

Online Surveys and Their Irresistible Lures

WHY SOCIAL MEDIA USERS FALL FOR SCAMS

Survey scams in social networking sites may look harmless and may just be a waste of time once users find out that they will not get what they were promised in the end. Keep in mind, however, that bad guys will not waste time coming up with ingenious scams if these will not translate to profit.

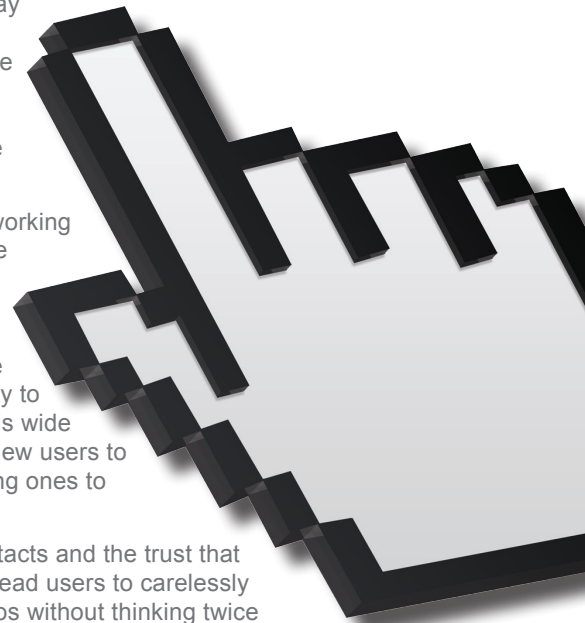
SOCIAL MEDIA: HOTBEDS FOR SCAMS

People spend a great deal of time every day immersed in their respective virtual communities, the most popular of which are social networking sites. In August 2010, Nielsen reported that along with blogging, social networking topped the list of favorite online activities in the United States.

Social media offers far more than just networking and/or contact building. To add value to the services they provide, sites like *Facebook* now allow users to post videos and pictures, write blog-type articles, and play games. Some social media sites also have built-in chat features as well as functionality to form groups and/or to organize events. This wide array of additional features are attracting new users to use social media as well as enticing existing ones to stay hooked.

Easily making information available to contacts and the trust that exists among social media “friends” often lead users to carelessly click random links to fake photos and videos without thinking twice about online security. These behaviors may be the primary criminal motivation behind the various crafty tricks employed to dupe users into giving out their personal credentials.

Every social networking site has a feature like *Facebook*’s wall that lets users post their own updates or see what their contacts are up to. Since the wall is the most accessible *Facebook* feature, it is also where most scams in the guise of videos and news riding on trending topics usually appear. We have seen several dubious *Facebook* posts with links, that when clicked, led to scams. We have taken note of the more notable social networking scams in [an infographic](#) published last month.



SURVEY SCAMS OFFER NOTHING FOR SOMETHING

Social media scams are defined as posts, events, and messages that arrive in chain-letter fashion and that ask recipients to give out personal information in exchange for false rewards. We have seen a lot of these use different Facebook features in order to spread. These scams persist because they take advantage of a very predictable human reaction. They bait people with interesting celebrity news—real or fake, nude pictures, fake videos, and false promises of free stuff or rewards. Curious users click embedded links for no other reason apart from the fact that these are clickable. We have seen several successful *Facebook* scams lead to online surveys and, consequently, to data theft in recent months.

One such scam offered users free tickets to “Breaking Dawn Part 2.” The wall posts for this scam featured the message, “Get a Free Tickets to Twilight Breaking Dawn Part 2! (note the grammatical errors),” a link that users needed to click in order to get what they were promised, and an image. Clicking the *Share Link* button posts the same message to the walls of affected users while clicking the image or text redirects them to a bigger version of the image with a poll question about the movie’s protagonist, Bella.



Figure 1. Free tickets to “*Breaking Dawn Part 2*” instead lead to a survey scam

Depending on the users’ answer to the question, they are redirected to specific pages that all required them to give out personal information of varying magnitudes. Some pages only asked for email addresses while others sought additional or different information like mobile phone numbers. Entering personal information led to various malicious payloads like receiving spam and further redirection to a survey page but never to what they were promised—free tickets to the said movie.

A similar *Facebook* scam was spotted in July 2011. Using Amy Winehouse's death as lure, it asked victims to answer an online survey. Starting with a wall post that supposedly leads to a shocking video shot before the singer's death, this scam led users to a page where they were asked to verify their ages. Clicking the link in the said post prompted the display of a notification informing the users that the same message will be posted on their walls. Afterward, another notification appears urging the users to prove if they are indeed human by taking either the "Are You Dumb or Smart?" or "Are You and Your Partner Compatible?" survey, which both required them to give out their mobile phone numbers. Answering any of the surveys, of course, did not lead to the promised video but instead exposed victims to information theft.



Figure 2. Amy Winehouse video instead leads to a survey scam

The Amy Winehouse scam was, however, not the first to use the "Are You Dumb or Smart?" survey. In fact, we saw the survey a little over a week before in non-*Facebook*-related scam that used Google+ as bait. This ruse made use of a specially crafted Web page from which interested parties could supposedly download invitations to the new social networking site. Trying to download an invitation led users to a page that listed surveys from which they must choose one for completion.

Closing the page containing this list directed users to a file-sharing site that offered two choices—to download a free invitation by answering one of several surveys or to do so using an existing account on the file-sharing site for a fee. Either way, users who chose to answer a survey at once or to opt for the other given choices ended up giving out personal information or even money in exchange for nothing.



Figure 3. Google+ invitation instead leads to a survey scam

ANSWERS TO SIMPLE QUESTIONS CAN TURN INTO HUGE PROFITS

Survey scams in social networking sites may look harmless and prove to be just a waste of time when users find out that they will not get what they were promised. Cybercriminals, however, earn huge profits from these fraudulent activities, otherwise they will not bother coming up with them.

Even though some surveys are legitimate, the way by which their creators trick users into answering them may prove suspicious. Take the Google+ survey scam as an example: Becoming a Google+ member is free so downloading an invitation to join the social networking site for a fee is indeed fraudulent. Users who fell for such a scam would not have received invitations, only given money to cybercriminals in the process.

Apart from getting instant payment such as in the Google+ scam, scammers can also earn from tricking victims into paying for nonexistent premium SMS services. This is, after all, one of the reasons why they ask users to give out their mobile phone numbers.

Redirecting users to various advertising sites can also be another means by which cybercriminals earn money. Unwitting users who fall for malicious advertisements and click links to related sites allow crooks to earn.

As has been previously said, scams persist because people allow them to. Social media users should be very conscious of clicking links that others, even their friends, share. Promises that are too good to be true are just that.

More often than not, the more eye-catching and share-worthy a post is, the more malicious it is likely to be. For more helpful tips and tricks to stay safe on social networking sites, read our e-book, "[A Guide to Threats on Social Media.](#)"



REFERENCES

- Bernadette Irinco. (August 26, 2011). *TrendLabs Malware Blog*. "The Geography of Social Media Threats (INFOGRAPHIC)." <http://blog.trendmicro.com/the-geography-of-social-media-threats-infographic/> (Retrieved September 2011).
- Christopher Talampas. (August 18, 2011). *TrendLabs Malware Blog*. "Free 'Breaking Dawn Part 2' Tickets Scam Spreads in Facebook." <http://blog.trendmicro.com/free-breaking-dawn-part-2-tickets-scam-spreads-in-facebook/> (Retrieved September 2011).
- Cris Lumague. (July 25, 2011). *TrendLabs Malware Blog*. "Amy Winehouse's Death Used in Online Attacks." <http://blog.trendmicro.com/amy-winehouses-death-used-in-online-attacks/> (Retrieved September 2011).
- Karla Agregado. (July 12, 2011). *TrendLabs Malware Blog*. "Survey Scam Offers Google+ Invites." <http://blog.trendmicro.com/survey-scam-offers-google-invites/> (Retrieved September 2011).
- Paul Pajares. (May 6, 2011). *TrendLabs Malware Blog*. "Facebook Spam Spreads Through Multiple Features." <http://blog.trendmicro.com/facebook-spam-spreads-through-multiple-features/> (Retrieved September 2011).
- The Nielsen Company. (August 2, 2010). *nielsenwire*. "What Americans Do Online: Social Media and Games Dominate Activity." http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity/ (Retrieved September 2011).
- TrendLabs. (May 2011). *Threat Encyclopedia*. "A Guide to Threats on Social Media." <http://about-threats.trendmicro.com/ebooks/socialmedia-101/> (Retrieved September 2011).