

It Takes a Thief
Easy Access to Your Customer Information
by
Raymond E. Muth, CPA, CISA, CISSP, CITP
President, BankLogic.Net, CPAs & Consultants

While much emphasis has been placed on firewalls, intrusion detection systems, anti-virus software, anti-spyware software and patching, the most critical security feature is often overlooked, the security education of your bank employees.

Social engineering is a term used to describe a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. While many of us may not understand how our so-called unsophisticated customers can get duped by Internet e-mail schemes, you may be surprised to know that it is not difficult to dupe bank employees from divulging their usernames and passwords through social engineering.

Let's take a simple technique that we employ that has yielded at least one network and core banking username and password in every bank in which we've been asked to perform social engineering. Your bank's domain name is firstnationalbank.com and we know that your username convention for e-mail is first initial last name. We also know that Fred Smith is your IT Manager and we have managed to gain a list of most of your employees. We will register an available domain that looks similar to yours. So fistnationalbank.com (notice the "r" is missing) is available and we register it so that all e-mail sent to that domain comes to us. Next we send out an e-mail from fsmith@fistnationalbank.com to each individual employee at about the same time on a Friday afternoon when everyone is looking forward to that weekend. In the e-mail to Mary Jones for example, Fred says something like this:

"Mary

I'm going to be doing a little tweaking over the weekend on our systems and I want to be sure you are up and running first thing Monday morning. I know how frustrated our customers get when things aren't running right. So please send me all your usernames and passwords so that I can verify you'll be OK Monday.

Thanks and Have a Great Weekend!
Fred"

Mary will see this e-mail from Fred and nine times out of ten, she won't even notice that this domain name is different than her bank's domain. It genuinely looks like it's from Fred. In a well-trained bank, Mary will likely pick up the phone and ask Fred why he is asking for this information. In some cases, Mary will e-mail something back to Fred like "Fred I don't think I'm supposed to be giving this to you" in which case we'll receive that e-mail without the prize we're looking for. But in other cases Mary will just send us her usernames and passwords.

So what good are a bunch of usernames and passwords if we cannot get into the network? You may also be surprised to learn how easy it sometimes is to plant a wireless access device in your bank without anyone being aware of it.

But first a few words about wireless - One of the standard questions we ask before performing an IT audit is “do you deploy wireless Internet access in your bank”. In some cases the answer is “yes” and we’ve found the access restricted and the security safeguards very good. But the answer to the question is most often “of course not”. However in a few banks we have found active wireless devices broadcasting the bank’s network traffic without the bank being aware. In two of those cases, third party network support people had plugged in wireless access devices for their ease in maintaining the bank’s network. In the third case, one of the bank’s IT personnel had it running for his own use and had just been sloppy. In none of these cases was wireless access authorized by the bank’s management. The point is wireless can be running stealthily in your bank with no alarms going off.

Thus one of the other tricks of our trade is to have one of us dress as a telephone repairman. We will go to the main office and sometimes the branches letting a staff person know that we are there to repair a circuit for Fred Smith. Usually the branches are very good and they will call Fred Smith and verify. I suspect this is because branches are more likely to be robbed and seem to have a greater awareness. Thus the most vulnerable place in our experience has been the main office where telephone repair work probably happens most frequently. If we get past the gatekeeper by saying “don’t worry we know where to go, we’ve been here before” it isn’t hard to find the bank’s DMARC (the point where the bank’s telephone service comes through). While banks usually have their computer rooms restricted, the DMARC is sometimes unrestricted. If it is unrestricted, it is a great place to plant a wireless access device. In other cases, banks will have unlocked or exposed wiring closets. These are great places to plant a wireless access device.

Once the device is planted, we can get to our laptop in the parking lot and using our phished usernames and passwords, we have access to your customer information. The really scary part about this scenario is that it does not require any advanced technical knowledge.

Now you’re probably thinking that no employee likes to be tricked. You’re absolutely right and I can tell you from my own experience that it is not a picnic. During seminars I often tell the audience that while my five minutes of fame came introducing the first Internet banking product in 1995, I was also the first banker hacked. That was an awful feeling that I’ll never forget. However it gave me religion about security and made me forever vigilant. So while social engineering may not be a pleasant experience, it’s far better than being exposed by a malicious perpetrator.

Information Security employee training is a critical component to keep customer information confidential. Make sure it is part of your GLBA program.

One final note – If you plan to engage a firm to perform social engineering, it is very important that all social engineering techniques are documented and approved by your Board and legal counsel.

Send e-mail to raymuth@banklogic.net