Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Which Disney© Princess are YOU?

Social engineering for identity theft has always been around. But now, with the advent of social networking sites such as Facebook, MySpace, and a host of others, it has become easier than ever to harvest personal information from unsuspecting targets. This paper looks into just how much personal information can be gathered by the seemingly-harmless What type of personality are you? quizzes that are so prevalent on social networking sites. The paper will then look at what the information could be used for, and how t...

Copyright SANS Institute

Author Retains Full Rights

AD

Which Disney© Princess are YOU?

(Web 2.0) Social Engineering on Social Networks

GIAC (GCIH) Gold Certification

Author: Joshua Brower, Josh@ToTheLastTribe.com

© 2010 SANS Institute, Author retains full rights.

Abstract

Social engineering for identity theft has always been around. But now, with the advent of social networking sites such as Facebook, MySpace, and a host of others, it has become easier than ever to harvest personal information from unsuspecting targets. This paper looks into just how much personal information can be gathered by the seemingly-harmless "What type of personality are you?" quizzes that are so prevalent on social networking sites. The paper will then look at what the information could be used for, and how to protect against this particular vector of social engineering.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

1. Introduction

Social engineering takes many form; some obvious, some not so obvious. One not so obvious form is that of questionnaires—be it a knock on the door to answer a survey for a "census" worker, or a "harmless" quiz found on a social networking site. Depending upon their content, they can serve as a very powerful means of capturing and correlating information for nefarious purposes.

The following example of an unedited quiz recently found on a popular social networking website illustrates just how seemingly unsuspecting, yet powerful, these questionnaires can be.

What does your password say about you?

Is your password good or is it easily going to be hacked and also what does it say about you?

1. *How long is your password?*

A) 3-5 letters/numbers

B) 6-8 letters/numbers

C) 11-14 letters /numbers

D) 9-10 letters/numbers

2. *Is your password your name with some other numbers or somebody in the family?*

A) Yep

B) No way! That's too easy for me!

C) Its exactly my name

D) It's my family members name with some other numbers.

Joshua Brower, Josh@ToTheLastTribe.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

© 2010 SANS Institute, Author retains full rights.

3. *Does your password have any numbers?*

A) Yea, it's all numbers actually!

B) Yea it's got a couple of mixed up numbers.

C) Nope!

D) Yea one number!

4. *Has your password/account have ever been* [sic] *hacked into?*

A) No never!

B) No but I told one of my friends it.

C) Yea once.

D) Twice actually.

* (Apps.Facebook.com)

According to the quiz statistics, eight-hundred people have already taken this particular quiz. (Apps.Facebook.com) What is remarkably staggering, is that while a quiz of this nature seems relatively harmless at first glance, the amount of information that can be captured, compiled, correlated, and acted upon with harmful results to the end user is quite large. What the end user does not realize is that even a seemingly harmless quiz like this is a form of social engineering.

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

1.1 Definition and History of Social Engineering

Ian Mann, (2008) author of "*Hacking the Human*," defines social engineering as the following: *"To manipulate people by deception, into giving out information, or performing an action"* (p. 11). This definition encompasses not only the gleaning of information, but also the possibility of "performing an action." In general terms, when social engineering is thought of, it is usually in relation to harvesting information and not necessarily in relation to performing an action. For example, if a security guard is manipulated into allowing an attacker through a security checkpoint, the attacker has not gained any particular information. However, they *have* manipulated the security guard into allowing them into an area (performing an action) where they were not authorized to be. (Mann, 2008)

Social engineering has been around since the beginning of time. In fact, one of the earliest documented examples of a phishing attack can be found in The Old Testament. In Genesis 27, Isaac had gone blind in his old age, and was on his deathbed. After his wife heard that he wanted to give the family blessing to the eldest son, she told their youngest son, Jacob, to go and deceive his father and receive the blessing instead. The problem was that the eldest son was a very hairy man, and Jacob was not. To deceive Isaac, Jacob covered himself in goatskins. This deception worked, and Isaac blessed Jacob instead of his eldest son. In this example, Isaac had fallen prey to what is known as a simple phishing scheme. (Dang, 2008)

Throughout history up to the modern day, there have been countless other examples which illustrate the effectiveness of social engineering. In the story of the Trojan horse of the Greeks, the Trojans had fallen prey to the Greek's social engineering tactics through their own over-confidence and gullibility. (Dang, 2008) Twentieth century social engineers, such as Frank Abaganale, portrayed in the movie, "*Catch Me if you Can*," pulled off astonishing stunts through social engineering methods. And Kevin Mitnick, one of the most well-known social engineers of the modern era, uttered these words as he was testifying before Congress of his misdeeds: *"I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it."* (Mitnick, 2002)

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

1.2 Current Day Social Engineering

With the advent of the Internet and the rapid advancement in mobile telecommunications devices and communications platforms, social engineering has, and continues to be, more prevalent than ever before. One major reason for this is that there is far less risk to social engineer across the Internet than in person. (Mann, 2008) Consider the personal risk, such as arrest or fines, between the following two social engineering scenarios: 1) An attacker social engineering their way into a physical "audit" of Company X, looking for an exploitable vulnerability to siphon their intellectual property out. 2) An attacker social engineering their way into Company X by sending a targeted phishing e-mail (spear phishing), to an employee, gaining their remote login credentials to access Company X's intellectual property over the Internet. Obviously, the personal risk would be much less in the second scenario.

Current day social engineering vectors take on many forms. They can vary from in-person exchanges, to over the phone conversations, through e-mail, or even through online social networking sites.

1.3 Social Engineering on Social Networking Sites

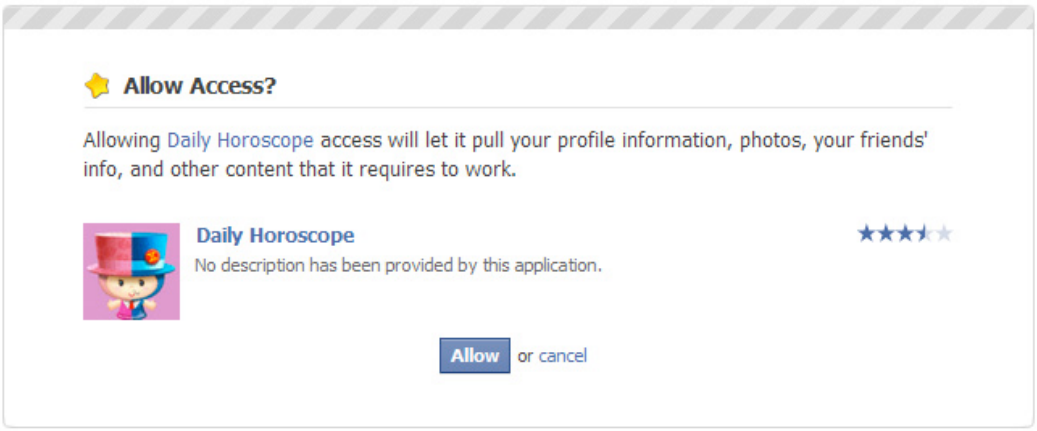
As the Internet continues to evolve, new and unique social engineering opportunities continue to come to light, such as the "Web 2.0" social networking sites. MySpace, Facebook, and Orkut, are just a few of the more popular examples of such sites that are among the most widely used today. These social networking sites are a gold mine for social engineering attacks as there is oftentimes an implicit trust assumed in the "befriending" of someone the user may or may not know that well.

One particular social engineering vector that is often found on many of the widely used social networking sites today is the *"What Type of Personality are You?"* quiz. These types of quizzes when taken by the end user will oftentimes yield a specific result, such as what Lord of The Rings character they are, or how long they will live, or who they are most compatible with. On the outside, they appear harmless and fun to the end user, and provide an entertainment value that is enticing, to say the least. However, on a deeper level, the quizzes themselves are one of the most insidious vectors of social

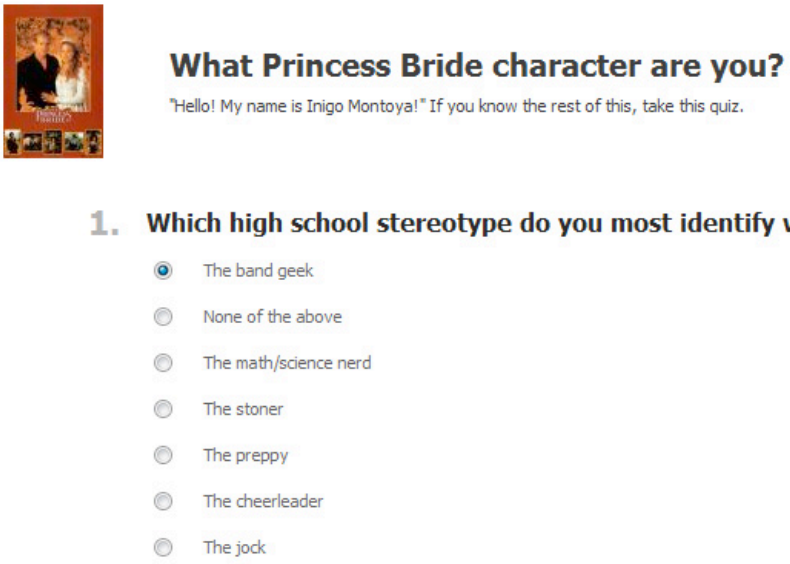
© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

engineering on social networks, because of the type and sheer amount of information gathered, and who has access to it. With these quizzes, the information is gathered in small amounts, in very unsuspecting ways, and the end user has absolutely no idea who has access to it. At least when a user adds an application on Facebook, it asks the user's permission to give the developers access to their information. Consider the following example:

Which would more likely give a user pause?



Or



Joshua Brower, Josh@ToTheLastTribe.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

More than likely, the first example would be the one to make a user pause and consider their actions, rather than the harmless quiz pictured in the second example. As such, the focus of this paper will look at, and concentrate on this particular vector of social engineering on social networks.

2. Main

2.1. Background

Although there are a number of social networking websites on the Internet, out of all of them, Facebook is currently the most-widely used. Numbers show, that as of February 2010, Facebook has four-hundred million active users. (Facebook.com) Recent reports show MySpace as having approximately sixty-six million active users (Insidefacebook.com), and Orkut at nearly fifty million active users. (Orkut.com) Facebook also provides an open API for developers to write their own applications, making Facebook the most prevalent social networking site for these types of quizzes. After considering the above reasons, it was decided to use Facebook as the social networking website of choice for the research, instead of the other social networking websites.

2.2. Goals & Procedures

The goal of the following procedure was to take a passive look into what quizzes users have already taken, and compile the results from the questions asked. In this scenario, five Facebook users were profiled. Next, all of the quizzes that the five users had taken over a two month span were noted and, using a sample Facebook account, those same quizzes were taken with the questions being noted. Finally, using the questions from the quizzes that each profiled user had taken, a personal profile was built. Since it was not possible to know exactly how each user had answered each question, the profiles were generated by using possible answers. Keep in mind that the quiz creator would know exactly how the users had answered. Finally, this procedure assumes a few things. As mentioned earlier, since the user allowed the quiz access to their Facebook profile, the developers of the application also have access to a lot more information, such

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

as pictures, status updates, etc. For this procedure, and the remainder of this paper, it will be assumed that the developers of the quizzes also know 1) The e-mail of the user, and 2) The name of the user. It may be that the developer knows a lot more, but for our purposes, this is all that needs to be assumed.

2.3. Results

For each Facebook user that was profiled, the answers to the questions on the quizzes have been compiled, and a simulated target profile of each was built as follows:

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Target #1 Profile

Information from Allowing Quiz Access to Profile
Name: Tiffany Radenberg

E-mail: tiffr83@gmail.com

Information from Quizzes

Basic Personal

Gender: Female

Birthday: Dec 12, 1983

Age: 26

Hair Color: Brown

Eye Color: Brown

Favorites

Favorite Color: Red

Favorite Music: Country

Favorite Animal: Horses

Personality

-Has at least 1 child, would like to have more kids

-Usually dresses nice, but casual

-Religious, to some extent (Prays before meals)

-Greatest Fear: That harm will befall loved ones

-Perfectionist

-OCD to some extent

-Competitive

-Independent

-Organized

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Target #2 Profile

Information from Allowing Quiz Access to Profile
Name: Jeff Luken

E-mail: vegies539@hotmail.com

Information from Quizzes

Basic Personal

Gender: Male

Birthday: November 13, 1979

Favorites

Favorite Drink: Smoothies

Favorite Ice Cream: Cooke Dough

Favorite Color: Blue

Favorite Musician: Weird Al Yankovic

Favorite Genre of Music: Classical

Favorite Movie: E.T.

Favorite Olympic Sport: Curling

Favorite Sport: Lacrosse

Personality

-Vegetarian

-Loves History & Non-Fiction books

-Drives a Volkswagen Bug

-Real Life Hero is Barack Obama

-Believes that self-defense is the only acceptable form of violence

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Target #3 Profile

Information from Allowing Quiz Access to Profile
Name: Mellissa Ourthe

E-mail: mali437@Juno.com

Information from Quizzes

Basic Personal

Height: 5'1"

Hair: Blonde and Wavy

Eyes: Brown

Pierced Nose

Favorites

Favorite Color: Purple

Favorite Candy: Reese's Peanut Butter Cups

Favorite food: Mexican

Favorite drink: Soda

Favorite Movie: Wall-E & Finding Nemo

Favorite Animal: Cats

Personality

-Drives a minivan

-Most important thing is family

-Always carries cell phone with her

-Self-proclaimed procrastinator

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Target #4 Profile

Information from Allowing Quiz Access to Profile
Name: Blake Keyes

E-mail: coldandchilly73@Yahoo.com

Information from Quizzes

Basic Personal

N/A

Favorites

Favorite TV Show: Heroes

Favorite Beverage: Black Coffee

Favorite Movie: Terminator

Favorite type of food: Italian

Personality

We know they have a family and they love to spend time with them.

Last vacation went camping and hiking

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Target #5 Profile

Information from Allowing Quiz Access to Profile
Name: Megan Jergens

E-mail: easygirlz174@yahoo.com

Information from Quizzes

Basic Personal
Gender: Female

Birthday: March 15, 1988

Age: 21

Hair Color: Blonde

Eye Color: Green

Lives in Defiance, Ohio

Favorites

Favorite Color: Pink

Favorite Music: Pop

Favorite Movie: Save the Last Dance

Favorite Animal: Cat

Favorite Flavor: Vanilla

Personality

-Dreams of working as a personal trainer

-Does not want kids

-Is not close with her family

-Curses a lot, mainly "shit"

-Does not like to cook

-Loves *Material Girl* by Madonna

-Sleeps on her back, facing the ceiling

-Snores

-Usually goes to bed between 8-9pm or earlier

-Drives a white 97 Oldsmobile Cutlass

-Has a credit card

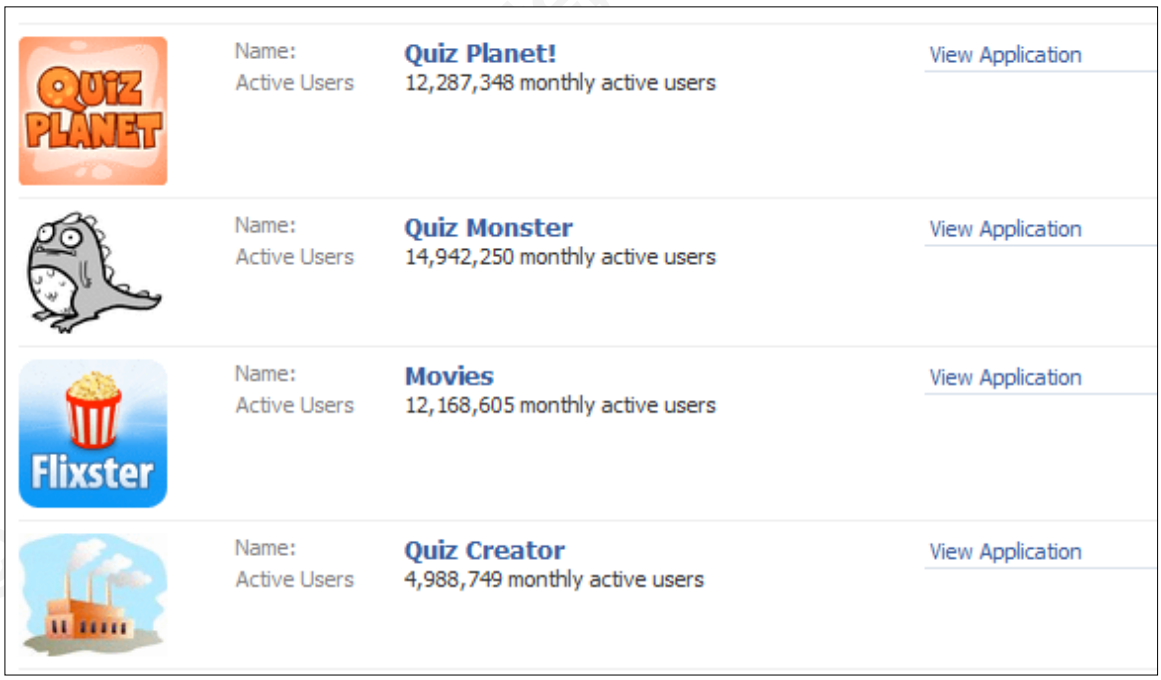
Joshua Brower, Josh@ToTheLastTribe.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.4. Taking It to the Next Level

As can be seen from the previous profiles, the first procedure garnered a very rich set of results to work with. To really take this particular social engineering vector to the next level, the goal of this next procedure would be to actively create a situation for users to take the quizzes like usual, but also be able to consolidate their results across multiple quizzes. Finally, a report would be able to be run on any given quiz taker.

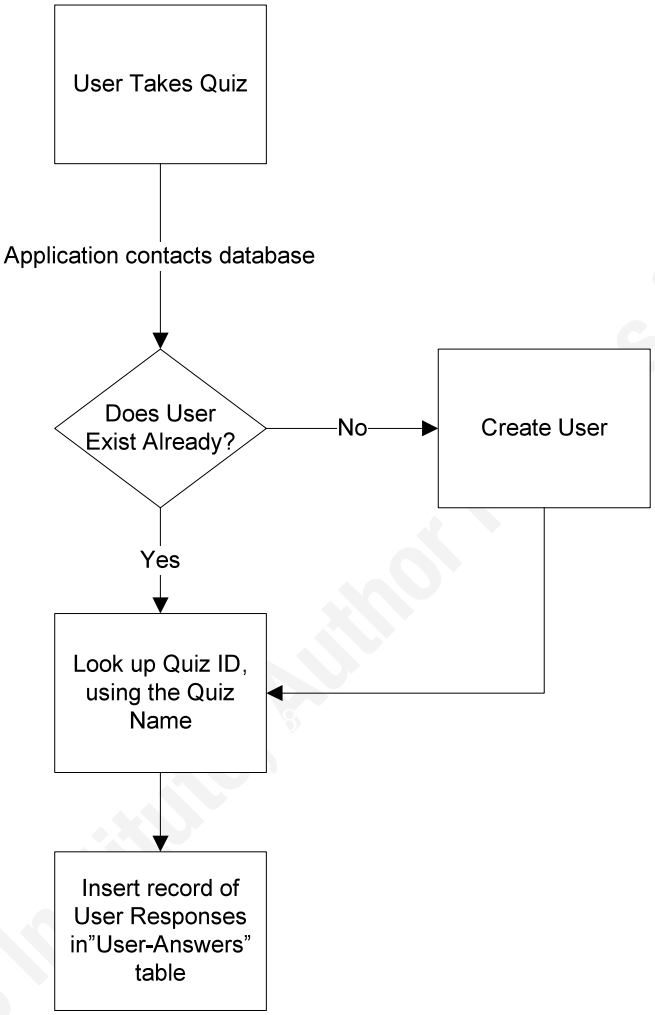
This could be accomplished by creating a Facebook application that allows users to both take and create quizzes. There are currently well over fifty of these types of applications available on Facebook. The difference is thus: As a user takes a quiz, the application contacts a back-end database that creates a unique ID for the user, and stores all of the answers to the quiz that the user is taking. It does this for every quiz that the user takes. To generate a profile for a user, a report is run that pulls all the information in the database for a given user, runs algorithms on it that categorizes and consolidates the data, formats it, and displays it for viewing. Considering that the top three quiz applications have over thirty-two million active users, the quantity of data that could be mined for each user is staggering. (Facebook.com)



Following are two aspects of the proposed program in flowchart form.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

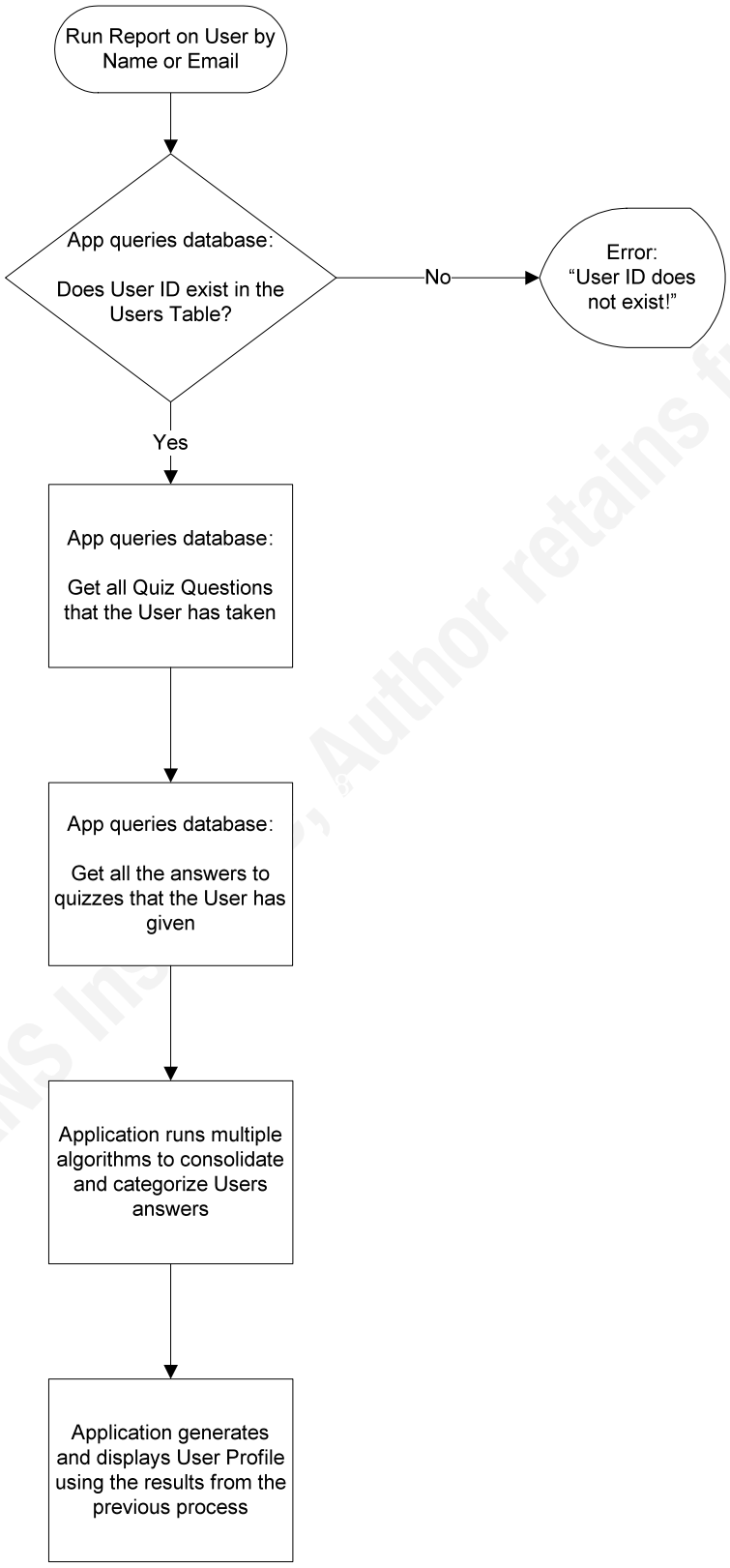
User Takes Quiz



Joshua Brower, Josh@ToTheLastTribe.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Run a report on a given user



Joshua Brower, Josh@ToTheLastTribe.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

This would be trivial for a competent programmer to develop. For those non-programmers, it would still be easily done, as some Facebook quiz applications are up for sale for as little as $500 for an exclusive license to the code. V. Fazilov (personal communication, December 18, 2009)

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.5. How the Resulting Profiles Could Be Used

There are three ways that the harvested information could be used: *Spear Phishing, Impersonation or Identity Theft,* and *In-Person Attack or Scam*.

2.5.1 Spear Phishing

Spear phishing is a very specifically-targeted phishing attempt. Reasons for spear phishing can vary from downloading some type of malware or adware on the target's machine, to being the next step in the process of gathering more information needed for the next pretext. Using the first target's profile, here is how a spear phishing attack could play out.

Attack Scenario:

Spear Phishing

Using the profile for Target #1, it is known that the user loves country music. An e-mail could be crafted, with the title having something to do with a country music star. i.e. *"Breaking News: Tim McGraw on deathbed after car accident!"* To see the linked video of this breaking news, the target is supplied with a link in the e-mail. When the link is clicked, the target is prompted to download an updated "codec" for their video player. However, what is not known to the target is that this "codec" is actually a key logger that silently installs, and sends captured usernames and passwords back to the attacker. Because it is known that the target loves country music, there is a much higher probability that the target will actually open the e-mail, and try and watch the linked video, than if the e-mail included some other random subject line.

2.5.2 Impersonation & Identity Theft

The second way of using the results is for the basis of building a profile on the target for some type of impersonation or even identity theft. With over ten million cases of identity theft reported in 2008, (a twenty-two percent increase from 2007), the US Department of Justice has identified identity theft as passing drug trafficking as the

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

number one crime in the USA. (The ID Theft Resource Center, 2010) There are different types of identity theft, with credit card fraud remaining the highest at twenty-six percent in 2008. Other types include utilities fraud, bank fraud, and employment fraud, among others. (Identity Theft Statitistc: Spend On Life, 2009) The following is a scenario of how Target #2's harvested information could be used in a case involving identity theft.

Attack Scenario:

Building a Profile for Identity Theft

The attacker's goal is bank fraud. Using the profile for Target #2 as the basis, the attacker can start to build a more in-depth profile of information about the target. Considering that the attacker has the target's name, gender, birthday, and e-mail address, it will take just a little bit of searching on Google to find out the target's location and phone number. From there, the attacker has a few different avenues on which he could proceed. One option would be to attack the target via a spear phishing scheme. The other option could involve an over-the-phone social engineering attack. Either way, the goal of the attacker is to find out where the target does their banking, and any other pertinent information that may be valuable. Since the attacker has quite a bit of personal information on the target already (i.e. vegetarian, Volkswagen Bug, favorites, etc) there are quite a few possibilities of pretexts. After obtaining the information, the attacker, with a well-developed profile of the target, directly attacks the bank. As a side note, as more and more banks are adding the concept of security questions as part of their authentication process, the questions are varied, but do include such questions as are on the quizzes that Target #2 answered. *Favorite Movie*, *Favorite Sport*, and *Real Life Hero,* are all questions that have been spotted in certain financial institutions' inventory of security questions. With such a detailed personal profile built on the foundations of the target's answers on the quiz, the chance of success in this scenario is very high.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.5.3 In-Person Attack or Scam

This type of attack targets the victim in a face to face attack or scam. As can be seen from the profiles, only Target #5 answered a question on a quiz that gave away their location. Also keep in mind that depending on the social network, the application developer may have been given location information for users of his application.

Attack Scenario:

In-Person Attack

The attacker's goal is simple theft. With the attacker knowing so much detail about Target #5, it would be trivial to do some research online and find out where the target lives and the street address. The attacker can assume that with the target being twenty-one years of age and not being close with family, then the target probably does not live with family. Knowing that the target goes to bed by 9:00 pm and drives a white 1997 Oldsmobile allows the attacker to profile when the best time for him to break in is. Once again, knowing so much detailed information about Target #5 makes it much easier to successfully pull off this type of attack.

2.5.4 Probability

Three types of attacks have been considered. One question that remains is whether any of these attacks are actually probable, as they may seem quite far-fetched. Would an attacker really conduct a physical theft against a user, using the information gathered from the user's quiz answers?

In fact, some of these scenarios *are* much more probable than others. The reason for this comes down to threats. A threat is *"a party with the capabilities and intentions to exploit a vulnerability in an asset."* (Bejtlich, 2005) In this case, the vulnerability would be a weakness that was created by the release of the target's personal information. There are two types of threats: structured and unstructured. Richard Bejlitch (2005) sums up each: "*Structured threats are adversaries with a formal methodology, a financial sponsor, and a defined objective. They include economic spies, organized criminals,*

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

terrorists, foreign intelligence agencies, and so-called 'information warriors.' Unstructured threats lack the methodology, money, and objective of structured threats. They are more likely to compromise victims out of an intellectual curiosity or as an instantiation of mindless automated code. Unstructured threats include 'recreational' crackers, malware without a defined object beyond widespread infection, and malicious insiders who abuse their status."(p. 7) Just having a threat does not make a particular attack more probable—the threat must have not only the intentions, but also the capabilities. In this particular social engineering vector, it is more likely that the threat to a user would be unstructured than structured, since this type of vector is more trolling for information that could reveal a vulnerability, than what a structured threat would do, i.e., identifying the target first, and using their answers to quizzes as a means to build a profile of information.

The point is that if there is a threat that is targeting the user, whether structured or unstructured, that possesses both intentions and the capabilities, then it is much more probable that one of the above attack scenarios could happen. For example, what if, in the identity theft scenario, as the attacker is learning more about the target, he came across the fact that the target works as an accountant for a Fortune 500 company? Depending on the attacker's proclivities, it may be worth it to him to attempt a physical attack on the target's home to steal the target's computer in hopes of gaining some confidential financial records of the company.

2.6. Managing the Risk

How does a user or an organization manage the risk of this particular vector of social engineering attack? It must be considered first from an individual perspective, and then from an organizational perspective

2.6.1 Managing the Individual Risk

As in the case of many such things, abstinence is the only 100% foolproof way of not falling prey to a social engineer through this particular vector. But, if the need

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

arises to find out which of the Simpsons© character the user resembles, the following guidelines will help safeguard the vigilant user.

-Depending on the social network, a user needs to remember that if they install the quiz application, the developers of the application will have access to the majority of the users, and the user's friends, profile information.

- A few specific types of information that should never be given out on these types of quizzes include:

- Mother's maiden name
- Personal banking details
- Personal password details
- Personally Identifiably Information (where the user lives, social security number, phone number, e-mail, etc.)

-The most important thing to remember when a user take these kinds of quizzes is to be keenly aware of what kind of information they are giving up. They need to ask themselves, *"If someone was out to get me, my family, or the company I work for, could any of this information help them in any way?"*

This may seem paranoid to the point of extreme, but by this point it is clear from the earlier attack scenarios how easy it would be to nefariously use this information.

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.6.2 Managing the Organizational Risk

Because the actions that an individual user takes can directly affect the organization they work for, each organization must factor this type of attack into their risk management program. As was mentioned previously, abstinence is the only 100% foolproof way of not falling prey to a social engineer through this particular vector. From an organizational perspective, this could mean one of three different approaches to managing this risk.

1) *User Education Only:*
   Depending on the organizational risk appetite specific to this vector, the organization may feel comfortable with not blocking social networking websites, but just educating their users to be aware, and to not fall for this particular attack. The individual risk management guidelines in the preceding section are a good place to start.

2) *User Education and Blocking Social Networking Websites:*
   If an organization feels that the risk warrants this option, the organization can use I.T. security controls. In this situation, using a content filter, the organization can block social networking websites. Since this attack is just one vector of social engineering, it must be understood that users need to be continually educated on the risks, since the organization cannot block social networking websites outside of the networks in its purview—for example, the users' home internet connection.

3) *Do Nothing:*
   Whether the reason for this choice is ignorance or apathy, the outcome remains the same: through this particular vector or another one, social engineers will take advantage of the organization through its uneducated users, and the lack of I.T security controls. The only uncertain aspect of this outcome is how big the fallout will be.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

3. Conclusion

Social engineering is like putting together a puzzle. As the social engineer gathers the little bits and pieces of seemingly unimportant information, a much larger picture starts to emerge. Whether it is a profile from a target for simple identity theft, or various information needed for a complex robbery, it can all start with simple social engineering tactics.

As social networking sites have exploded in popularity in the last five years, so has the risk of personal information exposure. This is because, at the crux of it, users do not know and/or care how easy it is to abuse the information that they so freely give out. It is a sad state of affairs when it is commonplace to see countless examples of users' social networking accounts spamming their friends, all because they had fallen prey to a social engineering attack that resulted in the compromise of their account authentication information.

Quizzes, that are so prevalent on social networking sites, can be one such tool that can bleed significant amounts of personal information from unsuspecting users. Although a wide-scale implementation of this attack would be difficult to implement, as data-mining fifty-million users on Facebook would be resource intensive, it does not negate the fact that the world is continuing towards the crest of a perfect storm: the continuing disinterest and ignorance of users to the theft of their personal information, and the ever-lowering bar of the difficulty of low-risk, electronic social engineering attacks.

With the continuing evolution of the Internet, malicious social engineers will continue to find and develop new and more complex ways of bilking unsuspecting users out of their personal information. Users and organizations must continue to be vigilant for these new avenues of guile and deception, and remember that they hold the key to the success or failure of the perpetrator.

Joshua Brower, Josh@ToTheLastTribe.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

4. References

Mann, Ian. *(2008). Hacking the human.* Aldershot, Hampshire, England: Gower

Mitnick, Kevin *(2002). The art of deception*. Indianapolis, Indiana: Wiley Publishing, Inc

Dang, H. (2008). The Origins of Social Engineering. *McAfee Security Journal*, Fall 2008, 4-8.

Bejtlich, R. (2005). *The Tao of Network Security Monitoring.* Boston: Pearson Education, Inc.

Identity Theft Statitistc: Spend On Life. (2009). Retrieved January 1, 2010, from Spend On Life Web site: http://www.spendonlife.com/guide/identity-theft-statistics

The ID Theft Resource Center. (2010). *Workplace Facts: ID Theft Center*. Retrieved January 1, 2010, from ID Theft Center: http://www.idtheftcenter.org/workplace_facts.html

(n.d.). Retrieved Feburary 9, 2010, from Facebook.com: http://www.facebook.com/press/info.php?statistics

(n.d.). Retrieved February 9, 2010, from Orkut.com: http://www.orkut.com/html/advertise/ROW/overview.html

(n.d.). Retrieved February 9, 2010, from http://www.insidefacebook.com: http://www.insidefacebook.com/2009/10/14/the-latest-numbers-on-facebooks-september-us-traffic-from-comscore-quantcast-compete/

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

(n.d.). Retrieved December 2009, from Facebook.com: http://www.facebook.com/search/?q=quiz&init=quick#!/search/?flt=1&q=quiz&o=128&sid=100000317983047.2752707218..1

© 2010 SANS Institute, Author retains full rights.

Joshua Brower, Josh@ToTheLastTribe.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Last Updated: October 13th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410 ICS/SCADA SEC Essentials	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
FOR572 Advanced Network Forensics	San Antonio, TXUS	Jan 05, 2014 - Jan 10, 2014	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	OnlineMDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced