



# P&RCIO NEWSLETTER

SERVING THE P&R COMMUNITY  
VOLUME 4, ISSUE 2



WINTER 2012

## Facebook-Based Security Threats on the Rise

### POINTS OF INTEREST:

- Facebook-Based Security Threats on the Rise
- To Share or Not to Share—That is the Question: Privacy and Information Sharing in Social Media

How much cybercrime happens on Facebook? About 4 million Facebook users experience spam on a daily basis, 20% of Facebook users have been exposed to malware, and Facebook sees about 600,000 cases of hijacked log-ins every day (Mashable). Security firm Commtech recently published its Internet Threats Trend Report that highlighted the world's largest social networking site, Facebook, and how it unintentionally proves to be a pivotal ally for malicious attacks of all sorts.

The report divides up Facebook attacks from the past year into three phases:

1. Social Engineering – The foundation of the attack begins with a post which encourages a user to take action. Attackers typically lure in victims using four different types of posts: information about free items; current news or events; something shocking or amazing that must be seen; or new Facebook applications under the guise of a game or a new functionality such as being able to view who has viewed a Facebook profile.

2. Spreading the Message – Facebook encourages users to build a network of friends who inherently trust each other. Attackers exploit this trust very easily to propagate malicious acts. Attackers typically lure victims into spreading a message by tricking users into sharing content under false pretenses, especially through use of Facebook's 'Like' button. The 'Like' button is a feature which allows users to indicate that they approve of content that's been posted by a friend, website, or other entity. Almost 48% of victims knowingly click on the 'Like' button on malicious content under the disguise of a legitimate page or feature as they believe they'll be rewarded for it. Attackers will often pro-

vide links to content that is legitimate, but many of the linked pages contain scripts that will generate a 'Like' on a victim's Facebook profile to encourage other friends of the victim to visit the site as well. Rogue, but legitimately added Facebook applications that have permission to post unlimited content on users' Facebook profiles and hijacking malware round out the other methods for attackers to spread their message. With the average Facebook user having about 130 friends, an average attack can easily spread to millions of users in just a matter of hours.

3. Ultimate Goal – Once all of the legwork has been completed for a successful attack, attackers will start seeing the benefits of their work. The majority of attacks convince users to submit their email address or personal information for a chance to win a prize from a well-known business. Attackers generate affiliate revenue by referring these potential new customers to a known business, but often times the end users are left with nothing. Other attacks result in spreading malware, hoaxes and other misinformation, or simply just making a point that they can wreak havoc on Facebook at the expense of others.

Social engineering provides the greatest opportunity for attacks on Facebook. Users should continue to take the same precautions they take with email and instant

### WHERE IS FACEBOOK BEING ATTACKED?



Image source Zone Alarm via Mashable.com



FREE Starbucks \$50 Gift Card - This Week Only



This offer will expire Tuesday, October 18, or when the remaining 2036 FREE Vouchers run out!

Step 1: You must click the share button: 0971

Step 2: Say Thanks below  
Example: "I love Starbucks!"  
(click "add a comment")

In October 2011, Facebook walls were bombarded with free Starbucks and Tim Horton gift card promotions. Users were tricked into a "like-jacking" cycle after accessing a nefarious link.



messaging, and check the validity of information that is presented—especially if it involves clicking a link or the ‘Like’ button on Facebook.

Facebook users are never totally safe from being scammed and preyed upon as profile information continues to be shared with third parties, malware remains prominent, and scammers are still allowed to create fake profiles. As it

## To Share or Not to Share — That is the Question: Privacy and Information Sharing in Social Media

Over the past year, Facebook and other social media sites, such as Twitter and Google, have made enhancements to their privacy features in response to growing attacks—from adversaries and regulators. As part of its settlement with the Federal Trade Commission (FTC) over privacy of information, the company has agreed to institute new internal controls.

The new controls, however, do not make these social media sites into secure digital locations for users’ private thoughts, photos, and information. As The Washington Post notes, the nature of the internet—let alone social media platforms that reside on it—is a way to distribute information:

“Facebook will never be ‘private’ - indeed, the very idea of making Facebook a more private place borders on the oxymoronic, a bit like expecting modesty at a [dance] club...[w]e expect more from the site vis-à-vis privacy than it can ever hope to deliver.”

The Post article also notes that user information is stored on dozens of servers across the planet and within friends’ browser caches (blocks of memory data), and is often sold to third parties including online advertisers and publishers. On the most basic level, social media does not correct for human error—for example, users cannot blame Facebook when they accept their ex-partners friend request who later proves no friend at all.

In reality, the only privacy control that works is the user themselves. As the Post emphasizes: “The only sure way

stands, there are settings users can change to protect themselves against cybercrime. Take precautionary measures to manage risk such as checking with family and friends on content they may have shared or changing your Facebook privacy settings. For more information, go to <https://www.facebook.com/about/privacy/>.

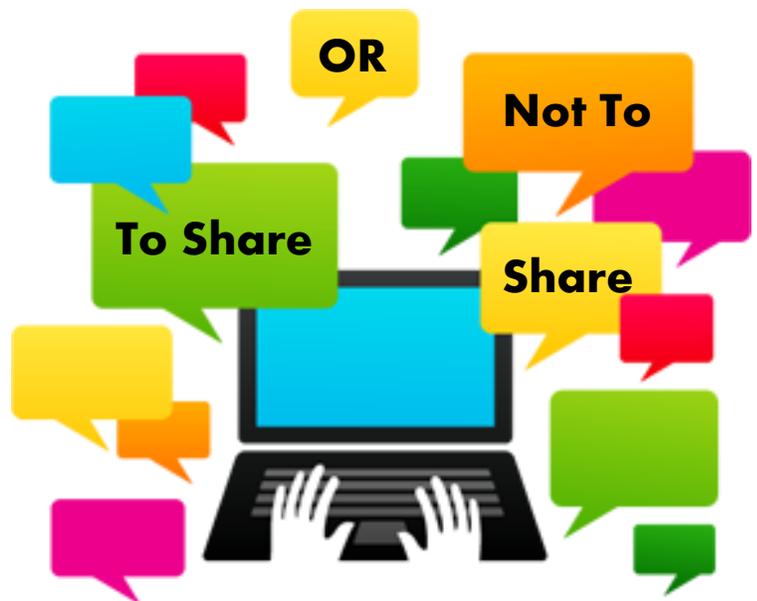
Sources:

“CommTouch Internet Threat Trend Report January 2012.” CommTouch. 27 Oct. 2011. Retrieved from <http://www.commtouch.com/threat-report-january-2012>.

“CommTouch Internet Threat Trend Report January 2012 Infographic.” CommTouch. 27 Oct. 2011. Retrieved from <http://blog.commtouch.com/cafe/wp-content/uploads/Infographic-Facebook-attack-trends-in-2011.jpg>.

Warren, Christina. “Warning: Facebook Free Starbucks and Tim Horton’s is a Scam.” Mashable.com. 18 Oct. 2011. Retrieved from <http://mashable.com/2011/10/18/starbucks-tim-hortons-facebook-scam/>.

Pann, Joann. “Facebook Spam and Cybercrime on the Rise: How You Can Avoid It [INFOGRAPHIC].” Mashable.com. 10 Jan. 2012. Retrieved from <http://mashable.com/2012/01/10/facebook-profile-safety/>.



to keep something private on Facebook is not to post it to Facebook.” Users need to adjust their expectations about privacy, modesty, and what it means to share. Anything anyone has ever posted is fair game for privacy concerns. Users should ensure they use the new privacy controls and sharing settings that these social media sites provide, but ultimately, the only true protector of privacy is the user.

Sources:

Manjoo, Farhad. “On Facebook, privacy is a myth.” The Washington Post [Washington, D.C.] 4 Dec. 2011, Technology & Innovation: pg G4.