9672 Via Excelencia #101
San Diego, CA 92126
www.idtheftcenter.org
Toll-Free (888) 400-5530

Facebook Social Media Survey

The Identity Theft Resource Center (ITRC) recently conducted a brief *Facebook Social Media Survey* to measure interaction trends between internet users and Facebook. The ITRC conducted this survey in order to better help victims with Facebook-related identity theft concerns and issues and received 446 responses.

"As our world transforms more and more into a cyber environment, social networking becomes a larger part of our lives. Because of this, it is important to understand how social networking users comprehend the safety risks while engaging on such sites. This can help in efforts to protect consumers by defining problem areas." says Nikki Junker, Social Media Coordinator for the ITRC.

"The survey results will help the ITRC in developing informative materials and documents. These publications aim to educate consumers in order to help minimize their risk of becoming victims of identity theft and mitigate the losses of those who have already become victims."

Executive Summary:

The following are the results from a survey recently conducted by the Identity Theft Resource Center on Facebook user beliefs and behaviors. The purpose of this survey was to determine the mindset of consumers in relation to concerns about identity theft (in particular, financial identity theft) and Facebook usage. The study also looked at the consequences suffered by users who had previously experienced Facebook account takeover.

The ITRC study shows that despite an overall increase in concern and awareness of identity theft related to Facebook, users did not always act in accordance with such concerns. Consumers still tend to believe that financial harm cannot be caused by Facebook usage. While a large number of those surveyed had been the "target" of identity theft while using the site, only a small number had actually experienced identity theft as a consequence. Although users did not seem to make a direct correlation between Facebook usage and financial identity theft, the majority of them did have unique passwords different from their online financial accounts, and most were careful to limit the amount of information they presented to the public.

According to a recently released study by Javelin on identity fraud[1], identity theft rose 12.6% in 2011. One factor they believe has contributed to this rise is the growing use of social networking among consumers.

One major concern brought to light by the ITRC study was the lack of consumer understanding regarding privacy settings on Facebook. When asked to identify whether or not particular statements were true, 63% of the survey respondents believed their information was only visible to friends if their profile was set to private. This belief leaves users vulnerable to having their personal information exposed. Users may believe that their privacy settings are limiting the exposure of personal information, when in fact the information is still exposed due to incorrect privacy settings. However, increased media coverage on this subject does appear to be making users more aware of the risks to their privacy, and the importance of Facebook privacy settings.

[1] Javelin Strategy & Research, 2012 *Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier*

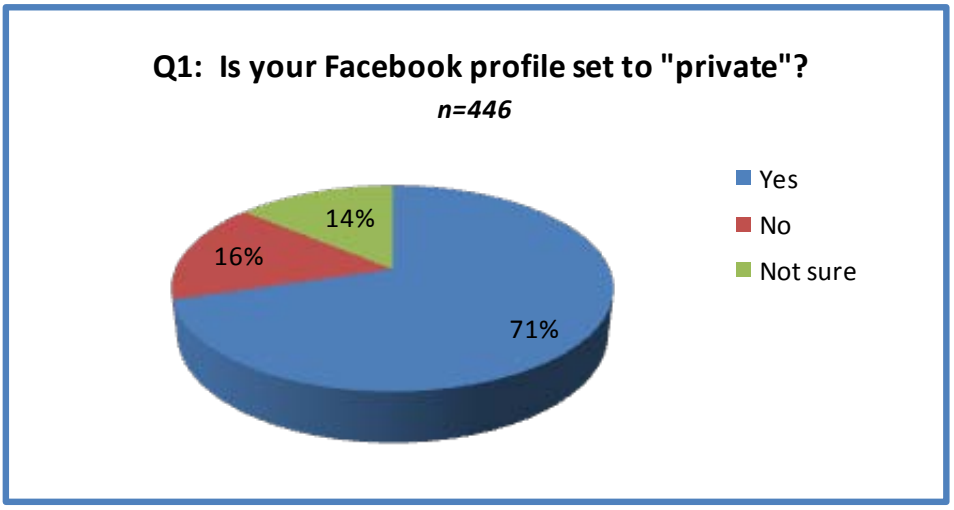
Overall, the ITRC study reflects the findings of other research done on Facebook usage and privacy concerns, such as the Pew Research Center's study titled: *The Tone of Life on Social Networking Sites*[2]. The Pew study found that "Users of online social network sites such as Facebook are editing their pages and tightening their privacy settings to protect their reputations in the age of digital sharing."

The issue still remains: many Facebook users are still at risk of becoming victims of identity theft. While most are taking minimal security precautions, they still largely fail to make the connection between Facebook usage and financial identity theft which past studies have shown to exist.

Key Findings:

1. Privacy settings on Facebook, and the difficulty in understanding their impact, have been the subject of several recent news articles and studies. The reason for ITRC interest on this issue is the recognition of potential exposure of personal information for consumers who have improper privacy settings. Setting the Facebook user profile to "private" is the most fundamental step in protecting user information from misuse.

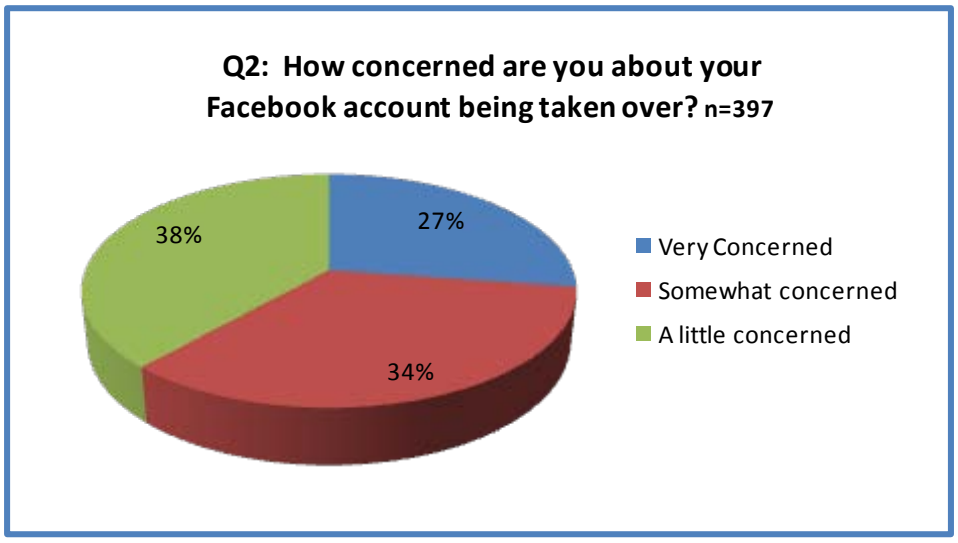
   The ITRC survey found that 14% of the respondents did not know what the privacy settings were on their Facebook profile, and an additional 16% did not have their profile set to "private." In comparison, 71% of those surveyed had their Facebook profile set to "private". In light of the greater awareness of social networking risks, it seems problematic that almost 3 in 10 users do not have profiles set to "private," or are not sure of their settings.



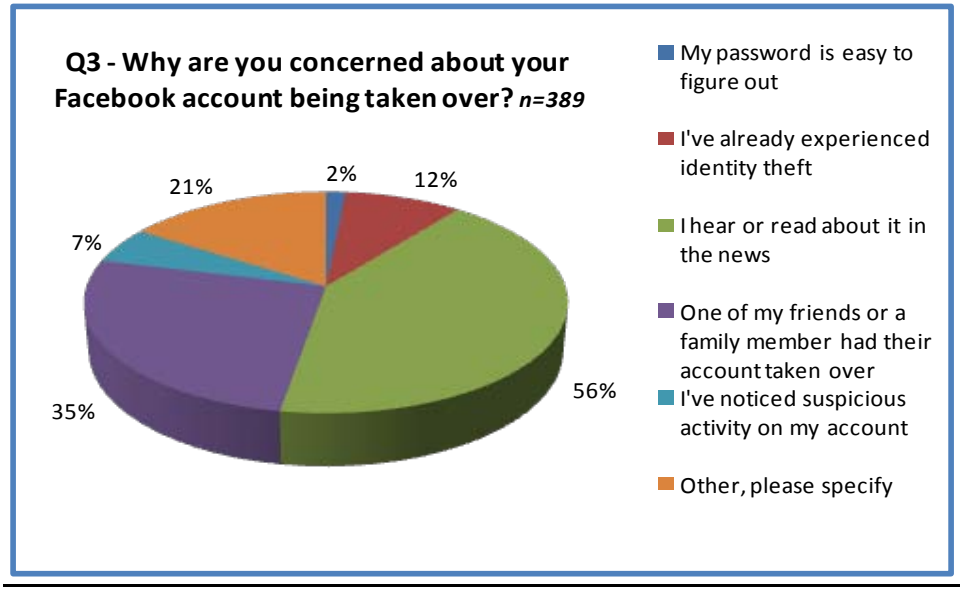
2. In an effort to measure user anxiety about becoming a victim of account takeover, the survey questioned users directly about their level of concern. This question is driven by a variety of account takeover cases of which ITRC is directly aware. In addition, Facebook has recently implemented measures to improve authentication and verification of users, and added procedures to help users prevent and/or rectify an account takeover occurrence.

   Concern about Facebook account takeover is spread somewhat evenly between a little concerned and somewhat concerned, with 38% of those surveyed reporting that they were only a little concerned about their Facebook account being taken over and 34% being somewhat concerned. 27% stated that they were very concerned.

[2] Pew Internet & American Life Project, 2012, *The tone of life on social networking sites*



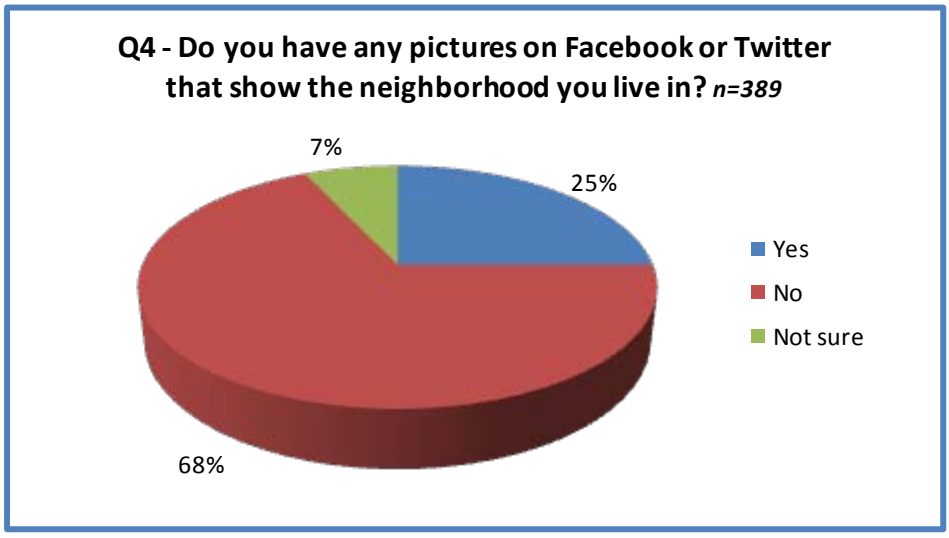
3. As a follow-up question to #2, 87% of the survey takers responded to this question. ITRC wanted to determine what might be the sources of concern about Facebook account takeover. 56% of the Facebook users are concerned about account takeover primarily due to heightened awareness of this issue from news and media. A substantial 35% of those surveyed reported that they had a family member or friend experience an account takeover. A surprising 12% reported having already been a victim of identity theft, and seemed to make the correlation between identity theft and Facebook account takeover. 1 in 5 respondents indicated "other" and listed a wide variety of reasons, including "fear of embarrassment or damage to my reputation,""lack of trust," "basic paranoia," "phishing emails received in Facebook," and "scams are getting more difficult to detect."



4. One area of concern expressed by the ITRC and many security experts are the types of information that are routinely posted on Facebook, without a complete understanding of the risk that may be involved. One of those risks is the posting of digital photographs which may have the GPS location embedded directly in the picture file. This process, called Geo Tagging, can be found on cell phones, digital cameras, i-Pads, and a variety of other mobile devices. Inadvertent publication of the precise location of the camera when a picture is taken can present a serious stalking risk, or lead to other criminal acts. In a test, an ITRC employee found Geo Tagging data in several photographs

downloaded from Facebook profiles. Simply pasting the GPS coordinates into Google Maps instantly provided street views of the homes and addresses.

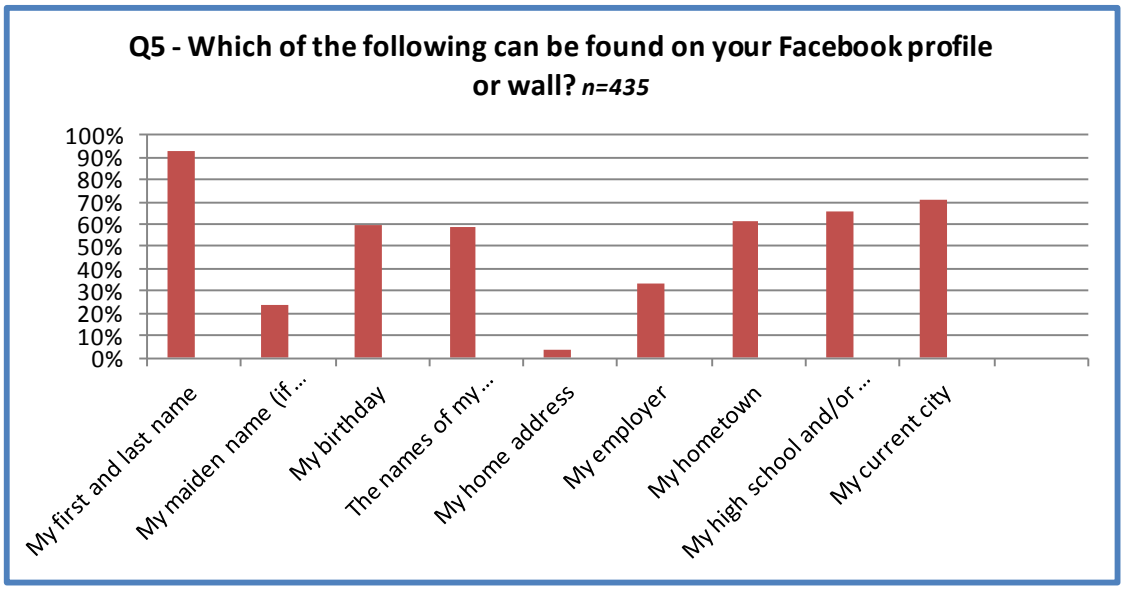
A quarter of those surveyed had posted pictures of the neighborhood in which they lived to their Facebook or Twitter profiles. Of course, the point of this question was to determine if the user population was aware of Geo Tagging. On a positive note nearly 70% indicated that they did not post pictures that identify their neighborhood. Although some pictures do not have Geo Tagging information embedded in them, it is important for social networking users to be aware that this hidden content can show their location, and the risk that may be present. In mobile devices with GPS it is important to disable Geo Tagging.



5. Over exposure of personal information, often from multiple sources, is one of the primary factors involved in identity theft cases. As with most social networking sites, Facebook requires a certain minimum amount of information in order to create a profile. Too much personal information can provide an identity thief with all of the necessary data to begin building an impersonation profile. In other cases, this information can be used in "social engineering" exploits, allowing phishing scams or other fraud to occur. The question below was designed to find out what types of personal information are routinely posted on Facebook profiles.

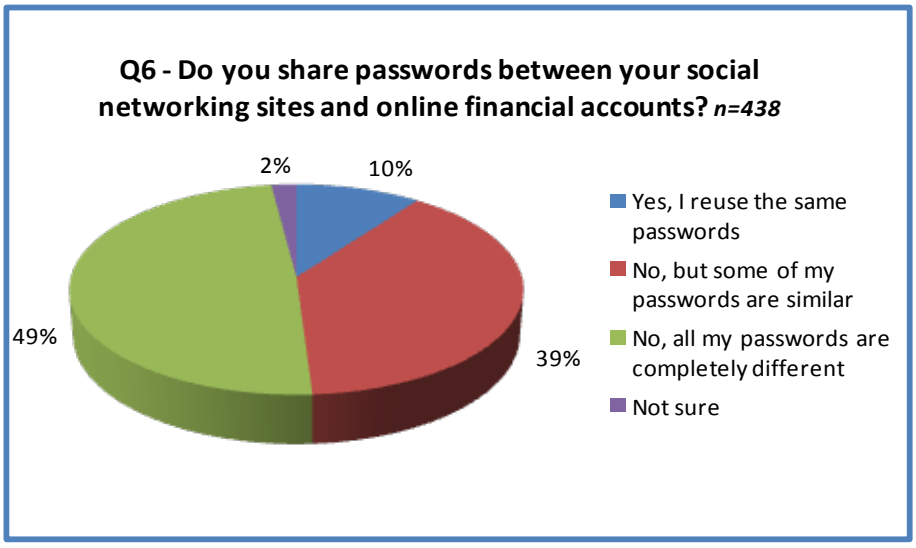
   93% of the respondents indicated that their full name could be found on their Facebook profile or wall. Very few people (only 4%) have their home address listed on their Facebook profile. Nearly 60% of those surveyed have the names of their family members listed on their profile and 33% of those surveyed have their current employer identified on their Facebook profile. At a minimum, many of these profiles may provide a good starting point for a thief to begin creating an impersonation file.

   Looking at the results in this question in relation to the results for Question 1, we find it likely that some percentage of these respondents do not have their profile set to private. Even when set to "private" some of this information is made available to the general public. When not set to private, all this information is available to anyone who seeks it.



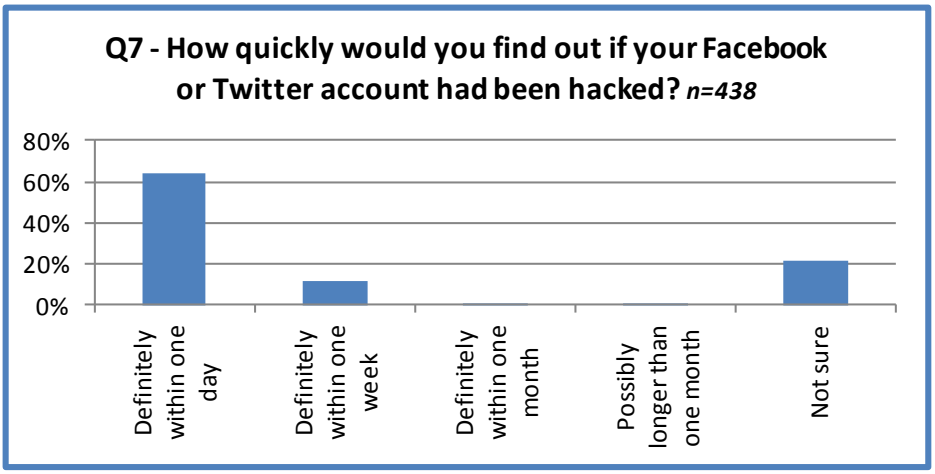
6. One of the concerns expressed by security experts is the use of passwords that are common, or very similar, for a person's different accounts (Facebook, financial, email, gaming, etc.). Common passwords, or even passwords that are very similar, allow a perpetrator to have a head start at cracking a password for a financial account.

   It is encouraging that nearly half of the survey participants have completely different passwords for all online accounts. Only 10% of those surveyed reuse the same passwords for their social networking accounts and their online financial accounts, while another 39% used passwords that are similar for various accounts.



7. It is known by ITRC and other identity theft experts that the length of time between the actual identity theft and the following discovery of that theft has a significant impact upon the amount of damage done to the victim. The purpose of this question was to determine how quickly the respondents believed it would take to discover that their account had been hacked. It should be noted that participants for this survey were contacted by use of Internet (including the ITRC website), and social media channels. This may have had a filtering effect upon the type of respondent, and therefore their response. However, the response below is in general agreement with the Pew study, which found that 85% of social networking users are active at least once a week.

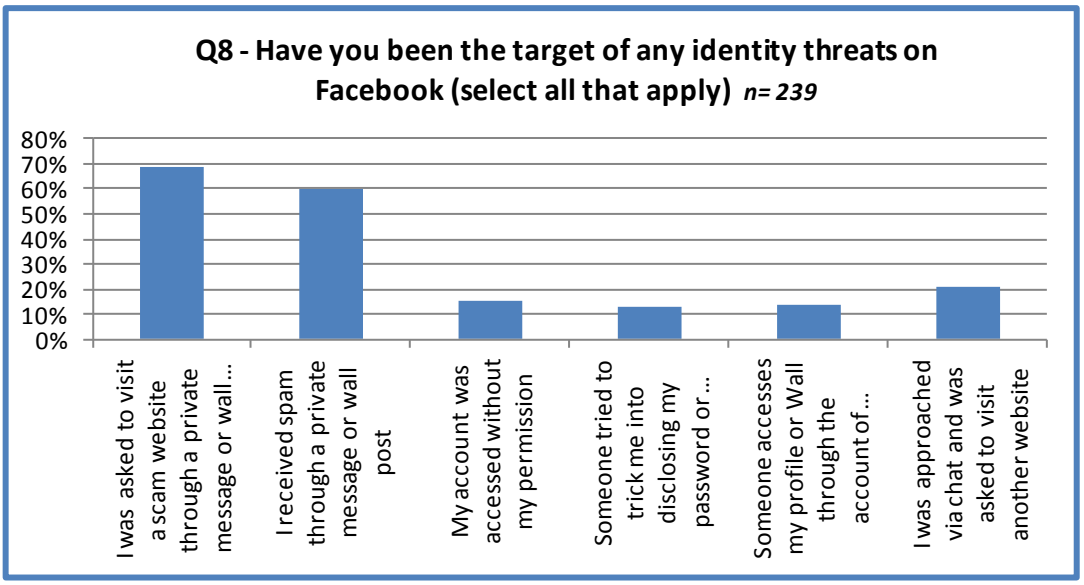
In regard to how long it would take before a Facebook or Twitter account takeover had occurred, 64% of those surveyed stated that they would be aware if their Facebook or Twitter accounts were compromised within one day, and 76% would know within a week. 21% are not sure how long it would take to find out that their account had been compromised. In general, this shows that social networking has become a part of daily life, and that 3 out of 4 respondents appear to be aware of their account integrity, and think they would notice very quickly.



8. Facebook threats seem to be more prevalent than we had thought. Based upon a growing number of reports about social networking and possible threats, this was a topic that we felt should be further explored. The survey sought to identify the types of threats we thought might be most common, based upon the experience of our victim advisors.

   More than half (54%) of the survey participants indicated that they had been the target of an identity threat. Nearly 70% of those responding had been asked to visit a scam website through a private message. 60% had received spam through a private message or wall post. One in five respondents had been approached via chat and asked to visit another website. 15% had their account accessed without their permission, and 13.4% had been "socially engineered" to disclose their password or other sensitive information. Lastly, 14.2% indicated that someone had accessed their profile through the account of someone on their "Friends" list.

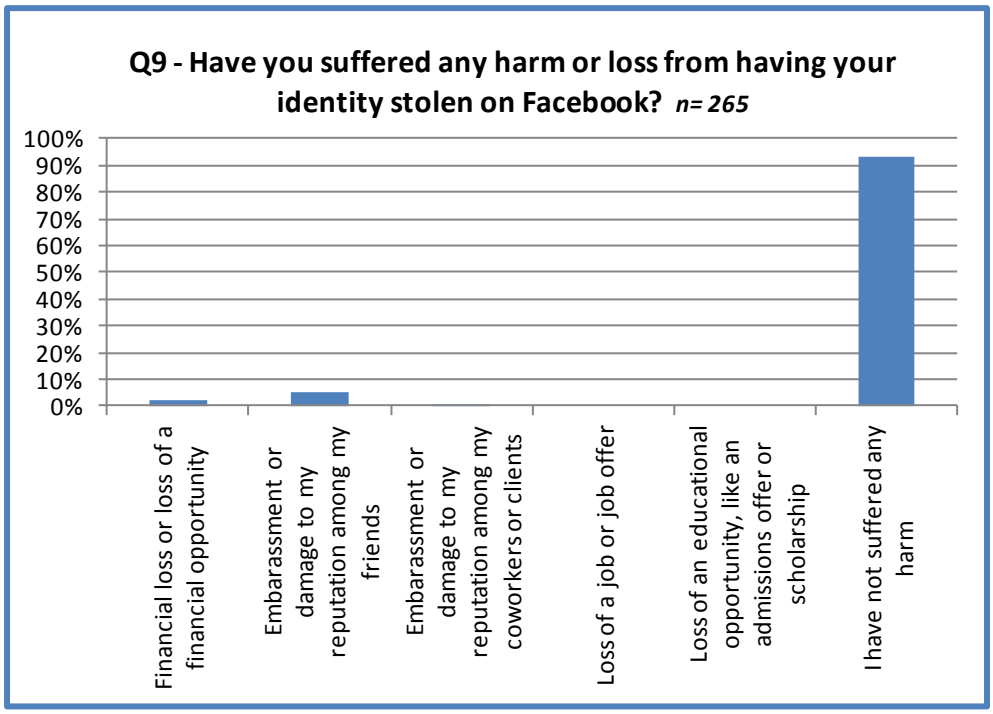
   Clearly, the fact that more than half of the respondents had been targeted for an identity threat indicates that Facebook users are an attractive target for those who attempt to harvest personal information. No doubt some of these interlopers are just harassers, but just as surely some are those who want the information for purposes of identity theft.



9. Historically, and as related in several studies, the majority of identity theft victims do not know how their personal information was compromised. This next question intended to determine if Facebook users relate any particular financial harm or reputational loss due to their usage of Facebook. According to the most recent Javelin[3] study Facebook users with a public profile had a fraud rate of 7.5% in 2011. Perhaps the fact that 71% of our survey respondents have their profile set to private explains somewhat the large response that they had suffered no harm from their Facebook usage.

   None of those surveyed had lost a job or educational opportunity due to account takeover. Only 2% had experienced financial loss compared with 93% of the respondents who said they had never suffered any harm at all related to their identity and usage of Facebook. The largest group (6%) who had suffered harm from Facebook usage were those who had suffered embarrassment or damage to their reputation amongst friends, coworkers or clients.

[3] Javelin Strategy & Research, 2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier

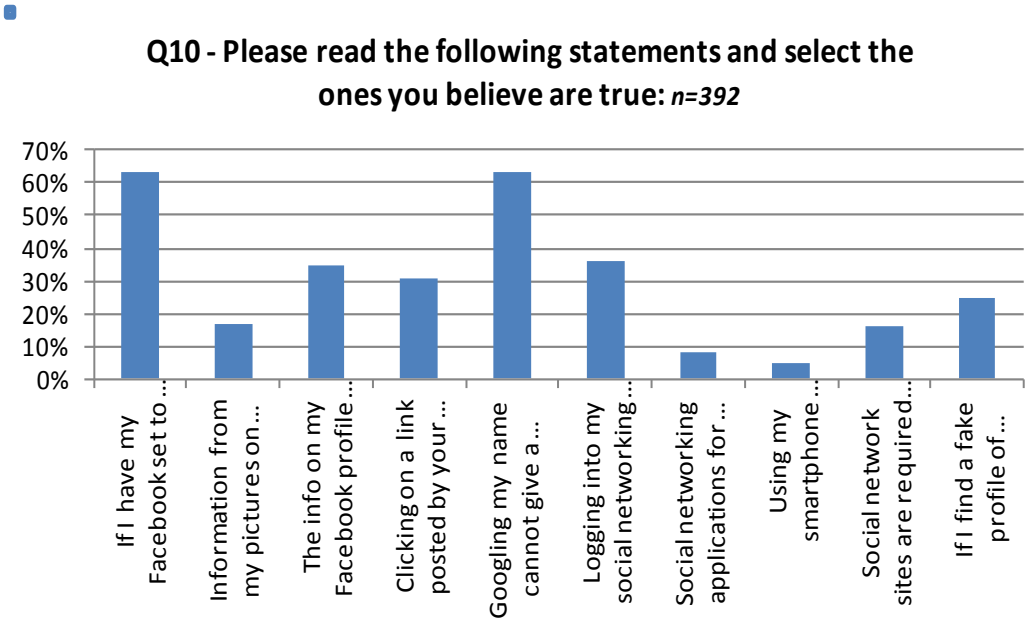


10. In today's digital world, there are many prevalent myths surrounding social networking and Facebook. This question was asked to determine how well Facebook users understand the correlation between various Facebook activities and settings, and the potential risk, responsibility, and liabilities for Facebook usage.

    The following True-False questions were asked (followed by the answer):

    - If I have my Facebook set to private only my friends can see my personal information.
        - *False: When using a basic privacy setting, personal information is visible to anyone viewing your Facebook profile. When using the basic privacy settings, information such as your full name, hometown, current city, employment, and other information about preferred activities may be seen publicly.*
    - Information from my pictures on Twitter or Facebook can tell a thief where I bank.
        - *True: Digital pictures containing Geo Tagging and/or use of Facebook "Check-ins," combined with other information, may provide an exact location.*
    - The information on my Facebook profile cannot lead to financial identity theft, because I don't have any identifying information on there (other than my name)
        - *False: Information such as place of employment, date of birth, and mother's maiden name can assist identity thieves with accessing financial accounts.*
    - Clicking on a link posted by your best friend on Facebook cannot give a thief access to your bank account.
        - *False: Links posted to Facebook walls may often point to websites where malware is loaded immediately (referred to as a "drive by shooting" by security experts). This malware may contain spyware or key logging programs which may provide hackers with complete financial account login information.*
    - Googling my name cannot give a thief access to my bank account.
        - *True: Your name alone is not the primary indicator of your identification for financial purposes.*

- Logging into my social networking profile using WiFi cannot give a thief access to my bank account.
    - *False: Public WiFi and many private WiFi locations are not secured, and may have additional users who will have the ability to "sniff" the Internet traffic you are sending while accessing financial accounts. This ability makes it possible for a thief to record the information you are using to access the account.*
- Social networking applications for my smart-phone were tested for safety before they were put on the market.
    - *False: Only Apple does pre-release testing for all applications available (only through Apple). "Jail-broken" iPhones are susceptible to rogue applications, as are most other systems including Droid and Blackberry.*
- Using my smart-phone when social networking is safer than my PC.
    - *False: Malware aimed at smart-phones is a growing industry, while very few security or antivirus programs exist or are in use for mobile devices.*
- Social network sites are required by law to assist consumers whose information has been compromised on their site.
    - *False: The user contract that an individual accepts in order to use social networking sites releases the provider from almost all liability for usage of their system.*
- If I find a fake profile of someone impersonating me, the site has to remove it within a specified time.
    - *False: Again, the user contract that an individual accepts in order to use a social networking service removes liability from the provider for the actions of others on the site.*



10. 63% of the survey respondents believed their information was only visible to friends if their profile was set to private. Unfortunately, this is false. This belief leaves users vulnerable to having their personal information exposed. Users may believe that their privacy settings are limiting the exposure of personal information, when in fact the information is still exposed due to incorrect privacy settings.

    Only 17% of the respondents recognized correctly that digital picture information can give accurate location data for a thief. Unfortunately, the majority of respondents did not recognize the potential risk of Geo-Tagged pictures.

More than 1/3rd of the respondents incorrectly believe that the information on their Facebook profile cannot lead to financial identity theft. Certainly some profiles have a wealth of information, and others are very sparse. However, most of the personal information presented on a Facebook profile can be used to help build an impersonation profile.

It is important for Facebook users to understand that the use of bad links is a major method of spreading malware. Extremely large bot-nets are created using this technique. However, 31% of those surveyed do not understand how easily a website link, even from a friend, can be used to accomplish injection of malware into the host computer.

It is evident from the survey that most respondents realize that Googling your name does not provide access to your bank account. Nearly 2/3rd of those surveyed got this right.

36% of those surveyed believed that logging into a social network on Wi-Fi cannot give a thief access to their bank account. Unfortunately, this is incorrect. The risks of unsecured WiFi are not clearly understood by these respondents. It is enlightening that the majority appear to have an awareness of the potential risks.

Only 8% of respondents were under the false belief that smart-phone apps are tested prior to release to the public. Thankfully, 92% got this question right. With the thousands of apps available to consumers it is important that the majority of consumers view these programs with some skepticism.

Survey takers also seemed to be knowledgeable about the issues surrounding Smartphone usage in regards to social networking. Only 5% thought that using a Smartphone when social networking was safer than a PC.

Social networking users are also unaware of the lack of responsibility the social networking sites are held to in the case of false impersonation and information compromise. 16% thought that social networking sites were required by law to assist consumers whose information has been compromised on their site and 25% thought that a site must remove a profile impersonating someone else within a specified amount of time. Although social networking companies are becoming more responsible in helping users with these problems, the usage agreements still put the responsibility upon the users.

Conclusion

Similar to findings in other areas affecting identity theft, the public expresses an increased awareness and concern relating to Facebook privacy and security, seemingly coupled with behaviors that sometimes ignore those same concerns. Facebook users did not express a strong relationship between their usage of the social networking site, and financial or other harms. A significant problem faced by those working in the identity theft field is that most identity theft cases cannot be easily or directly tied to a particular method of obtaining the personal information that is used to affect the crime. This fact makes it more difficult to present hard evidence of a connection to a particular activity, such as Facebook use.

It seems apparent that between the use of public (non-private) profiles, and the inclusion of a variety of personal information on typical user pages, that a significant number of users do not have an understanding of how “data aggregation” can be used by both benign and harmful entities to create a very accurate profile of a particular person. However, it is heartening to determine that most users do set their profile to “private,” a majority seem aware of the need for discrete passwords for different

accounts, and 3 out of 4 use their account at least once a week, making it more likely they would be aware of problems quickly.

The good news above is countered by responses that indicate Facebook threats are more prevalent than most would think. More than half the respondents had encountered one or more identity threats. Messages, private chats, and spam attempting to lure the user to a website were common, and social engineering for passwords and account access by proxy were not uncommon.

The increasing activity noted above to gain access to personal information via Facebook begs the question as to why the vast majority of those surveyed indicated they had suffered no harm or loss due to Facebook activity. It is our belief, as is a common thread in identity theft cases, that the majority of victims do not know how their personal identifying information was acquired or compromised.

The survey showed a continued lack of understanding of Facebook privacy settings, and how they affect data exposure. A significant percentage of users underestimate how their information (1/3rd) or pictures (5/6th) can be used in harmful ways, and about 1/3rd also did not understand how a simple website link can expose them to numerous security problems. The website www.insidefacebook.com reported on 3/27/12 that Facebook has 845 million monthly users. This widespread usage of Facebook means that a percentage of exposed users, such as 1/3rd, is a quite substantial population to be preyed upon.

Respondents were generally savvy about smart-phone usage and testing of applications. This issue, along with the potential problems of Geotagging, has been covered in recent media pieces. Considering that the majority of those surveyed were concerned about Facebook account takeover due to hearing or reading about it in the news, it is not unreasonable to link increased media exposure to public awareness on these issues.

The world of social media, mobile technology and information security is constantly evolving. In order for consumers to protect themselves against the rising threats of cybercrime, they must stay alert to developments. The level of concern amongst both the media and population will be critical in creating a continued rise of self-defense against threats.

Methodology

The survey was made available online to consumers from January 19th 2012 to February 29th 2012. It should be noted that participants for this survey were contacted by use of Internet (including the ITRC website), and social media channels. This may have had a filtering effect upon the type of respondent, and therefore their response. It was also dispersed via the ITRC social networks including those on Facebook, Twitter, LinkedIn and Google+. Additionally, the survey was announced through the ITRC blog and shared by ITRC partners and employees. The total number of participants for this survey totaled 446 Facebook users. Completion of the survey and submission of email contact information directly entered individuals into a sweepstakes for which the prize was a $100.00 gift card.

Definitions

Identity Theft: Identity Theft is a crime in which an impostor obtains key pieces of personal identifying information (PII) such as Social Security numbers and driver's license numbers and uses them for their own personal gain. The PII can be obtained from lost or stolen wallets, stolen mail, a data breach, computer virus, phishing, scams, or paper documents thrown out by you or a business (dumpster diving). However, in this study only loss of PII via social networking was considered. The crime varies widely, and can include check fraud, credit card fraud, financial identity theft, criminal identity theft, governmental identity theft, and medical identity theft.

Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data, especially your Social Security number, can be used in the worst cases to take over your identity. The result can be personal responsibility for large debts and/or crimes committed while

the thief is using the victim's name. In some cases, a victim's losses may include not only out-of-pocket financial losses, but may also include substantial financial costs associated with trying to restore his reputation in the community while also correcting erroneous information for which the criminal is responsible. [4]

Regarding **Identity Theft**, it should be noted that true identity theft involves the theft of driver's license, birth certificate, or Social Security number, account numbers, or other personal identifying information (PII) in order to open new accounts, get a job, get a loan, or commit crimes in the victim's name.

Social Network: A social network is defined as a web-based service that allows individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.[5]

[4] http://www.justice.gov/criminal/fraud/websites/idtheft.html

[5] boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html