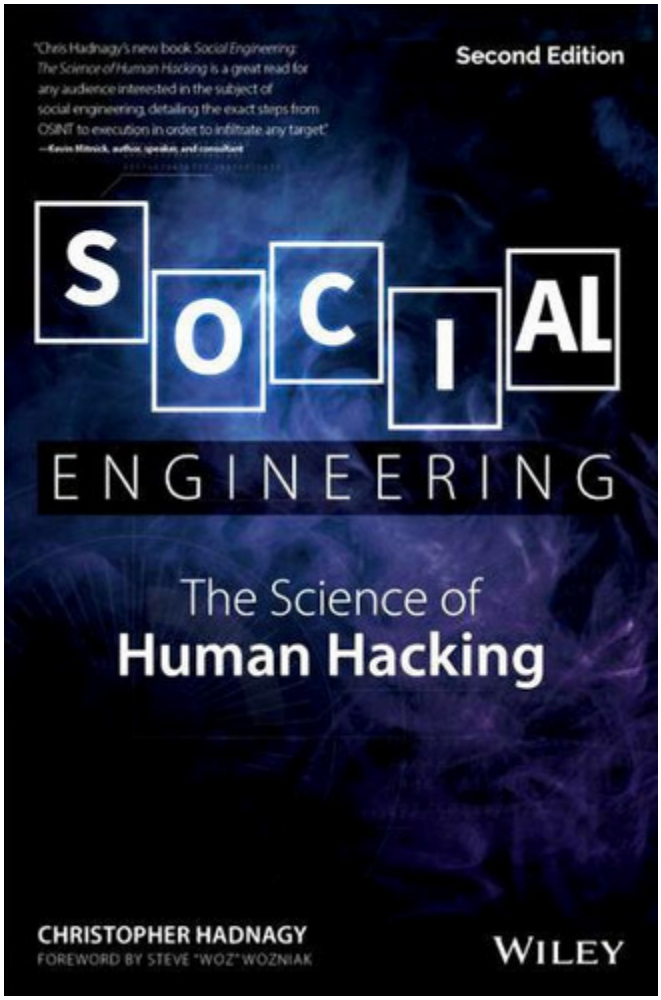
BOWLING GREEN DAILY NEWS

Book pushes readiness for evolving challenges

Posted: Sunday, March 17, 2019

"Social Engineering: The Science of Human Hacking, 2nd edition" by Christopher Hadnagy. Indianapolis: John Wiley & Sons, 2018, 320 pages, $35 (hardcover).



"From the dawn of recorded history, we see one account after another of humans tricking, duping, conning or scamming one another," Christopher Hadnagy asserts near the beginning of the second edition of "Social Engineering: The Science of Human Hacking," his recently revised primer on a phenomenon most of us encounter on a daily basis. "On the surface, there might not be much that's brand new when it comes to social engineering, but that doesn't mean that nothing ever changes."

In the broadest sense, social engineering entails an attempt to manage people in accordance with some predetermined assessment of what their appropriate role and function in society should be. Within the present context, it more specifically refers to the process of human manipulation in order to gain unauthorized access to computers, networks or physical locations – or, as Hadnagy defines it, "any act that influences a person to take an action that may or may not be in his or her best interests."

If your reaction was anything close to mine, the first thing you probably thought of involves some aspect of marketing and sales. In fact, many of the techniques Hadnagy describes are regularly employed as a way to get someone to spend money buying a product or procuring a service they do not really need or could even be harmful to them physically or mentally. One of the features I liked about this book is the way the author delves into not just the psychology of social engineering, but also the underlying biological mechanisms at play when someone is being "hacked." You don't need a degree in neuroscience to decipher the concepts being explained, but it might help to have a rudimentary understanding of basic brain chemistry.

"Social Engineering" consists of 11 relatively accessible chapters that address virtually every aspect of the topic at hand. I was pretty much hooked from the moment I began reading this interesting and insightful investigation into something most of us have heard about but very few understand. At the core of Hadnagy's thesis is the undeniable idea that any information a person has about us can potentially be used against us, especially by those who are well-versed on the strategies described in this book. Consider the following example from "Do You See What I See?" the second chapter and one of my favorites:

“I worked one job with my team in which we had been asked to perform OSINT (open source intelligence) and then attack a high-level target in the defense space. The goal was not to compromise the man, but to test his level of willingness to take an action he should not take. In a matter of a few hours, we knew the following things: 1) His favorite place to stop for coffee every morning, 2) The gym he went to before he went home, 3) Two of his favorite restaurants, 4) His home address, and 5) How much he hated city traffic. We found a domain that was basically one letter different from his gym’s domain. We set up a quick email that told him we were updating all accounts, and his credit card info was no longer valid. We asked him to ‘log in to enter his credit card info now,’ which prompted him to click through very quickly. Knowing the page was going to 404 out, we waited until we saw the click, and then we called him on the phone. The conversation went something like this:

Caller: Hello. Is this Mr. Smith?

Target: Yes, it is. Who is this?

Caller: This is Sarah over at Cold’s Gym. We sent an email out earlier today about our system upgrade. Well, the email had a bad URL, so we are calling our customers to apologize. I can send you out a new link or take your credit card and update it for you. What is easier for you?

Target: No problem, Sarah, here is my card number.

Caller: Thank you, Mr. Smith! See you tonight.

This attack worked because it hit topics familiar to him, and it was believable. With just a little OSINT, one phish and one call, we had a click, a credit card number and another five vectors prepared in case we needed them.”

Like me, many of you probably spent the last few moments reflecting on comparable encounters you have had and deciding whether you could have fallen victim to a similar scheme.

Hadnagy is the founder and chief executive of Social-Engineer LLC. He is a certified expert level graduate of Dr. Paul Ekman’s Micro Expressions courses; analyzing and interpreting non-verbal behaviors is one of his specialties. Moreover, he developed the first hands-on social engineering training course and certification for law enforcement, military and private sector professionals and regularly consults with a variety of companies and organizations, including the Pentagon. His previous books include “Unmasking the Social Engineer: The Human Element of Security” and “Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails.”

The most valuable takeaway from “Social Engineering,” for me anyway, was not the description of how it is employed, but rather how a knowledgeable and informed individual can use the insights provided to defend against these kinds of insidious intrusions into our privacy. Human nature has remained relatively immutable for the past several millennia. Those who understand how people think, act and feel have always exploited this to their advantage. The rise of advanced communication technologies, and especially social media, has only enhanced and multiplied the threat. Hadnagy is simply telling us how we can fight back.

As Steve Wozniak, the co-founder of Apple Computers, notes in the preface, “Chris’ book captures the very essence of social engineering, defining and shaping it for all of us to understand. Hacking has been around for a while, and human hacking has been around for as long as humans have. This book can prepare you, protect you and educate you how to recognize, defend and mitigate the risks that come from social engineering.”

I could not agree more. This one is highly recommended.

– Reviewed by Aaron W. Hughey, Department of Counseling and Student Affairs, Western Kentucky University.