.

The Role Of The Social Engineer:

Whilst It's almost certain that such calls are legit, It's a known fact that social engineers use their skills to perform malicious acts, by pretending to be an Internal employee with the Intention to obtain personal Information of some sort. Social engineers predominantly target companies on a large scale, for the reason that It's a lot harder for organizations to keep track of the legitimacy of 5,000 employees, as opposed to a small family-owned business of 20 workers. Here's how an SE'er can manipulate your staff over the phone, to hand out an employee's bank account details by simply asking for It!

Research And Preparation:

After **"researching your company"** to Identify Its structure and the vulnerability of your workers, the social engineer decides that he'll pretend to be one of many employees working In the **"accounts department"** of your building. He knows how the phone extension numbers are displayed, so he's prepared to spoof his caller ID to match the numeric format.

He's also aware that the **"timing of the SE"** Is crucial, so he's opted to execute the attack on a **"Thursday at around noon"**. Moreover, the **"background noise"** must suit the nature of the environment, so the SE'er has located a clip on YouTube with phones ringing, people talking and computer keyboards tapping away. He'll play this during the time of the call. Here's how the attack Is done.

The Social Engineering Attack In Action:

It's precisely 11:55 am on "payday", namely "Thursday". The SE'er Is sitting at home In readiness to SE a worker In your HR department. He's hit the play button on the YouTube clip, which represents an office environment. His caller ID Is also spoofed to match your company's Internal format.

The social engineer calls and says **"Hi, I'm calling from the account's department and was wondering If you could please help me. I've processed the pays for almost every employee, except Peter Dominican (this Is the real name of a worker by the way!). "My system crashed and I've lost his bank account details. Could you please read out his account number so I can finalize the payment?"** The HR person recognizes the extension number on the phone, Is aware that employee payments are processed around this time each week, and simply reads out the **"bank account number"** to the SE'er.

Preventative Measures And Conclusion:

SEing your employees, Is as simple as that. The above was a perfect social engineering example, that would've been quite difficult to differentiate from an authentic call. However, not every SE covers all angles. The most effective way to Identify a fake call, Is to **"listen to background noise"**. It's pretty difficult for anyone to match the **"exact nature"** of your company's office environment. One little slip-up,

will give away the entire SE.

If you believe a call appears suspicious, make it a habit to listen to everything running in the background during the conversation. For instance, if you hear nearby traffic, a baby crying, dogs barking or the Jerry Springer show playing, then you know the call is not authentic. If still in doubt, try and keep the caller on the line for as long as possible, with the intention to listen for any inconsistencies that indicate fictitious behavior.

You may reference my work, only if you credit its source
namely

<https://www.socialengineers.net>

Downloaded From:

<https://www.seing.org>

My Other Blog:

<https://www.manipulating.net>