SOCIAL ENGINEERING

Almost every week mass media communicates about *hackers* having stolen thousands of passwords and other sensitive private information. It is commonplace to read articles about hackers having taken advantage of system vulnerabilities to bypass security barriers in order to fraudulently access private and company networks.

One of the most famous ways of hacking is SOCIAL ENGINEERING. Social engineering is an art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.

For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

Even if you've got all the bells and whistles when it comes to securing your data centre, your cloud deployments, your building's physical security, and you've invested in defensive technologies, have the right security policies and processes in place and measure their effectiveness and continuously improve, still a crafty social engineer can find his way right through.

Social engineering has proven to be a very successful way for a criminal to "get inside" your organization/ on an individual’s personal life. Once a social engineer has a trusted employee's password, he can simply log in and snoop around for sensitive data. With an access card or code in order to physically get inside a facility, the criminal can access data, steal assets or even harm people.

Sometimes, if the hacker knows the person, he will just send a link that is so related to them just to get the victim to open it. And given the relationship, the victim will be quick to open the link since they trust the sender.

You don't need to go thrift store shopping to pull off a social engineering attack, though. They work just as well over e-mail, the phone, or social media. What all of the attacks have in common is that they use human nature to their advantage, preying on our greed, fear, curiosity, and even our desire to help others.

Criminals will often take weeks and months getting to know a place/ the target person before even coming in the door or making a phone call. Their preparation might include finding a company phone list or org chart and researching employees on social networking sites like LinkedIn or Facebook.

How they attack:

- **On the phone**

  A social engineer might call and pretend to be a fellow employee or a trusted outside authority (such as law enforcement or an auditor).

- **In the office**

  “Can you hold the door for me? I don't have my key/access card on me.” How often have you heard that in your building? While the person asking may not seem suspicious, this is a very common tactic used by social engineers.

- **Online**

  Social networking sites have made social engineering attacks easier to conduct. Today's attackers can go to sites like LinkedIn and find all of the users that work at a company and gather plenty of detailed information that can be used to further an attack.

Social engineers also take advantage of breaking news events, holidays, pop culture, and other devices to lure victims. Scammers often use fake charities to further their criminal goals around the holidays. For example, in the times of COVID, they pretended to be trusted companies giving help. Some sent links that were attractive to open and these always require credentials and passwords which the hacker wants.

Attackers will also customize phishing attacks to target known interests (e.g., favourite artists, actors, music, politics, philanthropies) that can be leveraged to entice users to click on malware-laced attachments.

Like in the image below, I received a link that directed to the check out on a post I had made on twitter and, because I was anxious to see and know about my tweet, I just clicked on the link, put my credentials as asked and realized later that it was a scam. With my details already given away.

Famous Social Engineering Attacks

A good way to get a sense of what social engineering tactics you should look out for is to know about what's been used in the past. For the moment let's focus on three social engineering techniques — independent of technological platforms — that have been successful for scammers in a big way.

- **Offer something sweet.** As any con artist will tell you, the easiest way to scam a person is to exploit their own greed.
- **Fake it till you make it.** One of the simplest — and surprisingly most successful — social engineering techniques is to simply pretend to be your victim. Many organizations do have barriers meant to prevent these kinds of brazen impersonations, but they can often be circumvented fairly easily.
- **Act like you're in charge.** Most of us are primed to respect authority — or, as it turns out, to respect people who *act* like they have the authority to do what they're doing. You can exploit varying degrees of knowledge of a company's internal processes to convince people that you have the right to be places or see things that you shouldn't, or that a communication coming from you is really coming from someone they respect.

5 Tips For Defending Against Social Engineering

- *Train and train again when it comes to security awareness.*

  Ensure that you have a comprehensive security awareness training program in place that is regularly updated to address both the general phishing threats and the new targeted cyberthreats. Remember, this is not just about clicking on links.

- *Provide a detailed briefing "roadshow" on the latest online fraud techniques to key staff.*

  Yes, include senior executives, but don't forget anyone who has authority to make wire transfers or other financial transactions. Remember that many of the true stories involving fraud occur with lower-level staff who get fooled into believing an executive is asking them to conduct an urgent action — usually bypassing normal procedures and/or controls.

- *Review existing processes, procedures and separation of duties for financial transfers and other important transactions.*

  Add extra controls, if needed. Remember that separation of duties and other protections may be compromised at some point by insider threats, so risk reviews may need to be reanalysed given the increased threats.

- *Consider new policies related to "out of band" transactions or urgent executive requests.*

  An email from the CEO's Gmail account should automatically raise a red flag to staff, but they need to understand the latest techniques being deployed by the dark side. You need authorized emergency procedures that are well-understood by all.

- *Review, refine and test your incident management and phishing reporting systems.*

  Run a tabletop exercise with management and with key personnel on a regular basis. Test controls and reverse-engineer potential areas of vulnerability.

In conclusion, Social engineering attacks are not only becoming more common against enterprises and SMBs, but they're also increasingly sophisticated. With hackers devising ever-more clever methods for fooling employees and individuals into handing over valuable company data, enterprises must use due diligence in an effort to stay two steps ahead of cyber criminals.