



Tuesday, May. 05, 2009

The Downside of Friends: Facebook's Hacking Problem

By Claire Suddath

You get a quick message from a friend on Facebook, click on the link and absentmindedly log in to a website pretending to be Facebook. This is what happened last week, when scammers unleashed a new attack on Facebook, collecting users' log-in information and passwords and pilfering victims' "friends" lists to target the next dopes. Listen up, people: Although Facebook has a reputation for Internet security — it identified the scam within hours, and the ripple effects only lasted for a couple days — at 200 million members and counting, the size and popularity of the social-networking site has made it the object of increasing attention from hackers and spammers. And if last week is any indication, it's only going to get worse.

"In the '90s, scammers used e-mail," says Michael Argast, a security analyst at Sophos, an antivirus software company. "Today, it's social networking." Argast explains that although people have been trained not to click on suspicious e-mails, they don't operate with the same sense of caution when presented with a link on Facebook or Twitter. Maybe that's why the number of phishing attacks on these kinds of sites — in which people are fishing for account information, as opposed to infecting your computer with a virus — has skyrocketed recently, from 4,600 attacks in 2007 to 11,000 in 2008. This year doesn't look any better, with 6,400 attacks in the first three months of 2009. ([Read "How Not to Be Hated on Facebook: 10 More Rules."](#))

Like anything on the Internet, Facebook has never been completely scam-free, but its privacy settings may create a false sense of security: most users can't interact with one another unless they are "friends" or belong to the same general network. The site at first glance would also seem less of a gold mine for swindlers since unlike financial websites, which offer access to victims' bank accounts, there is no direct financial gain from hacking into a Facebook account. But the bad guys know that many of us are lazy or forgetful and

use the same password on multiple sites. In early 2008, Facebook noticed a marked increase in the number of scams. "We're the most effective distribution platform on the Internet," says Ryan McGeehan, the company's incidence-response manager. "The level of person-to-person connection doesn't exist anywhere else. And as we get bigger, we become a bigger target."

Facebook monitors users' activity, and when someone goes from a few wall posts a week to hundreds of messages within a few minutes, the security team can logically assume that the account has been hacked. They'll notify the user, reset the password, and the whole issue is usually resolved within a few hours. But when thousands of users are hacked at once — and then their friends are hacked, and their friends' friends are hacked — it can take a few days for Facebook to fix the problem. That's what happened on April 29 and 30, when users found themselves accidentally logging in to a website called FBAction.net. Designed to look exactly like Facebook, the evil doppelgänger took their info and hacked their accounts.

When MarkMonitor, an outside security company employed by Facebook, shut down the fake website, the scam popped up again on a different site, FBStarter.com. (It too has since been disabled.) "My guess is this was a pretty organized group of people," says Fred Felman, MarkMonitor's chief marketing officer. Felman says the phishers, whoever they were (Internet scammers almost never get caught), were not using the most up-to-date technology, but their creativity and speed makes him think that they have experience and will probably do it again.

A similar phishing scam established a toehold on the website in January. And last year hackers broke into accounts by convincing people to click on links posted on their profile walls. Another common Facebook scam is to hack someone's account and then send messages to friends asking for money (like the old Nigerian businessman scam, but with a hey-it's-your-old-pal twist).

Facebook won't say how many accounts were compromised last week, but a rep notes that the site has never had a scammer hack more than a small fraction of its accounts, adding that the company's security team — which has more than 100 analysts, engineers and programmers — can handle whatever comes their way. "We're going to be attacked again in the future," says McGeehan, "and my role is to be prepared when it happens."

[Become a fan of TIME on Facebook.](#)

[See the 10 best social-networking applications.](#)

Copyright © 2009 Time Inc. All rights reserved. Reproduction in whole or in part without permission is prohibited.
[Privacy Policy](#)|[Add TIME Headlines to your Site](#)|[Contact Us](#)|[Customer Service](#)