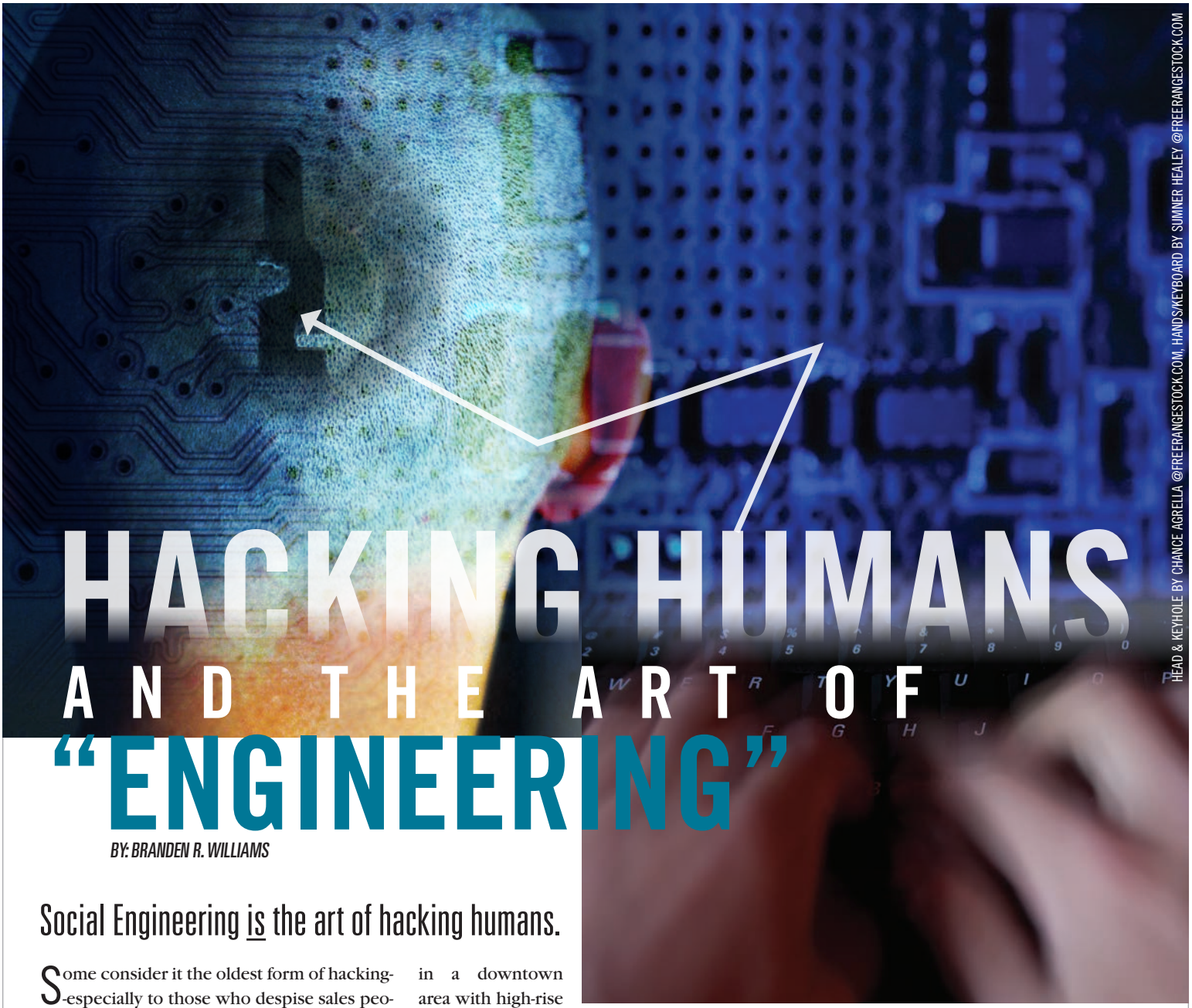

HEAD & KEYHOLE BY CHANCE AGRELLA @FREERANGESTOCK.COM, HANDS/KEYBOARD BY SUMNER HEALEY @FREERANGESTOCK.COM

HACKING HUMANS AND THE ART OF "ENGINEERING"

BY: BRANDEN R. WILLIAMS

Social Engineering is the art of hacking humans.

Some consider it the oldest form of hacking--especially to those who despise sales people who often use tactics to guide people into parting with their money. Social engineering, as a tactic, is just as critical to survival or target achievement as the right clothing, training and equipment. Many of us use it every day without even thinking about it. Let's look at some examples.

I am a security professional by trade. I focus on information security and compliance issues primarily, but have run the gamut of security requirements as both a practitioner and a consultant. A few years ago, an oil company contracted me to break into their wireless network. At the time, this was something that was relatively common. The audit department determined the effectiveness of various controls deployed by IT and security, including the ones on this wireless network. This particular client was in a city with over 300,000 people in a downtown area with high-rise buildings. They were on the 18th floor of one of these high rises. Their wireless signal was barely detectable outside of their office space and definitely not detectable from the top of an attached parking structure. I needed to see if an attacker could gain access to the wireless network where no physical security controls were present. While on the parking structure, I noticed several buildings on other city blocks that had windows facing my client's space. To test my client's network, I needed to get up to the same elevation as my client's space without prior authorization from any tenants in those offices. Seemingly impossible, right? Wrong.

Not only did I get access to both buildings, but one of the buildings had a bank branch on the ground floor that I had to walk through to get to the elevators. When you look official (I was wearing a polo and slacks while carrying a hand bag full of technical equipment), people tend to treat you "officially." The first building I visited had typical lobby-level security with a guard desk. I explained to the gentleman that I was doing an assessment for my client, pointed to their building while naming the client and asked if I could get on one of three floors to test their wireless network. The gentleman was a little bit uneasy, so I asked to speak to his supervisor. The security supervisor graciously offered to take me up to the floor I asked for and let me use an unoccupied space to run my tests. This was the hardest challenge I faced and the only time someone stopped me.

The other building seemed daunting as it had a well-known bank's logo on the top and a branch office of the bank on the ground floor.

NETWORK BY IANL @ FREERANGESTOCK.COM, WORKER BY WIXPHOTO.COM

The elevators were in the back of the bank, up a small flight of stairs and directly behind the bank tellers, who happily greeted me as I walked in the door. I confidently walked right past them to the elevator bank, saw an open one and hit the up button. Nothing happened. Then I noticed that I had a bit of good fortune that day because the elevator was in maintenance mode which required the occupant to hold down the door close button to force the doors shut and activate the elevator. When the elevator reaches the selected floor, the doors will remain open until someone holds down the door close button again. The best part of this was that since the elevator could only be switched into this mode from the inside, I was guaranteed to have an elevator waiting for me to get down.

Once on the floor I wanted, I talked my way past the receptionist of an architecture firm and was given free reign of their conference room. Nobody watched what I was doing and I could have just as easily been placing a covert hacking tool in that conference room to gain access to their networks and to watch or listen to their meetings. I spent a few minutes there, thanked them for being so gracious with their space and happily retreated back to my elevator, which was still waiting for me.

Do you want to try this for yourself[1]? Local delivery services are frequently targeted by social engineers to create a legitimate-looking identity. Your local flower shop probably has a website with a logo, address and phone number. If you know someone in your target location, you can serve as a delivery person with a small amount of money invested to make it believable. You would need a polo shirt and possibly a ball cap that matches the company's branding and logo, an ID badge that you can mock up with your favorite photo editor, a business card that looks professional[2], and some flowers or balloons[3]. Nearly all of this is available for less than $40 from internet retailers. I have also seen people dress up as telecom representatives and talk their way into very sensitive areas with believable work orders. People generally want to be helpful and a smile with a clean look can go a long way.

Tactics like this often will not get you into a government building, but they will definitely get you into some places—much like how young adults under 21 get served alcohol at bars or are able to purchase it from a liquor store. They look confident, they sound confident in what they order and they do not pay the waiter much mind. Imagine a 20-year-old going into a liquor store and asking for directions to the place where they stock the Two Exes beer versus a well dressed youth who walks confidently up to the sales clerk holding a bottle of Balvenie Doublewood. I'm not saying I had any personal experience with this, but it works more often than you might imagine.

Skilled social engineers are not only good at the arts of persuasion and manipulation, they will typically have some other skills from the security world that help them achieve their goals. For example, knowing how to defeat or get around locked doors is a common issue because no matter how hard you try, verbally pleading with a door will not cause it to unlock itself. Not everyone needs to learn how to pick a lock (though it is a skill that is fun to practice), but attackers will find benefits in knowing how to defeat the control. As an example, if you have ever had to present an ID badge to an electronic reader to get access through a magnetically locked door, you know that someone considers things behind that door to be valuable or sensitive enough not to issue physical keys to many individuals. In many cases, for convenience companies will put motion sensors on the other sides of those doors so that workers only have to approach the door to get out. These locks can be defeated by using a straw, some tape, and a

WHEN YOU LOOK AND ACT OFFICIAL, PEOPLE TEND TO TREAT YOU OFFICIALLY.

balloon (or a rag on a couple of coat hangers). Stick the assembly under the door, blow up the balloon, wave it around, and trigger the motion sensor. Expensive security system defeated! Sometimes doing something as simple as cutting the power to the floor will disengage these locks as well.

Spotting social engineering is no different from any other routinely used threat detection technique, be it professionally done or as part of our lizard-brain survival instinct. To discover a social engineer, learn to limit your trust of people you do not have personal relationships with and pay attention to things that appear out of place. Watch people's behaviors and see if they look uneasy. For those of you who remember the classic Sci-Fi flick, "The Matrix," what I am describing is equivalent to the scene with the woman in the red dress. Although in most cases, things that look out of place are not always as easy to spot (or as distracting) as she was. Good social engineers are extremely hard to spot as they will arm themselves with the knowledge needed to form a credible pretext, plenty of personal knowledge of their target with a potential to create and escalate some kind of emotional response, a back story to convince someone to do something they are not supposed to do and escape paths for when things go wrong. Those who work in teams can be significantly more effective using diversions, distractions and multiple points of interaction to mask their true intentions.

Social engineers play on deep-rooted human values that require us to help out those in need. When someone gives you an opportunity to help them out of a crisis or bad situation, most humans will take that opportunity. Don't trust an unknown caller claiming to be from Microsoft who says that your computer has a big virus on it. As more of our lives merge into digital technologies, many of these attacks leverage digital mediums for attack. Almost everyone with an email address has received an unsolicited email and some have attachments in them which are dangerous to open. The most successful heists will include aspects of physical and digital interaction for personal gain.

The best defense (unfortunately) is to trust nobody. It's OK to help your fellow humans, but understand the consequences of giving out seemingly innocuous information such as your trash pickup day or your preferred package delivery company. Social engineers use this information to build a profile on you or your company so they can perform an attack. It is OK to request the identification of someone you do not know and it's fine to make them wait while you verify their ID. Do not answer any questions until you know who you are talking to and know the conversation is legitimate. If you become suspicious, refer them to your boss or somewhere else. Saying that you do not have the information, but instructing them to send an email may be enough to halt that part of the attack. While these attacks can be tough to spot, it's up to you to detect and halt any of these attacks and train those around you to do the same. The world is shrinking at an alarming pace. What was once infeasible is now probable thanks to our ability to communicate globally, the advancement of technology and human's ability to adapt. Be prepared so that it does not happen to you. ✓

ADDITIONAL READING:

One of the best books on social engineering is *Social Engineering: The Art of Human Hacking,* by Christopher Hadnagy[4]. In this book, Hadnagy describes a complete framework for social engineering as well as listing a number of great examples from his past and from other industry luminaries such as Kevin Mitnick and Frank Abagnale, Jr.

ENDNOTES:

1. You are personally responsible for all consequences of your actions. Practicing the skills of a social engineer is valuable for understanding how criminals are likely to exploit you or your company. Comply with all relevant laws.
2. Not the ones that you print out at home and break along the perforation.
3. For a theatrical example (which includes an accomplice), check out the first 40 seconds of this clip from a classic film: http://youtu.be/oG5vsPJ5Tos
4. Hadnagy, Christopher, and Paul Ekman. Social Engineering: the Art of Human Hacking. Hoboken: Wiley, 2011.

BIO

Branden R. Williams, DBA, CISSP, CISM (www.brandenwilliams.com) is a security executive, Information Systems Security Association (ISSA) Fellow, and technology executive who specializes in consulting for global companies in support of digital business initiatives. He is the author of multiple books and the Branden Williams blog.