

Facebook users' app use contradicts their stated security concerns, study finds

July 22 2011

Although most Facebook users claim to be very uncomfortable with how third-party apps use their personal information, their actual behavior doesn't reflect this concern, a new study by School of Information researchers has discovered.

As Facebook and other social networking websites grow in popularity and become an archive of [personal information](#), they are ripe targets for marketers or hackers. Managing privacy online is increasingly important — and increasingly complicated.

Facebook presents a particular challenge, since many of its apps are provided by outside developers, including games like Mafia Wars and FarmVille. Users install 20 million Facebook apps every day, making their privacy vulnerable not just to Facebook's privacy practices, but also to the privacy practices of numerous additional companies. In 2010, [The Wall Street Journal](#) revealed that several of the most popular apps had shared users' personal information with advertisers, in violation of Facebook's privacy policies.

More than ninety percent of the study's respondents said they were uncomfortable with how Facebook apps access and use their personal information, once researchers explained it to them. Users' actual behavior didn't reflect their privacy concerns, though — perhaps because the way third-party apps interact with Facebook and what information the apps have access to can be complicated or confusing.

The study was conducted by I School doctoral student Jen King, visiting researcher Airi Lampinen, and 2011 MIMS graduate Alex Smolen. King will be presenting the research findings at next week's Symposium On Usable Privacy and Security in Pittsburgh, Pennsylvania.

Researchers initially suspected that “expert users” — the minority who actually understood Facebook's data-sharing practices — would be better at managing the online privacy of third-party apps. But the researchers were surprised to find that this wasn't true; the more knowledgeable users made the same mistakes as everyone else.

Although [Facebook](#) offers a complicated grid of privacy settings for its own data use, there are no similar controls for third-party apps; users' only option is not to use the app. “In our study, nobody appeared to have a consistent strategy for managing application privacy — not even the most knowledgeable users,” said study author Jen King.

One group stood out as both more knowledgeable and more concerned about online privacy: people who had been personally hurt. This group included people whose information had been inadvertently disclosed to someone they didn't want to see it — like a boss or a parent — or those who had had private or embarrassing information or photos posted online and wanted remove them.

The findings have important implications for privacy policymakers and designers. “It's tempting to think that if we just make more of an effort to explain how data-sharing works and what the risks are, that people will make smarter decisions,” said King. “This data suggests that education may not be enough. We may need to incorporate the lessons people learn when they've been burned.”

On-screen warning messages or [privacy](#) policies don't seem to make a difference, either, since users who had read them “neither knew more,

acted differently, nor felt more concerned about apps than [users](#) who had not reported reading these statements,” according to the study.

Provided by University of California - Berkeley

Citation: Facebook users' app use contradicts their stated security concerns, study finds (2011, July 22) retrieved 20 April 2024 from <https://phys.org/news/2011-07-facebook-users-app-contradicts-stated.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.