THE WALL STREET JOURNAL.
WSJ.com

BUSINESS | OCTOBER 31, 2011

Hackers Press the 'Schmooze' Button

By SUZANNE KAPNER

Chris Patten called a large investment-management firm to report that he was going through a divorce and was worried that his wife had set up an account under a false name.

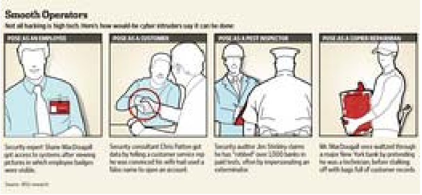
And with that story—entirely plausible but in this case a lie—a customer-service representative turned over customer account numbers and other details with a readiness that makes banks and other companies cringe.

Read More

Read the Social-Engineer.com report on identity-theft risks

Mr. Patten, a 35-year-old cybersecurity expert who was with the U.S. Air Force before he started working for a consulting firm in Kansas City, Mo., didn't actually use or sell the data, which he gathered in running a test for the investment firm of its security arrangements. But the ease with which the employee was persuaded to divulge the information points to a troubling trend, security experts and law enforcement officials say.

As banks and other large companies spend large amounts of money on building firewalls and using complex technology to fortify their systems, it is often their own employees who are letting identity thieves in the door.


Smooth Operators
Not all hacking is high tech. Here's how would-be cyber intruders say it can be done:
POSE AS AN EMPLOYEE
POSE AS A CUSTOMER
POSE AS A PEST INSPECTOR
POSE AS A COPIER REPAIRMAN
Security expert Shane MacDougall got access to systems after viewing pictures on which employee badges were visible.
Security consultant Chris Patten got data by telling a customer service rep he was convinced his wife had used a false name to open an account.
Security author Jim Stickley claims he has "robbed" over 1,000 banks in paid tests, often by impersonating an exterminator.
Mr. MacDougall once waltzed through a major New York bank by pretending he was a technician, before walking off with bags full of customer records.
Source: WSJ research

The largest banks are expected to spend tens of billions of dollars on cybersecurity this year, an increase of as much as 15% over 2010, as they rush to comply with new rules that require them to strengthen customer-authentication procedures and beef up other fraud detection measures, said Avivah Litan, an analyst with Gartner Research. But the success of low-tech approaches such as Mr. Patten's shows that increased spending alone won't be enough to insulate the banks, which are chock full of valuable data.

"It's getting harder for hackers to penetrate firewalls and other technological barriers, so they are reverting to lower-tech methods of attack," said David Kennedy, the head of security for Diebold Inc., the maker of automated teller machines. Mr. Kennedy said the type of attack Mr. Patten simulated, known in security circles as pretexting or social engineering, is one of the biggest threats his company facestoday.

The banks areaware of this threat and are countering with tougher customer-identification standards, among other things. Instead of simply providing a customer-service representative with a home address to retrieve a lost user name or password, Bank of America Corp. customers must now also know the cross street. They might also be asked to recall other identifying detailssuch as the last three transactions on the account.

But there is a limit to how many security measures companies can impose before they start to irritate consumers. "We don't want to put too much onus on the customer," said Robert Shiflet, a Bank of America fraud-prevention executive.

A 1999 law made it a crime to use false pretenses to obtain customer information from financial institutions, and the Federal Trade Commission Act also prohibits the use of deceptive practices.As social-networking sites such as Facebook and LinkedIn have become more popular, hackers are finding it easier than ever to cherry-pick personal information from cyberspace.

"The more information there is about you out there, the more information there is for someone to steal," said Charles Pavelites, a special agent with the FBI.

Spending more money doesn't necessarily make a company more secure. Target Corp. was one of the hardest to penetrate in a recently held contest in which large companies were hacked without their knowledge to educate them about the risks of social engineering. But Target spends about half as much each year on security as does Oracle Corp., which contestants found to be the least secure, according to a report from Social-Engineer.org, the event's organizer. "It's shocking how much confidential information companies post on the Internet," said Chris Hadnagy, Social-Engineer.org's founder.

Target says it takes information protection seriously and continues to invest in security technology. Oracle declined to comment.

Often, the first line of defense for large corporations is the customer-service representatives who man their phones. But hackers say they often find these employees easy prey, because of their high turnover, low pay and desire to be helpful. "If you sound confident enough, they will usually give you whatever you want," said one member of the hacking group Anonymous, who declined to provide his name.

All it took was a few hours of surfing the web for Shane MacDougall, the winner of the hacking contest, called the Schmooze Strikes Back, to turn up enough information to poke through Oracle's defenses.

On Oracle's web site, Mr. MacDougall found a video of the Redwood Shores, Calif.-based company's security facilities. A little more surfing turned up photos of a company party in which employee identification badges were clearly visible.

Armed with this information, Mr. MacDougall posed as an Oracle employee who was gathering information for a government contract. He called a satellite office and within 25 minutes persuaded an unwitting employee to divulge details about Oracle's operating and anti-virus systems. That information could have enabled him to steal sensitive customer data had he been an actual hacker.

"What is the point of creating all these security measures if I can just schmooze my way inside?" Mr. MacDougall said.