The Truth About Identity Theft, Stickley
0789737930 FT Press August 2008

TRUTH 11

Social engineering tactics

People often ask me how hard it is to hack a password. In reality, it is rare that I ever need to hack someone's password. Though there are numerous ways to gain passwords on a network and hundreds, if not thousands, of tools available to crack encrypted passwords, in the end I have found that it is far easier to simply ask for them.

A perfect example of this type of attack was a medium-sized bank that I was testing recently. The bank's concern was related to the new virtual private network (VPN) capabilities it had rolled out to a number of its staff. The VPN allowed staff to connect directly to their secured network while at home or on the road. There is no doubt that a VPN can increase productivity, but there are some pretty major risks that can come with that convenience. The bank explained that the VPN was tied into its Active Directory server. For people who are not technical, basically this just means that when employees log in via the VPN, they use the same credentials they use to log on to their computer at the office.

So I went back to my office, sat down, and picked up the phone. The first call I made was to find out the name of an employee in the IT department. I called the company's main line to the bank, pressed 0, and asked to speak with someone in the IT department. I was asked what I was calling about, so I told the employee I was receiving emails from that bank that seemed malicious. I could have used a number of excuses, but I have found that if you tie in an unhappy customer with a potential security issue, your call gets further up the food chain. In this case, I reached a man who I will call Bill Smith. I made up a story about the email, and after a few minutes, he was able to explain to me that I had called the wrong bank and it was actually another bank's email address that it was coming from. I thanked him for his help and hung up. Obviously, the email address I told him was different, because I didn't want any red flags to continue at the bank's office, and I wanted the call to end quickly.

That night I called the main office number and got the voice mail system. After browsing around for a while, I had gathered a number of names and extensions for employees throughout the organization. The next morning I was ready for action.

I called an employee at the company from the list I had obtained the night before and identified myself as Bill Smith from the IT department. My caller ID was spoofed (easily done with publicly available tools), so it appeared as though I were calling from an internal line. I explained to the employee that I was calling to see if she had any troubles logging into the system, adding that it appeared on my end that she was having login issues. She agreed to log off and log back in while we were talking. I told her that I wasn't seeing her account and asked for her username and password so that I could log in to her account on my end to check the problem. She gave them to me. I ultimately had access to the VPN—without raising any suspicion about my real identity or purpose.

And just like that, the call was over, and I had a username and password that was allowed VPN access into the network. Now, you might be thinking to yourself that you would never be so foolish as to fall for such as obvious attack, and maybe you're right. But generally I can get a pretty good read on a person as the call goes on and hang up long before I ever ask for the password, if I think that person may be on to me. Then I just move on to the next employee. You might also believe that these employees probably know each other and wonder how could I trick them. It's generally rare that the IT staff hang out with people in other departments. So odds are in my favor. Once I worked with a guy named Jake who was making one of these calls. About halfway through, the woman he was talking to stopped and asked, "Is this really Tommy?" Without missing a beat, Jake said, "Of course, it is, baby. You going out on a date tonight with me or what?" It was a gamble on his part, but it worked perfectly. She responded with, "Tommy, you are too funny!" The thing is, when you're an identity thief on the phone, you really have nothing to lose, so you can just go for it and see what happens.

Once I had the VPN access and was on the bank's network, it took me no time at all to gain access to the banking application. From there, I was able to pull up the accounts of every one of the bank's customers. This included names, account numbers, social security numbers—basically everything an identity thief would need.

Each time I have performed this type of attack and then later spoken with the employees who unwittingly gave me the keys to the kingdom, they have all said almost the same thing: They have been told to never give their password to anyone, but that the IT guy is the one who controls all that stuff, so they just assumed that if he wanted it, it was okay. Besides, the IT guy was the one who made their account, and he could change it if he wanted. When asked if they had ever considered that someone might impersonate the IT guy who they blindly trust, they generally said they just never thought it would happen.

The problem now is that you end up with the same advice that the employee had already been given. Never give out your password to anyone. The best advice that I can give is to relay this story, explain it to all employees, or take note of it yourself. If someone from IT, your manager, the CEO of the company, or the president of the United States calls you and at any point in time asks for your password, the answer should always be the same. Do not give out your password to anyone—I mean anyone—no matter how much that person pushes or how convincing, charming, or funny he may be. The answer should simply be “no.”

Do not give out your password to anyone.