



Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

[See a sample reprint in PDF format.](#)

[Order a reprint of this article now](#)

THE WALL STREET JOURNAL.

WSJ.com

TECHNOLOGY | JANUARY 29, 2009

Beware of Facebook 'Friends' Who May Trash Your Laptop

By JOSEPH DE AVILA

The message that popped into Laurie Gale's Facebook inbox last month seemed harmless enough -- a friend had seen a video of Ms. Gale and had sent a link so Ms. Gale could view it. The link led to a video site that prompted her to update her video software, which she did.

"Within seconds, everything started shutting itself down," says Ms. Gale, a 37-year-old lamp-works artist from Versailles, Ky. Ms. Gale's new Dell Inspiron laptop had been infected with malicious software, or malware, that has spread through social networking sites like Facebook and MySpace.

"I cried for an hour," Ms. Gale says. It took a trip to the local computer repair shop and several phone calls with Dell customer-service representatives for her to restore the computer to its factory settings. "It was three days of torture."

The popularity of social networks and social media sites has grabbed the attention of cyber crooks searching to pilfer passwords, called "phishing," and steal sensitive personal information. The hackers are exploiting users' sense of safety within these sites, says Pat Clawson, chief executive of Lumension Security, a computer security company.

Earlier this month, Twitter, a social site in which users communicate in short bursts of text, was hit in a campaign to steal users' account passwords. On business-networking site LinkedIn, criminals set up fake celebrity profiles that, when visited, downloaded malware onto users' machines.

Malware attacks in social networks are just as dangerous as ones conducted via email, security experts say. Hackers can mine infected computers for sensitive data like log-ins and passwords to financial sites. Infected computers can also be used to send out spam emails by the thousands.

Since the messages appear to come from friends, users often think they are safe, says Jose Nazario, a security researcher at Arbor Networks, a network-security company in Chelmsford, Mass. "I think the No. 1 thing that people have to remember is that it's not as gated of a community as you think it is," he says.

The malware that has made its way through social networks differs from the so-called "Conficker" worm that has spread to millions of personal and business computers in recent weeks, according to security experts. On social networks, malware writers typically trick users into infecting their own computers. The Conficker worm spreads through a vulnerability in Microsoft Windows and infected USB drives.

The attacks via social networks vary in means and intent. Messages may lure users with requests to click on a link to look at a photo or a video. The link may take the user to a phishing site or a site with malware. Some of the spam may be harmless advertising, but users should never risk clicking on such links, security experts say.

Sonny Holmes, a new Facebook user, got a message from his daughter in December about a photo she saw of him. He clicked on the link, and it sent him to a site that asked for his email account, Social Security number and several

personal health questions. "I decided post haste that I wasn't going to answer any of those questions," says Mr. Holmes, a 59-year-old pastor from North Charleston, S.C.

Later, his Facebook account started spamming all of his contacts. His laptop slowed to a crawl. Mr. Holmes had his church's information-technology department look at the computer, which the tech person was able to repair. Now "I'm very suspicious of things people send me," Mr. Holmes says.

Fewer than 1% of Facebook's 150 million users have become infected with malware using the site, says Max Kelly, Facebook's director of security. The site started seeing an uptick in malware attacks last summer.

Facebook uses automated systems to watch for unusual activity like accounts spamming their contacts, Mr. Kelly says. Once a compromised account is detected, Facebook will have the account's passwords reset, and spam messages get deleted. Facebook says it will pursue legal action against parties targeting its users. Just last year, the company filed a civil suit and was awarded \$873 million in damages in a default judgment against Atlantis Blue Capital and its Canadian owner for sending Facebook users unsolicited advertisements. The company's owner couldn't be located for comment.

MySpace saw malware attacks last summer, though the company says it hasn't had any reports of it in recent months. Only a "negligible amount" of MySpace's users have been infected with malware, according to the company. (MySpace is owned by [News Corp.](#), which also publishes The Wall Street Journal.)

Twitter co-founder Biz Stone says programmers at the site improved the log-in security after a phishing campaign snared unsuspecting users. In it, users were sent messages saying something like, "Hey, check out this funny blog about you," along with a link. The link took users to a phony Twitter log-in page where users were prompted to enter their passwords.

Mr. Stone says Twitter has a team that investigates malware threats, phishing attacks and spam on the site. The company also has automated processes that monitor for and delete malicious messages and links, he adds.

LinkedIn Corp. took action when phony accounts of celebrities promised nude photos. The accounts led to sites that contained malware. LinkedIn officials say they removed the fake accounts, but declined to say whether any users' computers were infected.

"We take these matters very seriously and remove these kinds of inappropriate profiles," says Kay Luo, a spokeswoman for LinkedIn. "In addition, we are continually adding new technologies and security protocols to prevent this type of abuse."

Users should use the same caution with messages on social networks as they would with email, says Ryan Naraine, a security expert with Kaspersky Lab, a computer-security company. Users should be especially wary of any messages from friends that don't sound like their friends wrote them. If they don't normally write OMG in a message, it's probably not them, says Mr. Kelly, Facebook's director of security.

Write to Joseph De Avila at joseph.deavila@wsj.com

Corrections & Amplifications

On business-networking site LinkedIn, visitors who clicked links on fake celebrity-profile pages were taken to third-party sites where malicious software, called malware, was hosted. A previous version of this article incorrectly implied that the malware was downloaded when users clicked on the profile pages themselves.

Printed in The Wall Street Journal, page D1

Copyright 2008 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law.

For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit

www.djreprints.com