

## Top 5 Tips To Make Social Engineering Your Career

Chris Hadnagy

Over the last year social engineering has gotten a lot of press. From the attacks on companies like Sony, HB Gary, PBS, Citibank et al to contests like the Social Engineering CTF at Defcon, it seems that social engineering has taken the front page. And rightfully so, as it is still the easiest and often most effective vector of attack. With that in mind, many people are interested in learning what it will take to either add social engineering skills to their tool chest (either personally or as part of their red team) or even become a full-time, professional social engineer.

And that was the impetus behind Chris Hadnagy's new monthly column exclusively at The Ethical Hacker Network, how to become a professional social engineer. So to get the ball rolling, I compiled this Top 5 List to help each person make this a career path or at least add it to their present security practices. As we move through the coming months, we'll explore the history, methodologies and practical experiments in attacking the human. It will not only be educational but eventually lucrative for you and your organizations.

Discuss in Forums {mos\_smf\_discuss:Hadnagy}

## TIP #1: Education

This first tip will seem a bit self-serving, since part of my job is to sell some of the most unique education to help professionals put social engineering into practice through the course called "Social Engineering for Penetration Testers." But there is more to it than that. Many college-aged young adults will ask what courses they can take to help in becoming a security professional.

Social engineering is a unique field that involves understanding how humans think and interact. I strongly encourage those interested in making social engineering their career to study communications, psychology and human interactions. I am not saying that you need to be a psychologist, but understanding the way in which humans interact or react to situations can go a long way in helping you become a social engineer.

If you are past the college age or simply do not want to go back to school, there are plenty of books and online courses to help you learn these details about psychology well enough to get by. There are even plenty of free university courses. So here's your first assignment; find free courses by accredited institutions and post them in the thread for this article.

In addition to understanding these topics it is also important to understand basic pentesting skills. Things like information gathering, networking, email and more. This type of education can help you to be a complete pentester with the skills needed to really help secure your clients. Again (totally self-serving) you can attend one of the many Social Engineering for Penetration Testers courses, but the skills that you need to be a proficient pentester can truly only come from high-quality, performance-based courses. The courses offered by Offensive Security are excellent and can help you learn those basic skills needed to become a top-notch pentester.

In the end though, one of the best educational philosophies is to continue self-education. Never stop learning. Make it your goal to continue trying your hand at learning new vectors of attack, understanding how they work and demonstrating them to customers. That deeper understanding will be an education for you and will benefit your customers.

## TIP #2: Experience

This one is harder, as it is the classic Catch-22 situation. To get the work you need experience, to get the experience you need the work. How can you get past this then?

If you are just starting out you can try to get a job in a pentesting firm on the low end of the totem pole just to build experience. You can even offer to intern for companies to help build your base of experience. Don't be ashamed to take these types of positions as they often lead to full-time employment. There are even examples right here in the EH-

Net forums of older professionals who have taken 1 step backwards in their career with an internship only to turn it into the experience they needed to land the job of their dreams.

In these times you need to pull out all the punches even including calling in favors with your friends and family as well as offering services for free with non-profits. Get help from anyone that crosses your mind to get small social engineering jobs. Getting some experience in the field will help you to know what to look for and how to help your customers be more secure. Plus, regardless of whether the gig lasts a week or a year, every job is yet another item to list on your resume.

### TIP #3: Practice Makes Perfect

This ties into the second tip perfectly and a good way to gain some experience. Practice. Now this doesn't mean to go out and start to social engineering unsuspecting companies stealing their data and passwords. What I mean is finding practical ways to start building your skillset to become a professional social engineer.

Want to practice your ability to build rapport &ndash; head out to public places and build your skills by striking up conversations with strangers and seeing how much you can learn from them.

Elicitation skills need tweaking? Head to a coffee shop and learn the art of conversation. Practice asking different types of questions and notice the different type of responses. As you do, you will build your foundation and learn what works and what doesn't.

You can practice phone skills when you have to call your family, vendors or customers. You can practice your nonverbal communication reading skills anywhere at work, play or home.

Pick a skill that you want to enhance and then start small and build from there. When they become second nature then move to another skill.

### Tip #4: Build a Name

Being a professional social engineer is an interesting field. Most of your clients will not want you walking around telling everyone what you did for them. If you were successful they may not want the world knowing the stories of how badly you pwn'ed them.

How else can you then build a name that will help potential customers see you as a solid choice for their social engineering needs?

You can take some time to build name by contributing to the community. Write an article, submit some research, do a few speeches on the topic &ndash; or a combination of all these. The more your name appears in quality magazines or journals or even on informal websites on the topic of social engineering, the more you have to point your customers and potential customers to that shows you can back what you claim.

And don&rsquo;t worry if it doesn&rsquo;t seem like it&rsquo;s enough at the time. Rome wasn&rsquo;t built in day. Even short talks at small events count as having speaking engagements under your belt. And it&rsquo;s always better to make rookie mistakes in a small venue first.

#### Tip #5: Be Aware

Being aware of what is going on in the world of security and social engineering can separate you from the competition. Understanding the seriousness of spear phishing, knowing the latest methods used to infiltrate companies and having the skill to implement innovative counter-measures is imperative.

This doesn&rsquo;t mean spending your life reading everything on the web, but you do need to be very aware of current news. I find it useful when I hear a story or read a news clip about an attack to try and understand the method of attack and analyze it for anything new.

Even if there is nothing new, then my goal turns to understanding how the attack worked, so I can use this information to educate my clients and help them see where they can improve. Also I find it helps both me and my clients, if I can demo how the &ldquo;bad guys&rdquo; make encoded malicious PDFs, how they phish their targets and other such attacks. This process not only helps me better my communication skills but also has the added benefit of creating appreciative clients for being able to see these attacks without having to fear the negative consequences.

#### Is Social Engineering for You?

I find that being a professional social engineer is very different from other career paths taken by my friends or family. It is not a part-time hobby or some job where you can leave the work at the office when the 5:00pm whistle blows. Social engineering professionally takes dedication and time to master the art. You have to be &ldquo;switched on&rdquo; most of the time and practice the skills non-maliciously to become proficient.

Is it for you? That is hard to say. I can tell you that being a professional social engineer is not only fun (who doesn&rsquo;t enjoy getting paid to exercise their dark side), but it is really rewarding. When you see that light bulb go off in your client&rsquo;s thinking, it makes you feel good that you had a part in that.

Either way, this series of exclusive articles on EH-Net will not only be fun, but it will be a great tool in determining if this is a career path for you. If it's not, you'll pick up some valuable life skills. If it is...

Until next month!

If you have comments or questions — please feel free to reach out to me at [logan@social-engineer.org](mailto:logan@social-engineer.org)

Chris Hadnagy, aka loganWHD, has been involved with computers and technology for over 14 years. Presently his focus is on the "human" aspect of technology such as social engineering and physical security. Chris has spent time in providing training in many topics around the globe and also has had many articles published in local, national and international magazines and journals. He is also the lead developer of Social-Engineer.Org as well as the author of the best-selling book, Social Engineering: The Art of Human Hacking.

He has launched a line of professional social engineering training and pen testing services at Social-Engineer.Com. His goal is to help companies remain secure by educating them on the methods the "bad guys" use. Analyzing, studying, dissecting then performing the very same attacks used by malicious hackers on some of the most recent attacks (i.e. Sony, HB Gary, LockHeed Martin, etc), Chris is able to help companies stay educated and secure. Chris can be found online at <http://www.social-engineer.org/>, <http://www.social-engineer.com/> and twitter as @humanhacker.