CNET News
InSecurity Complex

August 17, 2010 2:56 PM PDT

Social Engineering 101 (Q&A)

by Elinor Mills

303 retweet Share 3

One of the more interesting events at this year's **Defcon** hacker conference in Las Vegas late last month was a **social-engineering contest** that targeted big companies like Microsoft, Google, and Apple. Participants pretending to be headhunters and survey takers were able to trick employees at the companies into giving out information over the phone that if it landed in the wrong hands could be used to sneak malware onto machines at the company or otherwise get access to the company's data.

Chris Hadnagy of security consultancy, auditor and training firm Offensive Security (Credit: Offensive Security)

The contest proved a number of things. That it is easy for strangers to get potentially sensitive information over the phone if they have a good ruse. That workers at companies, even tech companies that spend a lot of time and resources protecting their networks from hackers, were practically handing over the keys to the data storerooms without knowing it. And that humans are the weakest link in the security ecosystem and yet many corporations fail to recognize that.

I learned about the risks from social-engineering personally when I worked at a company many years ago that was receiving calls on the main phone line from people who identified themselves as telephone workmen. They would say they needed an outside line to "test the system" and my colleagues would just hit the button to give them an outside line and hang up without a second thought. When I answered one of the calls I asked why it was taking them so long to do their work and the caller hung up. I reported it to the boss and later found out that the calls were made by inmates at a nearby prison who were phoning friends and family around the world for free thanks to the company's lax security.

Today, people get duped over the phone, but also over e-mail and via Facebook and other online avenues. In this edited interview CNET talked to Chris Hadnagy, operations manager at **Offensive Security**, which organized the Defcon social-engineering contest and does security auditing and training for companies, about the risks to this type of attack, what people can do to protect themselves, and why women might be less susceptible.

Q: What is social engineering?
Chris Hadnagy: We have a different definition than what's out there today. I define social engineering as any act where you try to manipulate a person to accomplish a goal and that that goal may or may not be in the target's interest. I broaden that because I feel that social engineering encompasses not just malicious hackers that are trying to get to your data, but aspects of social engineering are used in therapy, psychology, doctors, counselors, principals, teachers, almost every different field.

How has it changed from the days of Kevin Mitnick, when he was calling companies and pretending to be an employee to trick them into giving him passwords and other information?
Hadnagy: In his day it was more difficult because he did not have the resources we have today. He had a phone and whatever resources he could gather from public resources which were libraries or public records from the courthouse and once he was able to attain names through a few fake phone calls he kept building on a pretext and this is how his attack vectors went, which was very classy for that day and age. But now things have changed because people use social media to such an extent that their whole lives are on the Web. With sites like Blippy which people can tie into their Twitter and Facebook accounts and it in essence tweets every time you use a credit card or bank account, and it tweets what you've purchased and the amount. So you can go to these sites, find someone on Twitter, link them to a Blippy account and to Facebook and now you have their pictures, what they like to buy, what restaurants they go to, when they leave the house, when they work. And within an hour you can have a very detailed profile of a company or an individual based on the amount of social media they use. I think it makes it easier for professional as well as malicious social engineers today.

What other trends do you see in social engineering?
Hadnagy: The thing that hasn't changed is the human factor. People are trusting of other people, especially if there is a request for help. One of the biggest things that worked for the Capture the Flag contest at Defcon was a contestant who said "Can you please help me with this?" Asking people for help, the human vulnerability, has not changed over the years from even before Kevin's day. There is an inherent desire for people to help other people. There are trends of a positive nature, but they still get exploited. People are more security conscious today. People are more aware of the obvious attacks, the scamming and phishing. A few years back people were falling for the African 411 scams. Now, few people fall for

those. Most people who spend any time online are educated to the simple attacks. The negative is we're so desensitized to certain attacks that we don't take notice to things that are occurring to us right under our nose.

Any anecdotes to share about particularly egregious cases?
Hadnagy: When the earthquake happened in Haiti, literally about 24 hours after that one of the top-ranking sites in Google was a Web site that was doing malicious phishing. They claimed to have data on the identities of those who lost their lives in the earthquake. If you provide personal information they said they would e-mail you with facts about loved ones in that area. They were asking for detailed information and security questions like first names, last name, date of birth, address, mother's maiden name, and then of course that information was used for identity theft. The odd thing was it was such a well-known scam, but it wasn't all over the news.

So, the social engineering is primarily online?
Hadnagy: That's probably the largest majority of attacks that are known. The ones that are online and the large phishing scams. But every day people are stealing corporate secrets through dumpster diving and other more direct methods.

Is tricking someone over the phone easier or harder than doing it online?
Hadnagy: That's a good question. It depends on the information you're trying to gather. In a professional audit we will start off with online information gathering because that's where you can harvest most of the valuable information. There's a case we talk about in our trainings where just doing a little research you can find things online like people using their corporate e-mail addresses on forums to buy or sell things of a personal nature. Those pieces of data are invaluable to a social engineer. If I know you are interested in coin collecting I can set up a fake site about that topic and send you the link and embed it with malicious code. It depends on the goal of your attack whether you use the phone or just Web resources.

What else is involved in your audits of companies?
Hadnagy: We do training and pen [penetration] testing. When we do pen testing we always offer social engineering as part of the audit. I would say a large majority of the time companies reject the social engineering. And usually it has to do with "we don't fall for that" or "our employees know better." And we just stand back and think to ourselves, man, this is the easiest way in. We go to their Web site, read about their products, their locations, do a Whois lookup to find out about the owners and administrators of the Web site. We have a bunch of different tools that harvest e-mails for the company and get as many e-mail addresses for the company as possible. I use a tool called **Maltego** that uses open Web resources to find information on the companies. Gathering all that information into one place, allows you to build an attack vector.

There was one company I was auditing where 20 employees were part of a fantasy basketball league. Then we cloned the fantasy league site using a misspelling of the real name in the URL and called one of the employees saying we were from the fantasy basketball league and that we were coming out with a new service and we would like them to check it out for free for 30 days. I said I would shoot him an e-mail and he gets the e-mail, clicks on that link and the page looks exactly like his normal fantasy basketball league Web page but there is malicious code embedded in the background and his computer is hacked while he's browsing this Web site.

How do you mitigate against that?
Hadnagy: You have to keep your browser updated, as well as all your software. If you are going to use Internet Explorer then don't stay with an old version of IE. Another important thing is not allowing employees to do personal activities at work. It's a time waster and a money waster and this is mainly how social engineers will gain access to a company. If I find out you have a hobby that you like to do at work that's my attack vector. I just need to draw you to that Web site and 90 percent of the time you're going to click on it because you're interested in it, it's a hobby.

I've heard of people pretending to be a UPS man to get on site. Does that still happen?
Hadnagy: It used to be 7 or 8 years ago that you could go online and buy a UPS uniform, on eBay and other Web sites. They were so widely used for social-engineering attacks but you can't find the uniforms now anywhere. That used to be a big vector. Who doubts the UPS guy? If I dress up like a UPS man and grab a dolly and put boxes on it and come wheeling into your office, people will open doors for me and point me in the direction of the back room. That is not as easy now to accomplish unless you can obtain a uniform or make your own. Another vector to use is to pretend to be the tech support guy. That is probably the most widely used disguise. If I come to your business and say I need get in to take care of a server issue, most people don't call the support company to ask if we have an appointment. Once you are in the building you can do a number of different things. One of them is to drop a few USB keys, especially if they are fancy looking, or a blank CD with a label that says "employee bonuses." The USB key or CD is implanted with malicious code that will give you access to their computer and the whole network, most of the time. These are not 007 [James Bond] movie attacks. These are things that occur each and every day.

How can consumers and companies protect themselves against these attacks?
Hadnagy: There are a few things to mitigate these attacks. Keep your software up to date. If I know that a piece of software is constantly vulnerable and even the updates are vulnerable, I won't use it. But the biggest key is education. Security awareness programs seem to be massively flawed in corporate America. Companies give out posters, but they don't make it personal. After Defcon we decided to launch a security awareness program. We realized that the problem is that people are not aware that telling a stranger on the phone what version of Internet Explorer and Adobe Reader gives an attacker information they need to hack you. With those two pieces of information alone I could own your company. And all you need to

do is give me your e-mail address next and it's all over. So that's why we're launching a brand new security awareness program this week. We're going to show them real live attacks. Here's what can happen if you accept a malicious PDF. Hopefully when they see that they will realize that this is not just about corporate data. If attackers can get into my computer they can get to photos of my kids and learn where I live. If I checked my bank account from my company computer then my personal account can be hacked.

So, all of the companies targeted in the Defcon contest revealed information to the callers, right?
Hadnagy: By the end of the weekend we had called 15 companies and only one company did not falter and the only reason they didn't is because we didn't get a live person on the phone. That statistic really did shock us. We did expect some of the security and tech companies to shut us down. We thought that as soon as we asked a question that sounded at all fishy we would get put away. But that didn't happen. They were more willing in a lot of respects to answer questions than some of the non-tech companies. There were only five people who did not want to answer the questions. All five were women, which I find personally interesting and pleasing. Guys have big egos and so playing on that is easy. You tell him he's great at his job he'll spill the beans. But women are more cautious by nature and that makes them less susceptible to social-engineering attacks.

Which companies were targeted?
Hadnagy: BP, Shell, Google, Proctor & Gamble, Microsoft, Apple, Cisco, Ford, Coke, Pepsi, Wal-Mart, Symantec, Philip Morris, Dell, and Verizon. And all of them fell and gave out every piece of information we asked for, except for the company where we couldn't get a live person.

What types of data did contestants ask for?
Hadnagy: There were 30 to 35 different flags, or types of information, sought. These included do you have trash handling and who does it? Do you do off-site backups? What type of PBX system do you have? What operating system, mail client, antivirus, PDF reader, and browser do they use? Do they have a cafeteria and if so who supplies the food? Do you have employee termination and new-hire orientation information available to the public? Do you have shredding or document disposal? Do they have wireless? What brand and type of computers do they have?

How long did they have to make the calls?
Hadnagy: They could make as many calls as they wanted in 25 minutes. There were probably 140 some-odd phone calls made throughout the weekend. One guy had a survey and then hung up and pretended to be a head hunter. We had some contestants who would call back multiple times and get different pieces of information.

Did contestants do anything particularly interesting?
Hadnagy: We had one guy who never asked a direct question. If he wanted to know what kind

of browser, he didn't ask what type of browser they were using. He would say something like "Have they migrated you to IE 7 yet or are you still on 6?" And one question he asked, they said "We're not on IE at all, we're on another browser." And he did that for every question. He got answers without having to ask the question directly.

Did any contestant get all of the flags?
Hadnagy: No. We had no one that went through all of the list. Our biggest point value was to get the target to go to our URL. This is the biggest attack vector used by social engineers. You open up a browser and go to a URL that is given the target. If this was a malicious attack then that person would have been hacked. For every contestant that tried that vector it worked. We thought no one would fall for this, make them go to social-engineer.org, our Web site. Then we give them extra points, because we thought no way would it work. We had five or more that drove people to our URL and they went to it and opened it up. One guy was pointed to the name and the target said, "That's a nice logo." You want to chuckle a little bit but at the same time that's scary as heck.

What were the questions that led to the hang ups?
Hadnagy: Most of the people that put the smack down on us within 20 or 30 seconds of the phone call. One pretext was "Corporate hired us to do an IT survey and I need you to answer a few questions." And the response was, "If corporate hired you why is your number coming from the Bronx?" The person didn't just mindlessly answer the questions. She had looked at the caller ID. Another one who hung up just didn't like the questions. When the contestant asked about the browser, the respondent said "If you're from corporate wouldn't you know what browser I use?" and she hung up on him too. The woman who questioned the number she called back like eight times in a row too. That to me was a great lesson for us because what that showed was that they were not doing their jobs in a mindless way. That is one of the biggest ways in for social engineers. They are hoping that people are being mindless. They noticed every little detail that seemed out of place and that is why they did not fall victim to the contestants.

Were any of the contestants women?
Hadnagy: We had one woman contestant. I hope we have more next year because personally I think they'd be better at social engineering. Especially if you get a guy on the phone and there's a woman saying "Can you help me with this?" What guy is going to say no to that?

What other simple messages do you have to help people not be suckered by social engineers?
Hadnagy: We'll have a new **Web site** launching on Tuesday that will have lots of information about how to be more aware of such attacks. The **Social-engineer.org** site explains what the attackers are thinking and doing. In addition to not doing your job or your daily routine mindlessly, I would suggest keeping things in context. If I call you and start asking you questions that don't fit your job that should raise a red flag. Ask "Why do you need to know this?" Understand what is being asked of you and question why.

You mentioned that you work in a field called "neuro-linguistic hacking." What is that?

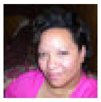
Hadnagy: Neuro-linguistic hacking is using body language and micro expressions and vocal tones to manipulate a person's emotional state. And if you can make that person enter into an emotional state that you want then it is easier to manipulate that person. As an example, people tend to be more compliant when they're feeling compassion and an emotion strongly linked to compassion is sadness. There has been research where they flashed micro expressions on a screen in like 200 millisecond time frames and used EKG monitors on their face to monitor their muscular movements. And they found that whatever emotion was flashed on the screen that person began to mirror. In essence you can make that person comply with a compassionate response more easily than if you had approached the person in a different state.

You've got a book coming out soon, right?

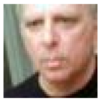
Hadnagy: Yes. It's due out in January 2011. It's called "Social Engineering: The Art of Human Hacking." It is a how-to book on social engineering. My approach to the book was thinking that the only way to truly be educated and secure is to know what the bad guys do. If you bury your head in the sand and you're unwilling to learn the methods of the bad guys you're more susceptible to fall for them.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Echo 130 Items Admin

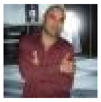


Angela Chock
"Social Engineering 101 (Q&A)" #news #technology
Today, 11:19:51 – Flag via Twitter



Steven Dale
Social Engineering 101 (Q&A) |
Today, 06:58:00 – Flag via Twitter

Scott W. Allen
Social Engineering 101 (Q&A)
Today, 10:35:02 – Flag via Twitter



Jehangir
Excellent article on social engineering and how scammers collect data on you: #socialengineering #scam
Yesterday, 23:18:22 – Flag via Twitter

Randy Marchany

Social Engineering 101 - Thanks to Valdis for this one.
Yesterday, 18:06:48 – Flag via Twitter

W2Comm
Could your use of social media lead your company to a Social Engineering security breach? CNET 101 explores
Yesterday, 16:42:09 – Flag via Twitter

Conor Rooney
Could your use of social media lead your company to a Social Engineering security breach, CNET 101 explores
Yesterday, 17:23:22 – Flag via Twitter

Mark A. Evertz
"humans r weakest link in the security ecosystem and yet many corporations fail to recognize that. " #socialengineering
Yesterday, 12:21:51 – Flag via Twitter

nibb13
Social Engineering 101 (Q&A) - CNET -
Yesterday, 11:56:05 – Flag via Twitter

ProfySpace
"I feel social engineering encompasses not just malicious hackers, but its aspects are used in different industries" -
Yesterday, 11:16:58 – Flag via Twitter

Infotex, Inc.
Defcon Social Engineering Lessons:
Yesterday, 10:56:33 – Flag via Twitter

Ashok Kumar DL
RT @infotexnow: Defcon Social Engineering Lessons:
Yesterday, 10:57:29 – Flag via Twitter

Frederic GOUTH
RT @infotexnow: Defcon Social Engineering Lessons:
Yesterday, 17:35:17 – Flag via Twitter

Howard Fuhs
Social Engineering 101-
Yesterday, 08:17:29 – Flag via Twitter

Ken Camp
Social Engineering 101 (Q&A) makes some good points
Yesterday, 00:59:14 – Flag via Twitter

Patrick Antivackis
Great interview following #defcon Social Engineering contest #security
Yesterday, 00:57:44 – Flag via Twitter

Craig Blewett
Even with best security systems a smooth talker can talk is way right into the mother lode.
Yesterday, 00:45:06 – Flag via Twitter

Wealthy Writer

Social Engineering 101 (Q&A): Today, people get duped over the phone, but also over e-mail and via Facebook..

2 days ago, 22:05:18 – Flag via Twitter

141Sercon

DH RTdennishapatinga: Social Engineering 101 (Q&A). #dh http://bit.ly/bdySbR

2 days ago, 22:00:01 – Flag via Twitter

More

Social Networking by Echo