



The Dark Side of Facebook Games

An Interactive Qualifying Project Report
submitted to the Faculty of
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
Degree of Bachelor of Science

By

Khondkar Faiaz Hasan

fhasan@wpi.edu

Mohammed Suhail Akhtar

suhail@wpi.edu

Date of Submission: 27th April, 2010

Advisor: Professor Alexander Emanuel

aemanuel@wpi.edu

Executive Summary

The purpose of this project is to analyze Facebook games and to investigate their negative effects on the social well being of users. An in-depth analysis of two Facebook games, Farmville and Mafia Wars is conducted. Both of these games are created by the game developer Zynga, and these two games are currently the highest revenue generating applications present on Facebook. Through this report, the objective is to present the various ways Facebook games could have a detrimental effect on their users.

In the first half of the project, the focus is mainly on the social networking site (SNS) Facebook, and its technicalities. This overview covers the history and the foundations of Facebook, as well as the different features it incorporates which eventually attracted users towards it. Later on, the focus is shifted towards Facebook applications, especially games, and an emphasis is made on presenting the intricate details on the game play and the thought process behind the two popular Zynga games, Farmville and Mafia Wars.

In the second half of the project, the authors' provide an explanation on the various privacy issues present in today's online networking world, and then move on to unveil the truth behind Facebook games and their revenue making philosophies. This task is carried out by choosing the two Zynga games Farmville and Mafia Wars and dissecting their revenue generating tactics. In the process, the game developer Zynga is also analyzed to portray the partly illegitimate business model used by it to generate its revenues.

To support the thesis developed by the authors of this project, both the authors took turns in playing the games Farmville and Mafia Wars, in order to understand their functionality and also to uncover the various addictive elements incorporated in them. Additionally, a semi-real Facebook profile was created and friend requests were sent out randomly to see how many Facebook users shared their personal information with a complete stranger. Even though this part of the project did not directly relate to Facebook games, the authors thought that it was important in the realm of social networking as privacy is the front runner in most of the issues with SNSs. With this semi-real profile experiment the authors got shocking data that revealed unnerving facts about Facebook users' carelessness with regard to protecting personal information. Furthermore, a survey on Facebook games was sent out to all WPI students to get an idea of the students' knowledge about the intricacies involved in Facebook games, and if anyone was actually adversely affected by them.

Eventually, the authors of this project felt that it is important to provide a few good quality recommendations that if seriously implemented, would make Facebook a safer environment for all its users, and would also make the users more aware of the intricacies involved in social networking sites.

Abstract

This project analyzes two popular Facebook games in depth and provides a detailed account of how they could greatly affect a user's privacy and integrity. An effort was made to summarize an overview of Facebook and its applications, and also to reveal the deceiving tricks of the trade of online gaming by focusing on two Zynga games: Farmville and Mafia Wars.

Table of Contents

Executive Summary	2
Abstract	3
List of Figures	6
List of Tables	7
Introduction.....	8
1. Background.....	9
1.1 Problem Statement	9
1.2 Social Network Sites	9
1.3 Facebook: An Overview.....	10
1.4 The Facebook Platform	14
1.5 Individual Facebook Features Explained	15
1.5.1 Primary Facebook Features.....	15
1.5.2 Secondary Facebook Features.....	23
1.6 Facebook Applications.....	30
1.7 Facebook Games	31
1.8 Farmville	33
1.9 Mafia Wars.....	42
1.10 Online Privacy.....	48
1.10.1 Introduction.....	48
1.10.2 Cyber bullying	49
1.10.3 Online Predators.....	50
1.10.4 Privacy Invasion.....	50
1.10.5 Identity Theft	50
1.11 Facebook Games and Privacy	51
1.11.1 Using Credit Cards.....	51
1.11.2 Giving up Email Addresses	52
1.11.3 Giving up Phone Numbers.....	53
1.11.4 Downloading Toolbars.....	53
1.12 Facebook Game Developer: Zynga.....	54
1.12.1 Business Model.....	54
1.12.2 Zynga and Privacy Concerns	64
2. Methodology.....	65

2.1	Playing Facebook Games: Farmville and Mafia Wars.....	65
2.2	The Facebook Profile Experiment.....	65
2.3	Survey on Facebook Games.....	70
3.	Recommendations	87
3.1	Facebook Users	87
3.2	Facebook	87
3.3	Parents	88
4.	Conclusion.....	90
	References.....	92

List of Figures

Figure 1: Personal Data Transmission	13
Figure 2: Profile	16
Figure 3: Friends	17
Figure 4: Messages Inbox	18
Figure 5: Facebook chat (IM)	19
Figure 6: Profile Page of Britney Spears	20
Figure 7: Facebook Ads	21
Figure 8: A screenshot of privacy controls	22
Figure 9: News feed	23
Figure 10: The wall	24
Figure 11: Facebook Share icon on CNN's website	25
Figure 12: Facebook Search.....	26
Figure 13: Photo Albums	27
Figure 14: Notes.....	28
Figure 15: Groups	29
Figure 16: Disclaimer	34
Figure 17: Play GUI.....	34
Figure 18: Farmville Features.....	35
Figure 19: Mouse Click Functionality	36
Figure 20: Market	37
Figure 21: Neighbors	38
Figure 22: Invite Friends.....	39
Figure 23: Add Farm Coins and Cash Option	40
Figure 24: Social Ads.....	41
Figure 25: Mafia Wars Homepage.....	43
Figure 26: Jobs.....	44
Figure 27: Fight.....	45
Figure 28: Business.....	45
Figure 29: Inventory	46
Figure 30: The Godfather.....	47
Figure 31: Profile	47
Figure 32: My Mafia.....	48
Figure 33: Facebook Phishing Scam [25].....	52
Figure 34: IQ Quiz [31]	53
Figure 35: Video Professor Scam [31].....	57
Figure 36: Unavailability Notice for Fishville [25]	58
Figure 37: Filtering of Ads [25].....	59
Figure 38: Zoo World Offer.....	60
Figure 39: Zoo World Survey asking for user's personal information.....	61
Figure 40: Facebook's Ad Guidelines	61

Figure 41: Playfish In-game currency offers 62
Figure 42: Playfish Offer Survey 63
Figure 43: Kristen Wachenfeld’s Profile Page 66
Figure 44: Percentages of Shared Profile Elements Visualized thru a bar chart 68
Figure 45: Different Profile Pictures for Kristen's profile 69

List of Tables

Table 1: Percentages of Shared Profile Elements 67

Introduction

Facebook.com started off as a social networking site (SNS) for the students of Harvard University and is now a network used by millions of people around the world, day in and day out. Our desire to know about the people around us in our lives has fueled the growth of Facebook over the last few years and still remains the biggest growth factor. While Facebook until recently was considered to be popular only among the youth, latest trends on the Facebook Statistics website show that the latest growing demographic of Facebook is people over the age of 35 [1]. Among the many reasons of joining Facebook, the most important one is to get in touch with old and current friends and acquaintances. Facebook seems to be gradually moving the trend of communications away from the more traditional ways of telephone and email toward the internet and cyberspace.

One particular aspect of Facebook that appears to have literally hooked millions of people onto its website is the games galore that third party developers have created. Developers like Zynga have made use of the Facebook Developer Platform to create highly-addictive games such as Mafia Wars, Farmville, Texas HoldEm Poker etc. which have a fan-following in the millions [28]. As with the advent of any new technology/entertainment avenue, Facebook games are under fire from various directions for allegedly taking advantage of users through online scams. Most of these scams involve a wide variety of “offers” that users unknowingly sign up for in-game benefits in return for advancing through different levels in the game. What the users don’t know however is that these “offers” are very deceiving by nature since they can get them to pay for services which they didn’t intend to sign up for. Additionally, users cannot really differentiate between the illegal ads versus the authentic ones since the scams usually outnumber the legitimate ads. Users of these games are often unknowingly led into this vicious marketing strategy called “lead-gen” [20], which pays for itself and serves the purpose of unscrupulous businesses which make money off of millions of people.

Other discreet issues that have surfaced following this latest fad of Facebook gaming are Privacy and Identity Theft. Users engaging in these online games sometimes naively give out a lot of personal information to third party developers, which can run the risk of falling into the wrong hands. In the words of New York Times reporter Brad Stone, “even the crooks are on social networks now — because millions of tightly connected potential victims are just waiting for them there” [2]. Facebook handles massive amounts of personal data that can be very beneficial to online predators and hackers, and using these third party applications increases the risk of this data being accessible by not too friendly people.

In this IQP report, the focus is on this latest trend of online gaming and how it can actually be a disaster in disguise for the people who indulge in this trend. Great emphasis is given on two particular Facebook games that have the majority of users: Mafia Wars and Farmville. These games will be analyzed in detail, in terms of the game play, their social impact on the users, the economic motives behind these games, and their effect on Facebook as a leading social networking website.

1. Background

1.1 Problem Statement

Ever since the advent of Facebook, several adverse issues relating to privacy concerns and other unsettling issues have been cropping up frequently. Most of the problems seem to be revolving around privacy concerns and identity theft. Since Facebook has enormous numbers of users and massive amounts of data stored on their servers, it is hard to ignore the security threats that it faces constantly. Even though a lot of research and measures have been taken regarding this very concern, not a lot has been done with Facebook games. Contrary to this, some suggest that the massive user-base of Facebook games indicates that most people are benefitting from it. However, this claim can be refuted since Facebook games are relatively new and have recently been under intense scrutiny for scandalous activity. The motives intended to fulfill through this project are to analyze this recently developed Facebook gaming environment, enlist any issues or negative attributes it might have and provide possible suggestions for users to stay safe whilst entertaining themselves online.

1.2 Social Network Sites

A social networking site (SNS) is an online community where users can create a public or semi-public profile within a secure framework and share it with other users who have similar profiles. This mainly allows users to better manage their social networks in one place, gain information and also share their major life events in a private and secure manner. Since the inception of the online social networking phenomenon, websites such as MySpace, Facebook and Orkut have been on the forefront of it all, attracting millions of internet users. Most users of social networking sites login on a daily basis, with Facebook specifically claiming, “50% of our active users log on to Facebook in any given day” [1].

SNSs allow users to connect with both friends and strangers alike, and it is up to the users how much information they want to share. This results in ties that will not be made otherwise. It becomes very beneficial in a closely bounded system like college or workplace, where individuals may decide to be ‘friends’ with individuals pertaining to the same system. Even though SNSs are a decent means to meet and interact with new people, a lot of users just want to keep in touch with the people they know and take advantage of the resources that the website has to offer [3].

The technical features employed by different SNSs play a major role in attracting users. Almost all SNSs have a ‘Profile’ page where users put information about themselves. The profile page interface varies from one site to another and usually comprises of similar features that follow a general guideline. Users have the option of making their profile as private as possible, and can also control it to display all information to a particular group of friends, and hide some from another group. Boyd and Ellison emphasize this characteristic of SNSs when they write that, “structural variations around visibility and access are one of the primary ways that SNSs differentiate themselves from each other” [4].

Facebook is the first social networking site to take a different approach to when users create a Facebook profile. Upon creating a profile, users have the privilege to access and view other users' profiles provided that they belong to the same network. When a new user tries to join Facebook, he or she is prompted to answer some questions, which typically comprises of questions revolving around personal attributes of the user like age, sex and location, and the profile is created using the answers to these questions. This information is displayed in the "Info" section of the 'Profile'. Like most SNSs, Facebook also encourages users to upload pictures of them and the users have the liberty to share the pictures with whoever they want.

1.3 Facebook: An Overview

Mark Zuckerberg founded Facebook in February 2004, while studying Computer Science at Harvard University [5]. Facebook was originally known as "The Facebook" and the name was taken from sheets of paper that Zuckerberg distributed among freshmen students and staff to profile them. With the introduction of Facebook, Zuckerberg's initial crude profiling network experienced enormous popularity, and within a month, half of Harvard's population had a profile of their own.

The network started to spread among other universities in the Boston area, the Ivy League schools and finally to other US Universities. In August 2005, Zuckerberg purchased the domain name Facebook.com, as it is known today, for \$200,000 [5]. In September 2005, it was opened to US high schools and in a short period of time the networking site was being used by students in other countries as well [5].

Facebook quickly established itself as "a social utility that helps people communicate more efficiently with their friends, family and coworkers" [1]. It focused all its efforts into creating technologies that enable users from all walks of life share information more efficiently, thereby creating a "digital map of people's real-world social connections"[1]. According to the Statistics on Facebook's website, "it is the second most-trafficked PHP (hypertext preprocessor) site in the world, and one of the largest MySQL installations anywhere, running thousands of databases" [1]. While empowering its members with sharing tools, Facebook has also pioneered in providing its users with a set of privacy controls that can be used to efficiently control the amount of information being shared.

Facebook has recently shown as having a greater global presence with the exponential growth in the number of users. Headquartered in Palo Alto, Calif., Facebook has offices in various cities both locally and globally. Along with its users, Facebook has also seen a steady growth in its employees, with just a little more than a 1000 people on its pay rolls today [1]. One of the reasons behind Facebook's explosive growth can be interpreted through the introduction of the Facebook Platform application, which invited developers from all over the world to develop various applications for the ever growing user population. In May 2007, Facebook CEO Mark Zuckerberg unveiled the Facebook Platform "calling on all developers to build the next-generation of applications with a deep integration into Facebook, distributed across its "social graph" and an opportunity to build new businesses" [6]. This essentially gave developers a medium to start innovating applications that were efficient, competitive and useful, thereby

increasing the usefulness factor of Facebook beyond just traditional social networking. The inception of the Facebook Platform made it relatively easier for developers to create applications for Facebook and also provided users with simple applications such as online games etcetera.

With an estimated 400 million plus users [1], Facebook definitely has wonderful features that serve to enhance every user's experience over the internet in terms of staying in touch with friends and relatives all over the world. In a very short time, it has become a trusted resource for both young and old users to share their lives with their beloved ones. Only a few years ago, before the advent of communication tools like instant messaging (IM), it was considered almost impossible to maintain cross border friendships and acquaintances, especially in the eyes of the majority. An exception to this statement however were the people who were avid writers and communicated through hand written letters going back and forth between states and countries; but nonetheless Facebook provided the break through.

Facebook countered all odds and revolutionized the way people communicated. It gave users the option of status updates, which weren't anything extra-ordinary, but the idea behind it gave the world a new means of communication and sharing. Facebook's innovations in the world of communication were the sharing of photos, videos, short text messages (wall posts), internet links, and even "pokes", which was Facebook's way of saying "Hi!" to friends. Each of these features is in itself a powerful resource that can aid people to keep in touch. Throughout its history, Facebook has been changing and evolving with its users, which makes it all the more versatile and never outdated.

In the year 2008, Facebook significantly added to its arsenal by starting its own IM option, which allowed users to talk to their friends in real time while pursuing their favorite activities on the Facebook website [34]. As Facebook developers accept it too, they did not create anything new by introducing the IM service into Facebook. All they did was to provide it as a feature in Facebook, so that users didn't have to switch between their Facebook page and their IM window, to talk with their friends. This made it convenient for users and also made sure more users were spending more time on Facebook for communicating with friends and family.

With the Facebook status feature, users could write short text messages stating what they were doing at the precise moment, or how their day went, or even what they feel like doing next. All that the Facebook administrators had to do was to create a simple yet ingenious way to make users update their statuses and they did just that by asking a naïve question; "What's on your mind?" Answering a question posed forth is essentially part of human tendency and this tendency manifested itself through the small status box that became the first thing a user comes across on as soon as they login to their Facebook account. It gave users a window to vent their frustrations, share their joys or sorrows, their moods and thoughts; it was everything that made users get further connected with their friends and relatives.

Amongst many other ways Facebook has proved its worth is the ability to create and post photo albums. Nothing can replace seeing your friends and family visually and Facebook tapped into exactly this resource to further strengthen their already internationally acclaimed social networking site. Facebook allows its members to create unlimited photo albums on the site, with each album consisting of a maximum of 200 photos. These photos enhance the communication experience by making available a large storage space for all of a user's photos that the user can share with anyone they desire. Facebook makes available for its users various privacy settings

that can be put in place to restrict and allow the viewing of a user's photos to certain people, which makes this feature all the more popular. According to Facebook, its more than 400 million users post 3 billion photos each day, which shows how important users think this feature is and how it is bringing friends and relatives closer to each other [1].

However, most human inventions tend to be a package deal, which come with both good and dark sides. To upset all the good Facebook has done to the world, there inarguably are a lot of unfavorable aspects to it. The widely spoken about concern is with regards to a user's privacy. Even after Facebook's attempts to provide users with the most powerful tools available to protect their privacy and identity online, there are inadvertently ways that hackers and scammers can use to cause havoc in a peaceful world of sharing. Nothing has signaled more red flags on Facebook than the games and other applications that acquire users' personal data to function. All the data that these applications require is directly transmitted to the developers behind these apps, who can scarcely be entrusted with this sensitive data. Not many applications come with a clear-cut privacy policy, and most applications are very ambiguous about the way they use this data. A blogger on the website "All about Identity" quotes Jay Stanley of the American Civil Liberties Union as saying,

It really is the Wild West out there on the internet. The concern here is when you take a Facebook quiz; it exposes not only a lot of your own personal information that's on your site to the sponsor of the quiz, but also your friends' information [13].

The blogger goes on to say that, "Access (to the personal information) is granted by simply clicking that allow key to download third party applications. Your profile stats, posts, pictures, all in the hands of people you don't know" [13].

The American Civil Liberties Union went to the extent of actually developing a Facebook quiz that shows people how much is at stake, as they answer through a seemingly innocent Facebook quiz. They started a Facebook fan page called "What do Quizzes Really Know about You" to create an awareness about this very serious yet not well known online phenomenon. Their campaigning motto is,

Facebook quizzes seem innocent enough. But did you know that when you or even your friend takes a quiz, by default that quiz has access to most of your personal information? Take our quiz and peek behind the scenes!" [13]

The following figure is a screenshot of the quiz developed by ACLU, which shows what data can be sent to the developers of an application or quiz on Facebook. The data could include anything from display picture, to favorite books, activities, date of birth, email address etcetera.

facebook Home Profile Friends Inbox Kristen Wachenfeld Settings Logout

QUESTION 1: When you take a quiz on Facebook, what can the quiz see about you?

- Only your answers to its questions.
- Only information that is set as "public" on your profile.
- Almost everything on your profile, even if you use privacy settings to limit access.**

Correct!

Even if you have your profile information and content set to "private," quizzes can see almost everything that you share with your friends on Facebook: your politics and religion, embarrassing photos, comments you leave on your friends' Wall. It doesn't seem like a quiz developer has any reason to poke around in your profile, but it's temptingly easy to do so.

For example, here are just a few things this quiz can see in your profile:

Group: Petition to cure AIDS, ...

of Wall Posts: 2

Favorite Books: The Great Gatsby, The Vagina ...

Activities: Hiking, Swimming, Sailing all by myself ...

Hometown: Worcester, Massachusetts



Showing examples of data being transmitted from a user's profile. In this instance, it is data from the user's friend's profile

Figure 1: Personal Data Transmission

As if this issue with personal information being shared with third party developers was not enough, Facebook had to face even bigger allegations relating to the games on their site. On October 31st, 2009, in a shocking revelation, Tech Crunch founder and co-editor Michael Arrington wrote an article on his website titled “Scamville: The Social Gaming Ecosystem Of Hell” in which he shook the very foundations of the social networking gaming industry [31]. He faithfully articulated in his article exactly how most of these big name game creators like Zynga on Facebook and other SNSs actually make their money, and essentially exposed the dark side of Facebook games to the world. Arrington proved that most of the games on Facebook are infested with scams that unconsciously have a gamer divulge important contact information such as cell phone numbers etc. to offer providers who then use this information as leverage through charging gamers with uncalled-for monthly subscriptions. Arrington also directly confronted the big bosses of the online gaming industry, the most consequential being the confrontation of Anu Shukla, CEO of Offerpal Media at the Virtual Goods Summit on 24th October, 2009 [35]. Shukla, who used very crude language while blatantly denying any involvement in this dirty business, had to eventually pay for this rather immature behavior when she was replaced soon after this incident. This single incident goes a long way into showing that Facebook games aren't as innocent as they seem and that the end users are paying a price at the expense of transforming startup companies like Zynga into multibillionaires in a very short span of time.

1.4 The Facebook Platform

Facebook developed the Facebook Developer platform in May 2007, which provides a framework for third party developers to create applications which are compatible with all other Facebook features [9]. As of November 21, 2009, there are approximately 58000 applications with over 200,000 developers evaluating the platform [9]. All Facebook figures and analytics mentioned in this section were accessed through Adonomics, a Facebook analytics service owned by Monterey, Calif., venture-capital firm Altura Ventures LLC. This service helps developers and investors to keep tabs on the growth, activity and value of all the applications present on Facebook.

An individual who is interested in launching their own application has to use Facebook's Application Programming Interface (API) servers to interact with the application server. This provides Facebook with the option of protecting its members from malicious content that could possibly have embedded itself in the data from the application servers. Facebook has the ultimate control over what information and or data is being transmitted through applications, which is a necessary security precaution aimed at protecting users.

The Facebook Platform comprises of six main components; API, FBML (Facebook Markup Language), XFBML (an extension to FBML), FQL (Facebook Query Language), and FBJS (Facebook Javascript) [9]. These constituents of the platform allow developers to create applications that users could use or share within the network. A summarized description of each of these components follows:

- The Facebook API enables developers to add social context to the intended application by using data from various sections of Facebook. The API uses a REST (Representational State Transfer)-like interface. Thus, Facebook method calls get transmitted by sending HTTP GET or POST requests to the master Facebook API server, Facebook API REST server. Almost any computer programming language could be used for communication with the REST server [6].
- The FBML, an evolved subset of HTML, enables developers to build applications using the platform [6].
- After using SQL for database management, Facebook administrators decided to come up with their own version of a query language, which they called the FQL. This query language allows developers to use a SQL-style interface but specific to Facebook. Since Facebook databases store massive amounts of data, administrators thought a better way to query Facebook data would be through FQL that would also account for access of queries through other Facebook API methods [6].
- And finally, the FBJS allow developers to implement JavaScript in their applications, if needed.

All in all, Facebook Platform is a holistic approach to developing applications, keeping in mind the specific needs of Facebook users.

1.5 Individual Facebook Features Explained

Facebook is expanding rapidly and with every passing month, it comes out with another new feature to add to its ever-growing features list. Based on the Facebook Statistics webpage [1], the core features of Facebook as of December 2009, are summarized in the next sub section.

1.5.1 Primary Facebook Features

1.5.1.1 Networks

Facebook is a membership based social networking website that revolves around networks. Each user can opt to stay in one regional network and several school, college or workplace networks. A user can view most of the profiles in their same networks and join most groups in those particular networks. Networks are a good feature of Facebook since they allow more sharing of information inside a particular network but not outside of it.

1.5.1.2 Profile

The profile page is the main source of information for each person. A user's display picture along with all of their personal information is listed on the profile page including but not limited to their name, age, sex, political views, religious views, education info, work info, interests etc. In addition to this information, clicking on different tabs in a profile lead to different pages of the website, related to the user who profile is being viewed.

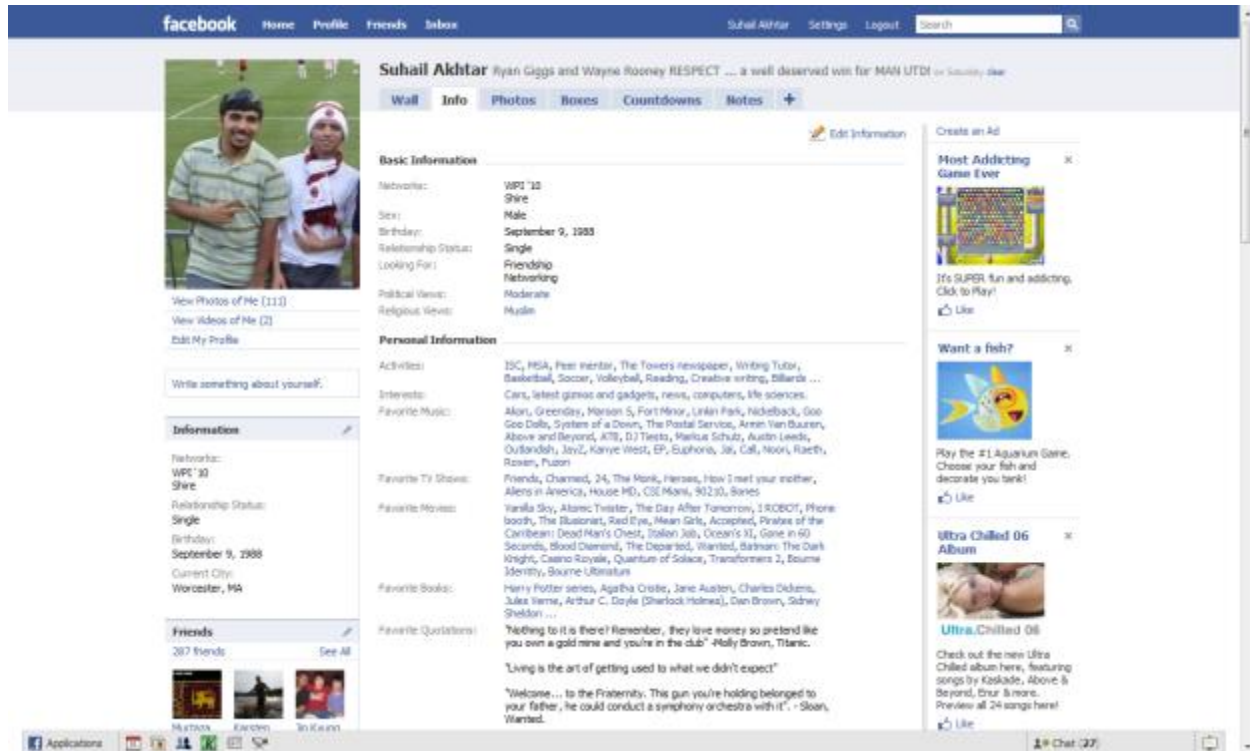


Figure 2: Profile

1.5.1.3 Friends

When logged into Facebook, users can find out about their friends by going onto the Friends page. Here they can find all of their friends, update friend details, assign friends to different groups, and also go to a specific friend's profile page by just clicking on the friend's name or picture.

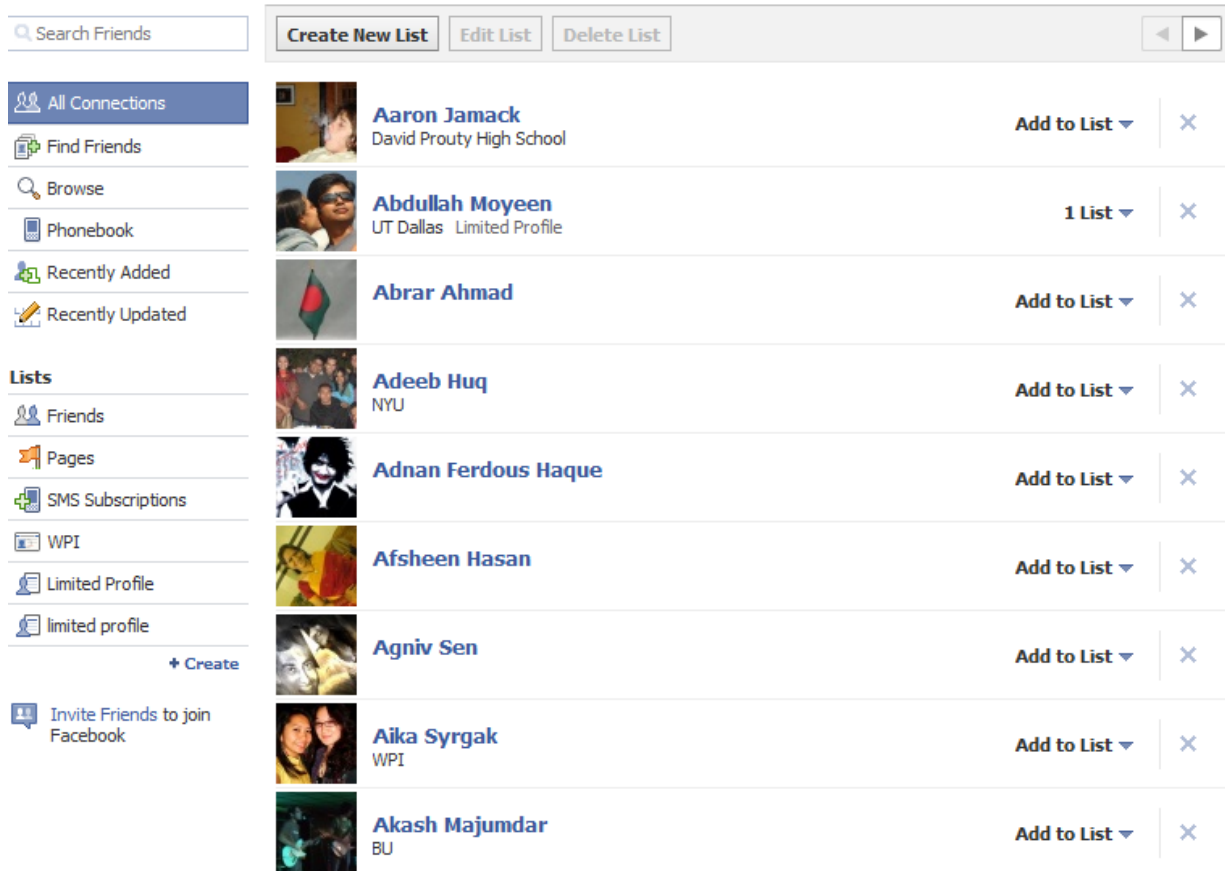


Figure 3: Friends

1.5.1.4 Inbox

Facebook provides its users with the means to communicate privately through text messages. In this feature, users have an inbox just like any email inbox where they can receive private messages from any of their friends or strangers (should their privacy settings allow it). A message can be sent to multiple recipients whereby each user can view the message sent to the whole group and can reply-all to the recipients. This feature is also commonly used to send out mass messages about event updates, group updates etc.

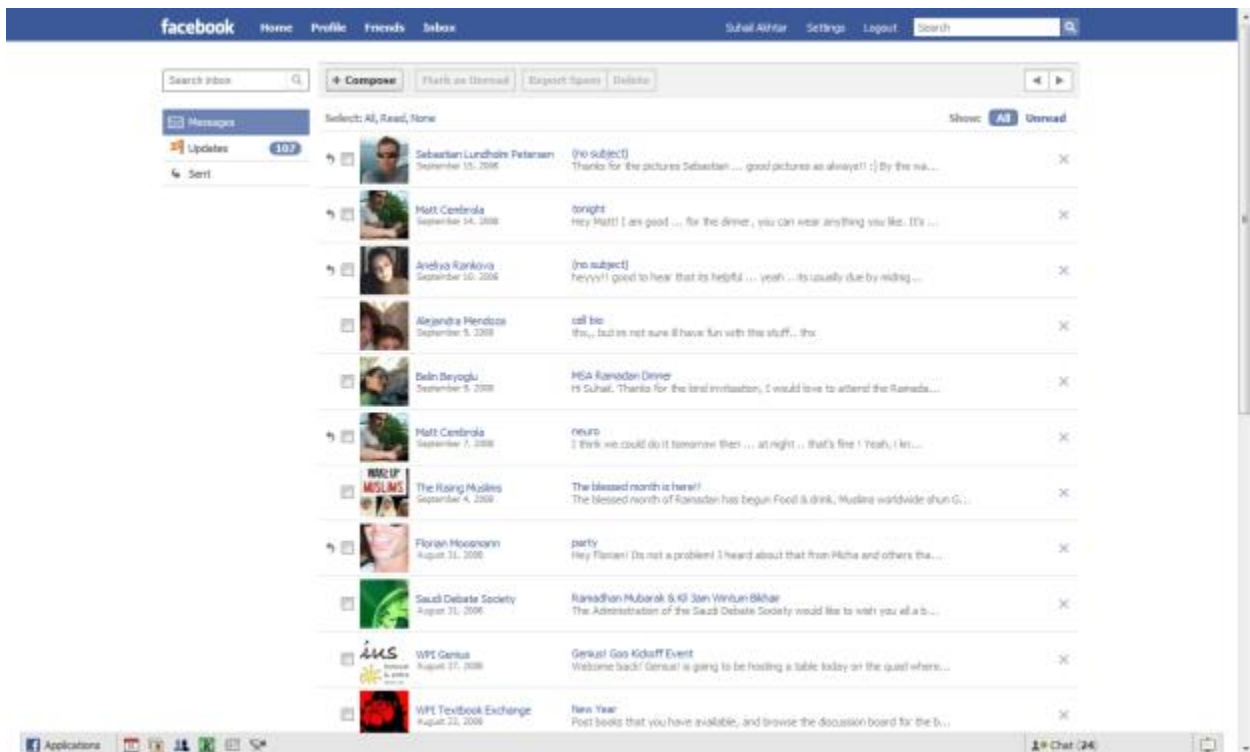


Figure 4: Messages Inbox

1.5.1.5 Facebook Chat

In April 2008, Facebook provided its users with the luxury of “real-time” conversations. Facebook started the “Facebook chat” feature that allowed users to take advantage of an IM-like feature embedded in the website that could be used to chat with any of their friends when they were simultaneously online. This revolutionized the way people communicated on Facebook since now instead of waiting for a reply to a previous wall post, users could just go online on Facebook chat and send instant messages to their friends. This feature didn’t really do away with Wall posts or private messages, rather it just complemented them and made Facebook a powerful source of communication, both in real-time and offline.



Figure 5: Facebook chat (IM)

1.5.1.6 Pages

Facebook Pages are an innovative way for businesses, artists, brand stores, and many different organizations to market themselves to the 300 million or so users of Facebook. This can be done at no extra charge, and any registered Facebook user can make a Facebook page. Like the example showed in Figure 6, pages of musicians and artists have a fan-following in the millions. Certain TV shows also have their pages through which they disperse important information about the show plot, show timings etc. Fans of a particular page can share information on that page with all of their friends, thereby spreading the word and marketing the product even further.



Figure 6: Profile Page of Britney Spears

1.5.1.7 Facebook Ads

A significant amount of advertising is done through Facebook nowadays and this advertising is built around the following parameters: the location of users, keywords pulled out from a users' profile, their connections, their relationship status, their age, their birthday, education qualifications, their gender, and workplace and even the language they speak. This is known as targeted advertising that targets specific groups of people with relevant products. This feature can also be used by everyday Facebook users at a nominal charge to advertise any cause/event that they might want to spread the word [7].



Figure 7: Facebook Ads

1.5.1.8 Privacy Controls

Since Facebook revolves around personal data of millions of people, privacy concerns are an obvious cause of worry for many. For this precise reason, Facebook has built in various levels of privacy settings that users can adopt to share information with only the people they choose to. As seen in figure 8, users can choose who sees what on their profile pages, their photos etc. Users can control what goes up on their News Feed (explained later on), and what information is available to Facebook applications (also explained later). Users can also block other users if they find it necessary, and this makes them completely invisible to the blocked person.

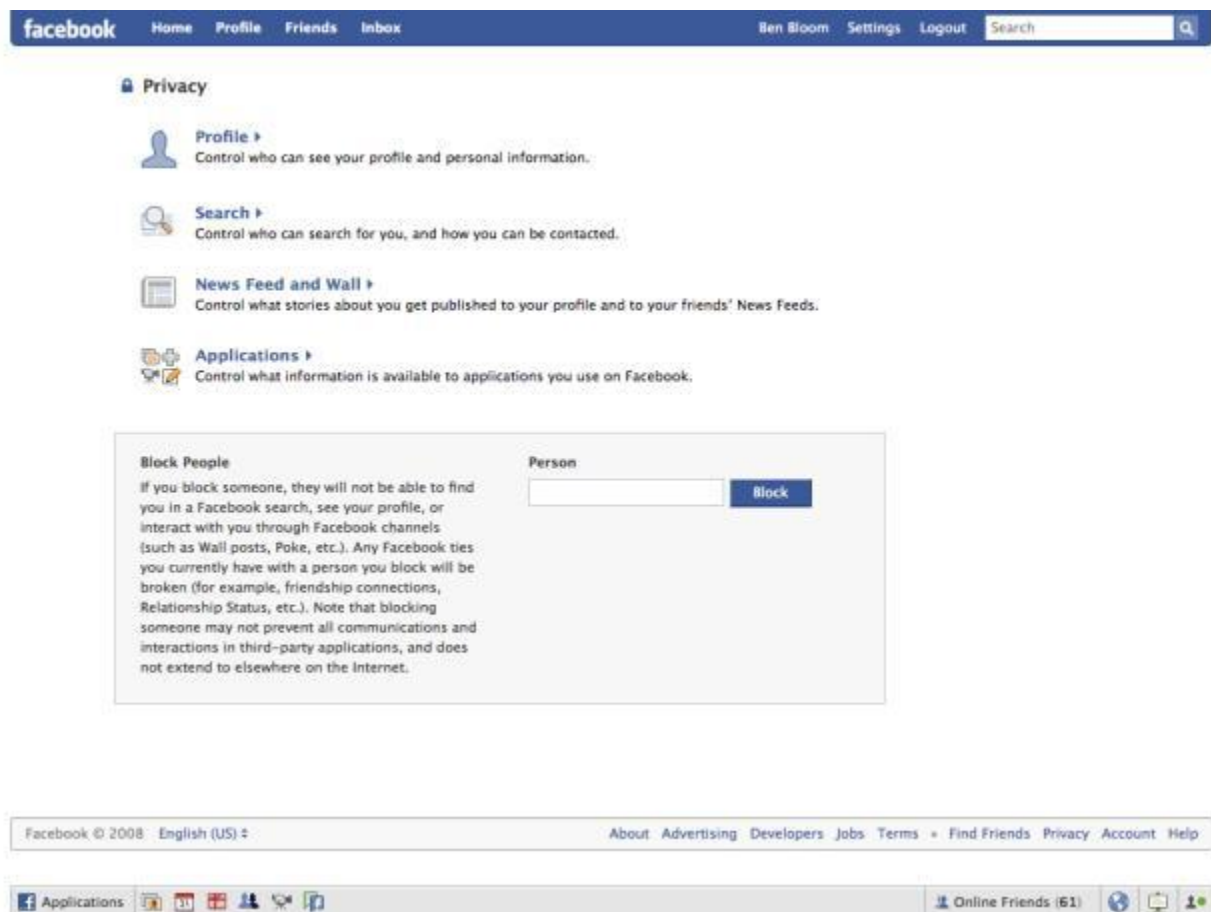


Figure 8: A screenshot of privacy controls

1.5.2 Secondary Facebook Features

1.5.2.1 News Feed

As the name suggests, the News Feed is a running commentary of the activities of users' friends' on Facebook. For example, if a user's friend uploads new pictures of their recent road trip, the user will be notified of this with a story appearing in the News Feed. Likewise, users' status updates and other links that they might post to their profile will also be displayed in the friends' News Feeds.



Figure 9: News feed

1.5.2.2 Wall

Each Facebook profile comes with a default “wall”. It is that area of a profile page where friends can write messages, post links, notes, events etcetera. Users are in complete control of the wall, as they can delete any post, block specific people from viewing the wall or writing on it, or completely make it invisible by adjusting the Privacy settings.



Figure 10: The wall

1.5.2.3 Share

Facebook has a unique way of sharing information across different websites and internally on Facebook’s site. On many partner websites such as cbs.com, cnn.com, nytimes.com etcetera, after most articles is a “share on Facebook” button that patrons can click on, to share the article with their friends on Facebook. Clicking on that link will publish the item on the user’s profile page and also on their friends’ new feeds.



Figure 11: Facebook Share icon on CNN's website [38]

1.5.2.4 Public Search Listing

Facebook has a built-in search engine that is currently based on SQL database servers. Users can search for other users on Facebook and can see specific information based on the individual privacy settings. At most, a user can see a profile picture and the name of the person searched for. A non-logged in user can see only the bare minimum information of a Facebook user which is termed a “public search listing”.

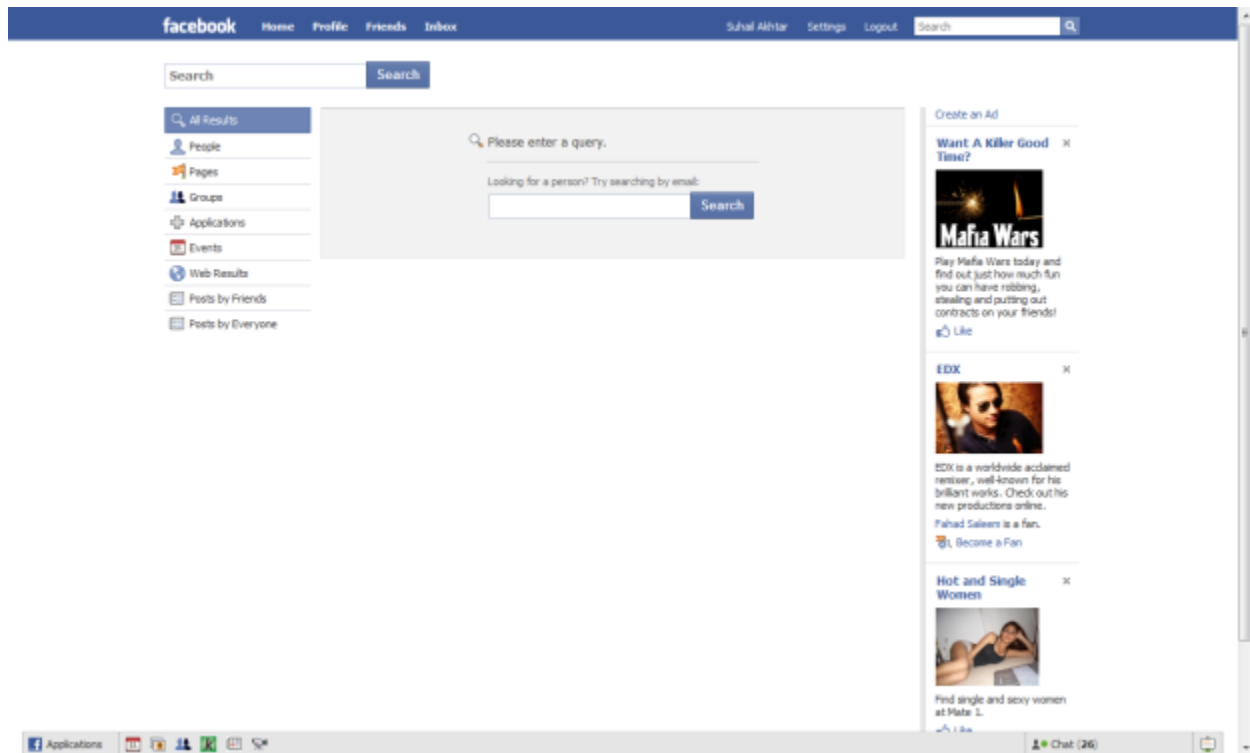


Figure 12: Facebook Search

1.5.2.5 Photos

This is unarguably one of the most popular features Facebook offers to its users and it is also one of the most used features. Users can create unlimited photo albums, each having a maximum of 200 photos. They can add captions to each photo, rotate photos while uploading and also tag their friends in the photo. Once a photo is uploaded, it can be viewed by other users based on the privacy settings of the album. Each album can have a different privacy setting which allows users the flexibility to share certain albums with only certain people or with everyone on Facebook.

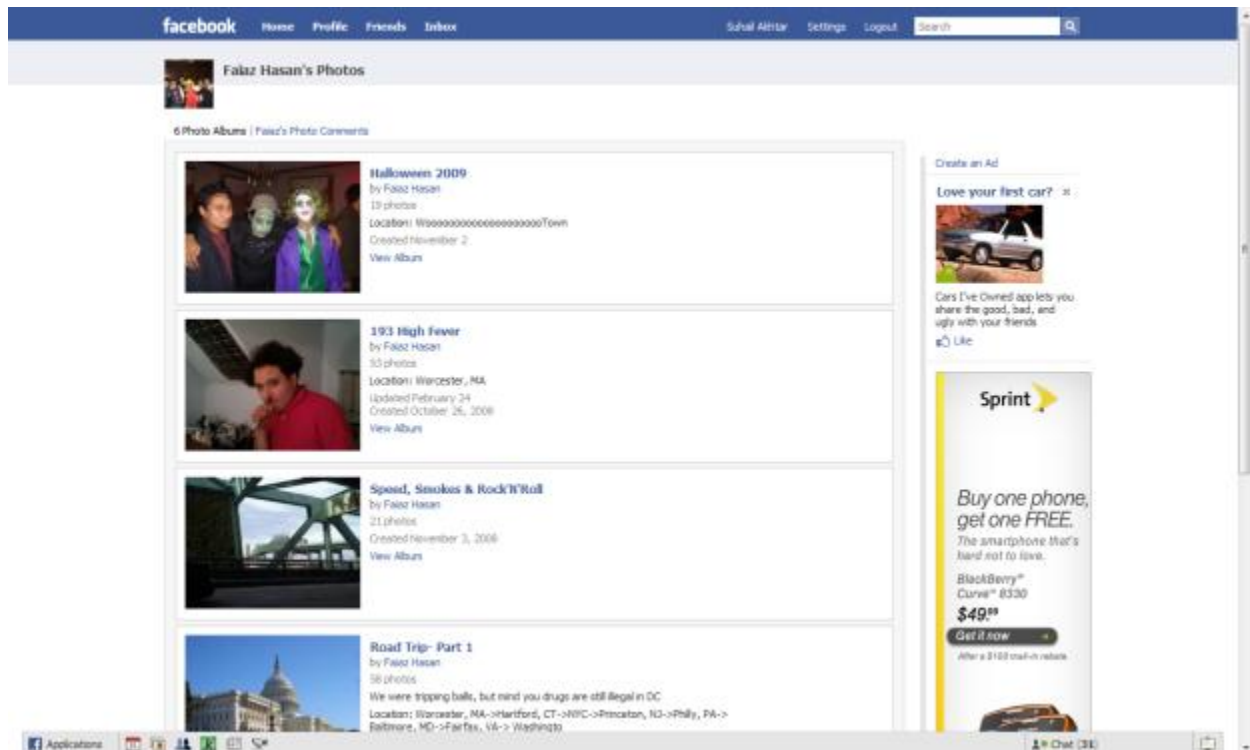


Figure 13: Photo Albums

1.5.2.6 Notes

Facebook gives users an option to express themselves even more through writing. This can be done through the Notes feature, which allows users to blog about anything with unlimited words. They can also tag their friends or post pictures along with the note. Users also have the option of importing an external blog onto their Facebook profiles through this feature.

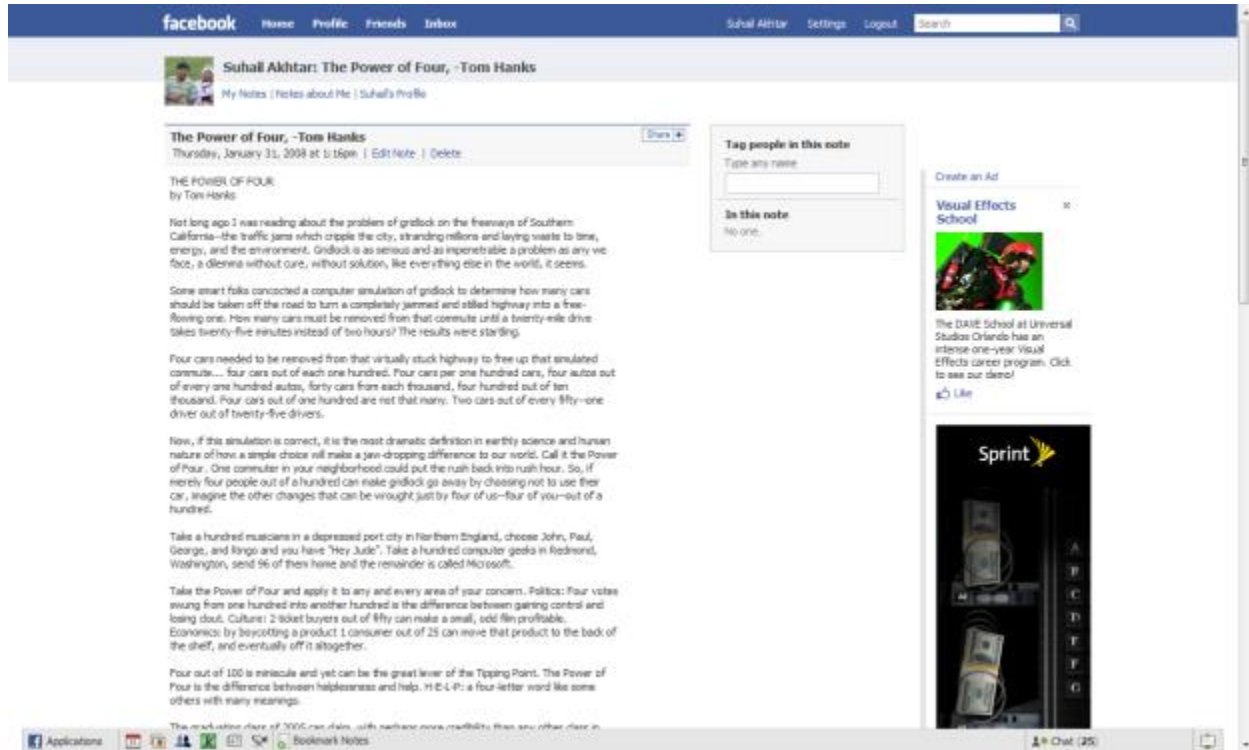


Figure 14: Notes

1.5.2.7 Groups

Facebook groups is another important feature of Facebook that lets users create a group page for their organization, favorite celebrity etc. and can then invite other users to become group members. Information can be shared on that particular topic by all members of the group.

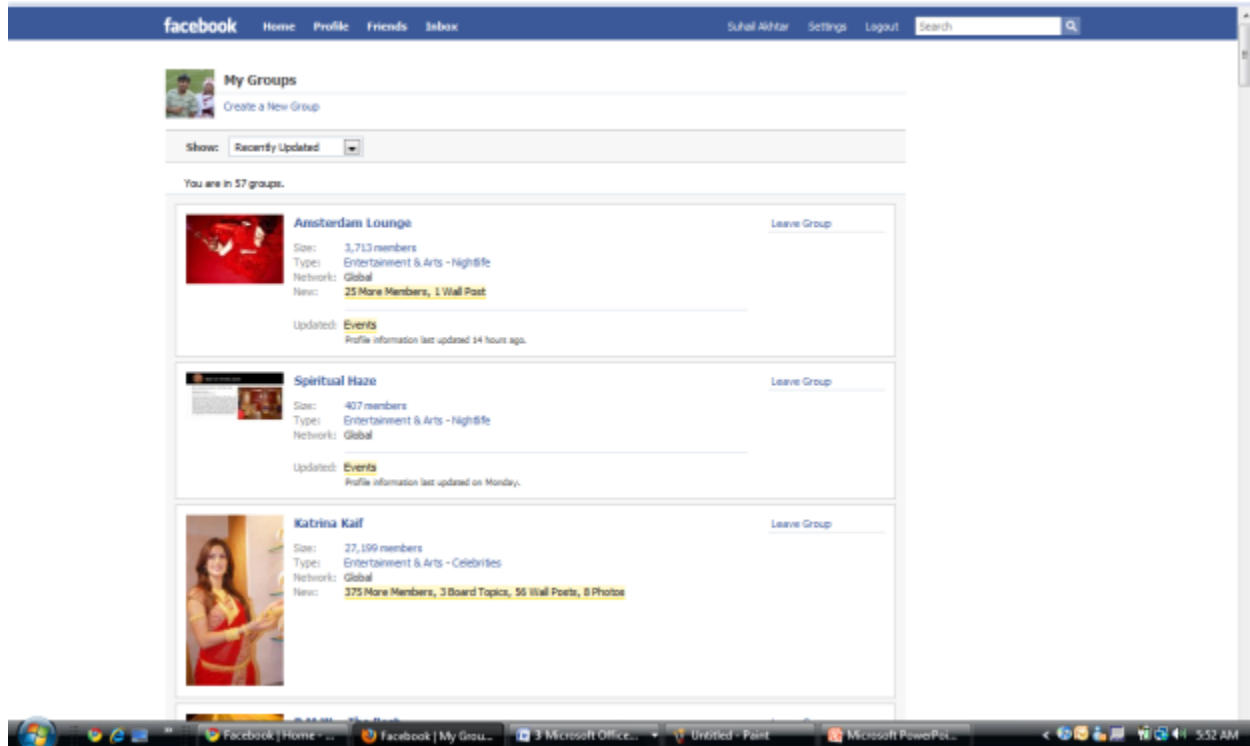


Figure 15: Groups

1.6 Facebook Applications

A Facebook application or app is a small program that could be added to the general Facebook interface to provide some additional functionality to a certain profile. Addition of Facebook apps is completely dependent on the user's choice and individuals have the preference to add what apps they want to add or not. Facebook apps allow users to customize their profile pages and that is the sole criteria of the apps that make it popular.

In May 2007, Facebook started inviting software developers to create free software programs that users of Facebook could install on their profile for entertainment. More than 250,000 developers have actively engaged in creating applications on Facebook, resulting in the creation of the Facebook Platform in May 2007 [6]. Not only does the Facebook platform help developers create quality applications, but it also allows them to mass distribute their finished product. Mark Zuckerberg, the CEO of Facebook called this "mass distribution through the social graph", wherein he described the "social graph" as the network of real connections through which people communicate and share information [6]. What Zuckerberg meant was that the quality of information being shared is greatly enhanced since there is a genuine end user for any service offered through Facebook, as opposed to the traditional internet industry which built its services on an uncertain end user, who might or might not be interested in using the service. He also pointed out how existing Facebook applications "such as Photos, have grown to be leaders in their categories" due to the efficient and resourceful spreading of information through the well defined social graph [6].

Additionally, developers of Facebook applications now have the option of promoting their application as a business and thrive on it through advertising to make money. Zuckerberg said,

This is good for us if developers build great applications then they're providing a service to our users and strengthening the social graph. This is a big opportunity. We provide the integration and distribution and developers provide the applications. We help users share more information and together we benefit [6].

Apart from mainstream applications like virtual gifts, movie picks, and games, large companies and brands have established their presence on Facebook recently, discovering the marketing potential it holds. Big name brands like Target, Apple Computers, Audi, Calvin Klein etcetera have fan pages on Facebook with hundreds of thousands of fans on each page. These brands constantly advertise their sales events, special deals, discounts etcetera to their fans through the fan page or other applications, thereby making the best use of the social graph [11]. According to Adonomics, 74 Facebook applications have a market value of more than \$1 million each. This clearly betrays the economical incentives behind Facebook applications and immediate surge of developers putting in efforts to come up with the best applications for Facebook.

1.7 Facebook Games

Games on Facebook, fomented on by amalgamating social networks and free-to-play games that psychologically persuade users to play games with their friends and family, in laconic terms, are huge money generating schemes. Users' interest and involvement with Facebook, have caused games to spread like a virus, and being extremely innovative and a pundit at persuading users, almost all Facebook games reward users for spreading the virus. The incentive of rewards, which is required to proceed forth in all games, is the sole reason for epidemic of such games.

The main purpose for any service based merchants is to generate as much money as possible, and the developers of SNSs games are no different. These SNSs and developers earn money in two primary ways: micro transactions and advertising [12].

Micro transactions, a form of micropayment, refer to the purchase of virtual goods available for sale in online games. Micropayments are just regular financial transactions, but the sum of money involved is really small [13]. Paypal defined it as monetary transactions of less than 12 USD. The goal of the micro transactions, as incorporated by Facebook Games, is to generate a small amount of money from each user, which eventually builds into a huge amount once the transactions from all the users are added up. This is only possible due to the presence of millions of active users participating in these games. For example, Farmville boasts participants in the range of approximately 70 million worldwide, and even if 20% of these people are being involved in spending an average of \$1 daily, then it still generates \$14 million a day. All these data are hypothetical, and is just used to show the lucrative profit that may easily be generated.

Advertisers on the other hand take a different approach to attract users. In micro transactions, method of trade is direct, whereas money generated through advertisements is entirely indirect. SocialAds, which act as targeted advertisements toward specific people based on personal information, appears on the right hand side of any Facebook screens. Even though it is against Facebook's ad terms of service to directly put in personal information into an ad, targeted ads through one's profile is allowed. Targeted advertisements have proven to be very effective for a particular website owner, as these advertisements pay the owner based on the number of people who visit their websites. And the fact that these advertisements are targeted makes it more likely for users to visit a website comprising of products/information/goods they may be interested in.

All sorts of games present on Facebook are competing against each other to get the number of users participating in the games. To attract users, developers follow a series of steps that make sure that users stay engaged. All the games on Facebook follow simple steps, which are described thoroughly in the next paragraphs.

The game play of each and every Facebook game is very simple. It does not involve a lot of thought or strategy. It mostly involves a series of clicks to go forward in the game and the player gets rewarded with something like points that the user needs to move forth in the game [12]. Easy game play creates little room for failure and thus encourages the user to play the game. It also makes sure that almost anyone could play the game, rather than gaming geeks, and may be done at any time to spend time.

Almost all games on Facebook have real time elements [12]. This prevents the users from reaching the end of the game quickly or finishing the game in one sitting. For example the game Mafia Wars requires players to have a certain amount of 'Pool of Energy' to advance in the game and after a certain number of activities, which are required by the user to fulfill to proceed in the game, the energy runs out. The player has to wait hours before the energy gets refilled. The only way the user could play and proceed in the game is by waiting for the energy to refill. This involves the user to log into Facebook almost every day or multiple times in the same day. This also allows the user to play the game in short spurts, and thus making sure it does not take too much time to play the game in one sitting.

The real time elements of Facebook games also play a major role psychologically to keep the user engaged. As the players cannot proceed forth in the game when they want to, it is likely that they feel an urge to advance faster than the game will let them. This is when Micro-transactions come to play. Users have the opportunity to buy more points, rewards, energy, etc with cash that may help them moving forward in the game without having to wait. These micro-transactions could be portrayed to the user directly or indirectly and somehow or the other gets players to spend money. If someone is inclined to pay money on game advantages directly, they may be lured by indirect ways. All games have commercial partners who will give players reward points in exchange of something simple like signing up for ringtones.

Facebook apps always use the entire social networks sites and somehow encourage the user to involve their friends. When a user and his friends are playing a game together, they can help each other out which would help them to advance forward. When friends are involved, users feel more compelled to play the games and they are more interested in the games as they are virtually communicating with people they know. This makes them feel that they are staying more connected with their friends and family. Some games directly ask users to involve their friends as they are required to proceed in the game.

1.8 Farmville

Farmville is the most popular game on Facebook. Like Mafia Wars, Farmville has also been developed by Zynga [14]. The game was launched in June 2009, and since its introduction, Farmville has become the most popular game on Facebook with approximately 64 million users as of November 2009 [14].

The basic concept of the game is to become an online farmer and farm virtual plots. Players can virtually grow everything from strawberries to cotton, raise animals such as cows and chickens and build farmhouses and fences. Once a user installs the Farmville application, they can see patches of land where they can start growing. The game involves a market where players can buy seeds, crops, animals, vehicles and land using “coins” and “cash”. Coins are the general currency used in Farmville, and a player can generate coins by selling crops. They can also earn cash at a rate of one dollar per experience level. A player plants seeds and once they grow into crops; he/she can sell it them to earn coins. By doing regular task like plowing, planting and harvesting, a player can earn “experience points”. Any player requires experience points to advance in the game and can unlock various items by increasing the number of experience points.

Farmville uses the social networking features of Facebook, and is one of the main reasons for its huge popularity. A player can set up their farm next to their friends’ farms or invite friends to join Farmville and be their neighbors. The player can visit his neighbor’s (friend’s) land and help with chores in that farm or just leave messages to talk to the friend. When friends are acquired as neighbors, it benefits the game play. A player can earn coins or experience points by helping the neighbors. A player has the option to send Gifts like crops or trees to neighbors or other friends who are not involved in the game.

Like other Facebook games, Farmville also incorporates real time elements. During the game play, a user has to wait for certain real hours in a day to harvest the crops they planted, thereby simulating some real life situations. For example a strawberry plant would grow in 4 hours whereas an eggplant would grow in 2 days [15]. Hence, to harvest a crop of strawberries, a player would have to wait for 4 hours, whereas for the eggplant, they would have to wait for 2 days or 48 hours. For players who feel the urge to progress without having to wait for hours, they can buy coins or cash from Zynga’s website or get bonuses after completing an offer from the advertisers.

Once a user takes the initiative to install Farmville as an application, Facebook directs him to a page that basically asks for the user’s permission to install Farmville as an application while briefly articulating the technicalities that would take place once Farmville is installed. The technicalities, as mentioned before, is just a term of agreement to which a user has to agree to in order to install the application, and basically states that once the application is installed it would access all personal information that is present in the user’s profile. All Facebook games thrive on user information to make the real time elements in every game more realistic to the user, and also provide a means to attract potential marketers to advertise using specific target products. Thus all Facebook games have this ‘Allow Access?’ term of agreement page, shown in Figure 16 below,

and is the first thing Facebook directs users to before anything related to the actual game could be accessed.

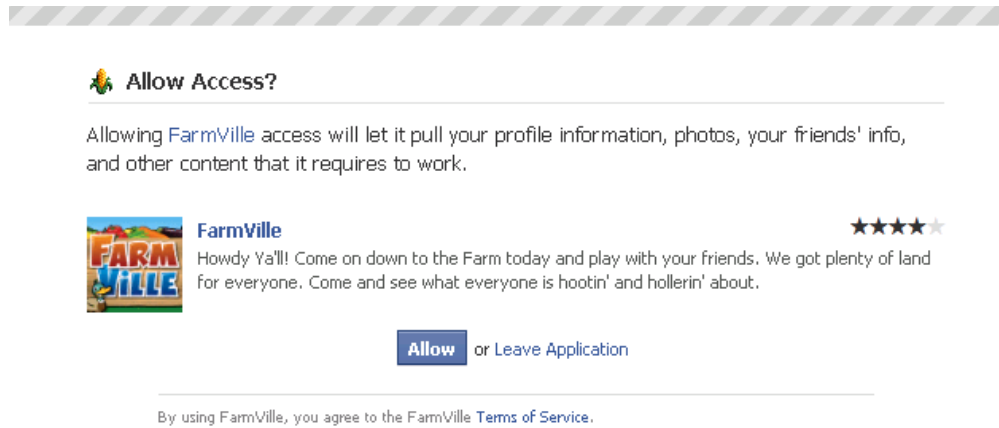


Figure 16: Disclaimer

Once a user concurs with the terms of agreement, the user is granted access to the game and from thereon he can start playing the game. Below is the screenshot of the Graphical User Interface of the game in Figure 17.

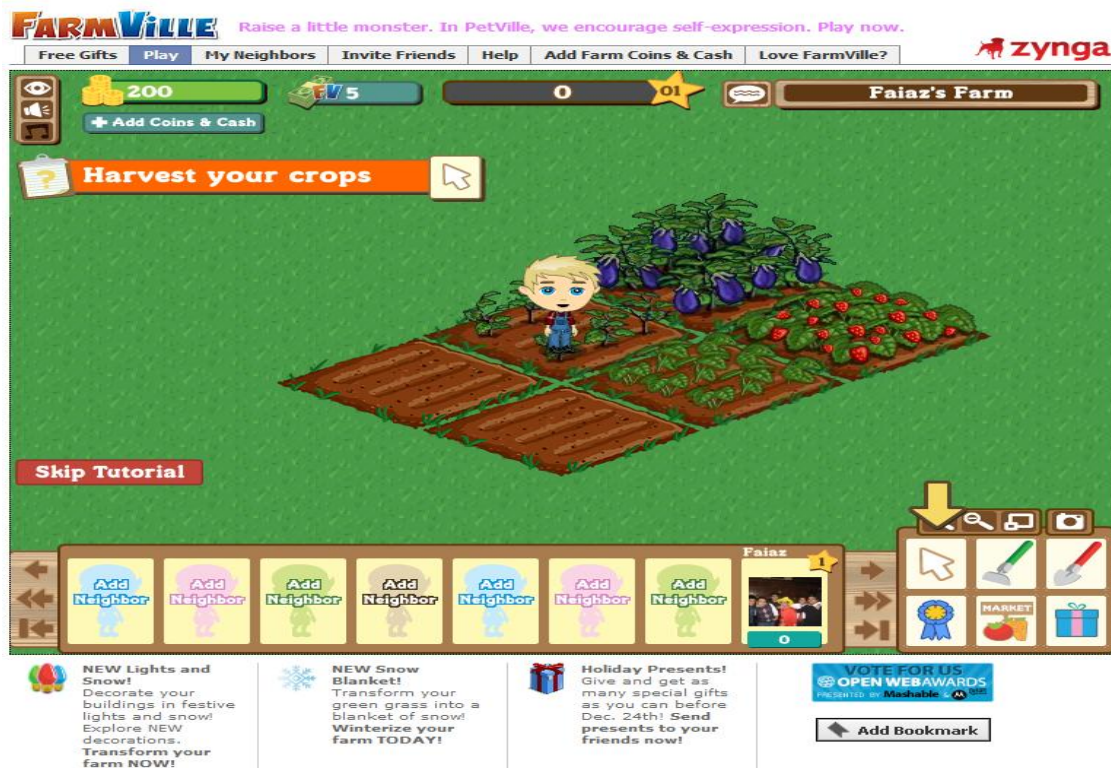


Figure 17: Play GUI

This is the first interface a user stumbles upon after installing the game. The game starts off with asking the user his/her gender and creates an avatar of the user based on character. Once the character is determined, Farmville offers a tutorial that guides users through the generic features and functions of the game.

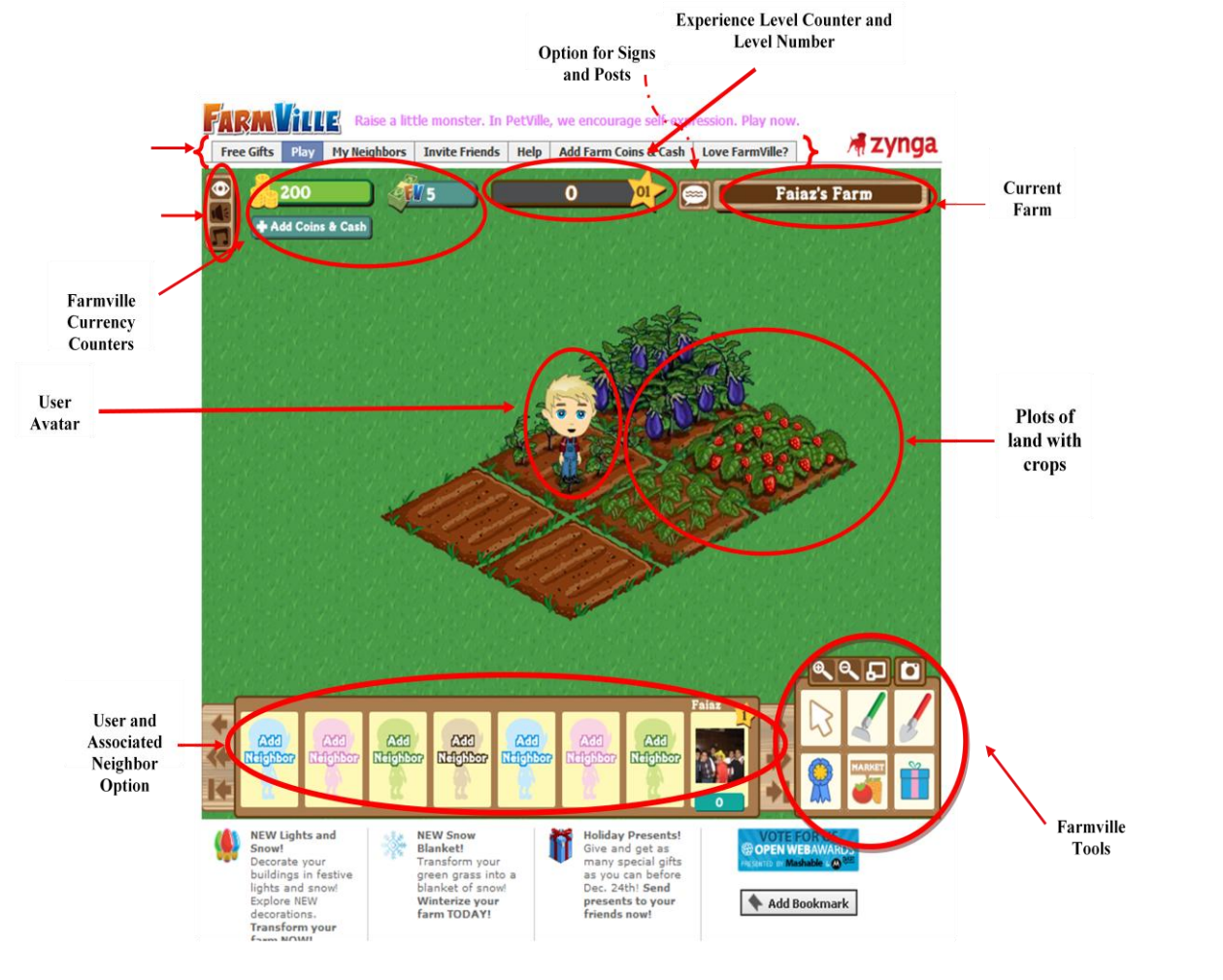


Figure 18: Farmville Features

The screenshot depicted in Figure 18 is used to explain the features and tools present in Farmville. At the top of the GUI screenshot, there is the Farmville currency counters. It basically keeps tracks of the virtual money that is being generated or used. As mentioned before there are two types of money: cash and coins. Coins are the general money which the user can either earn by selling crops or use to buy other objects for the farm.

Right next to the currency counter is the experience level counter and the level marker. The number inside the yellow star basically the current level the user is in. Once the player buys or sells properties or merchandize, the experience level increase by two points and once the experience level increase by twenty points, the player go to a new level. Completion of one level

and proceeding to a new level is dependent on the number of experience points earned and increase at increments of 20 experience points earned. The screenshot in Figure 18 is taken right at the beginning of the game and thus the experience points are zero and the level number is zero.

Right next to the experience point and level counter, there is a little sign which basically, when clicked, allows the user to leave signs and posts for other users or neighbors (friends having farms right next to the users farm) to see when he or she is not using Farmville.

In the screenshot above, there are virtual plots of lands, some of which are empty and some have crops in them. The user first plows these lands and then plants seeds in them. Once planted, the seeds take some time to grow into plants which can later be harvested to generate coins.

The options for plowing and buying seeds are present in the Farmville Tools Box. For a specific task, all the user has to do is move the cursor over any object present in the screen, and the anticipated task would show up telling the user what to do. The user then just clicks the mouse and the task takes place!

The user can choose the market icon present on Farmville Tools Box, and it would direct the user to the virtual market from where he can buy things for the market. Once planted, different seeds take different times to harvest and that adds real time elements to the game. Different plants in the market have different harvest times and the user has to literally wait for that long to harvest the virtual crops. This applies to all other products/merchandizes present in the market.



Figure 19: Mouse Click Functionality


Once clicked on the market tool (Figure 19), it directs the user to another page that displays the virtual market. The following screenshot shows the market, as it appears in Farmville.



Figure 20: Market


As seen in the screenshot (Figure 20), the market as a list of category of items available for purchase. Once clicked on one of those tabs, it displays the list of items available within that category. In the screenshot, it is currently showing all sorts of seeds that the user can choose to buy from. Under every single item, there is brief information on them. It shows the price of the seeds, the price at which the user can sell the fruits/crops for, necessary time for harvest and the level required to unlock the item (denoted as “XP Gained”). There is a next button that allows user to go to the next page to see more products for sale. There are many items that are locked and the only way a user can have access to them is by gaining experience and progressing forward in the game from one level to another.

Right next to the Farmville Tools Box, there is the list of the user and his friends, more commonly known as ‘neighbors’ in Farmville. As mentioned before, users can set their farms right next to their friends’ farms and be their neighbors or even invite their friends who are not on Farmville, to join Farmville and be their neighbors. This benefits the game play a lot and is always beneficial for the user in terms of generating experience points. Users can also go and help out on their friend’s farm to generate points. The screenshots below deals with the neighbor option on Farmville. One is for friends who are already on Farmville and the other is for inviting friends to Farmville as seen in Figures 21 and 22.


Aung

Aung is currently away and raccoons are ransacking his farm! Would you help scare them away?

[Go to Aung's farm](#)



You can have a lot more fun by visiting and helping your Neighbors. Ask your friends to be Neighbors below:


Shay Sarwar


[Send Gift](#)

[Add Shay as Neighbor](#)


Adeeb Hug


[Send Gift](#)

[Add Adeeb as Neighbor](#)


Cori Schollard

[Send Gift](#)

[Add Cori as Neighbor](#)



Tajwar Awal

[Send Gift](#)

[Add Tajwar as Neighbor](#)

Figure 21: Neighbors

FARMVILLE Head to FishVille – start your very own fish tank & fill it with cute baby fish!















Free Gifts Play My Neighbors **Invite Friends** Help Add Farm Coins & Cash Love FarmVille? 

Here are your friends who don't have FarmVille yet. Invite whoever you want -it's free! Skip

Add up to 60 of your friends by clicking on their pictures below.

Find Friends:

Filter Friends All Selected (0)

 Abrar Ahmad Bangladesh	 Adnan Ferdous Haque Bangladesh	 Agniv Sen Bangladesh	 Aika Syrgak WPI
 Akash Majumdar BU	 Akhil Kejriwal WPI	 Akif Rahim Iowa State	 Al-Hasanur Rahman Waterloo
 Albedith Diaz Dominican ...	 Alec Tolivaissa WPI	 Aleef Pasha Brunel	 Alexis Polack Clinton Se...
 Alia Kamal Duke	 Alihusain Yusuf Sirohiwala WPI	 Allison Holbrook University...	 Alsan Ali WPI
 Alyssa Vincent WPI	 Aman Verma RIT	 Amanda Kalish WPI	 Amani Mulk UCL

Invite by E-mail Address: Use commas to separate e-mails

Send FarmVille Invitation Skip

Figure 22: Invite Friends

Players also have to option to buy Farm Coins and Cash to buy more things for the farm. Unlike other elements of the game where users generate and collect money in virtual form, this option deals with real money. This is basically giving users, who might get impatient of waiting for plants to grow so that he can harvest them, the option to proceed in the game.

The screenshot below (Figure 23) shows the interface page the user is directed to once the tab for buying farm coins and cash is selected. It shows the products available for purchase and the method of payment. Users can also pay for these by other means, like downloading a ringtone and getting charged to their personal cell phone or home phone.

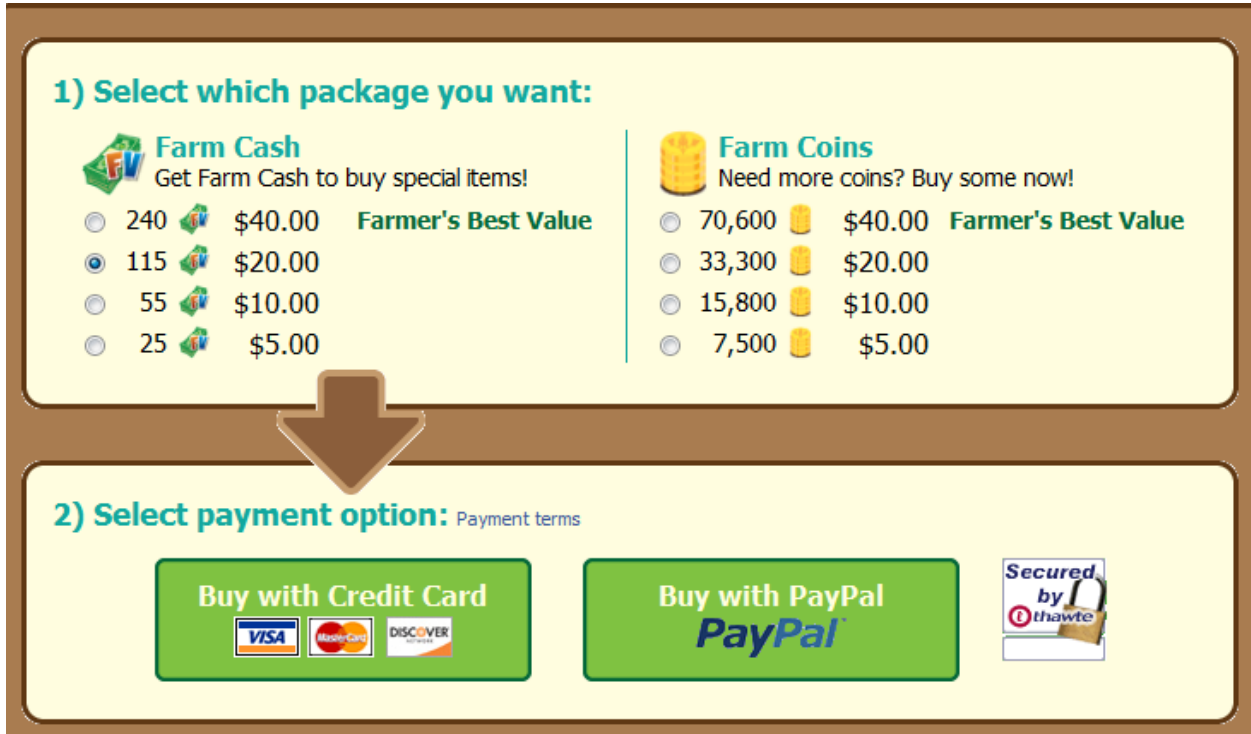


Figure 23: Add Farm Coins and Cash Option

On the right hand side of any Facebook page, there are ads from sponsors and merchants. The screenshot in Figure 24 shows the Social Ads on a Farmville page. These ads are examples of targeted marketing, and specific ads are from merchants who might attract the user, or just simply catch their attention. User choices presented in these ads is gathered from the personal information enlisted in the user's Facebook profile.

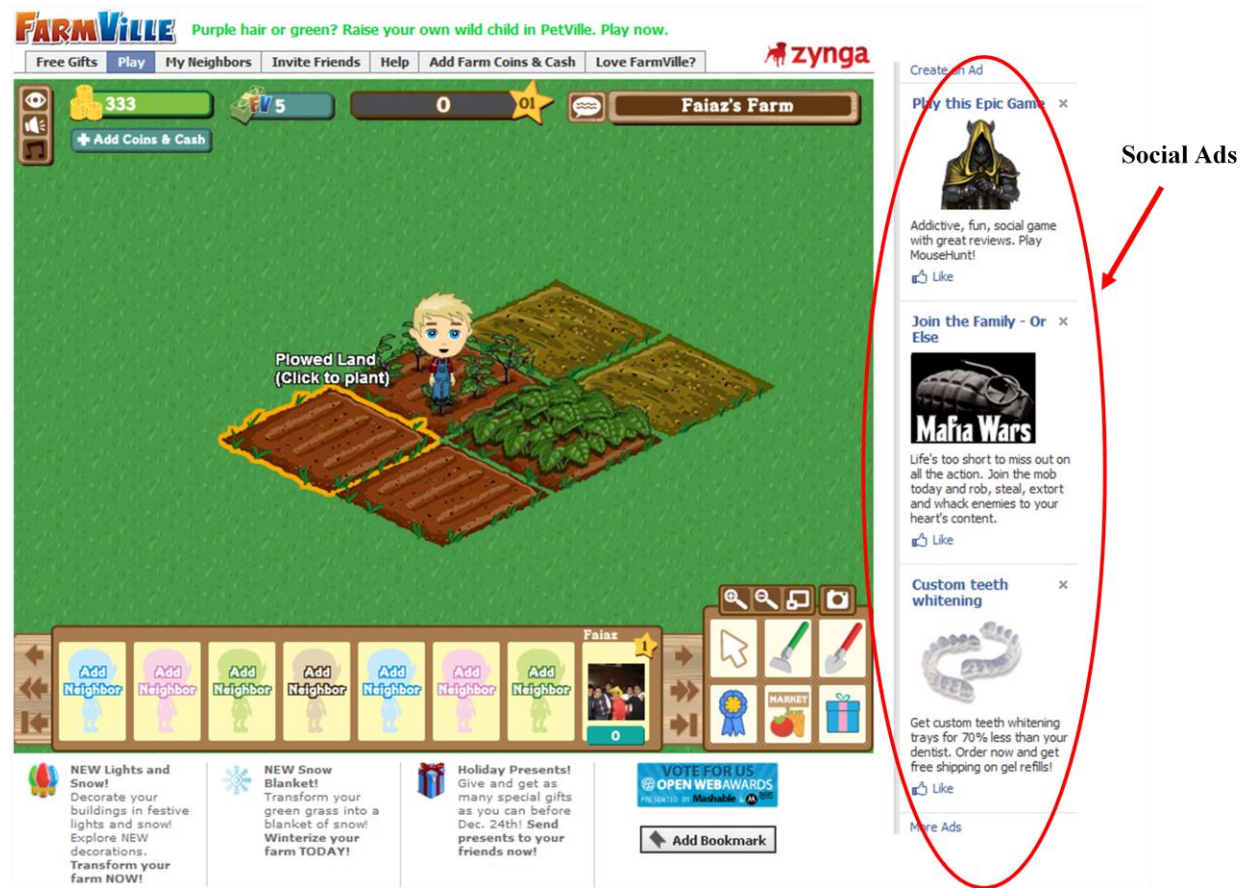


Figure 24: Social Ads

1.9 Mafia Wars

Mafia Wars is one of the most famous application based games being played on SNS nowadays. It has a simple yet addictive theme to it that keeps players coming back to it. According to Inside Facebook, there were 26.5 million people playing Mafia wars on Facebook as of December 16, 2009 [16]. Both Farmville and Mafia Wars have the same creator Zynga, who has made it big in the Internet industry recently, with the advent of these application-based online games.

The concept of Mafia Wars is to emulate real mafia members in the sense of completing ‘jobs’ and other criminal activity to gain reputation, money and credibility in the world of Mafia families. Players perform all these tasks in the game by clicking repeatedly on certain action buttons assigned to different tasks. The game initially is set in New York City and further extends to Bangkok, Cuba and Moscow. Players have to complete a pre-defined number of tasks and gain a pre-set number of experience points to advance to different levels [13].

In order to install and start playing Mafia Wars, a Facebook user has to go the application and install it in order to run it. Just like Farmville and other Facebook applications, first time users have to go through a disclaimer, which pops up and tells the user that all of his personal information can be used by the game developer in any way as detailed in the privacy policies of Facebook and Zynga. If the user accepts this agreement, only then they are able install the game [16].

Once that hurdle of accepting privacy policies is completed, a user starts off choosing which career path they would like to have in the game. There are three character options a player can choose from: Maniac, Fearless and Mogul. Each character has a special attribute useful during game play. The Maniac recovers ‘energy’ faster, the Fearless recovers ‘health’ faster and the Mogul makes money faster. The game starts after the user has made the initial character choice. Each player starts off doing jobs such as mugging, auto thefts, picking up fights with petty gangsters etc. It looks like the game play has all aspects of mafia activities covered in the sense that all the jobs are in one way or the other manifestations of criminal like activities. Once a player completes a certain number of jobs, they gain experience points which enables players to unlock different levels and work their way up the crime ladder to become the boss of all mafia families. There are a few basic Real Time Elements embedded in Mafia wars too, just like Farmville that make a users login to their Facebook accounts many times a day.

The following screenshot (Figure 25) depicts the graphical user interface (GUI), once a user logs into Mafia Wars.

Character Attributes

Travel Option

Character Status

Activities users engage to generate points

User Profile and Mafia Family

Game News

Friend Updates

Game News! view all
Wednesday December 16th 2009
Game Update: We have just released a few fixes to correct gameplay issues some players were having. The fixes include adding back fight loot, correcting Moscow episode progress issues, and improving the sending and receiving of gifts. We will be posting more detailed release notes in the next few days. View the **game news** for more information on today's release.
Scheduled Maintenance Downtime: Mafia Wars will be unavailable between 8AM - 11AM PST on Friday, December 18th. This is a scheduled maintenance period to improve performance and prevent additional issues. Thank you for understanding.

Limited Time Offers

 Loot a shipment of: Ugly Sweaters ★ 15 Attack 18 Defense Share this loot with your friends. Loot shipment	 Nitro Skates ★ 19 Attack 36 Defense Time left: 46:59:02 Buy For 25 Reward Points	HOLIDAY GIFTS SEND FREE GIFTS TO YOUR FRIENDS ▶
--	---	---

Player Updates [Clear Updates]

- 10 hours, 25 minutes ago:
 You were attacked by **lady k** 1 time. You lost the fight, taking 16 damage and losing **C\$0**.
- 11 hours, 22 minutes ago:
 **Don Adil** needs your help on a job in Cuba. [Click here to help out Don Adil.](#)
- 11 hours, 54 minutes ago:
 You earned the "Big Business" achievement by fully upgrading a single Cuban business other than the Bodega.

Life Perfect...

★ Attack:	60
🛡 Defense:	50
🩹 Health:	110
⚡ Energy:	430
🏃 Stamina:	42

[Use Energy Pack](#)

New! Join the Mafia Mailing List

Enter your email address to receive a limited time item, rewards, updates, and exclusive Zynga game information!

Enter Your Email Address:

[Submit](#)

privacy policy

Reminder: Zynga will never ask you for your password or log-in details. Please be careful. The safety of your personal information is important to us.

Figure 25: Mafia Wars Homepage

The screenshot of Mafia Wars in Figure 25, highlights the all the main features of the game. The top four features of Mafia Wars are depicted on the top of the page. The Character Attribute feature tells us about the current condition of the user. Right next to it is the Character Status feature. This summarizes the level and stage the player is on, and the current experience he has gathered. There is also a blue bar that shows the requirements the player has to fulfill to proceed to the next level. Right underneath that is the User Profile menu. Once clicked on it, it directs the user to a page provides a succinct overview of the friends he has in his ‘Mafia Family’. Next to it is the Activities menu that provides a link to the activities a user can engage him to gain the four major attributes and eventually gather experience points to go forth in the game. On the home page, there are also options on game news and other player updates.

The screenshot in Figure 26 is the link to a page once the ‘Job’ tab on the Character Attributes feature is clicked. It lays out a list of jobs the player can undertake to gain experience, and lose energy.

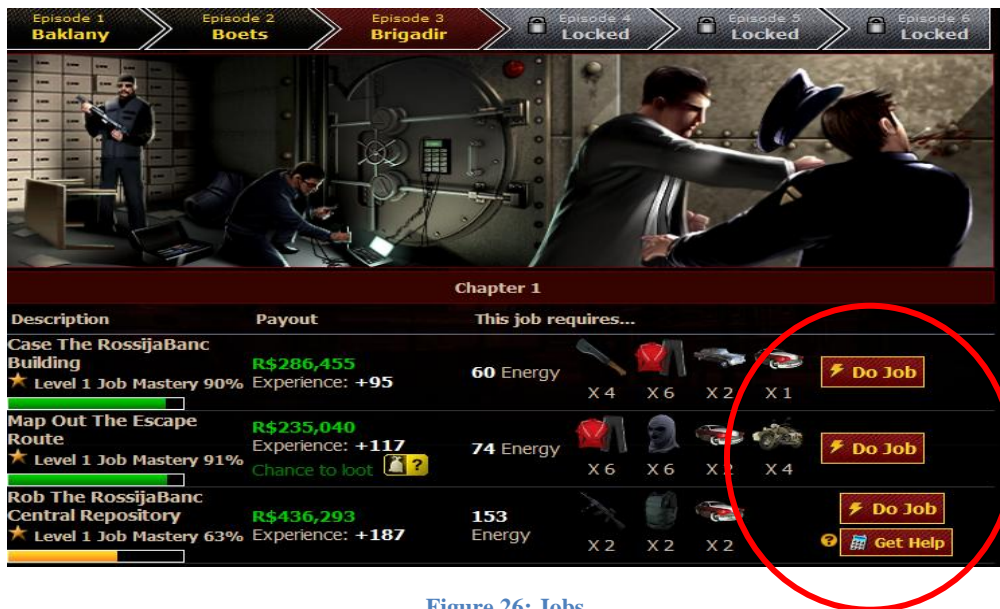


Figure 26: Jobs

This screenshot, in Figure 27, shows the page that only deals with the ‘Fight’ option. There are three different kinds of fights: Fight, War, and Mercenary. This page also shows a list of other players of Mafia Wars and the size of their respective family. A player can fight another player, and the decision of who wins the fight is based on the size of the family.



Figure 27: Fight

The Business section, as shown below in Figure 28, deals with a Godfather’s (player) option to get involved in businesses. Buying businesses require a lot of money, and thus several levels have to be accomplished before a user can invest in a business. But any business generates money and eventually makes the player’s character stronger.



Figure 28: Business

The screenshot in Figure 29 shows a list of items a player can purchase to increase power and skills. There is also the Collections & Vaults section where a user can store his items. Collectibles are also given out, based on a lottery system, and winning a lottery greatly enhances a player’s performance.

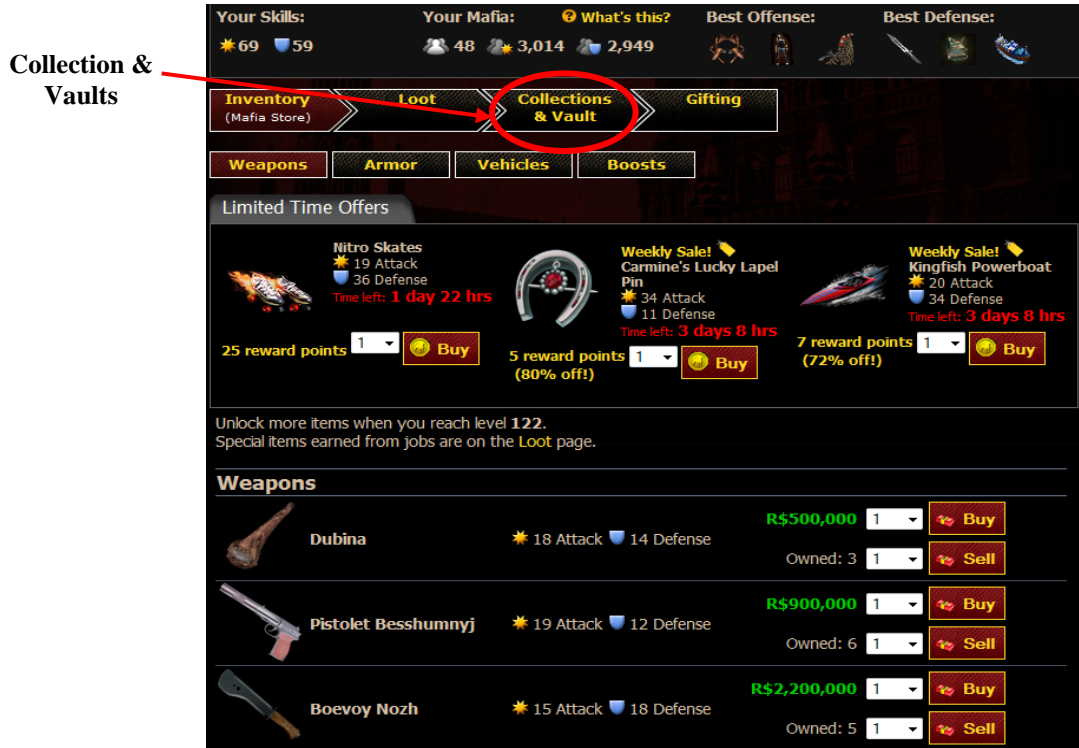


Figure 29: Inventory

Figure 30 depicts the main section where users are persuaded to spend money. This is the page that opens once the ‘The Godfather’ tab is pressed (Figure 30). As players proceed in the game, they slowly earn ‘Reward Points’, the strongest valued money in Mafia Wars. Reward Points are used to buy special items, which cannot be bought with regular money. The increase in reward points from one level to another is extremely small, and Mafia Wars advertises the purchase of reward points at a real nominal fee. These packages are always beneficial for the users, and thus proper luring into, always ends up with the players using their credit card.

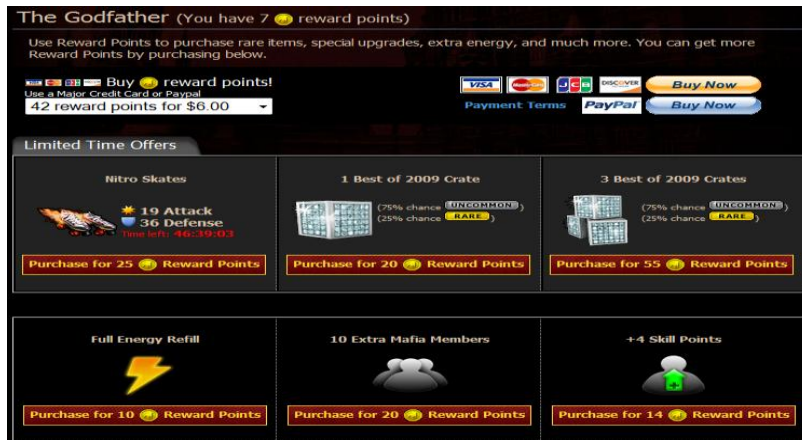


Figure 30: The Godfather

The screenshot of the profile page in Figure 31, basically summarizes the status of the player and displays various statistical data pertinent to the player.



Figure 31: Profile

My Mafia page, displayed in figure 32 below, holds all data related to the players friends. This is the option the player chooses to recruit friends for his own family and also has the option to invite more friends.



Figure 32: My Mafia

1.10 Online Privacy

1.10.1 Introduction

One of the biggest concerns revolving around Facebook involves privacy issues, and raises questions like how safe is it for a person to use Facebook? A part of this project consists of research on the different privacy issues that may arise from playing Facebook games. However, to understand the negative connotations associated with Facebook games in the realm of privacy and information safekeeping, it also has to be first understood why these privacy concerns arise and where are they initiated.

There are certain activities conducted online that attract issues with privacy. These activities are mentioned below and are common elements of every SNS on the internet since the whole point of existence of a SNS is to support the fulfillment of these activities. These are:

- Communication with friends and family
- Meeting people of choice, and making new friends
- Reconnecting with old friends
- Easy means to share messages, videos, photos, etc
- Participation in groups or causes of interests
- Using applications like games with other members

Facebook being the biggest SNS on the internet presently also has the largest user base of over 400 million [1], with members from various ages, including a lot of teenagers or even younger children. In 2008, approximately 15 million teens were using social networking sites, and nearly two million users were children (three to 11 years old) [21]. Amongst the teen users between the ages of 12 to 17 years old, 65% had a profile on an online social network [21]. As logic entails,

one cannot expect underage people to exhibit responsible character traits as expected from an adult. To start off with, anyone under the age of 18 already lacks maturity and experience and is more likely to share information that may prove harmful to them. Even though adults share information which they later may regret, it is expected of them to be responsible enough to not share ‘stuff’ that may harm them. These significant numbers of teens and kids and their online behavior on SNSs could eventually lead them to face unpleasant consequences with regards to their online privacy.

Some of the reasons that legitimize the fear of the consequences of over-sharing are as follows:

- a. Cyber bullies
- b. Online Predators
- c. Privacy Invasion
- d. Identity Theft

In the following sub-sections, each of these aforementioned privacy concerns will be explained.

1.10.2 Cyber bullying

Cyber bullying is described as an act of using the Internet or other technologies and their specific features like posting messages or sharing images to intentionally hurt or embarrass another person [21]. Facebook is the perfect environment for such an activity as it has a large number of users, and creating a profile for oneself is very easy. In a recent incident that surfaced in February, 2010, it was found that some prisoners had allegedly used their Facebook profiles to taunt and intimidate their victims by updating their statuses to obscene and intimidating messages [22]. This is a perfect example of cyber bullying and it also shows that it exists and is a growing phenomenon. Eventually the prisoners’ Facebook pages were deleted but this issue of cyber bullying is here to stay. There are a few types of cyber bullying that are listed as follows [21]:

- Flaming: Online fight sent via email or instant messages with angry or indecent language.
- Harassment: Being subject to repeated mean and insulting message
- Denigration: Destroying someone’s reputation by spreading rumors about them.
- Impersonation: Stealing someone’s identity and spreading rumors, gossip, or sharing materials to harm their reputation.
- Pranking: Tricking someone into revealing secrets or personal information, and in turn sharing it online with other members of the network.

Cyber bullying can affect a victim’s life negatively and may lower their self esteem which could lead to a whole list of other things such as a drop in grades (for students), depression, and suicidal thoughts due to constant intimidation etcetera.

1.10.3 Online Predators

Online predators refer to people who target and lure vulnerable teens or children, usually for sexual or other types of abusive purposes. The targeted victims could be subject to child grooming (befriending a child or teen and establishing an emotional connection with them in order to lower their inhibitions for sexual abuse), requests to participate in sexual activities or discussions, encouraging explicit sexual material like sharing pornography, and non-sexual harassment that would cause fear or embarrassment.

This is highly possible in the case of children who are not supervised on the internet or who maybe too shy to talk to their parents or guardians about their online experience. A general lack of experience and understanding of the online network may usually result in a teen or a child to be a victim of an online predator.

The Ad Council started campaigns against online predators in May 2004 and have since tirelessly pursued their mission of saving kids against these predators and spreading awareness amongst them. The most recent of their campaigns includes an ingenious video on youtube.com which gives viewers the choice of building up the story as they go by answering Yes or No. It starts off with a young girl receiving a text from an acquaintance, asking for a “hot picture” of her. The viewer can choose to send it or not by clicking on Yes or No. Once clicked on Yes, it shows the scenario of what could potentially happen. The photo gets circulated throughout her school as a fun text and eventually lands into the hands of an online predator [23]. Campaigns like these are an important way to create awareness amongst youngsters who might act on impulse and not think about their actions.

1.10.4 Privacy Invasion

Sometimes, internet users may be subject to a privacy invasion when they share their personal information with other users. This personal information could range from sharing passwords, photos, or online posts. Sharing personal information could be of disastrous consequences as this might eventually lead to an identity theft that could potentially defame an innocent person. Identity theft is explained in the next subsection.

1.10.5 Identity Theft

Identity theft refers to the loss of personal information like the password to a SNS profile, social security number, credit card information, cell phone number, etc, to a fraudster, who uses this information to steal money or get other benefits. Users may be subject to identity theft through ‘phony requests’ or solicitations that seem to come from legitimate sources [21]. In a SNS, loss of one’s identity may bring about a chain of identity thefts as the perpetrator gets access to the users friends and may persuade them to give up their confidential information, thereby creating a ripple effect that spreads throughout the website, if left unchecked.

1.11 Facebook Games and Privacy

After having covered the general aspects of online privacy, this section talks in detail about how Facebook as a SNS and its games can be a cause of privacy concerns. Facebook games prosper and generate a lot of revenue, which eventually creates the building block of their profit system and also shapes the most important violations of privacy concerns tied with the site. In section 1.7, it was briefly discussed how Facebook games make money and the economics behind it. An in-depth analysis of this topic will be done in subsequent sections, which would cover Facebook game creator Zynga, their business model, and their fraudulent marketing strategies.

One of the major disadvantages of playing Facebook games is that the users are vulnerable to an identity breach, without their knowledge. When players use their credit card to pay for in-game currency, they may be susceptible to loss of personal information. Trust issues related to online personal information have always been one of the major concerns since the advent of the internet. Part of it is due to the fact that internet users do not meet the other transacting party in person, and this fuels trust issues in the sense that the persons involved in an internet transaction have doubts about the legitimacy of each other. It becomes less of a stress factor when the online business has a good reputation, for example Amazon. But when it involves companies which are not well known, it raises the question if customers should trust them or not. With the introduction of lead-gen type scams involved in Facebook games like Zynga, generating a third of its total annual revenue, it is needless to say that customers are experiencing a privacy breach to its maximum.

For users who are less willing to use their credit cards or do not own one, there are other ways they could be manipulated to give up their information. Dennis Yu, CEO of BlitzLocal, a private advertising agency in Colorado, suggests that users are swindled out of their money or information in the following four ways [32],

- Using credit cards
- Giving up email addresses
- Giving up phone numbers
- Downloading toolbars

1.11.1 Using Credit Cards

Credit card fraud is one of the most prominent ways of swindling a person to give up their money. Many phony offers involve the usage of credit cards. Once a person uses his credit card to buy something, not only is he paying for something fake, but he is also susceptible to future privacy breach as he loses his credit card information to an illegitimate source. In almost all of Facebook games, users are required to buy in game currency using their credit card. Now if one of these offers is a scam, then the user loses his information.

1.11.2 Giving up Email Addresses

This type of scams offers users a variety of consumer goods just by signing up for it using the users' email address. Once a user give up their email address, the host advertisers use it either to gather information on the user or repeatedly keep on sending the user with offers that lead to other scams.

The former is described as email spamming, which is also known as junk email. Email spamming is described as the way to send unsolicited bulk messages to recipients. There are various different types of email spam, but the most common one associated with Facebook games is known as *phishing*. Phishing refers to luring users into putting their personal information like credit card number on fake websites using email forged to look like it is from a legitimate business like a bank [24].

In April 2009, Facebook users started getting emails from Facebook containing a message from a supposed friend, and always comprised of a subject heading "Hello" [25]. The message consisted of a link that directed the user to the actual Facebook page. But this link directed the user to a page that looked exactly like Facebook's start up page, but one glance at the web url said something else. The website address was fbaction.net, which mimicked Facebook to such an extent that it looked almost real. Once the user logged into this fake SNS, all his account information was taken in by the scammer, and the user was subjected to tremendous privacy breach. The screenshot below depicts the scam.

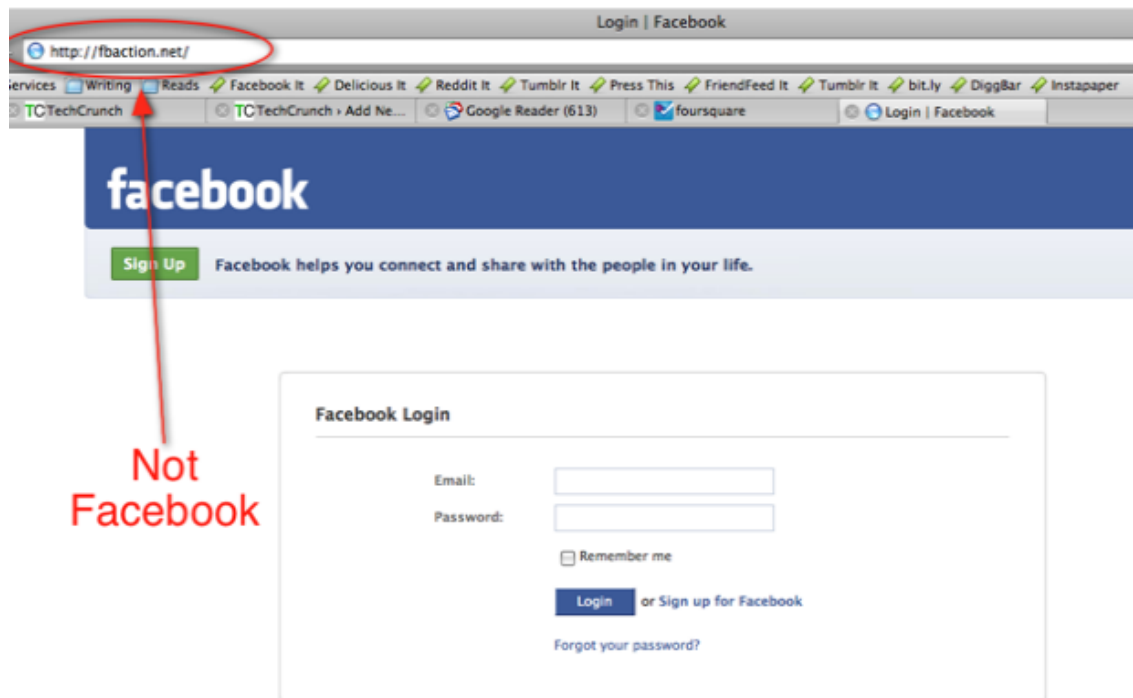


Figure 33: Facebook Phishing Scam [25]

Fbaction.net was eventually monitored by Facebook, and was removed from all users email messages. But scams like this every now and then show up as emails from Facebook.

1.11.3 Giving up Phone Numbers

Giving up phone numbers in exchange for something is one of the most prevalent scams present. Users, who are unwilling to use their credit card to buy in-game currency, may be more willing to get the currency in exchange for something they are interested in. The most common one is IQ Quizzes. This scam involves users to take an IQ Quiz and once the quiz is over, it asks for the users' phone number so that they can text the results. The screenshot in Figure 34 shows one such scam [31].



Figure 34: IQ Quiz [31]

Once a user gives up their cell phone number, they are automatically subscribed to a \$10/month subscription. TattoMedia is responsible for most mobile scams [31]. TattoMedia, along with three other advertisers, were eventually banned from Facebook.

1.11.4 Downloading Toolbars

This type of scams involves downloading a toolbar, a spyware to be more accurate, for a specified purpose [32]. A spyware is a type of a malware, short for harmful software, that when installed on computers gathers personal information about the user without the user's consent [26]. Zango may have been the most popular software company, specializing in spywares, before its bankruptcy in April 2009 [26]. Once downloaded, Zango provided users access to its partner products through its toolbar. But what users did not know, was that Zango secretly collected information on the websites the user visited and transmitted the data to the advertisers [26].

1.12 Facebook Game Developer: Zynga

In this section Facebook game developers are analyzed in detail, and the means undertaken by them to generate money. The two games used as examples in this project are developed by Zynga, and the analysis in this section is mostly geared towards Zynga as the primary game developer.

Zynga, the creator of Farmville and Mafia Wars, is the biggest developer of facebook games. Zynga was founded in July 2007 by Mark Pincus with the “vision of connecting the world through games” [36]. Zynga is involved in creating browser-based games which could be played all by themselves or as application widgets on SNSs like Facebook. It provides a platform for users to play games with their friends and family in real time, and thus has become excessively popular in SNSs. Zynga is the creator of the most popular games on Facebook, which created, besides Farmville and Mafia Wars, CafeWorld, Fishville and Zynga Poker [36].

Zynga initially started off with venture finance of around USD \$29 million in July 2008, which was led by Kleiner Perkins Caufield & Byers, and around that time they appointed former Electronics Arts Chief Creative Officer Bing Gordon on the board [36]. Gordon is regarded as one of the builders of the gaming industry, and added a lot of credibility to Zynga [36]. With the amount of revenue that was generated in a fraction of months, it is not a surprise that investors as well as pioneer game developers started taking interest in Zynga. In December 2009, Digital Sky Technologies, a Russian Investment Firm, purchased \$180 million stake in Zynga Inc. [37].

In June 2009, Zynga appointed Brian Reynolds as the chief designer of games. Since Reynolds joined Zynga, he was responsible for developing all the Zynga games, and started taking social strategy games to a different dimension [15]. Reynolds is regarded as one of the most talented and respected game designers of all time, and was honored by *PC Gamer* as one of 25 “Game Gods” [15]. Reynolds is one of the founders of two successful video game studios: Firaxis Games and Big Huge Games [15]. He helped create some of the most popular video games, including Civilization II, Alpha Centauri and Rise of Nations, and his games have sold over six million copies worldwide [15]. More recently, Reynolds has been leading operations in Zynga East, which expands the company on the East Coast [15].

1.12.1 Business Model

In an earlier section of Facebook Games there was a brief discussion on how almost all games generate their revenue. In this section, the business model used by Zynga to generate its money is analyzed in detail.

Like other Facebook games, Zynga is supported in two major ways: through credit card payments and partner businesses. Due to the real time elements implemented in these games, players have to wait a certain amount of time, usually hours, to generate resources from which they gain experience and money, which in turn helps the user to proceed further in the game. This affects almost all users psychologically in the sense that they cannot complete missions or

tasks in one sitting to reach the end. For example, in Farmville planted crops may take days to grow and the user has to wait that specified amount of time to harvest them to proceed forward.

Zynga gives the user the option to buy experience points or coins with real money via a credit card. For players who are less inclined to pay cash for game currency, a huge selection of offers are available from where they can get in game currency in exchange of an online lead generation advertising offer, described as lead gen-type [31].

1.12.1.1 Online Lead Generation

Online lead generation advertising is described as the various internet –based methods for generating customer leads [20]. It is a marketing term that refers to the generation of consumer interest into a business' merchandises or online services. A lead is defined as signing up for an advertiser's offer, and comprises of the user's contact information [20]. A lead consist of data fields about a user, and the campaigns usually include the users full name, email address, home address with zip code, and sometimes include gender and phone number [20]. There are two main types of leads in the lead-generation market: sales leads and marketing leads.

Sales leads are based on basic demographic criteria such as FICO score (e.g. credit score), income, age, household income (HHI), etc [20]. This information is later sold to advertisers, who are usually companies dealing with mortgage, insurance and finance amenities, and typically involves phone calls from these advertisers to the user [20].

Marketing leads are usually brand specific leads directed towards a specific advertiser's offer. Unlike sales leads, marketing leads are only sold to advertisers whose ads are already quite popular amongst users [20]. Once a user gets lured into a lead-gen offer, the games get paid and they eventually pay SNSs like Facebook in advertising, to get more users.

According to Andrew Trader, co-founder of Zynga, the total revenue of Zynga comes from three different sources. A third of its revenue comes from advertising and another third comes from virtual goods transactions, like in-game currency. The last third comes from lead-gen type offers from companies that sell/trade commercial goods for in-game currency. This last third comprises of any offers that allows users to get in-game cash in exchange of these offers, and is a mixture of legitimate offers like Netflix and illegitimate offers like IQ Quizzes or recurring mobile phone subscriptions [30].

1.12.1.2 Fraudulent Marketing Strategies

TechCrunch founder and co-editor Michael Arrington, one of the most powerful people on the internet as recognized by *Forbes* [17], suggests that most lead-gen type offers are scams. Scam is an attempt to defraud a person or group of people by gaining their confidence [32]. This may be an exaggeration, but a lot of the offers appear to be scams. Many offers make users pay more in-game currency than if they paid cash. Some offers appear as taking quizzes or surveys, and asks for the user to disclose their cell phone number by saying that they would send the result as a text to the user's phone, as these information are "private and personal". Once the user gives up their

cell phone number, they are lured into a fake mobile subscription [31]. But not all offers are scams. There are legitimate offers from advertisers like Netflix and Blockbuster [31].

Even though Facebook have rules on prohibiting scams, they hardly regulate it, and the fact that there are still so many scams available on these applications proves that developers have been routinely ignoring these scams. One reason to this could be that the SNSs generate a lot of profit themselves from these advertising. Zynga itself pays approximately \$50 million a year on Facebook advertising [31].

During a research conducted by TechCrunch on various aspects of social gaming [14], they asked CEO of TrialPay, Alex Rampell, to express his opinions on the future of social gaming and the risks involved. TrialPay is a company that enables customers to pay for one item while they are buying something else. It works with over 7500 companies like Skype, McAfee, etc, and according to TechCrunch, is one of the most legitimate businesses of its kind [14].

Rampell suggests that the advertisers who can pay the SNSs the most have the highest probability of surviving in the long run [14]. As it is an extremely competitive market for the advertisers, all of them thrive to generate huge revenues over a relatively short period of time. Thus, according to Rampell, the company that steals and cons the most is usually the company that ends up paying the SNSs the most [14]. This sometimes forces ethical competitors to either go bankrupt or incorporate similar means to survive. Even if some application developers do not want to run “scammy” offers, sometimes they are forced to do so in order to survive in the competitive business. It is not a problem at all if a developer dies, as there is always another one to take its place.

One of the biggest problems associated with scams is the large chain of “middle men” present between the users and the advertisers [14]. Rampell suggests that the chain most of the time looks like this:

User->App Developer-> Offer Provider “X”->Ad Network “Y”->Advertiser

The chain above comprises of five subjects. The first one in the chain is the user, typically the person playing a game, and the last one in the chain is the advertiser, who usually provides the user with visual advertisements. Right after the user is the Application Developer, ones who are making the games like Zynga. The two subjects after the “App Developer” are “Offer Provider” and “Ad Network”.

Offer Providers and Ad Networks are variables, as they are always changing, thus making them extremely volatile. Offer Providers are companies like TrialPay, which essentially make money by letting customers to pay for one item while they are buying something else. Ad Networks are companies that connect websites who are willing to run advertisements, to advertisers who eventually run their ads on the website. The reason that these two variables change a lot is because Application Developers are always rotating between different Offer Providers, while Offer Providers are always rotating between Ad Networks, even though the user and the advertisement stay the same. This makes it hard for game publishers and developers to monitor ads that are scams, and users are more easily susceptible to scams [14].

Moreover, once a user becomes a victim of a scam, complaints are usually directed towards advertisers because to most users, Offer Providers and Ad Networks are invisible. With or

without the game developers' knowledge, a scam accusation always affects the games negatively, as they are at the end of the day, the host of the ads [14].

One such example of a scam on Farmville was Video Professor. The offer suggested that users can receive Farm Cash if they sign up for a free learning CD from Video Professor [31]. The users are asked only to pay a \$10 shipping charge. However, on a different page from the checkout, it is found that the user is actually getting a whole set of CDs for \$189.95, and will be billed for it unless they return them within a specified amount of time. Most users never return the CDs as they are hardly aware that they have been charged the extra money [31]. The example of Video Professor is shown in the screenshot below (Figure 35).

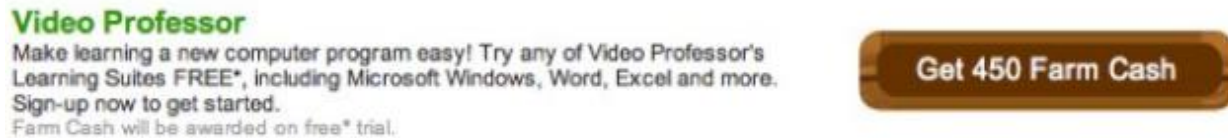


Figure 35: Video Professor Scam [31]

In November 2009, Zynga CEO Mark Pincus said in a blog that he would make sure that the games developed by Zynga do not include fraudulent offers [19]. He apologized for the scammy offers present, and blamed middlemen offer companies for the number of scams present. But from the very start of Zynga, using scams to generate money was a part of Zynga's revenue model. Earlier in 2009, Pincus gave a speech at Startup@Berkeley, an event held at UC Berkeley to bring together faculty, staff, students and entrepreneurs, where he clearly mentioned that scamming was a part of Zynga's business model from the start [19]. This speech was caught on video, and was virally spread all over the internet. The video is approximately 30 minutes long, and a section from the speech, in Mark Pincus' own words, is quoted below.

So I funded the company myself but I did every horrible thing in the book to, just to get revenues right away. I mean we gave our users poker chips if they downloaded this zwinky toolbar which was like, I dont know, I downloaded it once and couldn't get rid of it. *laughs* We did anything possible just to just get revenues so that we could grow and be a real business... So control your destiny. So that was a big lesson, controlling your business. So by the time we raised money we were profitable [19].

Now the question arises, how much money is being generated for the developers through these scams? Zynga, founded in July 2007, is currently valued at approximately \$120 million [28]. As mentioned earlier, Zynga generates a third of its revenues from lead-gen type offers. Michael Arrington from TechCrunch [30] suggests, that Zynga's gross revenue is around \$250 million a year, and around \$80 million comes from commercial offers. These commercial partners of Zynga consist of legitimate businesses like Netflix and Blockbuster, as well as fraudulent companies. Now the question is how much of this money is being produced by illegitimate offers? Netflix asks users to sign up for a free trial membership with a credit card number, and in return gives the users in-game currency. Players can cancel the trial membership and start all over again. But Netflix has a policy of paying for players only once. But the developers can use a

wide variety of partner chains to launder such leads, like one user registering for Netflix more than once, and get the users through payment [31].

But to say that Facebook is not doing anything about these scams would be wrong. One of Zynga's games, Fishville, was suspended by Facebook in November 2009, two days after its launching, for advertising violations [25]. Facebook announced that it would not let Zynga run the game Fishville until Zynga demonstrated satisfactory compliance with Facebook's restrictions involving ad offers [25]. Fishville was up and running again in late November of the same year. The screenshot in Figure 36, depicts the notice Facebook put up to inform its users' about the unavailability of the game Fishville.



Figure 36: Unavailability Notice for Fishville [16]

Facebook also shut down other ad networks due to same reasons, including big scammers like Tatto Media and Gambit [25]. The presence of scams in everyday Facebook usage would cause users to blame Facebook for not doing anything about these frauds. But then it raises the question whether in reality Facebook is doing anything about these lead-gen type offers. This creates a massive dilemma, as developers like Zynga may be intentionally filtering Facebook employees from seeing ads that do not comply with Facebook's terms and conditions, and on the other hand Facebook may be biased towards Zynga as it is Facebook's largest advertisers, generating around 10% to 20% of total Facebook revenue [25].

Michael Arrington suggests that there is a huge possibility that Zynga is trying to filter out specific users from seeing lead-gen type scam ads who might threaten Zynga's future. In November 2009 Mark Pincus, even after declaring that all Zynga games would be free off mobile ads, persistently tried to make money off scams. Less than a week after the announcement made by Pincus, Zynga released their game Fishville [25], which apparently consisted of ads on mobile subscription. Michael Arrington claims that he was not able to view any of the ads, but when his friend logged onto Fishville with the same IP address, all the ads were visible. Arrington believes that Zynga was filtering the ads in such a way, that he could not view any of the ads. He suggests that Zynga has been intentionally blocking ads to journalists, bloggers, or just anyone who have been criticizing Zynga. The ads were eventually removed after Arrington emailed Zynga [29]. Below is the picture taken by Arrington to prove that his friend was able to see the ads, whereas he was not.

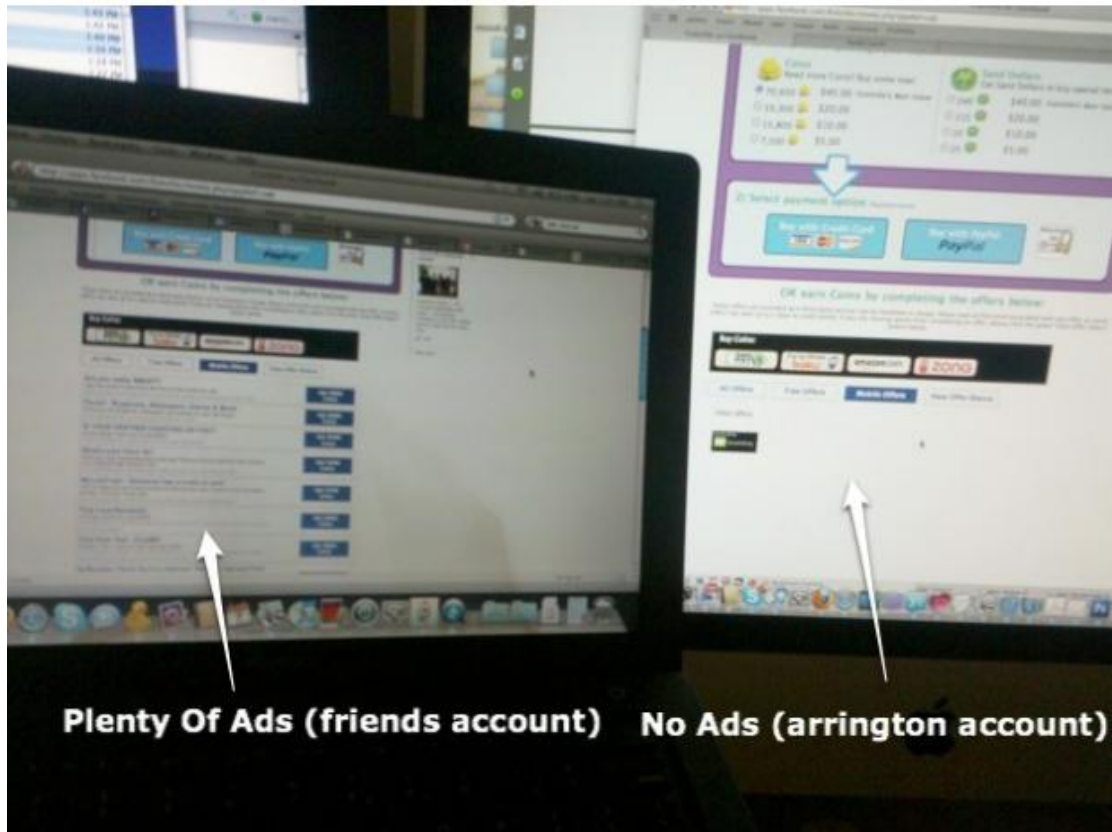


Figure 37: Filtering of Ads [29]

1.12.1.3 Examples of Current Fraudulent Offers

For the sole purpose of finding scams incorporated in offers, various games by different developers were analyzed, and the focal point was geared towards the highest revenue generating games, and the games that attracted maximum users. After a thorough analysis of games developed by Zynga, it was concluded that currently Zynga is not sheltering any illegitimate offers. Zynga is just one game developer on Facebook, and may even be the biggest, but that does not mean that other games by different developers do not pose any threats to users.

After reviewing Adonomics, the source for Facebook analytics, scam analysis was more focused on games developed by Playfish Ltd. and RockYou, as these two are the second and third highest revenue generating companies on Facebook, after Zynga. Games developed by Playfish have approximately 4.2 million daily users and is valued at almost \$54 million. RockYou, on the other hand attract significantly fewer daily users (approximately 2 million), but is valued at almost \$63 million. Thorough investigation of offers in exchange of in-game currency available in games mainly developed by these two developers, and the ones that had a huge number of users, led to hidden scams that do not comply with Facebook's terms and conditions, and may pose threat to users. Below is a list of games harboring some possible scams [28].

Zoo World

Zoo World is a game developed by RockYou and it boasts approximately 16 million active users monthly.

Possible Fraudulent Offer:

The screenshot shows the 'Buy Wildlife Points' section of the Zoo World website. At the top, there are payment options: 'Pay by Mobile boku', 'VISA MasterCard DISCOVER', and 'SMS pay'. Below this is a section titled 'Earn Wildlife Points through Surveys' with an 'Extra Bonus' progress bar at 0%. A red oval highlights a promotional banner that says 'free: Enable Instant Wildlife Points! Start earning Wildlife Points faster by enabling quick surveys, just click here. We will ask you a few questions and use your answers to start showing surveys that are best for you.' To the right of the banner is a button that says 'Enable and get up to 40 Wildlife Points'. Below the banner is a section titled 'Earn Wildlife Points through Offers' with filters for 'Free', 'Mobile', and 'Popular'. A table lists various offers and the number of Wildlife Points they provide.

Offer	Wildlife Points
Popular & Free: Netlix DVD Delivery Service - Free Trial & GET Wildlife Points!	90 Wildlife Points
3 Disney Movies - \$1.99 Each! (Free Shipping)	108 Wildlife Points
Get your FREE Credit Report and Score!	90 Wildlife Points
Try Gamefly for 1 Month for \$8.95!	116 Wildlife Points
BLOCKBUSTER by Mail: as low as \$4.49 for a 1-month trial!	134 Wildlife Points
Free: Be the first to know about great deals at Home Depot!	4 Wildlife Points
Free: Join AARP & receive FREE Travel Kit!	38 Wildlife Points
Popular: Get 50% off of your first month at BLOCKBUSTER	108 Wildlife Points
The Entertainment Book	21 Wildlife Points
Free: Get Zwinked! Turn yourself into a 3D image!	11 Wildlife Points
Popular & Free: Play Sushi-Aqua Bubble	4 Wildlife Points

Figure 38: Zoo World Offer

Once clicked on it the offer, it asks the user to fill out a survey which consists of question relating to the user's personal data as shown in Figure 39.

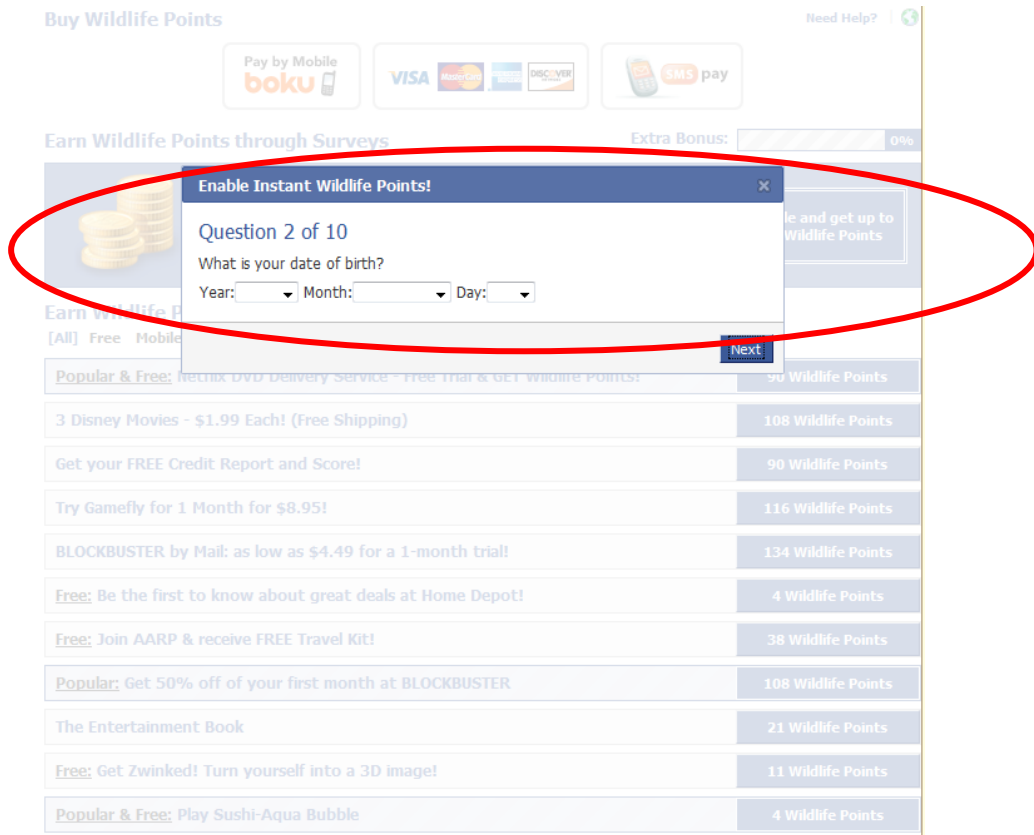


Figure 39: Zoo World Survey asking for user’s personal information

In Facebook’s advertising terms and conditions, it clearly mentions that advertisements cannot offer incentives to gather personal information on the user. The screenshot in Figure 40 refers to that section of Facebook’s ad guidelines.

10. Ads for Alcoholic Beverages

- a. Ads must be targeted to people 21 years old or older in the US, 19 years old or older in Canada, 18 years old or older in the UK, and 21 years old or older everywhere else. All Facebook Pages viewer restrictions must be set at 21+ regardless of the country they are in or targeted to. In the case where a user’s age cannot be determined, the ad cannot be displayed to the user in question. (does not apply to applications on Facebook Platform)
- b. Ads cannot include content that might appeal to (or mislead) minors by implying that the consumption of alcoholic beverages is fashionable or the accepted course of behavior for those who are underage.
- c. Ads cannot include or target any person under the legal drinking age in the region the ad appears, or be suggestive of the presence of those who are underage. Additionally, ads appearing in applications on Facebook Platform must adhere to the Platform Policies Alcohol Content Policy.
- d. Ads cannot portray or promote intoxication.
- e. Ads cannot induce people to consume alcohol in excess, make references to the intoxicating effects of alcohol, depict activities that encourage excessive consumption or that encourage drinking at a rapid rate, or suggest the strength of the alcoholic beverage being advertised.
- f. Ads cannot promote any giveaways as a reward for purchasing the alcoholic product.
- g. It is recommended that the ad creative contain text that promotes drinking responsibly, eg. "Drink Responsibly" or "Drink Smart".

11. Copyrights and trademarks

- a. Ads cannot include any content that infringes upon the rights of any third party, including copyright, trademark, privacy, publicity or other personal or proprietary right.
- b. The advertiser must have intellectual property rights to the creative and be permitted to display such creative as advertising on the Facebook Site.

12. Spam

- a. Ads cannot contain, facilitate or promote 'spam' or other advertising or marketing content that violates applicable laws, regulations or industry standards.

13. Incentives

- a. Ads cannot offer incentives to viewers for clicking on the ad, for submitting Personally Identifiable Information (such as name, date of birth, phone number, social security number, physical addresses, or email addresses), or for performing any other tasks.

Figure 40: Facebook’s Ad Guidelines

Pet Society

This is a game developed by Playfish Ltd, and has approximately 3 million users.

Possible Fraudulent Offer:

The in-game currency offers present in Pet Society are depicted in the following screenshot.

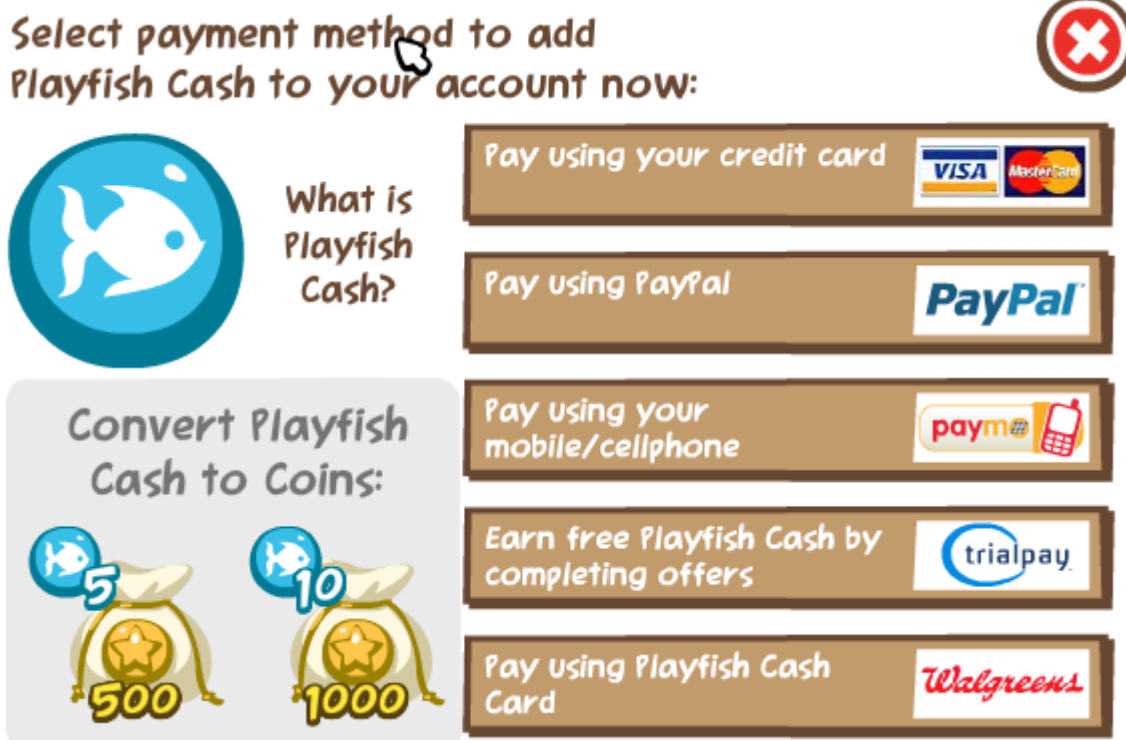


Figure 41: Playfish In-game currency offers

Out of the offers displayed, the only one that looks “fishy” is the one where the offer asks the user to earn free in-game currency by completing offers, and surprisingly the Offer Provider is Trialpay, which, according to TechCrunch is one of the legitimate businesses in the market. Once clicked on it, the user gets directed to a page which is shown in the screenshot in Figure 42.



Complete 1 offer and you're done!

You're getting	Regularly	Now
10 Playfish Cash	\$1.99	\$0.00

Complete surveys

We pay for 10 Playfish Cash



You have selected 'Join ZoomPanel for FREE!'

To complete Join ZoomPanel for FREE!, you have to:

- Sign up for ZoomPanel and complete the following survey.
- No credit card required.
- You must be a **NEW CUSTOMER** and provide your valid home address to qualify ZoomPanel.

[Go back to browse other offers now](#)

Contact information required

We need your information to contact you once your order has been completed.

First name

Last name

Email address

Confirm email

Continue

We value your privacy and will not sell your information to anyone. See [Privacy Policy](#).

Figure 42: Playfish Offer Survey

From the offer, anyone can clearly see that to complete the offer the user has to put in his/her personal information. Even though the privacy policy right underneath that says that Playfish does not sell any user's personal information to anyone, it is still not complying with Facebook's ad guidelines, and is asking for the user's personal information by providing an incentive, such that the user can accumulate in-game currency, regularly costing \$1.99, for free by completing a survey.

1.12.2 Zynga and Privacy Concerns

Zynga, generating millions through lead-gen type scam offers; provide these advertisers with immense amount of personal data obtained from its users. As mentioned before, once a user tries to install an application on his profile, he has to accept the disclaimer that information is going to be taken from his profile. Game Developers and Facebook are the only ones to blame to make such data available to strangers.

In November 2009, a class-action law suit was filed against Facebook and Zynga by the law firm Kershaw Cutter and Ratinoff on behalf Facebook users for illegally charging the users millions by luring them to sign up for subscriptions, that cause the victims to pay repeatedly without their knowledge or consent [18]. Facebook blatantly denied the accusations, and blamed outside ad networks for violating Facebook's terms and services and putting those scam ads up [18].

2. Methodology

In order to qualify the extensive background research done on this topic, the authors of this report decided to perform three experimental methods. These include:

1. Personally logging in to play both games (Farmville and Mafia Wars) extensively;
2. Creating a pseudo real profile to add random college students and see their response; and
3. Send out a university-wide survey that would gauge in the trends of Facebook gaming in the student community.

The intention behind these methods was to see how much of the events revolving around Facebook in the world were actually affecting college students. While the background research in itself was sufficient to justify the thesis of this report, it was necessary to incorporate several methods that would eventually support the thesis statement.

2.1 Playing Facebook Games: Farmville and Mafia Wars

The authors decided that there was no better way to get a feel for the Facebook games than to actually start playing them individually. Pursuing this thought-process both authors selected a game each and played it for extensive periods of time to try and understand what all the hype about these games was about. Both authors found their respective games very addictive after a certain level of indulgence and had then understood about the various “hooks” designed and embedded into the games that keep players returning to play again and again. Most of the background research conducted on the intricacies of these games in sections 1.8 and 1.9 stems from the fact that both the authors participated in playing the games and recorded details as they played.

2.2 The Facebook Profile Experiment

Although this project revolves around Facebook games and their intricacies, an integral part of it is also intertwined with privacy concerns such as safeguarding of personal information. This is essential because the whole concept behind a SNS is to share information in a safe and secure environment, and if this is not being fulfilled or is being violated in any way, then it does not serve the purpose of the SNS. It is thought that the youth of today is not as careful and discreet while sharing information on the internet with their peers, especially on Facebook and this could possibly be the cause for a breach in the secure environments that SNS administrators built for their sites. To analyze this claim, the following experimental approach was devised and implemented, which provided thought provoking results. The logic behind this method of analysis was to look at privacy and accountability. Users are tested on the basis of retaining private information from a stranger online and based on their choice of action; the results from the experiment can be concluded.

This experiment was based on Sophos’ Facebook Identity Probe 2009 [33]. With the cooperation of Kristen Wachenfeld, a student at Clark University and a close friend of the authors of this report, a semi-real Facebook profile was created. This profile contained a lot of factual information about Wachenfeld which was real and accurate in most cases. However, in place of an actual photograph of her, a picture of a cat was uploaded initially which was later changed to a few other pictures that never divulged the real physical/facial appearance of Wachenfeld. Figure 43 is a screenshot of the profile with all the information entered.

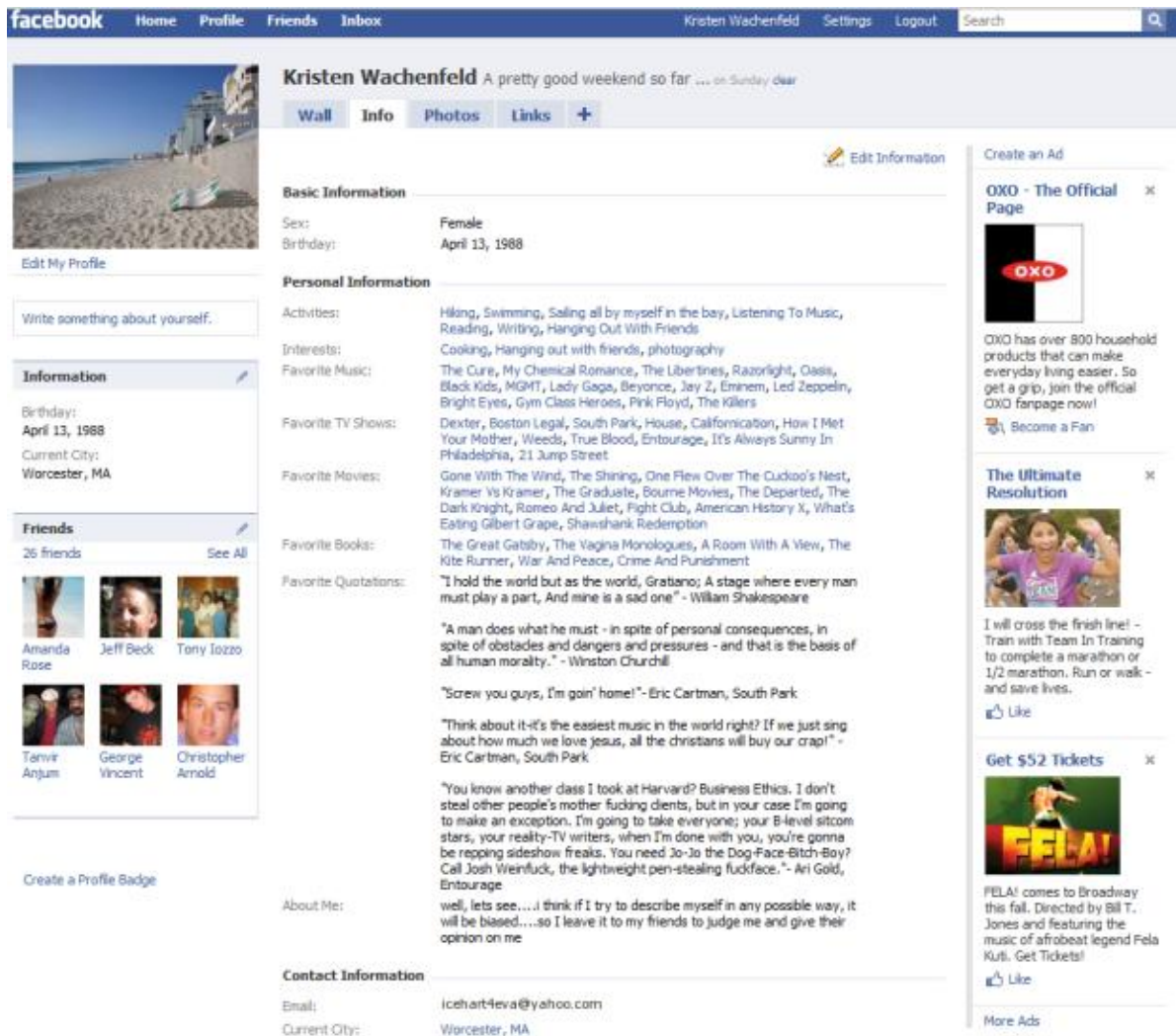


Figure 43: Kristen Wachenfeld’s Profile Page

Over a time span of three months, exactly a 100 users were sent friend requests from Wachenfeld’s profile and three users added her as a friend of their own accord. It has to be mentioned however that two of these three users knew Wachenfeld personally and perhaps

thought that she had created a new profile. The third person however, was a stranger who just added Wachenfeld without even knowing her. Out of the 100 users who were added as friends, 5 users were real acquaintances/friends who readily accepted the requests. Since this was an ongoing experiment, at the time this portion of the report was being written, Kristen Wachenfeld, the “semi-real” 21 year old girl from Worcester, Massachusetts, had 48 friends from various colleges and high schools in Massachusetts. Of the 100 total requests sent out, 43 users declined the friend request and nine users had neither accepted it nor declined it. In the words of Facebook itself, these nine friend requests were called “pending friend requests” for Wachenfeld. Interestingly, towards the end of this experiment it was found that one particular person on Wachenfeld’s friend list had actually removed her as a friend, and it is not clear what might have led him to do that.

A statistical analysis of the aforementioned experiment revealed interesting and mesmerizing data on the user behavioral patterns. A shocking 100% of Wachenfeld’s friends shared their entire photo albums with her, not to mention some very revealing pictures. Again a 100% of Wachenfeld’s friends decided to display their friend lists, which numbered from 150 to 800 people approximately. This trend carried on throughout the parameters that were tested which included Full Date of Birth, Partial Date of Birth, Address, Email id, IM chat id, Phone, Education/Work information, Groups, Interests, names of parents and or siblings and even names of their significant others (boyfriend/spouse, girlfriend/wife). However, not all of these details were shared at the same percentages as others. Table 1 shows a complete breakdown of the percentages for all of these elements, and Figure 44 makes it easier to visualize this data.

Information Detail	%age
Relationship Status	18.8%
Parents' names	12.5%
Siblings' names	22.9%
Personal Interests	68.8%
Groups	89.6%
Friends	100.0%
Photos	95.8%
IM chat Id	56.3%
Address	18.8%
Phone	27.1%
Edu/Work	97.9%
Town/City	81.3%
Email	87.5%
Part DOB	14.6%
Full DOB	75.0%

Table 1: Percentages of Shared Profile Elements

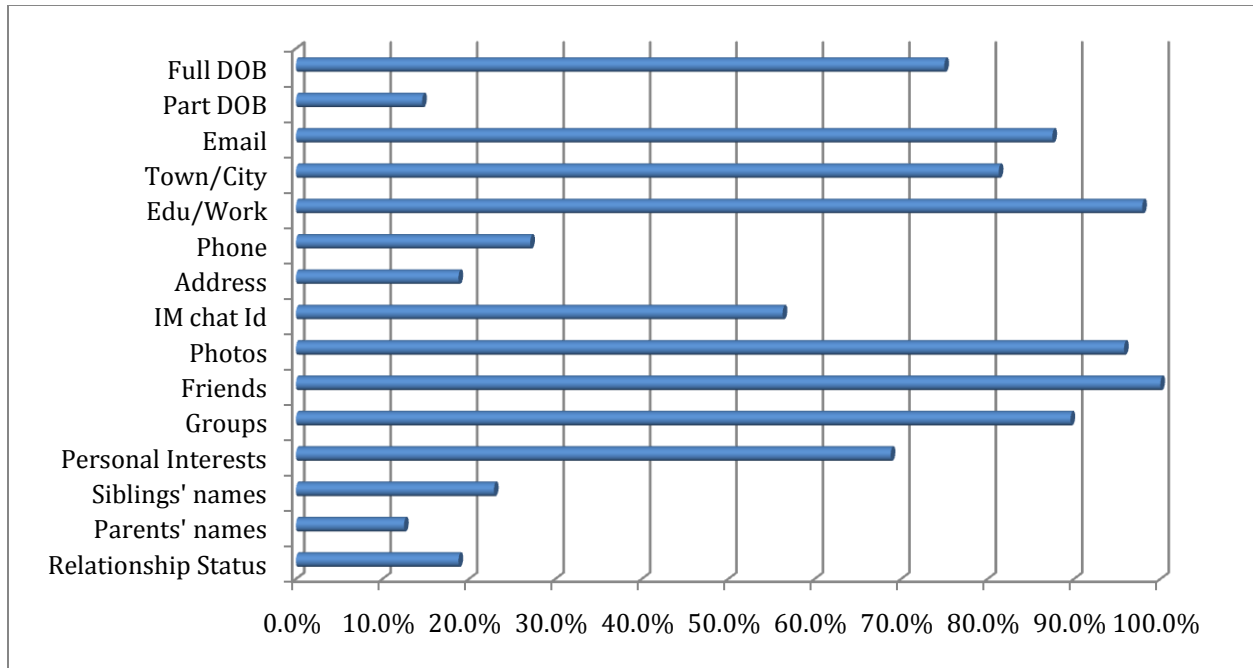


Figure 44: Percentages of Shared Profile Elements Visualized thru a bar chart

Over 70% of the users had shared their full date of birth with Wachenfeld which clearly betrays that the teenagers do not understand the importance of this specific piece of information. Similarly, more than 85% of Wachenfeld's friends shared their email address with her, and about 96% of them also told Wachenfeld their educational qualifications or current workplace. The only two pieces of contact information that weren't as easily shared as the others were the phone number and the physical address.

All these vast arrays of personal information, if fallen into the wrong hands can prove highly disastrous. For the purpose of this study and to have the readers of this report realize these serious consequences, a hypothetical situation the authors came up based on Sophos' study [33], was that an identity thief could easily impersonate another person using the data obtained through this experiment. With a little bit of scouring around, a seasoned cybercriminal can possibly issue credit cards in another person's name, solicit bank information, defame the other person by creating a fake profile and possibly even create a fake passport. To explain these highly possible and undesirable criminal activities, a regular bank transaction can be taken as an example. Most banks nowadays use just the date of birth and/or a pre-assigned pin as a security bypass while authenticating user requests through the telephone and gaining access to this small piece of information can prove beneficial to a cybercriminal and detrimental to the person whose identity has been stolen.

This statistical data, although revolves around a group of randomly selected 100 people, nonetheless can be considered very influential. Based on this small group of Facebook users, it can be concluded that 43% of the people on Facebook are more than willing to share most of their personal information with a complete stranger that they have never met or even seen before.

It was made sure that there was no way to associate the name of Wachenfeld with a face and hence anonymous pictures such as those in Figure 45 were used as her display pictures.



Figure 45: Different Profile Pictures for Kristen's profile

This could be considered as shocking evidence of how human beings, especially teenagers and college students have turned towards sharing everything in their life over these SNSs, not just with friends but also with complete strangers, in the hopes of striking the new “friendship” or the “perfect date”. It cannot be concluded whether this trend of sharing more and more over the internet is for the better or for worse but there should certainly be some reservations that could be put in place to educate the SNS users about the dangers of sharing their personal information and photos with random people. On the one hand, SNSs like Facebook are getting people closer than ever in terms of communicating and sharing their views and opinions about things, or even in keeping up with day to day lives. On the other hand it can turn into a dirty mess when private information wrongly falls into the hands of the antisocial elements of the society.

This experimental data cannot be considered all inclusive or even entirely conclusive since there are a few undeniable short comings that are explained in the following points.

1. Small sample group: Facebook has more than 400 million members on its website and for this study we randomly selected a 100 of those 400 million people, which is a minuscule number compared to the total number of members.
2. Photo Albums: Even though it appears that a 100% of Wachenfeld's friends shared their personal photo albums, it cannot be determined whether all of the photos saved on their Facebook profiles are actually visible to Wachenfeld. Facebook's privacy controls enable users to choose what photos to display to their friends and what not to.
3. Personal Contact Information: Traditionally it is thought that Facebook users share mostly true and accurate information of themselves through their profiles. This is driven by the fact that Facebook provides users with different privacy controls to limit what information is on display to their friends and that users actually take advantage of this option. However, there is no infallible way to conclude that all the information provided on users' profiles are 100% accurate.
4. Profile authenticity: It could not be concluded whether all of Wachenfeld's friends were in fact real people. Fake profiles are abundant on Facebook even though it goes against its Statement of Rights and Responsibilities, and there was no plausible way to find out if a given profile belonged to an actual person or if it was a fake profile.

2.3 Survey on Facebook Games

In order to determine the Facebook gaming trends at WPI, primarily an engineering college, a survey questionnaire was designed. The focus of this survey was to find out how common were Facebook games among the student population, and figure out whether any of the students had actually fallen prey to the notorious scams on Facebook. There were 15 questions asked on the survey with most of the questions being multiple choices, in which survey respondents had to pick an answer that best describes their personal scenario. A few questions provided the option to pick more than one response and one question had a fill-in space provided to list out all the Facebook games that respondents have ever played. The survey yield results from 495 participants, which in itself is not a true reflection of the Facebook community, as Facebook has a user base of 400 million.

This survey questionnaire was created using a service by Google Documents that allows users to create form based surveys that get saved online in the user's Google account and a link of the same can be sent to multiple people. The responses automatically get saved in an Excel based spreadsheet that can then be exported into different file formats.

The questionnaire in its original textual form is as follows:

1. Are you
 - a. Male
 - b. Female

2. What is your class year at WPI?
 - a. Freshman
 - b. Sophomore
 - c. Junior
 - d. Senior
 - e. Graduate Student

3. Have you ever befriended a stranger on Facebook for the purposes of advancing through levels in a Facebook games?
(For example, added strangers as “friends” to increase your mafia in Mafia Wars.)
 - a. Yes
 - b. No
 - c. Maybe

4. Has your computer ever been infected with viruses through Facebook?
 - a. Yes
 - b. No
 - c. Maybe

5. Do you play Facebook games? If yes, please list a few games that you currently have played. (For example, Mafia Wars, Farmville, Texas Hold'em Poker etc.)

6. How often do you engage in Facebook games that sell in-game benefits (ex. Farmville coins, money etc.) to users?
 - a. Multiple times everyday
 - b. Once everyday
 - c. About thrice a week
 - d. About once a week
 - e. About once a month
 - f. I do not play Facebook Games

7. Would you pay with “real money using a credit card or paypal to buy in-game currency (ex. Farmville coins, cash etc.)?
 - a. Yes
 - b. No
 - c. Maybe

8. What do you think is at stake while playing Facebook games?
 - a. Your personal information (contact info, photos, interests etc.)
 - b. Information of your friends (their contact info, photos, interests etc.)
 - c. Both a. and b.
 - d. Nothing

9. Have you ever given any personal information (such as your phone number, credit card information, email address, date of birth etc.) for in-game benefits (Ex. Farmville coins, money etc)?
 - a. Yes
 - b. No

10. Have you ever been a subject to scams on Facebook, like noticing “unknown” charges on your cell-phone bill for services you have NOT subscribed (For ex. Ringtones, horoscopes, etc)?
 - a. Yes
 - b. No

11. Please select all that you think are potential ways of scamming people through Facebook. Select one or more.
 - a. Soliciting cell-phone numbers
 - b. Soliciting credit card numbers
 - c. Using personal information to build a fake profile and solicit information
 - d. Steal photos and use them for blackmailing
 - e. None of the above

12. Would you be willing to fill out a survey or take a quiz (Ex. IQ Test) in exchange game benefits (For ex. Farmville coins, cash etc.)?
 - a. Yes
 - b. No
 - c. Maybe

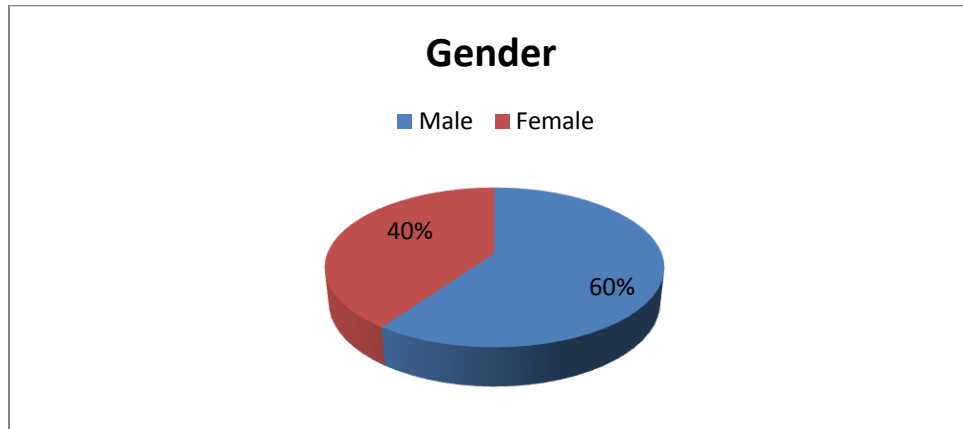
13. Have you ever taken any quizzes (For ex. IQ tests, Life partner quizzes) or completed surveys on Facebook that asked for personal information like your name, date of birth, email address etc.)?
 - a. Yes
 - b. No
 - c. Maybe

14. Would you still be interested in playing Facebook games if you found out that you were scammed?
 - a. Yes
 - b. No
 - c. Not sure

15. What would you suggest a friend in case he/she starts playing Facebook games and you know there is a threat of personal information being mishandled?
 - a. Never play any games on Facebook
 - b. Just don't give out personal information (cell-phone numbers, address etc.)
 - c. Don't worry, it's just an online game
 - d. Indifferent to the scenario

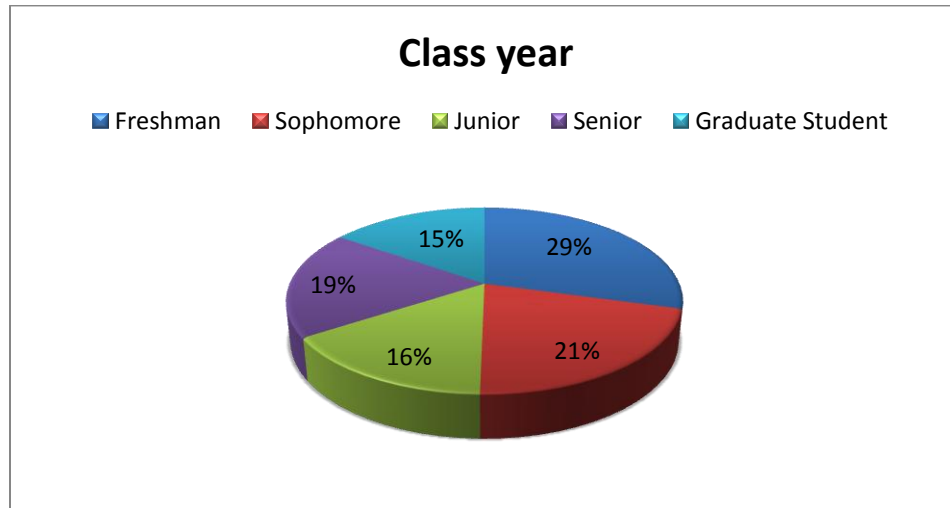
For each question, the thought process behind framing that question and the detailed analysis of the results obtained is as follows:

1. Are you
 - a. Male
 - b. Female



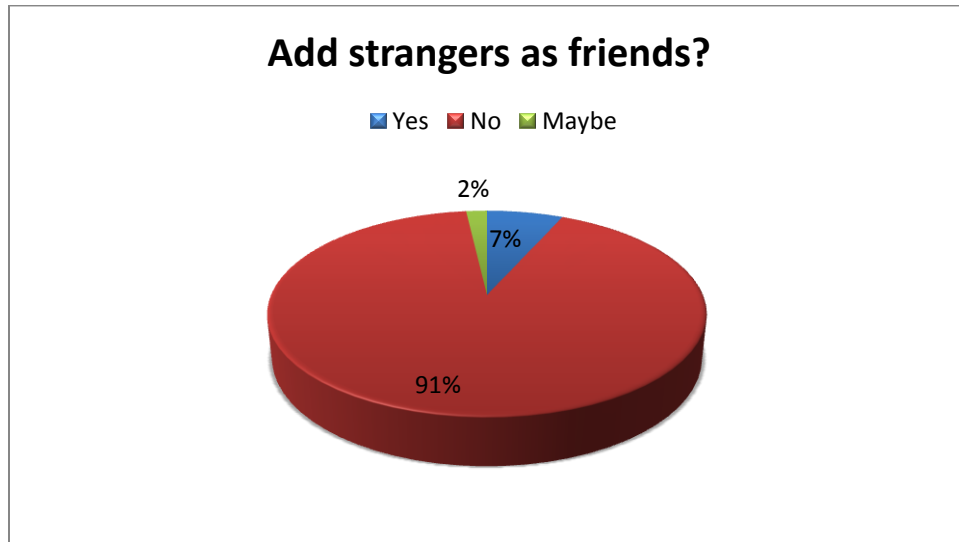
This question was posed to elaborate on the gender ratio in the study which would help the authors find out if Facebook games are common to both males and females or not. From the results it is evident that more males engage in Facebook games than females. Note here that the initial gender ratio at WPI itself is approximately 3 males to every female. Hence this result is somewhat reflects that ratio, as more males were expected to play Facebook Games than females.

2. What is your class year at WPI?
- Freshman
 - Sophomore
 - Junior
 - Senior
 - Graduate Student



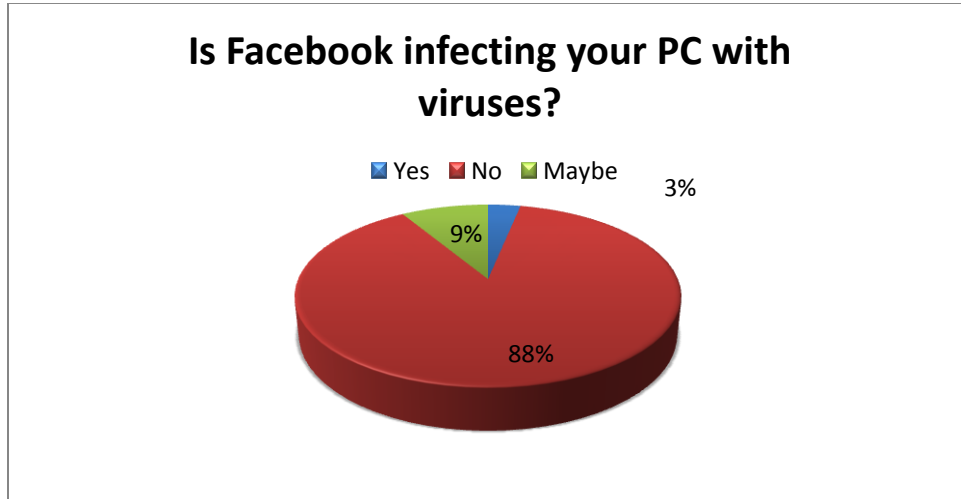
This question was essentially posed to see which group of students engages the most in Facebook games. From the results it was found that 29% of the respondents belonged to the freshman class, 21% belonged to the sophomore class, 16% were from the junior class, 19% were from the senior class and 15% were graduate students. This shows that it is clearly equal amongst all classes, with the freshman accounting for the highest percentage. A caveat that could be applied in this case is that these figures are reflective of only the people who actually responded to the survey and not the entire student body, although the survey was sent out to the entire university students. Hence it could be said that more freshmen actually answered the survey questionnaire and hence their higher numbers. It could also actually mean that freshmen are the most relaxed group of students in this study since they take comparatively easier classes than their seniors and are just out of high school, which suggests that they still carry the typical teenager mentality of indulging more in gaming and other recreational activities as compared to the older students. This also could be an indication of maturity and exposure, which definitely develops in students/people with age and number of years spent in college.

3. Have you ever befriended a stranger on Facebook for the purposes of advancing through levels in a Facebook games?
(For example, added strangers as “friends” to increase your mafia in Mafia Wars.)
- Yes
 - No
 - Maybe



Coming back to the question of privacy and sharing information with strangers on Facebook, it was thought this question would be a very relevant to ask. However, an overwhelming 91% of the 495 respondents replied saying they have not added strangers as friends on Facebook for the purposes of Facebook gaming. This clearly is an indication that the sample group being surveyed is intelligent about not sharing their information with strangers. That still leaves a staggering 34 students, who may potentially be at risk.

4. Has your computer ever been infected with viruses through Facebook?
- Yes
 - No
 - Maybe

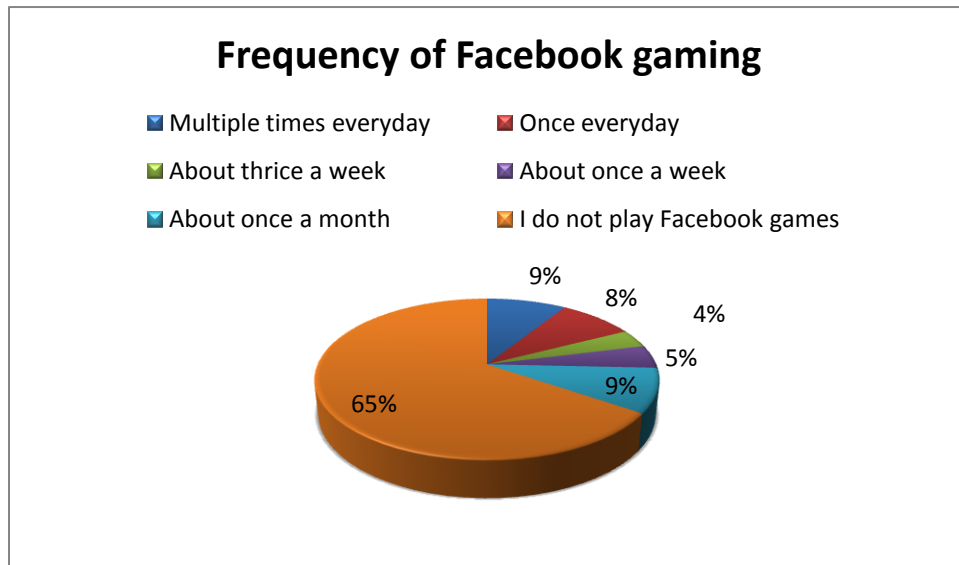


Although it does not directly relate to the project under investigation, this question was asked to get a sense of what Facebook users thought about getting viruses through Facebook. Based on the responses, 88% of the respondents said they never had any issues with having their computers infected by viruses through Facebook, but 9% of the surveyed said they suspect Facebook to be a cause of their computer being infected with a virus. 3% forthright said they think Facebook was the reason behind their virus troubles.

5. Do you play Facebook games? If yes, please list a few games that you currently have played. (For example, Mafia Wars, Farmville, Texas Hold'em Poker etc.)

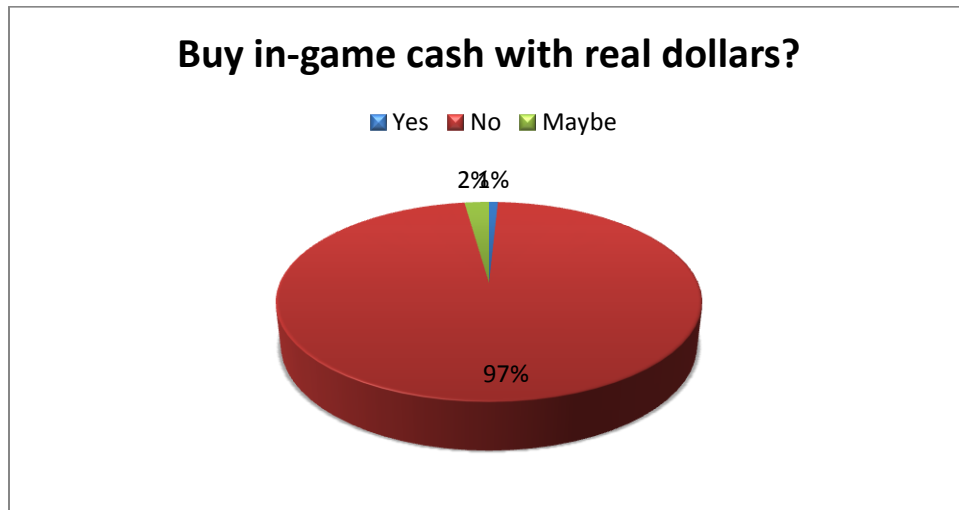
This question was framed in order to get a sense of what games are being played by users on Facebook. Respondents entered several games apart from Farmville and Mafia Wars such as Fishville, Zoo World, Bejeweled, Mob wars, Sorority life, etcetera. This basically shows that Facebook clearly has thousands of games that cater to every kind of user.

6. How often do you engage in Facebook games that sell in-game benefits (ex. Farmville coins, money etc.) to users?
 - a. Multiple times everyday
 - b. Once everyday
 - c. About thrice a week
 - d. About once a week
 - e. About once a month
 - f. I do not play Facebook Games



This was one of the most important questions in the survey in the sense that this clearly shows how much time an average Facebook gamer spends on gaming. More than half of the respondents (65%) said they do not play Facebook games, which equates to only 171 Facebook gamers and their gaming activity ranged from playing multiple times a day to once a month according to the pie chart. A majority of these gamers login to Facebook to play games at least once a day.

7. Would you pay with “real money using a credit card or paypal to buy in-game currency (ex. Farmville coins, cash etc)?
- Yes
 - No
 - Maybe



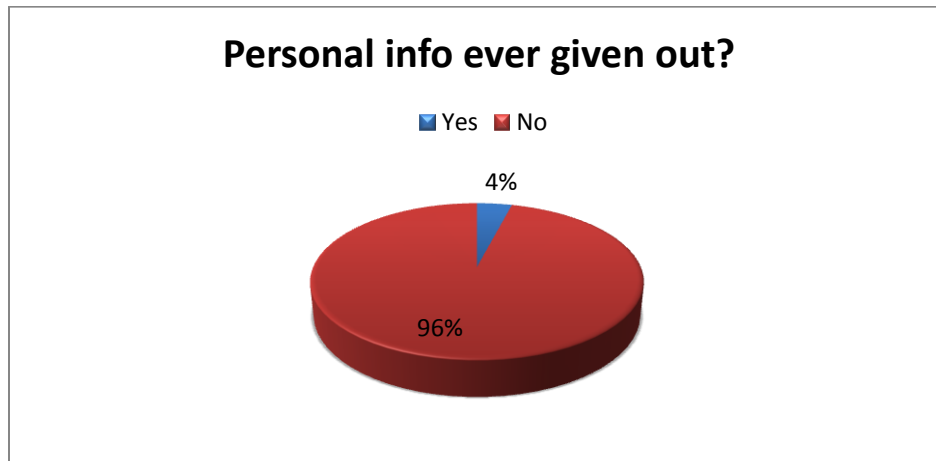
Based on our project research, this question was another important question that aimed to seek information on whether Facebook gamers actually would spend money on these games. An overwhelming majority, 97% of the respondents replied negatively saying they would not. Only a meager 1% said they would, and 2% of them said they wouldn't mind trying it out.

8. What do you think is at stake while playing Facebook games?
 - a. Your personal information (contact info, photos, interests etc.)
 - b. Information of your friends (their contact info, photos, interests etc.)
 - c. Both a. and b.
 - d. Nothing



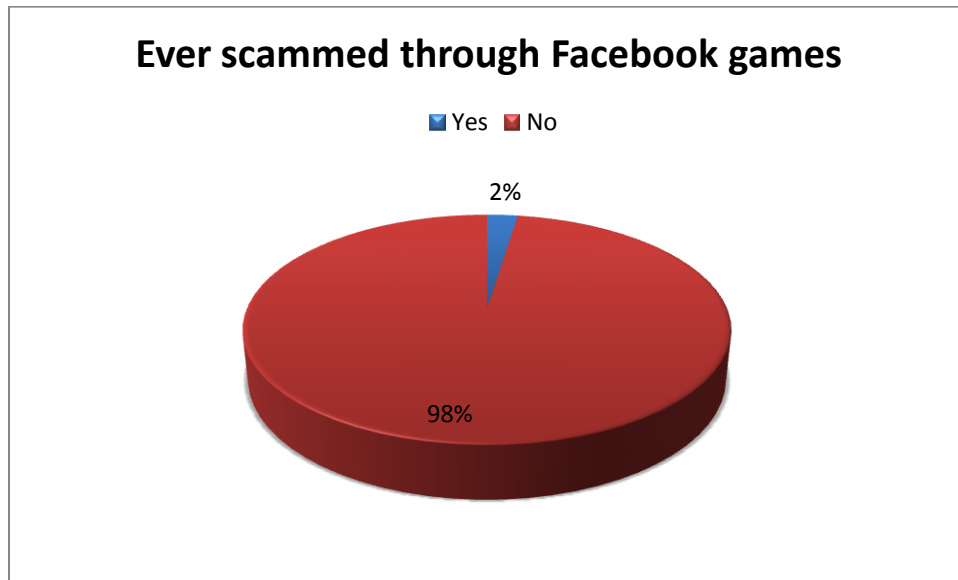
The authors felt this was an important question that would measure the awareness level amongst Facebook gamers and non-gamers alike about the dangers associated with playing Facebook games. More than half of the survey respondents (59%) said their personal info as well as their friends' personal information could be at risk. However, 27% of the people seem to suggest that nothing is actually at stake and it is safe to play Facebook games without unconsciously sharing their personal profile information.

9. Have you ever given any personal information (such as your phone number, credit card information, email address, date of birth etc.) for in-game benefits (Ex. Farmville coins, money etc)?
- Yes
 - No



This question aimed to obtain data on how many users actually willingly gave out their personal information for in-game benefits. 96% of the people surveyed replied no, whereas 4% said they had given out personal information. This again shows that most people are reserved when giving out personal information out to strange third party developers for any amount of in-game benefits, which is actually a good sign.

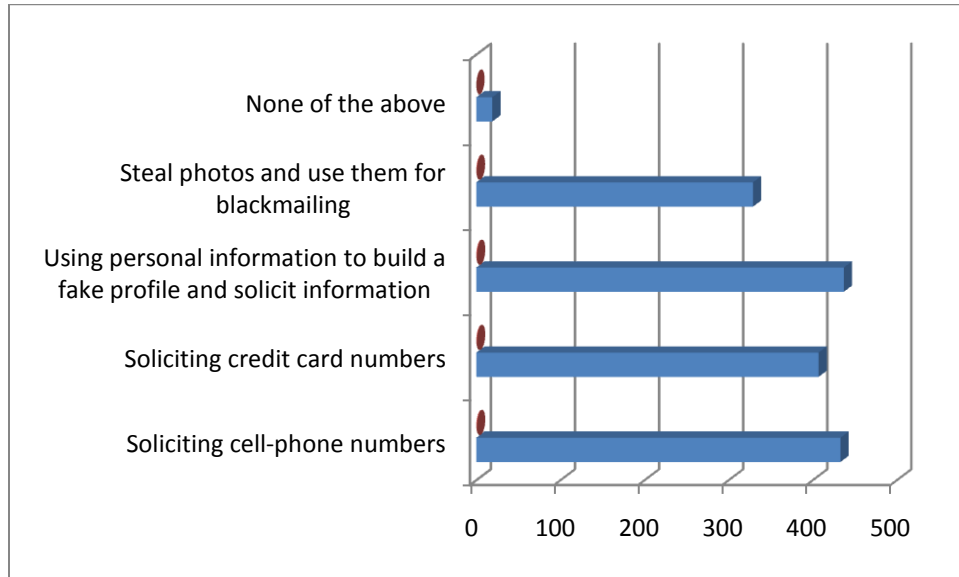
10. Have you ever been a subject to scams on Facebook, like noticing “unknown” charges on your cell-phone bill for services you have NOT subscribed (For ex. Ringtones, horoscopes, etc)?
- Yes
 - No



After finding out from a personal associate that he was scammed, the authors thought this question was more than important to ask since it would actually flesh out the truth behind the extent of scams on Facebook. To the authors' content, 2% of the respondents believed they have been scammed through Facebook games while 98% said they did not think so.

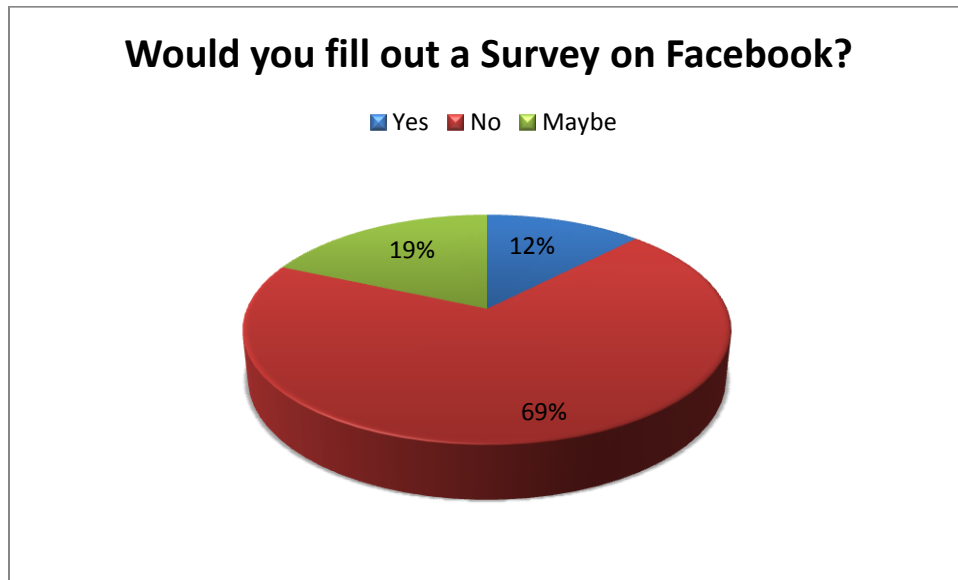
11. Please select all that you think are potential ways of scamming people through Facebook.
 Select one or more.

- a. Soliciting cell-phone numbers
- b. Soliciting credit card numbers
- c. Using personal information to build a fake profile and solicit information
- d. Steal photos and use them for blackmailing
- e. None of the above



This was another question that was meant to measure the level of awareness among Facebook users about the alleged fears of over-sharing on Facebook. Most users seemed to choose multiple ways of scamming, while a straight 4% of the respondents thought that none of the listed ways could be used to steal personal information.

12. Would you be willing to fill out a survey or take a quiz (Ex. IQ Test) in exchange game benefits (For ex. Farmville coins, cash etc.)?
- Yes
 - No
 - Maybe



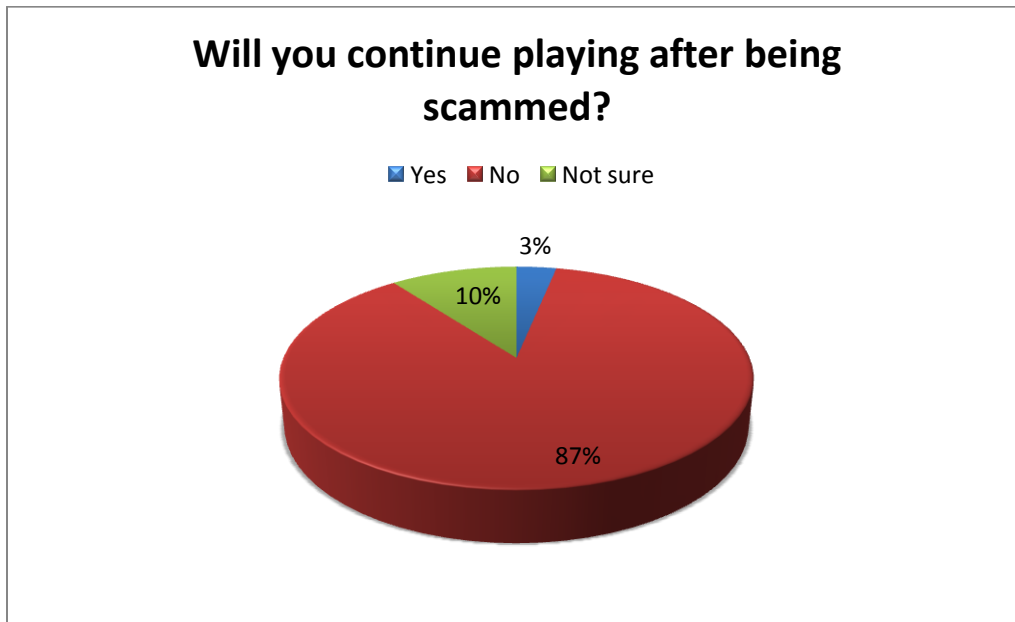
This question was an indirect approach to figure out whether Facebook users would be deceived into giving their personal information to third party developers in the form of answering a survey in exchange for in-game benefits. About a third of the respondents said they would not fill out any surveys or take quizzes while gaming on Facebook to get in-game benefits. However, 12% said they actually will and 18% said they might do so. If the worst case scenario is considered, then 30% of the whole experimental population might be at risk. With the relatively small number of survey population, 495 out of approximately 300 million facebook users, it is definitely a concerning information.

13. Have you ever taken any quizzes (For ex. IQ tests, Life partner quizzes) or completed surveys on Facebook that asked for personal information like your name, date of birth, email address etc.)?
- Yes
 - No
 - Maybe



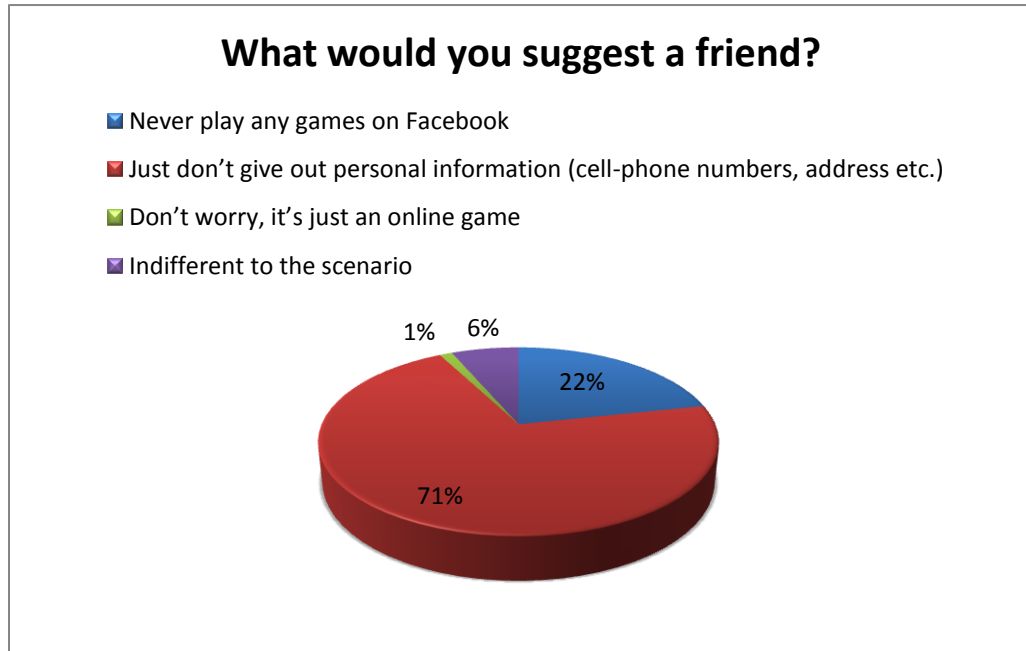
This question was similar to question 12 but it differs in a subtle way. While question 12 was more of a hypothetical question that asked users “if” they would fill out a survey, question 13 asks whether they actually have filled one out already to which 76% answered in the negative and 16% answered in the affirmative while 8% of the people said they might have taken one.

14. Would you still be interested in playing Facebook games if you found out that you were scammed?
- Yes
 - No
 - Not sure



This question was framed to know whether Facebook gamers would return back to gaming if they found out they were scammed and a great majority (87%) said they would not, while 3% said they it does not change anything. About 10% of the people found themselves in a dilemma and were not sure if they would or would not return to playing.

15. What would you suggest a friend in case he/she starts playing Facebook games and you know there is a threat of personal information being mishandled?
- Never play any games on Facebook
 - Just don't give out personal information (cell-phone numbers, address etc.)
 - Don't worry, it's just an online game
 - Indifferent to the scenario



This final question was aimed at seeing if Facebook users would actually look out for their online friends and warn them about the alleged scams in Facebook games. An impressive 71% said they would actually warn their friends to not give out any personal info while playing games on Facebook, while 22% surprisingly said they would actually prevent their friends from playing any games at all. About 6% were not really bothered about the hypothetical scenario and 1% of the respondents said they don't really see the connection between playing Facebook games and the threat to their personal information.

3. Recommendations

In recent years, SNSs have proven to be a fragile ecosystem, where both users and moderators can harm each other. Online Predators, for example, can harm a user psychologically and to some extent physically, and at the same time they can ruin the reputation of the SNS. To make sure that this whole system works properly and creates a safer environment for everyone, both the users and the SNS have to take individual responsibilities to make it happen. In this section of the project, the authors decided to suggest some methods, which they believe, that once undertaken, would create a safer environment. The authors felt that by providing a few suggestions, they would contribute to the betterment of the society in terms of providing a better understanding of this online phenomenon of Facebook, and also in terms of helping anyone to make better life choices with technologies, such as Facebook, in the future.

3.1 Facebook Users

One of the major goals, the authors of this project wanted to achieve was, through this project, raise awareness regarding various ways the Facebook users could get harmed. The survey, even though it does not truly reflect the true characteristics portrayed by Facebook users, is still a starting point for raising awareness. And as every man can only truly protect himself by knowing the intricacies involved in any ecosystem, the authors of this report feel that there are certain responsibilities that needs to be fulfilled by Facebook users, and they are enumerated in the list below.

1. Know the various ways privacy is at stake on Facebook.
2. Never to relay out personal information to any source, unless the source's legitimacy is confirmed.
3. Never be friends with strangers, with whom the user bears no affiliation. If for some reason there is a need to befriend a stranger, make sure that a limited profile is used for further protection of information.
4. If impersonation of anyone known is noticed, make sure that responsibility is undertaken to inform both the person being impersonated and Facebook.
5. Spread awareness of the ways information is at stake on Facebook.

3.2 Facebook

As mentioned before, an increase in the number of scams on a SNS like Facebook would eventually affect its reputation, and thus reduce the number of people participating in applications like Facebook games. This is one thing Facebook would never want, as the revenue generated from its applications has contributed significantly to turn it into multibillion dollar business. Moreover, Facebook being the host for all its users has to make sure that the amount of information the users are sharing is safe.

In the background section (1.12.1.2), it was mentioned how hard it is to monitor illegitimate offers, and as more time goes by, it is getting harder for both Facebook and game developers to monitor scams. Even if Facebook is knowingly being lenient on both developers and offer providers for profit gain, they have to understand that to survive in the long run they have to focus more on legitimate offers. In other words their focal point should be quality, not quantity.

Below is a list of guidelines that are being recommended which once incorporated, should serve towards the well-being of the entire Facebook community.

1. Facebook should try to regulate the ad offers that appear on its applications regularly [14]. Even if it seems extremely tedious, it may be one of the major ways to filter out developers or offer providers who are letting such scams be available. Once Facebook starts to single out these particular subjects, it can take necessary actions against them.
2. Offer Providers should try to establish direct relationships with the Advertisers, thus creating quality feedback loops [14]. Immense amount of advertising deals are direct, and so once a feedback loop is established, it would be much easier to filter out illegitimate sources if traffic.
3. Application developers, mainly the ones who care about quality over quantity could work directly with the Advertisers. Eliminating Offer Providers' direct work relationship with advertisers would definitely make things a lot harder for the Developers. Offer Providers connect the Developers with huge amounts of advertisements that generate tremendous amount of profit over a relatively short period of time, and removing them from the chain would increase the amount of work for the Developers, and their annual revenue would go down. But a direct relationship with Advertisers would make it a lot easier for the Developers to focus on quality [14].
4. If possible, Facebook should try to put a limit on the number of offers a user can sign up for over a certain period of time. Even if this does not protect the users completely (what if a user, for example, who is allowed to sign up for three offers a week signs up for three illegitimate offers?), it might reduce the risks of getting scammed.
5. Facebook may also try to limit users only to a very few Advertisers, for example two, and build a long term relationship with them. For example a user can buy in-game currency in exchange for an item like McAfee VirusScan by transacting with only one Advertiser of their choice [14]. This in the long run would increase quality.
6. Game Developers, Offer Providers, Ad Networks, and Advertisers should try to establish long-term partnerships with one another. This would definitely increase the quality of the offers available to the users, and may also provide more money to the game Developers in the long run as the risk of them getting banned from Facebook goes down.

3.3 Parents

With the gain in popularity of SNS like Facebook, more and more users are creating profiles for various reasons that range from keeping in touch with friends to simply "fitting in". Facebook is without a doubt an amazing tool to interact with friends and family through computers and mobile devices. Sometimes kids and teenagers include too much personal information on their profile, and may indulge in inappropriate behaviors which could get them in trouble or inadvertently

place them at risk by what they share online (McAfee). There are many reasons why underage users may be driven to do things like that. First of all underage users lack experience, and sometimes it is hard for them to justify between wrong and right if they are previously not warned about them. For this reason, it is believed that parents should interfere with their children's personal life regarding online activities, and make sure that their kids are safe when they socialize online. Below is a list of measures that should be undertaken by parents to guarantee their kids' safety.

1. Parents should educate themselves about the different aspects of social networking, and how it is incorporated online in sites like Facebook [21]. The easiest way to do this is by creating profiles on Facebook. This way parents can befriend their children and keep an eye on their daily online activities, and monitor what the kids share online. This is definitely not a guaranteed method, as kids can put their parents under "Limited Profile" option, and share only specific things with them.
2. Parents should try to engage themselves in conversations with their children about their daily online activities. This might help them unfold different things their kids are interested in, and thus could give them an opportunity to research problems associated with that certain online activity. Moreover, WiredSafety.org research has proven that teens who discuss SNSs with their parents behave safer online [21]. Parents should talk to their children about being discreet online and not sharing important information, and problems that may arise from them, and how it may affect their reputation. This should include personal information like phone numbers, email address, personal photos, date of birth, credit card numbers, etc.
3. Kids should only be allowed to spend a certain amount of time a day on their computer, or on the internet. Initially this might annoy the teens in the sense that time on the internet is being restricted, but eventually they would understand.
4. Children should be advised to be careful of strangers they meet online, and how these "friends" could be online predators or cyber bullies [21].
5. Parents should have an open relation with their kids which is mainly built on trust, and should encourage their kids to talk about things they may find unusual or odd on the internet. A relationship built on trust and friendship would also encourage the teens to open up more and talk about more uncomfortable situations like if they get threatened, etc [21].
6. Parents should check for warning signs and symptoms in their children and talk to them [21]. These signs could indicate if their children have been a victim of illegitimate online activities and may include:
 - Feeling upset after using the computer
 - Withdrawing from family and friends
 - Isolating themselves from all sorts of social activities, and staying home most of the time
 - Using computers late at night
 - Getting upset if he/she cannot use the computer
7. If children are uncomfortable to speak to their parents, they should be directed towards an adult they trust.

8. Parents' should educate their children about how to report inappropriate behavior to SNSs. For example in the case of Facebook, all they need to do is send an email to abuse@facebook.com.
9. In order to make sure that strangers are not impersonating a teenager/child, parents should try to search their children's names on SNSs, with different variations in nicknames, and this would give them a rough idea about the presence of an impersonator. They could also check their child's friends list, and try to figure out if there are anyone on it who is a suspicious candidate, for example a middle aged man from another state who has no connection with their kid. This search should always be cross referenced with various aspects of their child's profile, for example their network, groups, interests etc. Parents under any cost should always ask their children about their unlikely acquaintances before they can reach any conclusion.
10. Parents and guardians should educate themselves about various aspects of threats that may arise from SNSs applications, and should have updated computer security software installed to protect their computer from malware, viruses, and other threats [21].

4. Conclusion

Through an in-depth analysis of the two Facebook games and their maker, Zynga Inc., the authors of this report came to an initial conclusion that this particular segment of the computer gaming industry that manifests itself through Facebook is not as transparent as it might seem. There are multiple parties involved in the entire gaming process, starting with the game Developers like Zynga who create the game, to the Advertisers who target their advertisements to the users, to the Offer providers who take a cut in bringing these advertisements to the end user and finally the end users themselves, who are people from all walks of life. This whole cycle of producing a service and providing it to the consumers through deceiving means, operates in perfect harmony until it takes a brave and outspoken individual like Michael Arrington to expose the dirty tricks of the trade. Facebook started off as just a social networking site with the sole intention of connecting people while surpassing all natural and manmade boundaries, but six years down the road finds itself in the midst of a sticky concoction of scams and lies and billions of dollars. It is seen as minting billions of dollars at the expense of those same loyal members that helped it grow exponentially, while skillfully dodging any claims of foul play on its part.

While it isn't only the game Developers like Zynga who are the ones to blame; the consumers, who in this case happen to be Facebook members, are equally responsible for fueling the growth of a system that is based on deceit, falsehood and an insatiable greed for enormous amounts of wealth. From all the intricacies involved in this entire gaming business, the authors observed a few minute details that directly lead to a revealing truth about human nature. Human beings by nature are competent and do not allow any opportunity to surpass without proving their mettle. Through playing games like Mafia wars, the authors have learnt that the engineers at Zynga have only exploited this minor flaw in the human nature and have capitalized immensely on it. Adding addictive elements to each of their games through the use of real time elements and other various

strategies, Zynga owner Mark Pincus made sure he has a steady flow of consumers, hungry for his exciting games. In essence however, Pincus, in collaboration with the Offer providers and Advertisers, has artfully concealed a multibillion dollar corporation behind what could be naively assumed as an innocent gaming business which provides entertainment to its consumers. Every player who spends hours on Mafia Wars and Farmville each day has only one aim in mind while he/she is at it; to earn as much virtual wealth as possible and to emerge victorious against his/her peers. For the gamer, it doesn't really matter if the way to attain that ultimate superiority involves committing every crime in the book, albeit in a virtual world, or if it involves shelling out hard earned money, all for that single moment of self gratification.

Along the way, Facebook users have forgotten that this 21st century world is not a Utopia but a world with every imaginable anti-social character. With every increasing member on Facebook, the wealth of personal information in the hands of a single corporation multiplies manifolds, and a little leniency or short coming in safeguarding one's personal information online can prove highly consequential. Throughout this report, the authors have shown repeatedly the threat to personal information and privacy from various types of malicious characters present in these times, both online and offline.

The authors believe that further research on this project should be carried out in the near future when Facebook will have grown even bigger and maybe a little safer or otherwise. It would be interesting to see how long this trend of exponential increase in Facebook users will continue once all the scams and all the dark secrets of the industry are revealed. Would Facebook continue to bare the tides on its huge success in the SNS realm, or will it eventually sink under its own mistakes and long ignored wrongdoings?

References

- [1.] **Facebook Inc.** “Facebook Statistics.” [Online] 2009. [Cited: November 20, 2009.] <http://www.facebook.com/press/info.php?statistics>.
- [2.] **Stone, Brad.** “Viruses That Leave Victims Red in the Facebook.” *The New York Times Internet*. [Online] December 13, 2009. [Cited: December 15, 2009.] http://www.nytimes.com/2009/12/14/technology/internet/14virus.html?_r=1&em.
- [3.] **Boyd, Danah M. and Ellison, Nicole B.** “*Social Network Sites: Definition, History, and Scholarship*”. s.l. : Michigan State University Press, 2007.
- [4.] **McClard, Anne; Anderson, Ken.** “*Focus on Facebook: Who Are We Anyway?*” Anthropology News, s.l. : In Focus, 2008.
- [5.] **Facebook Inc.** “Facebook: Press Room.” [Online] May 24, 2007. [Cited: December 16, 2009.] <http://www.facebook.com/press/releases.php?p=3102>.
- [6.] **Facebook.** “facebook DEVELOPERS.” *www.facebook.com*. [Online] Facebook, 2009. <http://developers.facebook.com/#>.
- [7.] **Smith, Justin.** “Inside Facebook.” [Online] July 27, 2009. [Cited: December 17, 2009.] <http://www.insidefacebook.com/2009/07/27/10-powerful-ways-to-target-facebook-ads-that-every-performance-advertiser-should-know/>
- [8.] **The Big Money.** “The Big Money Facebook 50.” [Online] November 2009. [Cited: December 16, 2009.] <http://www.thebigmoney.com/slideshow/big-money-facebook-50-0>
- [9.] **Helen A.S. Popkin.** “Facebook’s fantasy games cost more than time.” *msnbc.com*. [Online] MSNBC, November 6, 2009. [Cited: November 11, 2009.] <http://www.msnbc.msn.com/id/33626149>.
- [10.] **Reisinger, Don.** “Facebook games to hold you over until Civilization Network.” *cnet.com*. [Online] CNET, October 23, 2009. [Cited: November 23, 2009.] http://news.cnet.com/8301-17939_109-10382265-2.html.
- [11.] **Rao, Valentina.** “*Facebook Applications and Playful Mood: The Construction of Facebook as a "Third Place"*.” Pornaia (Pisa) : s.n.
- [12.] **Inside Facebook.** Page Data: Mafia Wars. [Online] December 2009. [Cited: December 17, 2009.] <http://pagedata.insidefacebook.com/page/view/391656/>.

[13.] **ACLU.** “What do Quizzes Really Know About You? on Facebook.” [Online] 2009. [Cited: December 17, 2009.]

[http://www.facebook.com/apps/application.php?id=114232425072#/apps/application.php?v=info&id=114232425072.](http://www.facebook.com/apps/application.php?id=114232425072#/apps/application.php?v=info&id=114232425072)

[14.] **Tampell, Alex.** “Tragedy Of The Social Gaming Commons: A Blueprint For Change.” *TechCrunch*. [Online] WordPress.com VIP, November 3, 2009. [Cited: February 6, 2010.] [http://techcrunch.com/2009/11/03/tragedy-of-the-social-gaming-commons-a-blueprint-for-change/.](http://techcrunch.com/2009/11/03/tragedy-of-the-social-gaming-commons-a-blueprint-for-change/)

[15.] **Business Wire.** “Legendary Game Designer Brian Reynolds Joins Zynga as Chief Designer.” *Business Wire*. [Online] Business Wire, June 30, 2009. [Cited: February 6, 2010.] [http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20090630005379&newsLang=en.](http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20090630005379&newsLang=en)

[16.] **Arrington, Michael.** “Zynga's FishVille Sleeps With The Fishes For Ad Violations.” *TechCrunch*. [Online] WordPress.com VIP, November 8, 2009. [Cited: January 31, 2010.] [http://techcrunch.com/2009/11/08/zyngas-fishville-swims-with-the-fishes-for-ad-violations/.](http://techcrunch.com/2009/11/08/zyngas-fishville-swims-with-the-fishes-for-ad-violations/)

[17.] **Ewalt, David M.** “In Pictures: The Web Celeb 25.” *Forbes*. [Online] Forbes, January 23, 2007. [Cited: January 23, 2010.] [http://www.forbes.com/2007/01/23/web-celeb-25-tech-media_cx_de_06webceleb_0123top_slides_11.html?thisSpeed=15000.](http://www.forbes.com/2007/01/23/web-celeb-25-tech-media_cx_de_06webceleb_0123top_slides_11.html?thisSpeed=15000)

[18.] **Times, Financial.** “Facebook in Lawsuit over Unauthorized Charges.” *Financial Times*. [Online] Financial Times, November 25, 2009. [http://www.ft.com/cms/s/0/058f5260-d92c-11de-b2d5-00144feabdc0.html?nclick_check=1.](http://www.ft.com/cms/s/0/058f5260-d92c-11de-b2d5-00144feabdc0.html?nclick_check=1)

[19.] **Arrington, Michael.** “Zynga CEO Mark Pincus: "I Did Every Horrible Thing In The Book Just To Get Revenues".” *TechCrunch*. [Online] WordPress.com VIP, November 6, 2009. [Cited: January 31, 2010.] <http://techcrunch.com/2009/11/06/zynga-scamville-mark-pinkus-faceboo/>

[20.] **Pontiflex Inc.** “The Online Lead Generation Glossary.” *Pontiflex*. [Online] 2008. <http://www.pontiflex.com>

[21.] **McAfee Inc.** “A Parent's Guide to Social Networking Sites.” *McAfee Inc. Web site*. [Online] 2009. [Cited: January 30, 2010.] <http://us.mcafee.com/en-us/local/docs/SocialNetworkinge-guide.pdf>

[22.] **Lawless, Jill and Perry, Dan.** “Prisoner Lose Facebook Pages After Victim Taunts.” *The Huffington Post*. [Online] HuffingtonPost.com, Inc., February 2, 2010. [Cited: February 16, 2010.] http://www.huffingtonpost.com/2010/02/11/prisoners-lose-facebook-p_n_458059.html

- [23.] **AdCouncil.** "Online Sexual Exploitation." *AdCouncil*. [Online] AdCouncil, 2010. [Cited: February 26, 2010.]
<http://www.adcouncil.org/default.aspx?id=56>
- [24.] **SOPHOS.** "Simple steps to avoid being phished." *SOPHOS*. [Online] SOPHOS. [Cited: March 2, 2010.]
<http://www.sophos.com/security/best-practice/phishing.html>.
- [25.] **Siegler, MG.** "Phishing Attack Underway At Facebook. Don't Sign In To Fbaction.net." *TechCrunch*. [Online] TechCrunch, April 29, 2009. [Cited: February 4, 2010.]
<http://techcrunch.com/2009/04/29/phishing-attack-underway-at-facebook-dont-sign-in-to-fbactionnet/>
- [26.] **Dudley, Brier.** "Zango goes bango, CEO bankrupt." *The Seattle Times Company*. [Online] The Seattle Times Company, April 22, 2009. [Cited: February 3, 2010.]
http://seattletimes.nwsourc.com/html/technologybrierdudleysblog/2009109821_zango_goes_bango_ceo_bankrupt.html
- [27.] **Sophos.** "Only one in 28 emails legitimate, Sophos report reveals rising tide of spam in April - June 2008." *Sophos*. [Online] Sophos, July 15, 2008. [Cited: January 30, 2010.]
<http://www.sophos.com/pressoffice/news/articles/2008/07/dirtydozjul08.html>
- [28.] **Adonomics.** "Zynga|Adonomics." *Adonomics*. [Online] Adknowledge, Inc. [Cited: February 3, 2010.]
<http://adonomics.com/company/Zynga>
- [29.] **Arrington, Michael.** "'Horrible Things' Slink Back Into Zynga." *TechCrunch*. [Online] WordPress.com VIP, November 7, 2009. [Cited: February 1, 2010.]
<http://techcrunch.com/2009/11/07/horrible-things-slink-back-into-zynga/>
- [30.] **Arrington, Michael.** "Scamville: Zynga Says 1/3 Of Revenue Comes From Lead Gen And Other Offers." *TechCrunch*. [Online] WordPress.com VIP, November 2, 2009. [Cited: February 1, 2010.]
<http://techcrunch.com/2009/11/02/scamville-zynga-says-13-of-revenue-comes-from-lead-gen-and-other-offers/>
- [31.] **Arrington, Michael.** "Scamville: The Social Gaming Ecosystem of Hell." *TechCrunch*. [Online] WordPress.com VIP, October 31, 2009. [Cited: January 29, 2010.]
<http://techcrunch.com/2009/10/31/scamville-the-social-gaming-ecosystem-of-hell/>
- [32.] **Yu, Dennis.** "How to Spam Facebook Like A Pro: An Insider's Confession." *TechCrunch*. [Online] WordPress.com VIP, November 1, 2009. [Cited: January 30, 2010.]
<http://techcrunch.com/2009/11/01/how-to-spam-facebook-like-a-pro-an-insiders-confession/>

- [33.] **Ducklin, Paul.** “Sophos Australia Facebook ID probe 2009”. *Sophos* [Online] Sophos Australia, December 6, 2009. [Cited: February 10, 2010]
<http://www.sophos.com/blogs/duck/g/2009/12/06/facebook-id-probe-2009/>
- [34.] **Wiseman, Josh,** “Facebook Chat: Now we’re talking”. *Facebook Blog* [Online] Facebook, April 6, 2008. [Cited: September 9, 2009]
<http://blog.facebook.com/blog.php?post=12811122130>
- [35.] **Reuters,** “TechCrunch founder gets last laugh”. *Reuters Blogs* [Online] Reuters November 6, 2009. [Cited: March 2, 2010]
<http://blogs.reuters.com/small-business/2009/11/06/techcrunch-founder-gets-last-laugh/>
- [36.] **Zynga.** About Zynga. [Online] Zynga. <http://www.zynga.com/about/>
- [37.] **Letzing, John.** “Facebook’s Russian Backer, Digital Sky Technologies, Buys Into Zynga.” *Wall Street Journal.* [Online] Dow Jones & Company, Inc., December 16, 2009. [Cited: February 3, 2010.]
<http://online.wsj.com/article/BT-CO-20091216-713927.html>
- [38.] **Gross, Doug.** MIT wins \$40,000 prize in nationwide balloon-hunt contest. *CNN Tech.* [Online] December 7, 2009. <http://www.cnn.com/2009/TECH/12/05/darpa.balloon.challenge/>.