



# AT&T deceptive on data theft

By Ted Samson

September 1, 2006

AT&T may have been up front about the theft of customers' data, but it was less forthcoming about its fate, seemingly putting its own best interests ahead of customers'.

News sources widely covered the report this week that [an AT&T Web site had been hacked over the weekend](#) and the perpetrators had made off with the personal data of 19,000 users. The company stressed that the breach was noticed quickly, the site was shut down, the authorities were notified. It all seemed well in hand.

Turns out that the day AT&T let the media know about the theft -- last Tuesday -- it circulated an internal memo announcing that the data had already been put to use in an intricate phishing scam, [according to reports](#). (Dave Lazarus at SFGate.com reports getting his hands on AT&T's internal memo.)

The hackers made good use of their data bounty. Sending out messages supposedly from "SBCdslstore.com," the phishermen informed recipients: "we recently tried to charge your credit card for your SBCdslstore.com order and it was rejected by the bank because it has no complete information."

"Each message included a legitimate order number culled from the AT&T vendor's database to create an illusion of authenticity. Messages also included the recipient's home address and the last four digits of his or her credit card number," Lazarus said.

AT&T claims it sent personal e-mails to those customers whose data had been swiped, alerting them to the risk. Real nice, guys. Sending such an important message to your customers via e-mail, which could easily be confused as spam or, hey, a phishing attempt, is simply irresponsible.

Rather, I think the company should have been forthcoming and let the media do its job in helping alert customers to what was happening to their data. Yes, it would have taken some lumps in the process, but now, I'd say it's in for a few more.

Also irksome: **The hack of AT&T's Web site is [yet another string of data thefts](#) where a third party vendor dropped the security ball. (Others of recent note include the Dept. of Veteran Affairs and Chevron.) In this case, the breach occurred "not within AT&T's own system but at 'an AT&T vendor that operates an order processing computer' for the online DSL store," Lazarus writes.**

**The names of the vendor was not disclosed.**

So vendors, in addition to being clear and honest with your customers about what's happened to their data, you need to hold your partners accountable when they make this kind of goof. This isn't the same as a partner delivering a late shipment due to a clerical error. We're talking about the credit history and privacy of real, live people. Your customers. The ones who keep your organization in business.

And never forget: Whether you're the CEO or the head of the mailroom, you could be next.

---

## **Phishing expedition at heart of AT&T hacking**

- [David Lazarus](#)

Friday, September 1, 2006

When AT&T said in a press release this week that "unauthorized persons illegally hacked into a computer system and accessed personal data" from thousands of DSL customers, it wasn't telling the whole story.

Internal company documents show that the security breach was only the first step in a more elaborate scam that involved bogus e-mail being sent to AT&T customers that attempted to trick them into revealing additional info that could be used for widespread fraud or identity theft.

"We haven't seen anything like this before," acknowledged Walt Sharp, an AT&T spokesman.

The company says that individual customers were notified by e-mail -- real ones this time -- about the full scope of the scam. But myriad news accounts written off AT&T's press release failed to show how extensively the company's customers may have been duped.

The company said for public consumption that hackers had "accessed personal data, including credit card information, from several thousand customers who purchased DSL equipment through the company's online Web store."

It said the electronic break-in occurred last weekend and that AT&T technicians discovered the security breach "within hours." The company said its online DSL store was immediately shut down.

It also said AT&T quickly notified major credit card companies and is "working with law enforcement to investigate the incident and pursue the perpetrators."

What AT&T didn't say in its press release is that the stolen info for an unknown portion of about 19,000 customers was immediately put to use as part of an unusually deceptive phishing scam.

Phishing is an online con job in which a message is purportedly sent from a legitimate company -- PayPal, eBay and banks are common ruses. The message typically requests that the recipient click on a link and provide sensitive info as part of routine account maintenance or to process a transaction.

In reality, the message is a hoax, intended to fool unwary Internet users into handing over credit card numbers, Social Security numbers and other keys to the identity-theft kingdom.

An urgent memo was sent to AT&T insiders Tuesday around the same time the company's press release was issued. It's a good deal more forthcoming about the incident.

**The memo (a copy of which has made its way to my hands) says the security breach occurred Saturday not within AT&T's own system but at "an AT&T vendor that operates an order processing computer" for the online DSL store.**

"The information that was provided by customers who ordered DSL-related equipment included name, address, e-mail address, phone number, credit card number and credit card expiration," the memo says, adding that the hacked data didn't include Social Security numbers or birth dates.

But the hackers had a scheme to get this extra info. After accessing the customer data, they incorporated it into phishing messages that were promptly sent to AT&T's DSL customers.

The messages, ostensibly from "SBCdslstore.com," told recipients that "we recently tried to charge your credit card for your SBCdslstore.com order and it was rejected by the bank because it has no complete information."

Each message included a legitimate order number culled from the AT&T vendor's database to create an illusion of authenticity. Messages also included the recipient's home address and the last four digits of his or her credit card number.

"To update the credit card information details for your order, please select this link," the message instructed, directing people to a "spoof site" with an illegitimate sbcdslstore.org (not .com) Web address.

Once at the official-looking spoof site, message recipients were instructed to provide confidential data that the hackers hadn't found in the AT&T vendor's database, including Social Security numbers and birth dates.

"I did a double take on it," said Russ Irwin, a Silicon Valley venture capitalist who recently purchased a wall adapter from AT&T's online store and was one of the thousands of people who were subsequently phished.

"I saw my order number and my credit card number, and I thought at first it must be real," he said. "Then I saw the dot-org address and I knew better."

Irwin, who invests in technology companies for a living, said he's seen his share of phishing e-mail over the years.

"Somebody did a pretty good job with this one," he said. "Having all that information gave it a lot of credibility."

AT&T's press release this week made no mention of the phishing aspect of the scam. But the company's internal memo warns employees to be on the lookout for phony e-mail.

"Impacted customers may receive an e-mail that appears to be from AT&T but is actually from the unauthorized person requesting additional personal information such as Social Security number, driver's license number, date of birth or other credit card information," it says.

AT&T's Sharp said individual customers were warned of the phishing threat in e-mail this week from AT&T.

"We don't know how many people received the phishing e-mails," he said. "We indicated (to customers) that there was an apparent phishing expedition going on that was linked to this incident and was not from AT&T."

**Sharp said the company's press release omitted this aspect of the situation because "the focus was to let people know they need to get ahold of their credit card companies and that we're prepared to offer free credit monitoring."**

**He declined to comment on whether the security breach originated domestically or overseas** (many such hack attacks have been traced to Eastern Europe). He also declined to comment on which law enforcement agencies are involved.

Sharp said there are no leads in the case at this time.

*David Lazarus' column appears Wednesdays, Fridays and Sundays. Send tips or feedback to [dlazarus@sfchronicle.com](mailto:dlazarus@sfchronicle.com).*