Cory Hatter

Jake Ellis

Social Media and Security

Ghiyoung Im

December 5, 2011

**Introduction**

In today’s society two thirds of online adults in the United States use social media. In fact, one in every nine people on Earth has an account with Facebook. Out of roughly 6,900,000,000 people on the planet, 800,000,000 of them use Facebook. The average user spends approximately 15 hours and 33 minutes a month on the site. The current social media craze began with the introduction of MySpace in 2003. Since then the popularity of social media sites has grown exponentially. Social media has spread from recreational use to the business industry, dating industry and everything in between.

**Social Media Sites Explained**

Some of the more popular social media sites are Facebook, Twitter, FourSquare, and LinkedIn. The first two sites are for geared towards recreational use. These sites focus on having the ability to connect with your friends and family. Twitter is a site that provides instant updates from your friends, industry experts, favorite celebrities and what’s happening around the world. These updates are referred to as ‘Tweets.’ These Tweets are statements, quotes, stories or anything that users deem interesting. In order to receive these updates you must follow users. Following is Twitters way of creating relationships between users. In order for a user to receive Tweets from another person the user must follow their desired person. A Twitter user has the capability to “tag” a follower in tweet by using the @ symbol before the user’s name. This allows the user creating the tweet, to communicate with a follower.

In comparison to Twitter, Facebook is similar in many ways. Facebook uses the same update concept, although they call their posts “status updates” and in order to view these status updates each user must agree to be “Friends.” Friend requests are given from one user to another and can be accepted or denied. If the user chooses to accept the request, the two users become connected instantly. Once the users are connected they are allowed to view photos, videos, and chat with each other. If a user uploads a picture to his or her profile, he or she is able to “tag” another user. When a “tag” is set, it will display the user’s name as a link to their profile for everyone to see. One major difference between Facebook and Twitter is the ability to generate “wall posts” between friends. A “wall post” is simply a message written on the profile of a user from a friend. Each status update is displayed on a news feed written on the Facebook home page. Notifications are displayed on a user’s profile to show the user that he or she has a wall post, tagged photo, or status update.

Foursquare is a classified as a location-based social networking website geared primarily towards mobile devices. When a user arrives at a venue they use Foursquare to “check-in” using their mobile phones. Foursquare uses the GPS hardware in your mobile phone to locate the venue that you are at. By checking in to various venues users gain badges. The more places you check into the more badges you earn, in hopes of becoming a superuser. Superusers are categorized as levels 1 through 3, with 3 being the highest-ranking superuser. A level one superuser can edit venue information such as address or phone number. A level two superuser can do things like merge duplicate venue postings or adjust the latitude and longitude of the venue. Finally, a level three superuser can create and remove venue aliases.

As a business alternative to Facebook, Twitter or Foursquare, LinkedIn provides many of the same features. Users “connect” with classmates, business partners, colleagues, and friends in order to create business relationships, job opportunities and develop their careers. User’s profiles contain personal information, work history, resumes and other business-related material unlike Facebook’s more recreational atmosphere. LinkedIn is a social media site for professionals who seek to develop business relationships and employment opportunities.

**Security Concerns with Social Media**

Social media encourages people to share information. However, most users never consider the dangers that can be hidden in sharing information over the Internet. Users should not turn a blind eye to their privacy. By posting something on Facebook or Tweeting something on Twitter, people don’t always realize that what they say can possibly be seen by anyone in the world at any time. By not checking out the privacy policies that their social network sites enact, a user may find that they are revealing more information than they had originally planned. For example, if a Facebook user has their privacy settings set to public, anyone in the world can look at everything on that user’s profile. Also, if a Twitter user doesn’t protect their tweets, anyone in the world can look at that user’s tweets. It’s important for user’s security to make sure they select the proper level of security for their own account. Information that is just supposed to be shared among friends is sometimes shared with the entire world.

Facebook is the currently the most popular social networking site in the world. There have been many security concerns in relation to Facebook’s database security, privacy policies, and login credentials being stolen. An anonymous Facebook employee revealed that Facebook previously had a master key that could be used to access any user profile. The key was used by typing in the user’s user ID and then the master key as the password. In fact, the password was accessible by any Facebook employee, but the original engineers were supposedly the only people who knew about it. The key has been destroyed according to the employee; however, the employee also mentions that all user messages are stored on databases that are accessible by Facebook employees. So realistically the master key was irrelevant anyways. So the question is: Is it ethical to allow random Facebook employees to see messages sent between Facebook users?

<http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm>

Another issue relating to Facebook is the application that users are allowed to use. Many of these apps require you to share some of your information that you have on your profile in order to play. Sometimes, the data that you share are stored on third party servers. Facebook can’t guarantee how the data will be used and who will have access to it. These third party servers aren’t subject to Facebook’s privacy policies or terms of service. Users should be leery about the applications they choose to play because of the amount of privacy that must be given up. Many of the third party servers aren’t as protected as Facebook’s servers and if they are hacked your personal information may be vulnerable.

Another security issue with social networking sites is having your account hacked. Facebook has recently said that they have 600,000 account passwords and usernames stolen each day. <http://redtape.msnbc.msn.com/_news/2011/10/28/8527819-facebook-says-600000-account-logins-compromised-every-day>. Facebook claims to stop the vast majority of them, but they still aren’t successful in stopping all attempts. Users should realize that at any moment their account could become compromised and all their information can be revealed. Private information that you would want no one to know should be kept away from social network sites and the Internet in general because once it’s in cyberspace, it’s never coming out.

Twitter also has its share of security issues. <http://www.koozai.com/blog/internet-news/does-twitter-have-security-issues-recent-twitter-hacks-raise-fears-893/> [http://www.crn.com/news/security/231601250/nbc-news-twitter-hack-issues-fake-news-of-ground-zero-terrorist-attack.htm;jsessionid=XQjtHUSVgSVTTwNUxtNrEg\*\*.ecappj01](http://www.crn.com/news/security/231601250/nbc-news-twitter-hack-issues-fake-news-of-ground-zero-terrorist-attack.htm;jsessionid=XQjtHUSVgSVTTwNUxtNrEg**.ecappj01) This past fourth of July, FoxNews’ Twitter account was hacked and messages were created stating that President Barack Obama had been assassinated. NBC’s Twitter account was hacked as well. The Tweets spoke of a plane attack on ground zero. If major news corporation’s Twitter accounts can be hacked, what does that say about the safety of an individual’s Twitter account? <http://news.cnet.com/8301-17939_109-10162649-2.html> Another concern with Twitter is the TinyURL technology that Twitter uses. Links that are tweeted on Twitter appear in paraphrased versions of the actual URL. This means that a user could click a link that they think will lead them to a legitimate website, but instead it’s possible that they are on their way to becoming a victim of phishing. Phishing occurs when attackers attempt to gain usernames, passwords or credit card information by creating a fake website that masquerades as a legitimate website. When a person types in their login credentials or financial information that data is recorded by the attacker and they have successfully phished your personal information. Users must be aware of the dangers that are present when it comes to TinyURLs.

Foursquare has also seen security issues in its past as well. In the summer of 2010, a white-hat hacker alerted Foursquare that he had found vulnerabilities in their system. <http://www.phonedog.com/2010/06/30/foursquare-security-breach-exposes-875-000-check-ins/>

The hacker was able to get 70% of all check-ins in the San Francisco area over a three week period no matter what privacy setting Foursquare users had chosen. Another security concern that the users should have is the entire premise of Foursquare’s GPS location concept. The location based social networking site announces where you are when you check-in to a venue. Instead of the check-in being interpreted as, “I’m at the movies at 9:00pm,” the check-in can be interpreted as, “It’s 9:00pm and I’m not home.” This can leave way for potential home invasions and theft. If a person with malicious intent was to find out that you’re not home, they could break into your house and steal your private property. Users should take this into consideration before using Foursquare.

LinkedIn has also been subject to security issues. When you sign in using your username and password the site creates a cookie called “LEO\_AUTH\_TOKEN,” which gives the user access to their account. <http://www.buzzom.com/2011/05/social-networking-giant-linkedin-has-security-flaws/> The problem is not the creation of the cookie, it’s how long the cookie remains on your computer. The same type of technology is commonly used in banking and it’s deleted after a very short time frame such as 24 hours or X amount of minutes after it senses no account activity. LinkedIn’s cookie used to remain on your computer for twelve months! Recently, LinkedIn reduced that amount of time to 90 days. However, that still gives attackers 90 days to sniff for your cookie after your most recent login. Once this cookie is found, an attacker can change information on the users profile page.

**Prevention Techniques**

As we have seen there are numerous ways for social networking sites to be dangerous. Although, there are also ways of preventing harmful attacks from taking place that may save a user a priceless amount of time and money.

One of the most basic and easiest techniques begins with the user’s password. A password is meant to protect an account by using a phrase, number, word, or any collection of characters used at log in. The password is chosen by the owner of the account and can be anything that matches the website’s criteria. Most websites such as, Facebook, require that the password must be at least 6 characters long, have at lease one number, at least one capital letter, at least one lower case letter, and it cannot match the username. Using simple things like the user’s first and last name, pet names, family names, or favorite sports teams are not quality passwords. It is also a bad idea to use the same password for multiple accounts such as email, banking, Facebook, and more.

Top quality passwords must include an assortment of numbers upper and lower case letters, as well as special characters such as ([\*$#@!.,\_](mailto:*$#@!.,_)). The more complex and intricate a password is, the less likely it will be susceptible to a brute force or dictionary attack. . A brute force attack is when a hacker attempts any and all combinations of passwords until one eventually works.

These passwords may be difficult to remember compared to a spouses name but it will be worth not getting an account hacked. A great way to remember passwords is to write them down and store them in a safe location such as a locked safe or a secret spot at home. There are software programs that will create a virtual safe on your computer where you can store password files in order to keep them safe and easy to access.

Once you have created an acceptable password the next process is to update it frequently to ensure that a hacker does not have enough time to brute force hack an account. Frequently usually means monthly or even weekly. The more often you change the password means the less amount of time a hacker can perform an attack because most brute force attacks take hours, days, or even weeks depending on the processing power of their machine.

The next prevention technique is the way a user interacts with the social networking site. A user should not create relationships with any and everyone they can because it could be a potential hacker, predator, or criminal. Authorities recommend only follow, friend, or connect with the people you know because some “hot chick” a man may think looks like a movie star may actually turn out to be a male pedophile.

The Next prevention technique is to be aware of what you are clicking on. Many social networking sites have adds and pop ups. A user should not click on anything without fully understanding what it is. A good program to use for this type of thing is called “No script”. This programs blocks out all java script, which is mainly used for moving ads and videos and gives the user the ability to add or deny certain scripts. The advantage of using something like No Script is it reduces the possibility of clicking on spam or infected links.

Another basic prevention technique is creating secure privacy settings. When an account is initially created the privacy settings are let to default which could be absolutely nothing. Privacy settings control whom can see the page, what they can see, and when they can see it. If the settings are set to default then it is possible anyone can see everything about a user even if they don’t know him/her. A strong privacy setting is a great way to block out people from seeing important information although users need to implement all other techniques as well.

Lastly, being cautious of what emails you read coming from social networking sites. It is very easy for other users to access a user’s information listed on the profile because many times the site will automatically add the email address linked to the account onto the associated profile page. Once the hacker acquires an email address they are capable of sending the user infected messages used to retrieve personal information or hack into the profile.