FEATURE

Social engineering stories

Like good movies, a successful social engineering scam usually leaves both the perpetrator, and the victim, with an impression they'll never forget. We spoke to security experts about memorable social engineering stories.

By Joan Goodchild and Senior Editor
Content Director, CSO
MAY 24, 2010 7:00 AM PST

Winn Schwartau has been writing, lecturing and consulting on security for more than 25 years. The founder of The Security Awareness Company says while technology has changed, the most influential factor in security has not—the employee or end user.

"We don't touch networks, we touch people," says Schwartau. "Because, in the end, the weakest link in all of this stuff is the person at the keyboard."

Schwartau says security managers are up against a combination of ignorance, apathy and arrogance when it comes to individual awareness.

[Learn what makes these 6 social engineering techniques so effective. | Get the latest from CSO by signing up for our newsletters.]

Also see Social Engineering: The Basics

"One thing we've recognized over the last several years is the user doesn't care about the company. He cares about his paycheck, his review, his incremental raises," he explained. "A lot of companies claim to have some kind of policies about user behavior,

Schwartau ran through some memorable moments he's encountered in his decades consulting in security awareness training. Social engineering, he says, has new players and forms, but the underlying techniques usually remain the same.

Social engineering story 1:

The postman rings, security pays the price

Winn Schwartau: We had been hired by a large financial services firm in New York to do security awareness training. We wanted to do an assessment of where people were with awareness based upon all of the training and policies they had going on prior to our involvement with them. So we created a social engineering test.

It was not the traditional 'call someone on the phone and try to social engineer them.' What we did is take their letterhead and write a letter. We sent it through regular mail to about 30 percent of the employees. Approximately 1200 people. The letter said essentially: "Hi, we're from corporate information security. The reason you are receiving this letter is because we know social engineering occurs at work and we are going to upgrade our systems. We then went into some detailed technical babble about how we were going to migrate this data base to this and a lot of stuff the average person is just

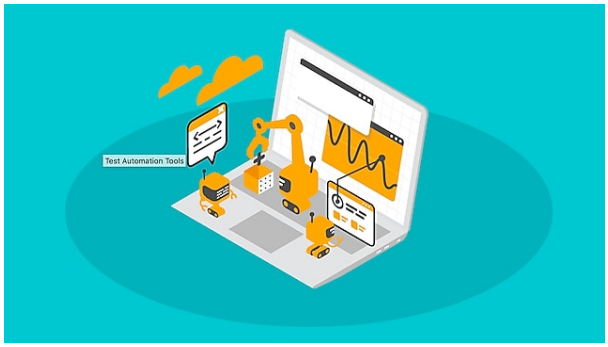
It went on to say "We know you're concerned about security and that is the reason for this letter. We don't want you to communicate any of this information over anything but mail, because that is the only secure way to do this. We need your personal details on the following things so we can transfer them into the system and verify them for accuracy because we've been having trouble with databases in this transition."

We told recipients: "Please do not email or fax this information. Use ONLY the self-addressed, stamped envelope," which we addressed to an address that was not the company's address. We told them we had done that because we did not want anyone at work intercepting this in the office. We also told them we had set up a special, secure P.O. box that only the security department had access to.

After it was sent out, we received about a 28 percent response. A very simple social-engineering test and more than a quarter of the people targeted fell for it.

Also read Social engineering attacks: Highlights from 2010 [CSO Insider registration required]

We've done this in other places with phishing emails. In one place, we sent an incredibly enticing email offering free stuff. We did that AFTER extensive training and certification of the entire organization, which was in excess of 95 percent passing the awareness assessments. But the response to the phishing email, even after the training, was forty percent.



No matter how many tests, assessments, and other measures, you put into place, it's not going to work against human nature. We can help it with training, and measure an incremental increase in awareness, but you will never achieve 100 percent success.

Takeaway: Part of awareness training needs to include specific instructions not to give out personal information to any person or department.

"Let them know: Our department will never ask you for these kinds of details," said Schwartau. "The proper procedure when launching a new system is to issue new credentials. You never ask for existing credentials."

Social engineering story 2:

Get burned after reading

Schwartau:I got this email recently from what looked like Bank of America. I bank with Bank of America and I do about 98 percent of my banking online.

The email was from SiteKey, their site verification system, which is actually a pretty good system. It said "Hey, this from SiteKey and this is really urgent because you just transferred some money and we need to verify that."

Now, I knew it was a scam because I'm a professional paranoid. But I'm looking through the email, the addresses, and they are all correct! The logos, the site key information; all correct. All I could think was "How they heck are they pulling this off?"

Also see Mind Games: How Social Engineers Win Your Confidence

Finally, after quite a while, I realized it: The reason I could not figure it out is because I was on my laptop with a 13-inch screen with low resolution. Underneath the links, the addresses, it said 'Bank of Americil.com.' Small i, small l. I knew better from the get go. But how many people are going to fall for something like that?

Takeaway: Like the security department at work, a legitimate financial institution will never ask you for credentials through email. They will have you call the number on back of your card, or visit the homepage you always go to. Never, ever trust anyone who comes to you asking for credentials, said Schwartau. That is not how it's done.

In our next installment, Social engineering stories: The sequel, we hear from John Sileo, a security expert who is passionate about privacy after having his identity stolen - twice.

Next read this

- *The 10 most powerful cybersecurity companies*
- *12 cheap or free cybersecurity training resources*
- *5 risk management mistakes CISOs still make*
- *6 security metrics that matter – and 4 that don't*
- *8 video chat apps compared: Which is best for security?*
- *How to rob a bank: A social engineering walkthrough*
- *10 ways to get more from your security budget*
- *Cybercrime in a recession: 10 things every CISO needs to know*
- *The CISO's guide to securely handling layoffs*

Joan Goodchild is a content director with IDG's marketing services division. She is the former editor

The 10 most powerful cybersecurity companies

You May Also Like

What is pretexting? Definition, examples and prevention

Managing vendor and supply chain risk in a recession

Senate subcommittee blasts FCC and Team Telecom approach to Chinese supply

Want better mobile security or privacy? Try these Android and iOS alternatives

Brute-force attacks explained, and why they are on the rise

New DOE document names China, Russia as threats to US bulk power system