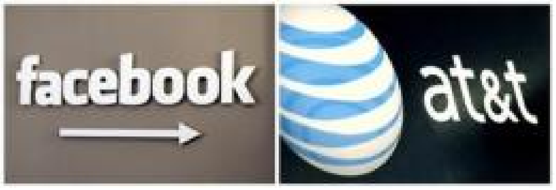
Network flaw causes scary Web error

January 15 2010, By JORDAN ROBERTSON , AP Technology Writer



In this combo made from file photos, the Facebook, left, and AT&T logos are shown. (AP Photo)

(AP) -- A Georgia mother and her two daughters logged onto Facebook from mobile phones last weekend and wound up in a startling place: strangers' accounts with full access to troves of private information.

The glitch - the result of a routing problem at the family's wireless carrier, AT&T - revealed a little known security flaw with far reaching implications for everyone on the Internet, not just Facebook users.

In each case, the Internet lost track of who was who, putting the women into the wrong accounts. It doesn't appear the users could have done anything to stop it. The problem adds a dimension to researchers' warnings that there are many ways online information - from mundane data to dark secrets - can go awry.

Several security experts said they had not heard of a case like this, in which the wrong person was shown a Web page whose user name and password had been entered by someone else. It's not clear whether such episodes are rare or simply not reported. But experts said such flaws could occur on e-mail services, for instance, and that something similar could happen on a PC, not just a phone.

"The fact that it did happen is proof that it could potentially happen again and with something a lot more important than Facebook," said Nathan Hamiel, founder of the Hexagon Security Group, a research organization.

Candace Sawyer, 26, says she immediately suspected something was wrong when she tried to visit her Facebook page Saturday morning.

After typing Facebook.com into her Nokia smart phone, she was taken into the site without being asked for her user name or password. She was in an account that didn't look like hers. She had fewer friend requests than she remembered. Then she found a picture of the page's owner.

"He's white - I'm not," she said with a laugh.

Sawyer logged off and asked her sister, Mari, 31, her partner in a dessert catering company, and their mother, Fran, 57, to see whether they had the same problem on their phones.

Mari landed inside another woman's page.

Fran's phone - which had never been used to access Facebook before - took her inside yet another stranger's page, one belonging to a young woman from Indiana. They sent an e-mail to one of their own accounts to prove it.

They were dumbfounded.

"I thought it was the phone - `Maybe this phone is just weird and does magical, horrible things and I have to get rid of it,'" said Candace Sawyer.

The women, who live together in East Point, Ga., outside Atlanta, had recently upgraded to the same model of phone and all used the same carrier, AT&T.

Sawyer contacted The Associated Press after reporting the problem to Facebook and AT&T.

The problem wasn't in the phones. It was a flaw in the infrastructure connecting the phones to the Internet.

That illuminates a grave problem.

Generally Web sites and computers are compromised from within. A hacker can get a Web page or computers to run programming code that they shouldn't. But in this case, it was a security gap between the phone and the Web site that exposed strangers' Facebook pages to the Sawyers. Misconfigured equipment, poorly written network software or other technical errors could have caused AT&T to fumble the information flowing from the Sawyers' phones to Facebook and back.

Fortunately, Hamiel said, the vulnerability would be of limited use to a hacker interested in pulling off widespread mayhem, because this hole would let him access only one account at a time. To do more damage the criminal would have to pull off the unlikely feat of gaining full control of the piece of equipment that routes Internet traffic to individual users.

AT&T spokesman Michael Coe said its wireless customers have landed in the wrong Facebook pages in "a limited number of instances" and that a network problem behind those episodes is being fixed.

The Sawyers experienced a different glitch. Coe said an investigation points to a "misdirected cookie." A cookie is a file some Web sites place on computers to store identifying information - including the user name that Facebook members would enter to access their pages. Coe said technicians couldn't figure out how the cookie had been routed to the wrong phone, leading it into the wrong Facebook account.

He also said AT&T could confirm only that the problem occurred on one of the Sawyers' phones, possibly because they had logged off Facebook on the other two before reporting the incident.

Facebook declined to comment and referred questions to AT&T.

Some Web sites would be immune from this kind of mix-up, particularly those that use encryption. A Web browser would have trouble deciphering the encryption on a page that a computer user didn't actually seek, said Chris Wysopal, co-founder of Veracode Inc., a security company.

Sensitive sites and those used for banking and e-commerce generally use encryption. But most other sites, including some Web-based e-mail services, don't use it. One way of checking: The Web addresses of encrypted sites begin with "https" rather than "http." Facebook uses encryption when user names and passwords are entered, to cloak the sign-on from snoops, but after the credentials are entered the encryption is dropped.

It's unclear how many people were affected by the problem the Sawyers discovered, and whether it was limited to Facebook.

The reason all three women experienced the glitch is a function of the way cellular networks are designed. In some cases, all the mobile Internet traffic for a particular area is routed through the same piece of networking equipment. If that piece of equipment is misbehaving or set up incorrectly, strange things happen when computers down the line receive the data.

Usually that means a Web site simply won't load, said Alberto Solino, director of security consulting services for Core Security Technologies. In the Sawyers' case, "somehow they got the wrong user but they could keep using that account for a long period of time. That's what's strange," he said.

The AP tried to contact two of the people whose Facebook pages were exposed to the Sawyers, but the calls and e-mails were not returned. It's unclear whether they are also AT&T customers, though security experts said that's likely the case.

Indeed, it was the case in a similar incident in November.

Stephen Simburg, 25, who works in marketing, was home for Thanksgiving in Vancouver, Wash., when he logged onto Facebook from his cell phone. He didn't recognize the people who had written him messages.

"I thought I had gotten really popular all of a sudden, or something was wrong," he said. Then he saw the picture of the account owner: A young woman.

He got her e-mail address from the site, logged off and wrote the woman a message. He asked whether he had met her at some point and she had borrowed his phone to check her Facebook account.

"No," she wrote back, "but I was just telling my family that I ended up in your profile!"

Simburg and the woman figured out they were both using AT&T to access Facebook on their phones. (AT&T had no comment because the incident wasn't reported to the company.)

"I felt like I had been let down by the phone company and by Facebook," he said.

He says he has put the incident behind him. But one piece of it remains: He and the young woman are now Facebook friends.

Citation: Network flaw causes scary Web error (2010, January 15) retrieved 26 April 2024 from https://phys.org/news/2010-01-network-flaw-scary-web-error.html