Social Engineering - Information Gathering via Social Media and Other Online Sources

By: Brad Voris

Introduction:

Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent or malicious purposes. In order to gain a list vulnerabilities to exploit, reconnaissance of the victim(s) is absolutely necessary. Every target is different. Each victim will have a specific vulnerability or set of vulnerabilities that could be exploited in a specific way. This article will not go into detail about exploiting those vulnerabilities but using an example will briefly go over tools and data that is typically gather for these types of social engineering attacks.

Research the victim(s):

Researching the victim(s) from social media and other online sources.

Google.com (generic cached pages minimize the amount of time you really have to spend digging through an entire site)
Linkedin.com (work victim has done, technology they use or have used)
Facebook.com (search for questionnaires, family and friends with unlocked profiles, weak security leaking and timelines for activities)
Youtube.com (what videos do they watch frequently: travel, eating, reviews, etc.)
Twitter.com (what do they feel strongly about: politics, social causes, timelines, etc.)
Instagram.com (what type of pictures do they post: locations, family, friends, activities and timelines.)
Housing records (find home address if a home was purchased, sometimes you can find co-habitant information)
Yelp.com reviews (locations or services the victim has used or subscribed to and timelines associated to them)

A good example of the utilization of social media for potential exploitation:

I bought a used vehicle and my satellite radio subscription expired. I contacted the service provider to update my information so that I could re-enable service on my radio. While I online chatting with support, I was asked to verify the email address associated to the subscriber ID from my vehicle. I didn't have one because I was a new customer. The service provider shared the email address with me for verification. It wasn't my email address but the one of the previous vehicle owner. The service provider inadvertently provided me with a valuable piece of identifiable information.

Using this email address I was able to get a full name from generic Google search in correlation to the location from which I had bought my vehicle. With the full name I could find a fairly locked down Facebook profile. However there were visible family members from the Facebook profile. I

went through each facebook profile systematically writing down as much information as the users had divulged. Gathering a general location I was able to find a home address, business address and school location.

What information was gathered from online services and social media:

First/Last Name, DOB, Home Address of previous vehicle owner, limited medical history, place of business
First/Last Name, DOB, Home Address of spouse, place of business (contact information included)
First/Last Name, DOB, Home Address of Children, address and location where children went to school (one had just graduated highschool and was about to go to college)
Parents, siblings, cousins contact information, age, home address
List of places the family went on vacation, duration of each vacation and when said family would be going on their next vacation
List of places the frequently ate at during the week/weekend
List of locations the family traveled to frequently

Learning the five W's about a victim:

Who: Knowing a victim(s) and/or family members
Where: Knowing when a victim or a family member of a victim is home, place of business, out eating or at school is extremely valuable. (location)
What: Knowing the work that they do (or family) or how they contribute (or feel they contribute)
When: Posts on social media give timestamps for activities and locations
Why: Irrelevant for this case "*...motives are incidental.*" - Scream

Armed with this knowledge a payload could be designed to exfiltrate any kind of data from the victim(s), organization, etc.

Conclusion:

While I am not recommending or condoning the exploitation of others it is very easy to see how victims can be taken advantage of by hemorrhaging PII and sensitive personal information about themselves on the internet. Social media allows us to share everything about ourselves and our family but it also allows other people who could use this information for malicious purposes.

About the author:

Brad Voris specializes in infrastructure architecture and security design, and has designed and managed infrastructures for global organizations. He holds CISSP, MCP, MTA, NSE1, Network+, and VCA-DCV certifications. To hear more from Brad, check out his website www.VictimOfTechnology.com or visit his Linkedin.com profile.