When a Stranger Calls, Beware of The Pretext

By Frank Ahrens
Washington Post Staff Writer
Saturday, September 9, 2006; D01

You get a phone call from someone who says they're taking a survey for a reputable sounding research firm. They ask you a few questions that seem relatively harmless -- what's private anymore, anyway, right? -- such as the name of your phone company or investment firm or even the name of your pet.

You may have just been pretexted.

A pretext is a false motive put forth to hide a real one. "Pretexting," pretending you are someone else to obtain information, is at the center of an unspooling boardroom scandal at the Silicon Valley computer company Hewlett-Packard. The company has admitted that it hired a private investigator who obtained the phone records of HP board members by using a contractor who posed as the board member. The contractor also used pretexting methods to obtain the phone records of nine reporters who cover the company.

Pretexting as a buzzword appears to have entered the argot of scammers as early as 1992, when it popped up in a Computerworld magazine article. Back then, pretexters were gaining individuals' data from the Social Security Administration by pretending to call from Social Security offices where the computers had shut down. Today, pretexters prey on customer call centers at phone companies, banks and other treasure troves of personal data, working to improperly obtain the keys that can unlock all sorts of valuable information.

Once pretexters get the personal information, they sell it to "data brokers," who in turn may sell it to private investigators working a divorce case, say, or shadier characters hoping to steal identities. Often, all they need is the password to an online bank or investment account -- frequently, the name of a customer's pet.

The grift of pretending you're someone you're not to obtain something that doesn't belong to you is an ageless one, as old as crime, but today, the stakes are higher and the tools more sophisticated.

A security specialist said it has been a "tradition for decades" for chief executives of big companies to hire private investigators to spy on colleagues, calling it a "common power play."

"It's also the tip of the proverbial iceberg of CEOs at Fortune 500 companies . . . to engage fly-by-night organizations to obtain things they cannot obtain," said James M. Atkinson, president of the Granite Island Group, a Massachusetts security company. "It's just that it hasn't come out as ugly as HP."

Pretexting is joining "spamming," "phishing," "phreaking" and other digital ruses used to obtain your data. Pretexters now use electronic devices that show false phone numbers on caller ID systems, a practice known as "spoofing."
Pretexters pay companies to make calls for them in order to disguise the origin of the calls, security consultant Robert Douglas said.

In 1999, Congress passed the Gramm-Leach-Bliley Act, outlawing the use of pretexting to obtain financial data from customers or institutions. The Federal Trade Commission has investigated businesses that advertise pretexting services.

But the law's boundaries are fuzzy. Even though its language is limited to financial data, lawyers have disagreed on whether it could be used to prosecute pretexters who have obtained non-financial data. Also, some private investigators maintain that no laws have been broken if the pretexted data is not used illegally. In the HP case, the California attorney general said on Wednesday he was unsure if laws had been broken. By Thursday, he said he was certain they had.

What is not in dispute is how easy it is to obtain closely held personal data.

Earlier this year, a blogger paid $89.95 to obtain the records of about 100 cellphone calls made by Ret. Gen. Wesley K. Clark.

Although sites such as Locatecell.com and dozens of others for years advertised phone records for sale, the Clark incident raised the specter of not only major privacy breaches but also potential national security concerns.

The Clark stunt led to a series of hearings on Capitol Hill over the summer, and resulted in House passage of legislation that imposed criminal penalties for accessing consumer phone records through pretexting. Some state legislatures are considering stiffening their own measures to prevent and punish pretexting by companies.

But security experts worry that lawmakers are focusing too narrowly.

"This is a much broader arena than just cellphones," Douglas said. "They steal your cable TV records, satellite TV records, gas records, power records and all the rest. Anything that will give them personal information about you that will add to the puzzle they're putting together, they will seek out. Often they will use one consumer company against another."

Police can use a form of pretexting during interrogations -- misleading a suspect into believing officers have evidence against him on one charge to get him to confess to another. And pretexting to get someone's phone records without their knowledge, such as in the HP case, has been a reliable tool for some private investigators.

"Going after someone's phone records -- that's black-letter stuff," said James H. Rowe, a former investigator on the Senate Watergate committee and executive vice president of the James Mintz Group Inc., an investigation firm. "That's not even in the world of being gray."

Staff writers Ellen Nakashima and Yuki Noguchi contributed to this report.

© 2006 The Washington Post Company
Search Over 1 Billion Records! Online Reports in 40 Categories.
www.Investigate123.com

Setec Investigations
Computer Forensic Investigations Expert Witness & Litigation Support
www.SetecInvestigations.com

Private Investigators
The biggest source of free info on Private Investigators
free-public-records.big.com