

SWITCHED

AOL ORIGINAL 5 Popular Facebook Scams (and How to Avoid Them)

by Terrence O'Brien on September 15, 2009 at 01:31 PM



Just as bearded hipsters migrate from bar to bar in pursuit of young ladies to ogle, so too have scammers and hackers followed their prey from MySpace to Facebook. As a result, the social network once deemed the "safe" option is now plagued by legions of 419 scammers, phishers, and peddlers of

malware.

Fortunately, there are a few simple rules Facebookers can follow to stay safe: Never click on suspicious links from friends; use a service like **LongURL** before following any shortened links; and assume that anyone begging for money is up to no good. And if you do happen to fall victim to a scam, quickly alert your friends (to prevent spreading the damage), then alert Facebook administrators and, if it's serious, law enforcement as well.

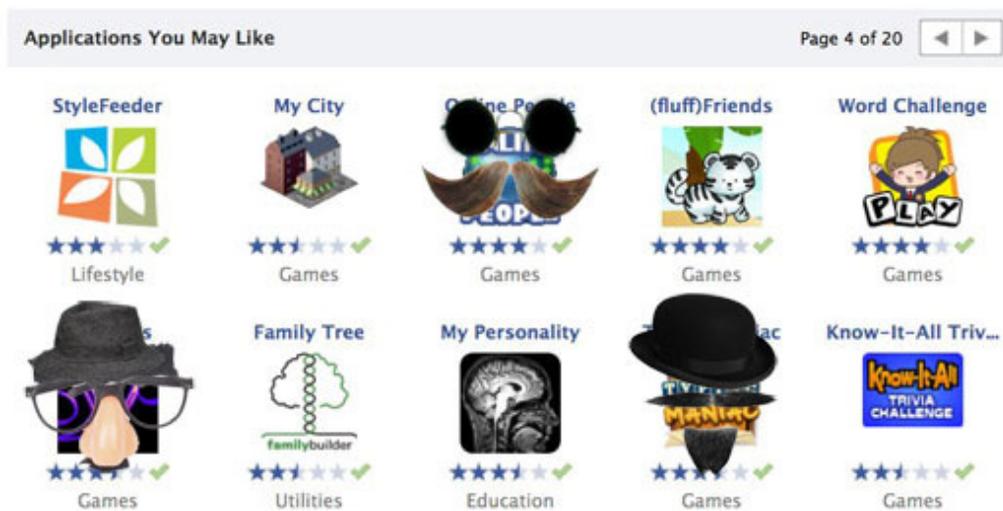
Since a reputable source once counseled that **knowing is half the battle**, here's a rundown of the Facebook scams most demanding of your awareness and good judgment:



1) The friendly 419 scam: The notorious 419 scams have sadly become ubiquitous on the Internet. While they began as e-mail cons, usually involving promises of a vast fortune from a Nigerian prince, they



have morphed into a new and more sophisticated ploy that involves hijacking the Facebook account of a friend in order to fool kind souls into thinking they're helping a pal. Thieves use an account to garner sympathy as they claim to be in desperate need of cash, often because they've been robbed or detained while traveling abroad. One duped Missouri woman wound up **handing over \$4,000** before she realized she'd been had.



2) Hidden fee apps:

There are plenty of Facebook apps and **quizzes** with questionable **motives** and **privacy policies**, but there are some that are outright scams. Take, for instance, the sad tale of **Leanne Saylor**, who fell prey to scammers after taking a simple IQ quiz on the service. To receive her

results, she was required to submit her cell phone number and wait for a text. When she didn't receive anything, Saylor entered her phone number two more times. When she opened her next cell phone bill, she discovered three charges from the app, totaling a whopping \$44. AT&T blocked future fees, but Saylor learned the hard way that she should never give out her cell phone number to strangers, much less strange apps.

3) Fake login pages:

A particularly sneaky method of ensnaring Facebookers lies in the **loads of phishing messages** that lead to convincing-but-fake versions of the Facebook login page. Typically, these spam e-mails are brief and contain a link, usually ending in ".im" or ".at." (We received one

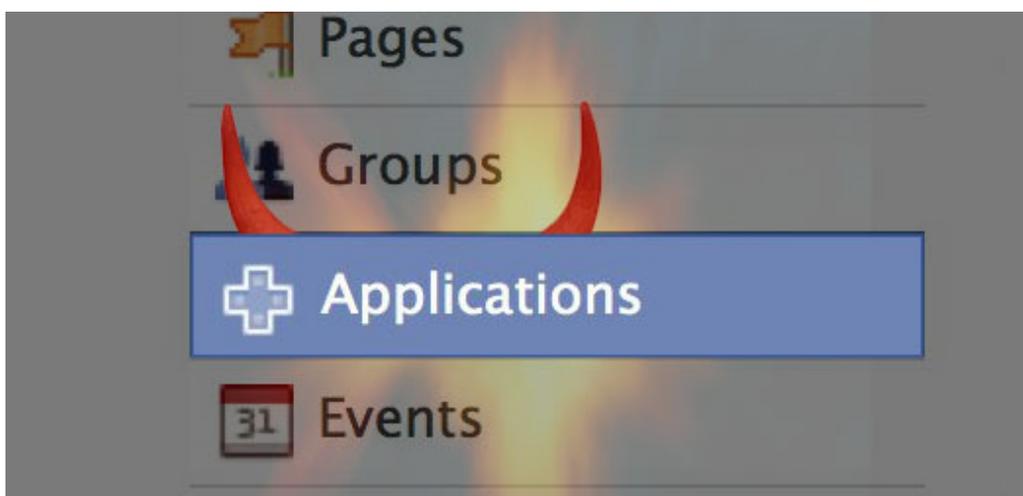
that simply read, "Look at goodmall.be.") Once you enter your e-mail and password to 'log in,' it's game over; a hacker has control of your account and will quickly use it to perpetrate any one of the scams listed here. What's worse, they'll impersonate you to spread phishing e-mails to all of your friends.

4) Malware links:





Once an account is hijacked, it can be used to deluge that account holder's friends with messages containing links to malicious sites. It's rough stuff. These poisonous software packages leave you vulnerable to the theft of even more data, including all the passwords, account numbers and credit card information you may have entered into your PC. Recently, a barrage of spam messages featuring a link to "**CoooooL Video**" actually led to nothing but a nasty malware infection.



5) Facebook apps that are malware:

Creating Facebook applications has become so easy that hackers have created apps with the sole aim of tricking you into handing over your personal data or Facebook password. Some versions **impersonate one of the standard Facebook** features, like

"Your Photos" and "Friend's Gifts," and send convincing notifications, like "someone has commented on your photo," or so-and-so "has posted on your wall." But clicking on them either leads to a fake login page, or a window asking for permission to access your Facebook account. These scams are particularly tough to spot because they mimic actual Facebook notifications. The only way to protect yourself is to look for tiny inconsistencies in the false apps (e.g., odd or incorrect icons, clunky wording and poor English usage). It seems your teacher wasn't lying after all when she said learning grammar was important.

Next >> '14 Facebook Ills (and How to Cure Most of Them)