Date of acceptance Grade

Instructor

# Review of Social Networking Sites' Security and Privacy

Shun Yang

Helsinki September 10, 2015

M.Sc. Thesis

UNIVERSITY OF HELSINKI
Department of Computer Science

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

| | |
|---|---|
| Tiedekunta — Fakultet — Faculty<br>Faculty of Science | Laitos — Institution — Department<br>Department of Computer Science |

Tekijä — Författare — Author
Shun Yang

Työn nimi — Arbetets titel — Title
Review of Social Networking Sites' Security and Privacy

Oppiaine — Läroämne — Subject
Computer Science

| | | |
|---|---|---|
| Työn laji — Arbetets art — Level<br>M.Sc. Thesis | Aika — Datum — Month and year<br>September 10, 2015 | Sivumäärä — Sidoantal — Number of pages<br>60 pages + 0 appendices |

Tiivistelmä — Referat — Abstract

Nowadays social media networking has dramatically increased. Social networking sites like Facebook make users create huge amount of profiles and share personal information within networking of different users. Social networking exposes personal information far beyond the group of friends. And that information or data on social media networking could be potential threat to people's information security and privacy.

In this review, we are going to view the privacy risks and security problems of social media websites. We also present the types of potential security attacks and how they are made. We will show the basic security requirements for social media networking and present some useful security solutions from both personal users and networking experts.

Avainsanat — Nyckelord — Keywords
social networking sites, security, privacy

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — övriga uppgifter — Additional information

# Contents

# 1 Introduction and related work

Social Networks Sites (SNS) such as Facebook, MySpace, Twitter and LinkedIn have become extremely popular. Most SNS provide basic features, such as online communication, interaction and creating profiles. SNS allow users to post rich information, search friends, and establish relations with new friends. Users can share ideas, events and activities on SNS and also comment on each others' post. To date, we already have a lot of social media applications, some of which are quite popular on mobile devices, see Figure 1 from google image.

Figure 1: Examples of popular SNS applications used on Smart phone

We review previous studies about security and privacy issues of SNS. We start from the background of security and privacy issues of SNS.

The authors of [bE07] described features of SNSs, proposed a comprehensive definition of SNS. The authors also presented the history of SNS discussing key changes and developments. In [FPT14], the authors reviewed some typical attacks conducted on SNSs and presented some solutions to improve the security of SNSs. [Gun11] addressed different privacy and security issues and presented the techniques that attackers use to overcome social network security mechanisms. [BC09] showed that majority of users' personal attributes can be derived from social contacts. The authors gave solutions to remove risky friends and group risky friends and apply access controls to the group to limit visibility. [MJB11] presented an empirical evaluation of actual preferences and behavior of Facebook users which revealed the inconsistencies between users' sharing intentions and privacy settings. In [NWM10], the authors proved that highly personal, sensitive, and potentially stigmatizing information is being disclosed on SNSs.

In [RKK14], the authors gave detail descriptions of two kinds of profile cloning attacks on SNSs and proposed a new approach of defining strength of relationship and profile similarity to detect clone identities. The authors of [SKV10] analysed how spammers attack SNSs. The authors analysed collected data of spamming activity and identified anomalous behaviour. [BHI$^{+}$08] studied Facebook's policies and usage that might make users vulnerable to sophisticated attacks via context-aware email. [TCJ10] presents a novel co-classification framework to simultaneously detect spam attacks and spammers on SNSs based on content and link-based features. In [Hon12], the authors gave an introduction to the current state of phishing. The authors present how phishing attacks work, why people fall for them, and the actual damage caused. The authors of [SP07] discussed the ways and means of defending against phishing and pharming by using three approaches of technology, law enforcement and customer education and awareness.

As regards the necessary actions for maintaining secured SNS, many requirements are needed. In [SW09], the authors showed that information security management guidelines play an important role in managing and certifying information security in all organizations including ones that run SNSs. The authors of [DB00] showed that confidentiality, integrity, availability, responsibility, integrity, trust and ethicality principles are the keys for successful information security management. [VSVS04] identified the 10 most important aspects which result in companies experiencing severe problems in implementing a successful comprehensive information security plan. In [WJC99][GL04], the authors presented how a firewall achieves maximum network security and maximum user convenience. The authors of [SS94] explained access control and its relationship to other security services such as authentication, auditing. and administration. The authors then reviewed access control policies commonly found in current systems, and a brief consideration of access control administration. [NJ05] compared the performance of four popular secret key encryption algorithms including DES, 3DES, AES and Blowfish. [HDL$^{+}$90] and [BL09] discussed an approach to obtain network security based on capturing and analysing network activity. All these aspects are relevant for SNSs

Next we review some papers on technical solutions that can be used in securing

SNSs. In [ERB03], the authors presented salient issues and proposed solutions of generic Web users' Web privacy. The authors of [WK08] made a survey which systematically analyzes existing privacy-enhanced personalization solutions and their underlying privacy protection techniques. In [BS03], the authors presented technological solutions combined with laws, societal norms and aspects related to markets. [FH98] provided a common sense definition of a Virtual Private Network, and an overview of different approaches to building Virtual Private Network. In [RC99] [CLM$^+$02], the authors described the specification of the Platform for Privacy Preferences (P3P), along with its normative references, including all the specification necessary for the implementation of interoperable P3P applications. [LAE$^+$04] presented a practical and efficient approach to incorporating privacy policy enforcement into an existing application and database environment, and explored some of the semantic trade-offs introduced by enforcing these privacy policy rules. The authors presented the founding principles of a Hippocratic database [GJK08], outlined several technologies that advance these principles, evaluated the state of the art in Hippocratic database-enabling technologies. In [Mal14], the authors proposed two privacy-preserving protocols and one group signature based framework that focus on the design of advanced privacy-preserving cryptographic protocols. The authors of [CS09] presented a framework of data anonymization techniques. The authors proposed a framework for efficient privacy preservation in terms of execution time and information loss in [GKKM07].

In [KDWS03] and [KDWS05], the authors presented the theoretical foundation of the random value distortion technique which preserve data privacy and extensive experimental results. [LKR06] explored the use of random projection matrices for privacy preserving data mining and proved that after perturbation, the distance-related statistical properties of the original data are still well maintained without divulging the dimensionality and the exact data values. In [Evf02], the authors presented different ways and results of randomization of categorical and numerical data. The authors of [AP04] [AY08] developed a new and flexible approach which maps the original data set into a new anonymized data set and which does not require new problem-specific algorithms for privacy preserving data mining.

The authors of [AP08] presented a survey of the broad areas of privacy-preserving data mining and the underlying algorithms. [LP02] introduced the concept of privacy preserving data mining and presented a solution demanding very few rounds of communication and reasonable bandwidth that is considerably more efficient than generic solutions. [MGA12] reviewed a good number of existing Privacy-Preserving

Data Mining techniques and proposed some future research directions. The authors of [VBF$^+$04] gave an overview of privacy preserving data mining and proposed a classification hierarchy to analyse the work with the concepts of basis set.
Some legislation solutions are also presented to solve security and privacy of SNS. The authors of [WWDF12] recommended steps for social media policy development. IT departments, Human Resources and Legal Counsel will increasingly need to work together to develop the organization's social media policies. [Doy11] gave a brief sketch of Computer Fraud and Abuse Act and some of its federal statutory companions, including the amendments found in the Identity Theft Enforcement and Restitution Act. There are also some other Acts such as [OAW12] and [DJ09] which gave some legislation solutions.

The rest of the thesis is organized as follows. We present the related background for SNSs in Section 2. Section 3 describes the potential attacks, and Section 4 displays requirements for security and privacy of SNS. Section 5 shows solutions to security and privacy issues of social networking sites. Finally, we make summary in Section 6.

# 2 Background

To begin with the background, we firstly need to understand what exactly is social networking. The twenty-first century is characterized by communication and transportation technologies. These technologies shrink the world, make it smaller, and thus bring persons geographically far from each other into close social contact.
SNS is one of the most popular ways for communication in modern world. In this section, we will present the development of social networking sites, the basic concepts of security and privacy and show how they exist in social networking sites.

## 2.1 Social Networking Sites' history and development

To review the history and development of SNS, we need to start from the definition of SNS, and then follow the timeline of SNSs and view how SNS's technologies and properties have changed.

### 2.1.1 Definition of Social Networking Site

A SNS is defined as an online platform that allows users to create a public profile and interact with other users on the website. SNSs are web-based services that allow individuals to create a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system [ZSZF10].

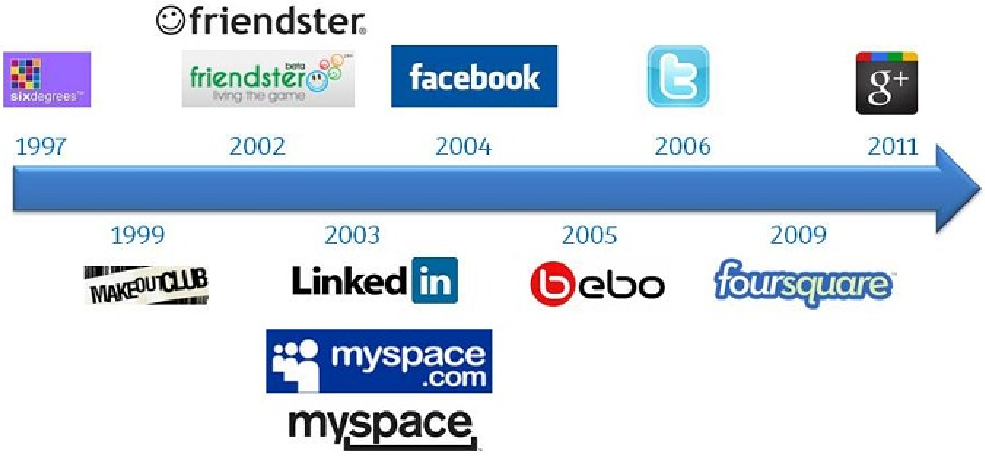


Figure 2: popular SNS timeline from 1997 to 2011

For most popular SNSs showing up from 1997 to 2011, see Figure 2 from google image. SNSs have kept a stable increasing trend generally though they have met some problems, such as technical difficulties, and management problems.

### 2.1.2 Early Social Networking Sites

Many SNSs showed up early, such as Geocities, TheGlobe, AOL Instant Messenger, SixDegrees, Classmates, Friendzy, Hi-5, AsianAvenue, BlackPlanet, MiGente and Yahoo. We will present some outstanding SNSs among these pioneers.

***SixDegrees*** existed from 1997 to 2001, and it was the first widely recognizable SNS. SixDegree allowed users to create individual profiles, invite friends, organize groups, list friends and then surf the friend lists of other users. SixDegrees was a good tool to help users connect with and send messages to each other. SixDegrees attracted millions of users while it failed to run a sustainable business [bE07].

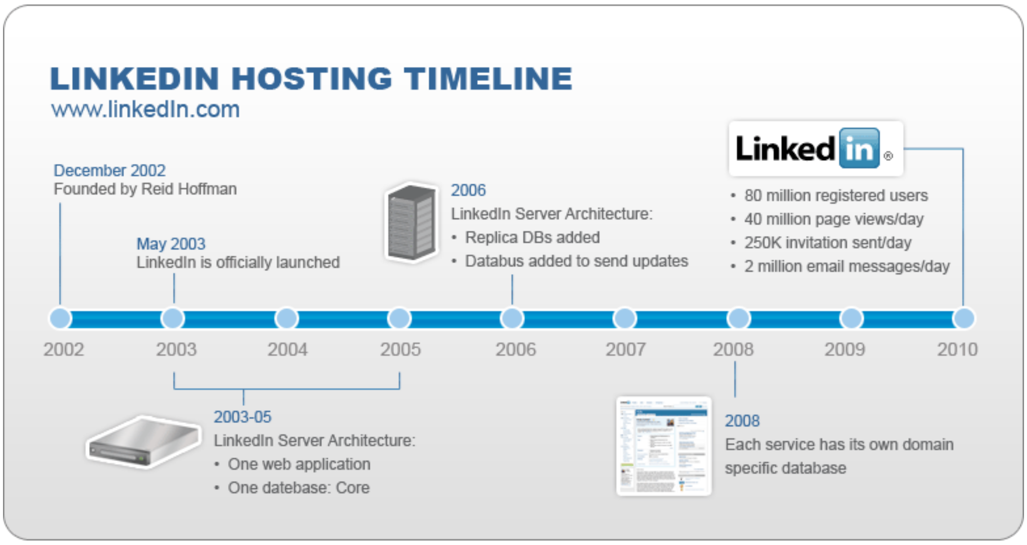
***Hi5*** is another popular early SNS which was established in 2003 and became the 8th largest SNS by middle of 2006. In 2009, Hi5 refocused itself to be a social gaming platform and has been kept open to game developers. Hi5 runs profile privacy differently than most other SNSs as users' network consist of not only their directly connected (first degree) contacts, but also friends of friends (second degree) and friends of friends of friends (third degree) contacts.

### 2.1.3 Modern Social Networking Sites

For recent years, we have a new era for SNS. More successful SNSs have been generated, such as Friendster, LinkedIn, MySpace, Facebook, twitter, and Google+. These SNSs have more powerful functionality and better user experience.

***Friendster*** was founded in 2002. Friendster was the first real model for SNS. It was the pioneer of using the concept of online networking between real-world friends.
Friendster allowed users to discover their friends and friends of friends to expand their networks. Friendster was a SNS for dating which aimed to offer a safe place to meet new people faster than in real-life. Later Friendster met technical difficulties and questionable management, it briefly abandoned social networking and now remains as an online game site.
***LinkedIn*** was founded in 2003 and was one of the earliest SNSs devoted to business people. Later, LinkedIn allowed users to post their profiles to interact with each other by private messaging. The profiles on LinkedIn are basically resumes of users.
Following the time, LinkedIn implemented some other important features, such as question and answer forums, groups, and real-time updates etc. LinkedIn contacts can be regarded as professional connections between users. LinkedIn is a wonderful SNS resource which business people use to build connections with other professionals. The details of LinkedIn timeline are presented in Figure 3 from google image.

***MySpace*** was founded in 2003 and had became the most popular SNS in the world by 2006. MySpace cloned Friendster initially and then continuously built up better functionality. MySpace gave users more freedom with music, videos and funky feature-filled online environment which lead to better customization. MySpace allowed users to completely customize the look of their profiles. Users were also allowed to embed videos from other sites on their profiles and post artists' music on MySpace.
From the start, MySpace supported communication through private messages. Users could make comments that were posted to a user's profile publicly, and users could also send out bulletins to all friends. MySpace let each user automatically run a blog



LINKEDIN HOSTING TIMELINE

www.linkedIn.com

December 2002
Founded by Reid Hoffman

May 2003
LinkedIn is officially launched

2006
LinkedIn Server Architecture:
- Replica DBs added
- Databus added to send updates

- 80 million registered users
- 40 million page views/day
- 250K invitation sent/day
- 2 million email messages/day

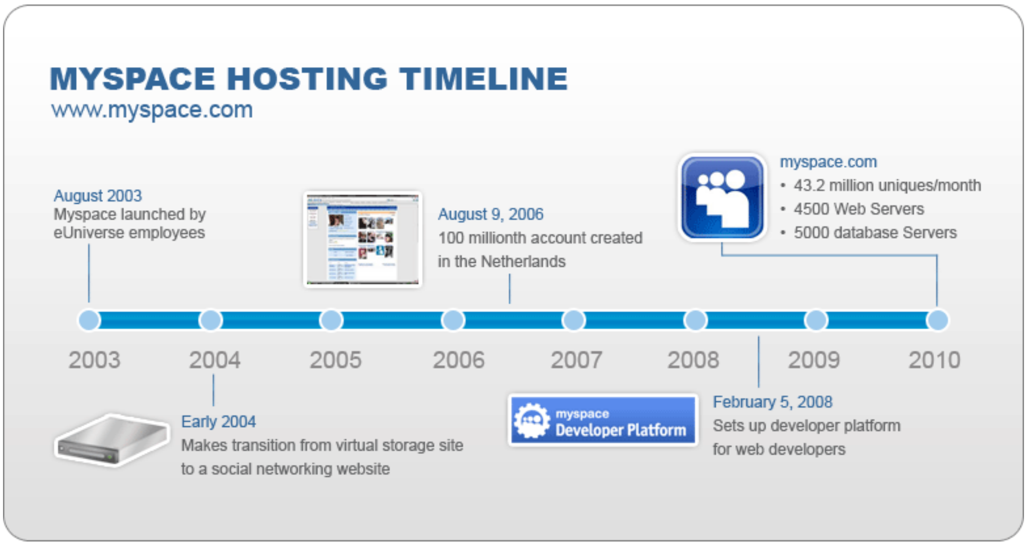
2003-05
LinkedIn Server Architecture:
- One web application
- One datebase: Core

2008
Each service has its own domain specific database

Figure 3: Linkedin Hosting Timeline

and these blogs became a big part of users' profiles. MySpace introduced instant messaging in 2006 which allowed users to communicate with their friends. MySpace included some other additions to its functionality such as a news feed and real-time status updates showing friend activity.

While the number of users have declined, MySpace turned to a social networking sites targeted to bands and musicians. We can check how MySpace grows from the



MYSPACE HOSTING TIMELINE

www.myspace.com

August 2003
Myspace launched by eUniverse employees

August 9, 2006
100 millionth account created in the Netherlands

myspace.com
- 43.2 million uniques/month
- 4500 Web Servers
- 5000 database Servers

Early 2004
Makes transition from virtual storage site to a social networking website

February 5, 2008
Sets up developer platform for web developers

Figure 4: MySpace Hosting Timeline

timeline described in Figure 4 from google image.

***Facebook*** was generated in 2004 initially targeting only college students in Harvard.

When it opened to everyone, it grew exponentially to become the world's most popular SNS by 2008.

Facebook doesn't have same kind of customization as MySpace. Facebook allows users to post photos and videos. Over the past few years, Facebook has added some other features such as instant messaging, applications and application developer platform. Private messaging is available and users can also write on other users' walls, which offers users different methods to communicate with each other. Wall posts are visible to users' friends. Users can easily change their privacy settings which allow different users to see different parts of their profiles based on the relationships. The basic privacy could be set to "only friends", "friends of friends", or "everyone".

Users could post visible notes to all friends. Users could also make comment and "like" the posts of their friends. Within the comment sections, users could have a lot of conversations with multiple people. Facebook has had a stable growth with business, see Figure 5 from google image.

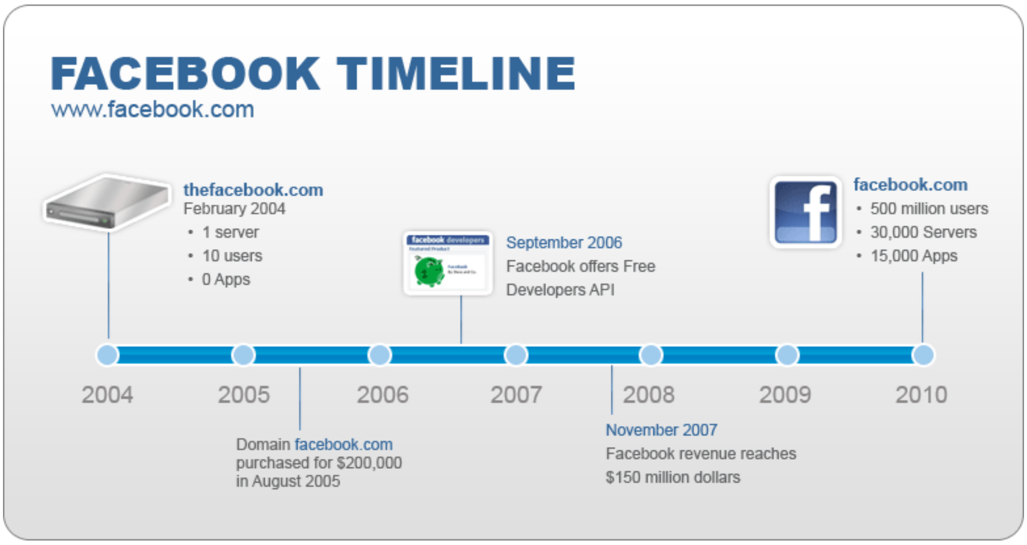


Figure 5: Facebook Timeline

### 2.1.4 Evolution of Social Networking Sites

At 2015, the top SNS is Facebook. Looking back, Facebook gained huge success based on innovative features of its platform and a series of smart moves.

In 2007, Facebook Platform was launched and it was the beginning of success. Facebook released the open API which attracted a massive amount of attention from third-party developers. Facebook made it possible for third-party developers to create applications that work within Facebook itself. Facebook had so huge amount of applications built on its platform that Facebook launched the Facebook Application Store to organize, display and sell these applications. What is more, Facebook's ubiquitous "Like" button which involve the users into interactive participation. These actions bring remarkable benefit for Fackbook and lead to sustainable growing.

## 2.2 Security and Privacy issues of Social Networking Site

No matter how social networking sites expand, security and privacy issues always follow and remain as big challenges for users. In this thesis, the security and privacy issues of SNS mainly focus on users' personal data. To unfold this research, we firstly need to learn the basic concepts of privacy and security, and secondly study some real cases on SNS.

### 2.2.1 Basic concepts of Security and Privacy

In practice, SNSs ensure that individual data being stored is safe from unauthorized access and use, users data is reliable and accurate and it is available when it is needed. Data security is also called information security. We apply data security technologies, to ensure SNS's digital data, hard drives, hardware and software are unreadable to hackers and unauthorized users.

Usually, SNS's security objectives consists of the integrity, availability and privacy of data, see Table 1.

Data integrity means user data have not been modified, and user data remain the same as the original data. One typical attack against data integrity is a man-in-the-middle attack. In the man-in-the-middle attack, hackers will stop and modify the data during data transmission.

Data availability ensure that user could always access website resource and information. It is important to make sure that authorized users can access data at any time. While denial of service is one type of attack which could stop authorized users access data normally, this type of attack aims to interrupt service.

Data privacy is related to the appropriate use of information. In other words, merchants, companies and third parties should use the data provided to them only for the legal purpose. Data privacy is also called information privacy. Data privacy apply information technology to decide what data of individuals or SNSs can be

Table 1: SNS's Security Objectives

| ***Types*** | ***Descriptions*** |
|---|---|
| Integrity | Users' data and identities have to be protected against unauthorized interference and modification |
| Availability | Users' data have to be available whenever they are needed |
| Privacy | All of users' information and actions have to be concealed from any third-party internal or external to the system, except clearly reveal by users [ZBW12] |

shared with third parties.

### 2.2.2 Security issues of personal data

As popularity of SNSs grows, our personal data meet higher risks. All data on SNS are under security threat, even in well-protected sites. Statistics of cybercrime around the world show that America, China and Germany are on the top list with cybercrime, see Figure 6 from google image. All SNSs are potential targets of cybercrime, and bad people would use personal data on SNS for illegal purposes.

SNSs generate huge amount of data every single day. Personal identifiable information and other kinds of sensitive data are under threats internally and externally. Typically, we have three kinds of data controllers on social networking sites: users, SNS providers and application providers, see Table 2. All users on social networking sites create profiles for themselves. These profiles contain much information, such as users' gender, age, interests, geographical location, photos, and biographical information (hometown, education, employment history, etc.). Personal data maintained on SNS could be leaked, lost, stolen or accessed illegally.

Criminals such as identity thieves, spammers, virus writers, scam artists, debt collectors, stalkers and hackers follow all SNSs. Even some corporations gather information of potential consumers from SNS for a market advantage. Companies that run SNS business might collect a variety of data of individual users, in order to sell to advertisers and personalize the services for the users.

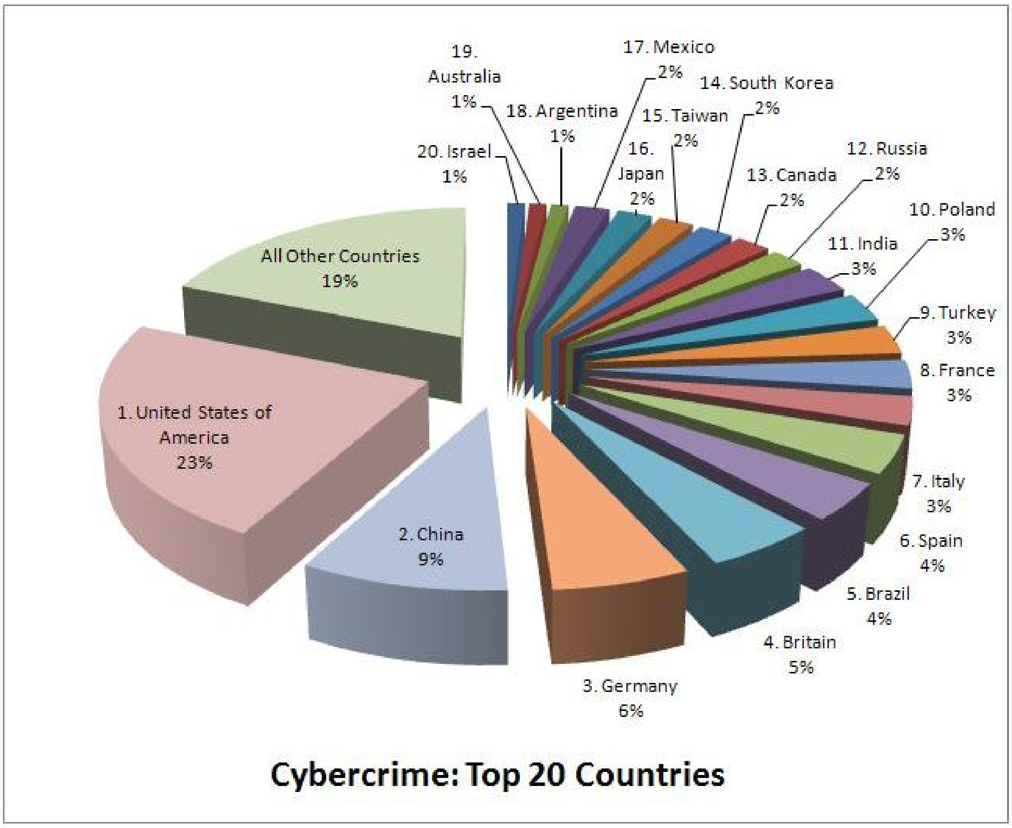


Figure 6: Top 20 Countries with most Cybercrime

### 2.2.3 Privacy risks in social networking sites

According to survey of Pew Research Center [RKK+13], a lot of personal information is available on SNS, see Figure 7 from google image.
Users do not want all of their information be public. Some users prefer part of their information to be viewed by specified connected friends. Some users even want most of their information be private. When posting some information on a social networking site, we typically expect that authorized friends can see it. But we have no idea who else can view it, and what exactly is visible. On SNSs, users' information can become public in a various ways, see Table 3.

Some companies that run the social networking sites are collecting users' personal information by different means for different intentions, see Table 4.

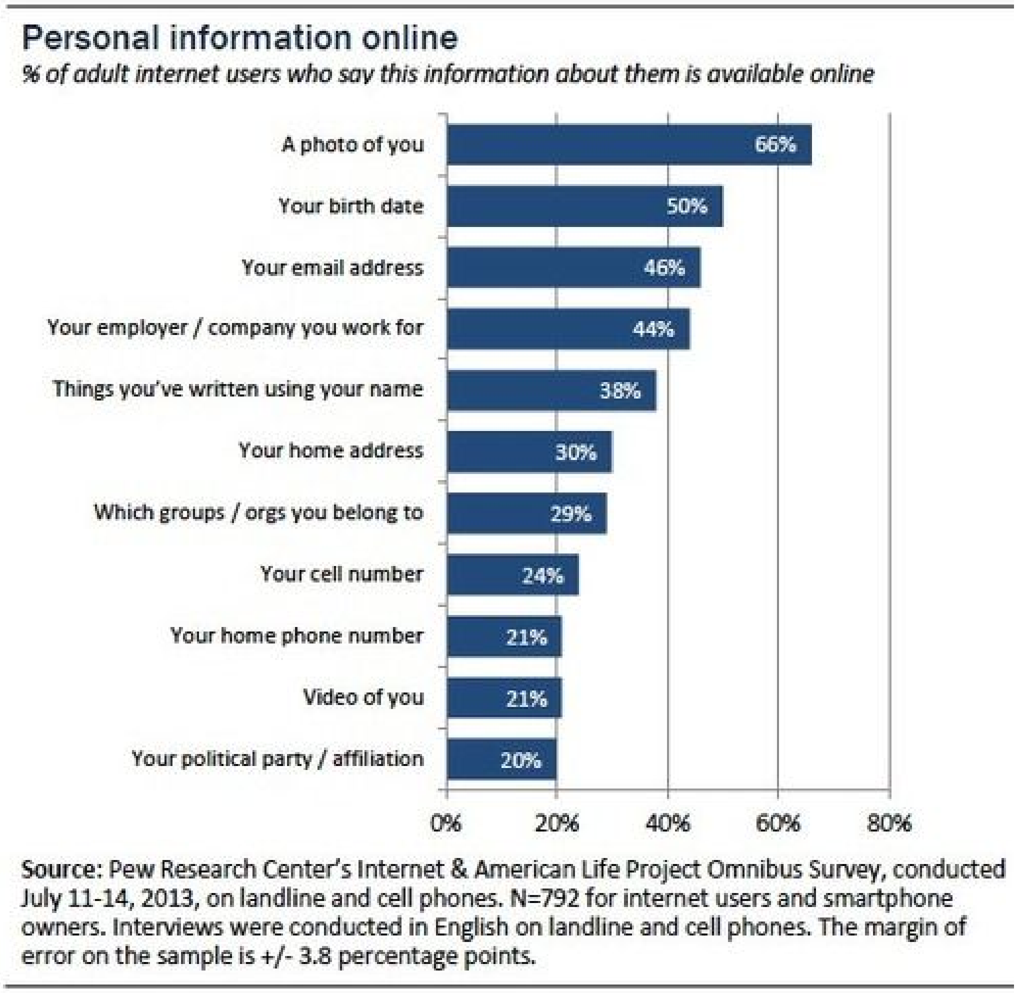
SNSs integrate third-party content which gives third-party developers access to user data. For current networking environments, most third-party applications usually request users for permission to access users' personal information. To guarantee the basic functions of application, users just need to provide some basic information.

Table 2: Typical kinds of data controllers on SNS

| ***Types*** | ***Descriptions*** |
|---|---|
| Users | Users are regarded as data subjects in most cases. |
| SNS providers | SNS providers provide the means for the processing of user data and provide all the basic services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes, including advertising provided by third parties. |
| Application providers | Application providers develop applications which run on SNS and users decide to use such an application. |

Accessing extra information could be forbidden. The SNS's service provider should supervise the application to use information access control, in order to get rid of threats against privacy.

A SNS sometimes change our privacy settings, to make what used to be visible only to our friends visible to everyone. This is one reason why we need to be concerned about the privacy risks on SNSs.



Personal information online

*% of adult internet users who say this information about them is available online*

**Source:** Pew Research Center's Internet & American Life Project Omnibus Survey, conducted July 11-14, 2013, on landline and cell phones. N=792 for internet users and smartphone owners. Interviews were conducted in English on landline and cell phones. The margin of error on the sample is +/- 3.8 percentage points.

Figure 7: Personal Information Online

# 3 Potential attacks against social media sites

There have been potential attacks against SNSs, and in this section we introduce and describe only the most known and widespread attacks. Generally, there are two different kinds of attackers: intruders and insiders [FPT14].

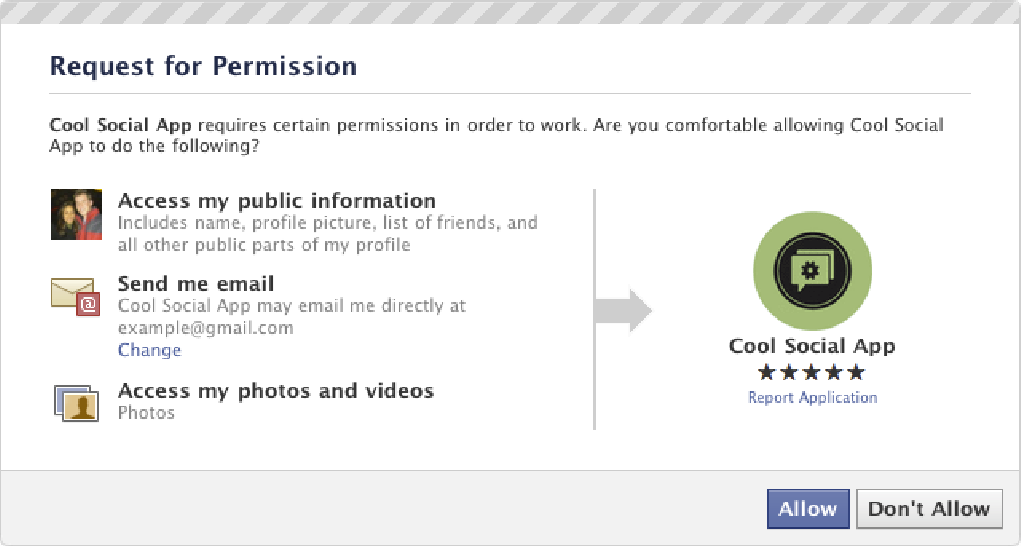
Intruders are attackers outside the SNS system. Intruders need to access the system without proper authorization, or take malicious actions to conduct the attack.

Insiders are attackers inside the SNS system. Legitimate users or entities participating in the systems operations can assume malicious behaviours. For example, SNS service provider could be an insider.

We will present passive attacks, active attacks, malware attacks, identity theft attacks, spam attacks, phishing attacks and pharming attacks. These attacks are more

Table 3: How user information become public on SNS

| ***How user information become public on SNS*** |
|---|
| Users post information as public without adjusting privacy settings to restrict access. |
| A SNS adjusts its privacy policy sometimes without a user's permission. Though content is posted with restrictive privacy settings, it still might become public after privacy policies get modified. |
| Third-party applications might have been granted access to view users' information, with the ability to see posts and contacts privately, see Figure 8. |
| Certain information might be publicly visible by default, and users can not restrict access to it. For this situation, the users could change the privacy settings to set the information private, so that only the approved users can view it, and other information still remain public. |
| Approved friends might potentially bypassing privacy settings that they could copy and repost information like photos, without permission of users. |



Request for Permission

**Cool Social App** requires certain permissions in order to work. Are you comfortable allowing Cool Social App to do the following?

**Access my public information**
Includes name, profile picture, list of friends, and all other public parts of my profile

**Send me email**
Cool Social App may email me directly at example@gmail.com
Change

**Access my photos and videos**
Photos

Figure 8: Facebook third-party application request the permission to access users' information

Table 4: Entities collecting users' data

| ***Entities collecting users' data*** | | |
|---|---|---|
| Types | Purposes | Examples |
| legal | Advertisers interested in personal information for more potential customers | Analysis of the data obtained from users, present their advertisements of related products to those users who most likely to be interested |
| | Third-party application developers who incorporate information to personalize applications | Online games interact with the social network users |
| illegal | Steal users' identities | Gain personal information either based on information a user posts or that others post about the user |
| | For other kinds of criminals | Scam or harass individual users, or infect users' computers with malicious software |

and more common on SNSs nowadays.

## 3.1 Passive attacks

Passive attacks do not disrupt proper operation of networking. Attacker snoops data exchanged in the network without altering it. Since the operation of network is not affected under passive attacks, it is difficult to detect passive attacks.

We have three common types of passive attacks: Eavesdropping, Monitoring and Traffic analysis. The detailed descriptions are given below.

***Eavesdropping*** — aims to find some secret or confidential information that should be kept secret during the communication. Confidential information might, for example, be private or public key of sender or receiver or any password. In general, majority of network communications occur in an unsecured format, which allows an attacker who has gained access to data paths in users' network to eavesdrop the traffic. Eavesdropping the communications is also referred to as sniffing or snooping.

***Traffic analysis*** — the eavesdropper analyses the traffic and observes the frequency and length of message being exchanged, then identify communicating hosts, and determine the location. The eavesdropper would use all information to predict the nature of communication. All incoming and outgoing traffic of network is only analysed without being altered. Even when message content is encrypted, the attacker may still be able to observe the pattern of these messages. The attacker could determine the identity and location of communicating users and could observe the frequency and length of messages being exchanged. This information would be useful for guessing the nature of the communication.

In passive attacks, neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, we still have methods to prevent the success of passive attacks, by using strong encryption. It is more feasible to prevent passive attacks from being effective than to detect these attacks. Passive attacks could also be preparation of active attacks.

## 3.2 Active attacks

We have four common types of active attacks on SNS: Masquerade/Spoofing, Replay, Modification and Denial of service. The detail of these attacks are given below.

***Masquerade/Spoofing*** — an entity pretends to be a different entity. For Spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else.

***Replay*** — capture and subsequent retransmission of data.

***Modification*** — the modification consists of substitution, insertion, or destruction. Legitimate messages are altered or deleted, or fake messages are generated.

***Denial of service*** — Normal use or management of the system is prevented or inhibited.

Active attacks are more difficult to prevent, but they could be detected more easily. Active attacks are quite effective when applied after passive attacks, since passive attacks offer the attacker a lot of useful information before the active attacks.

## 3.3 Malware Attacks

Malware is short expression for malicious software. Malware is defined as any software designed to do something that users would not wish it to do, have not asked it to do, and users often have no knowledge of malware until it is too late. Malware is used by attackers to get access to computer systems, collect sensitive information, or disrupt computer operation.

According to AV-TEST Institute, the number of new malware are continuously increasing from 2010, see Figure 9 from google image. Among all those malware, we have two kinds of malware: infectious malware and concealing malware.

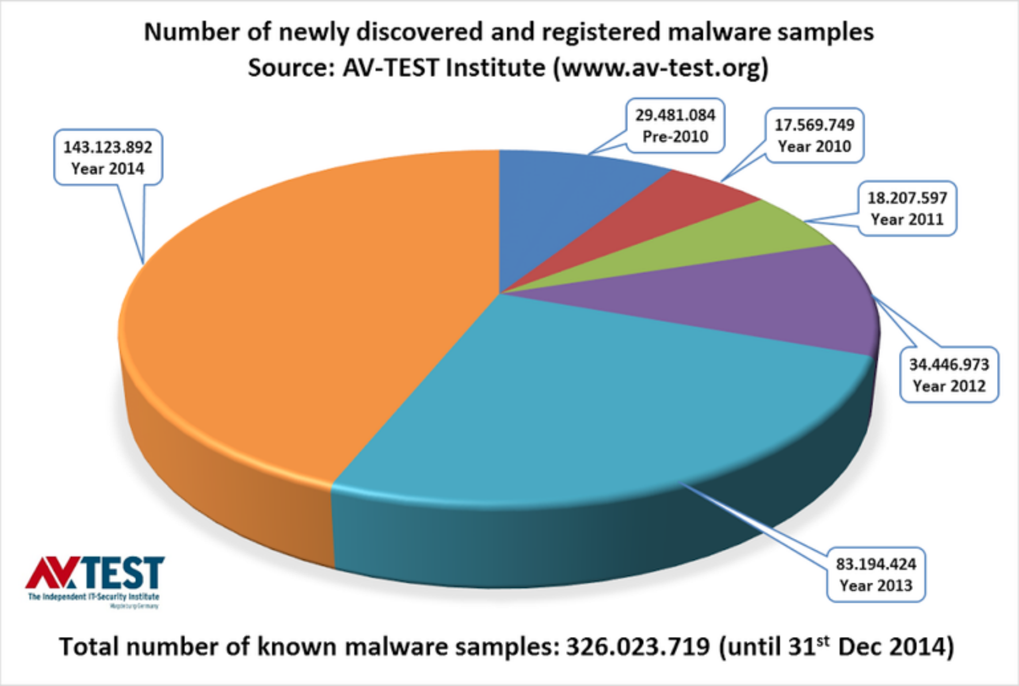


Figure 9: Number of newly discovered and registered malware samples

Infectious malware can replicate itself from one user to the others. It means that infectious malware can spread effectively. Viruses and worms are the primary items to be considered as infectious malware, see the detailed descriptions below:

***Viruses*** — Viruses destroy data or look for things like passwords, credit card numbers, or other sensitive data. Users' information is then often sent to another computer. A virus can also use users' computer to relay spam email or pornography or to coordinate attacks against websites on the Internet. Virus works by copying itself and spreading to other computers.

Viruses often attach themselves to various programs and execute code when users

launch these infected programs, to spread themselves to other computers. Viruses can also spread out through documents, script files and cross-site scripting vulnerabilities in web applications. Attackers could use viruses to steal information, create botnets, render advertisements and cause harm to networks etc.
***Worms*** — Worms replicate themselves over a network. Worms often arrive via email, peruse user's address book, and then send a copy of themselves to others in address book, masquerading the message as if they are from the victim user. By exploiting operating system vulnerabilities, worms could spread over computer networks. Worms make harm to their host networks when they overload web servers and consume bandwidth.

Infectious malware is good at replicating itself to spread, and concealing malware is good at hiding itself. Concealing malware hide from the users and then steal users' information. Typical concealing malware types are trojan horses, rootkits, backdoors and keyloggers etc, see the following descriptions:
***Trojan horses*** — Trojans are written to discover users' financial information, taking over computer's system resources. Trojans can delete users' data, compromise security, relay spam or porn.
***Rootkits*** — Rootkit is the hardest of all malware to be detected and removed; many experts recommend completely wiping the hard drive and reinstalling everything from scratch. Rootkit is designed to gather the identity information from user's computer without user's knowledge. Rootkits hide themselves from users by modifying users' operating systems, then take control of computers when users are away from the computers.
***Backdoors*** — Backdoors are quite similar to Trojans or worms, while they open a backdoor onto a computer. Backdoors provide network connections for hackers or other malware which need to enter.
***Keyloggers*** — Keylogger records everything users type on their personal computers in order to glean log-in names, passwords, and other sensitive information, and send them on to the source of the keylogging program.
According to different purposes of malware, we can classify them to several common malware categories as listed below [RHW$^+$08]:
***Adware*** — Adware is short for advertising-supported malware. Adware could display advertisements on our computer. Adware is the least dangerous malware while it is the most lucrative one. Pop-up advertisements on websites and display advertisements by software are common examples of adware.
***Spyware*** — Spyware can monitor users' movements on SNS, send information back

to a central computer that then target users with advertising. Spyware have functions to spy on user activity without users' knowledge.

Spyware's functions consist of keystrokes collecting, activity monitoring and data gathering etc. Spyware could also modify security settings of browsers and software to interfere Internet connections. Spyware exploites software vulnerabilities and bundles itself with legitimate software, to spread itself over the network. What is worse, spyware is nearly impossible to remove.

***Crimeware*** — Crimeware is designed to automate financial crime by performing identity theft to access online accounts of users at financial institutions and online retailers for the express purpose of stealing funds from those accounts or performing unauthorized transactions to the benefit of the thief controlling the crimeware. Crimeware is often used to export private information from a network for financial exploitation. Crimeware is viewed as a growing concern in network security as this type of threat seeks to steal confidential information.

***Downloader*** — A program that is stealthily installed in users' computer. After installation, it connects to a remote server and downloads additional programs and files, such as spyware. Spyware is installed in users' computer without knowledge.

***Browser hijackers*** — When users' homepage changes, users may have been infected with one form or another of a Browser hijacker. This dangerous malware will redirect users' normal search activity and give users the results the developers want users to see. Its intention is to make money from users' web surfing. Using this homepage and not removing the malware lets the source developers capture users' surfing interests. This is especially dangerous when banking or shopping online. These homepages might look harmless, but it may be infectious.

## 3.4 Identity Theft Attacks

Most users on SNS are not aware that their identities might be stolen. Users share their personal data such as their real names, birthdays, e-mail addresses on SNS. User's profile is usually set to public by default and most users never change it. These actions will give chance to identity theft attackers. Attacker would collect personal information of users, then impersonate the users by creating a fake identity and cheat the users' friends in order to take advantage of the trusted relationships on SNSs.

As described in [HCSS14], there exists two types of identity theft attack: profile cloning attack and cross-site profile cloning attack.

During profile cloning attack, attacker creates a fake account with the victim's photo and name on the same SNS and sends friend requests to the victim's friends. If the victim's friends do not realize attacker's friend request is from a fake identity, they would accept the attacker as their friend. The attacker can rebuild the victim's friend network and make the fake identity be more similar to the victim. What is worse, the attacker can view the victim's friends' profiles, then the attacker can make more fake identities according to these profiles.

During cross-site profile cloning attack, attacker copies victim's information and creates a fake account on another SNS which the victim does not use. Then, the attacker could try to connect with the victim's friends who are on the both SNSs.

Based on the work of [MT05], we conclude several common methods used by identity theft: Protocol weakness, Naive users, Malicious software and Data acquisition.

***Protocol weakness*** — Many Internet standard protocols are designed for ease of use rather than security and verification of identities. The protocol weakness create opportunities for identity theft attacker.

***Naive users*** — Naive users are unaware of networking weakness and security issues on SNS, their naive actions online might put them under all kinds of attacks.

***Malicious software*** — Malicious software is so evil that it would take control of a personal computer and allow identity theft activities undergo successfully.

***Data acquisition*** — Attacker might buy the data of users from data controller of SNS, and these data controller could be service provider of SNS. Once the attacker get the data, he could misuse data to steal users' identities.

To resist the Identity Theft Attack, we could improve the privacy setting.

## 3.5 Spam Attacks

Spam is defined as electronic equivalent of junk mail. Electronic spamming takes advantage of electronic messaging systems to send unsolicited, bulk and unwanted messages. Most of SNS are not immune to spam attacks.

Normally, spammers hack into users' accounts on SNSs and send spam links to the list of users' trusted friends. According to Kaspersky' Spam Report, China, America and south Korea are suffering highest spam attacks, see Figure 10 from google image.

Sometimes, we can not avoid spam attacks, while we can still reduce them. Below are some useful ways:

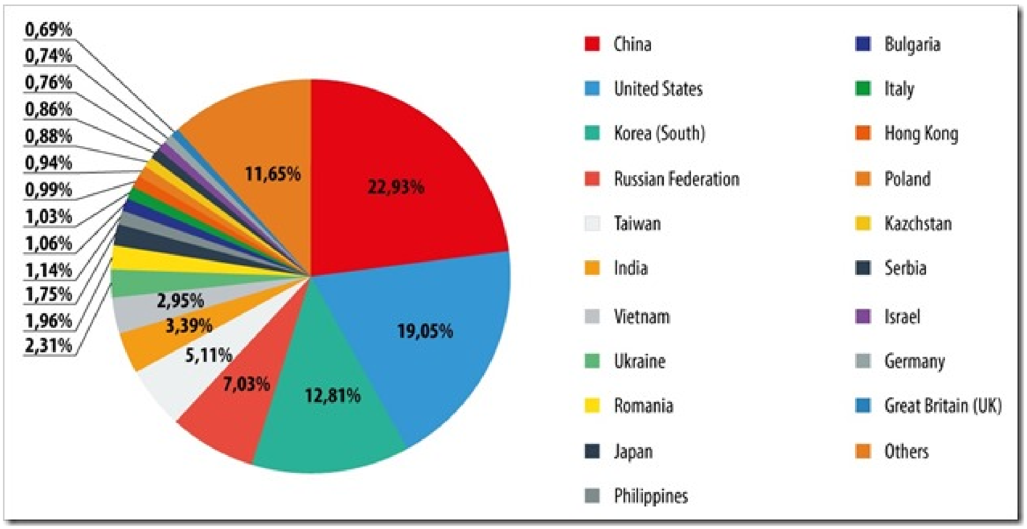


Figure 10: Spam Attacks Distribution Around the World

Consider hiding email address from SNS profiles or only allowing certain people to view our personal information.

Most Internet service providers and email providers offer spam filters, see Figure 11 from google image. Enable filters on the email programs and keep checking the mail folder to ensure the filters are working properly.

Reporting spam will be helpful to prevent the messages from being directly delivered to our inbox. Most email clients report instances of spam or offer ways to mark an email as spam.

## 3.6 Phishing Attacks

In [Hon12], Phishing attack is defined as a kind of social engineering attack in which criminals use spoofed email messages to trick people into sharing sensitive information or installing malware on their personal computers.

In a phishing attack, the attacker will try to trick his victim into visiting a fake website by using phishing techniques. The motive of phishing attack is usually financial.

In phishing attacks, the hacker would create a fake web site. The website looks exactly like a popular site such as the Facebook or Twitter. Then the hacker sends e-mail messages to trick the users into clicking a link that leads to the fake site. When the users attempt to log on with their account information, the hacker records the username and password and then tries that information on the real site.

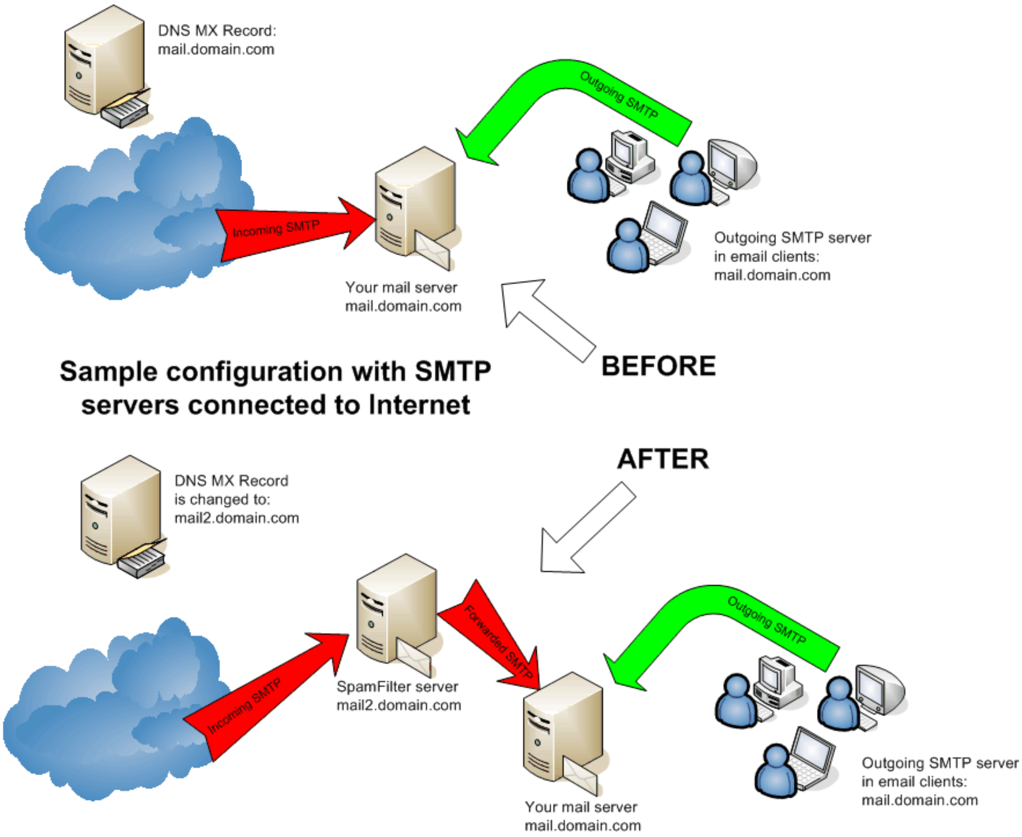


Figure 11: Email configured with Filter

The process of phishing attacks consists of four steps: initiation, execution, user action and completion, see the detailed descriptions below:

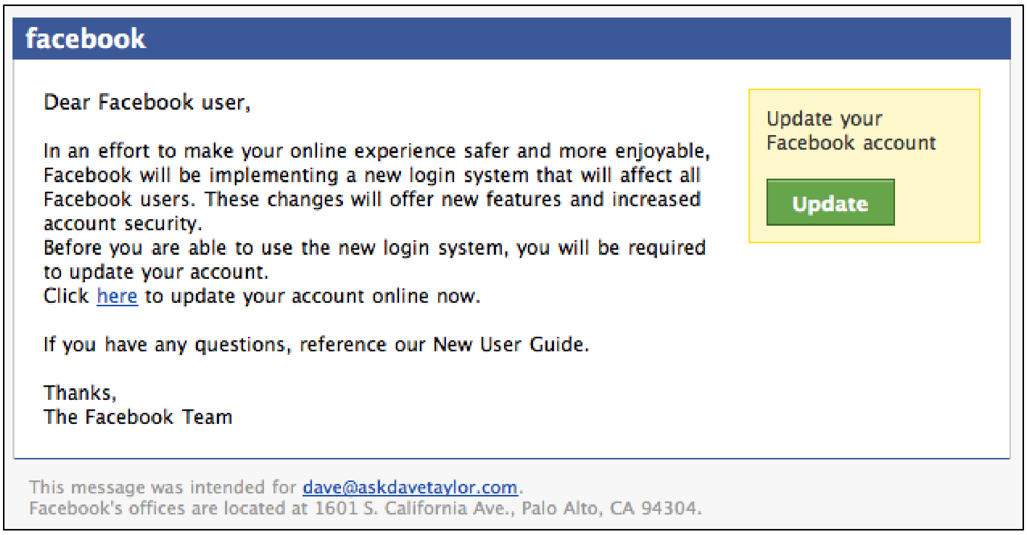
***Initiation*** — The phisher firstly build a fake SNS which is similar to the real SNS. Phisher would use malware to hack some computers to become zombies. The zombies will be remotely controlled and used to send huge amount of malicious mails to other users later.

***Execution*** — Phisher would send spam to users, and in the spam phisher tries to lure the users with different kinds of traps. For example, spam might say “the password of your Facebook account has been changed” to trick the victims to clink a link connected with the fake Facebook website. Then, the phisher just needs to wait for victims to visit the fake website.

***User action*** — If the user falls into the ’bait’ trap, by clicking on the link, and submits personal information or other sensitive information on the spoofed site, these details are recorded and sent to the ’phisher’.

***Completion*** — The phishing attack is completed when the ’phisher’ receives victims’ personal information. Then the phisher can use these information to transfer money, and commit identity fraud etc.

Let us take an example of phishing attack based on spam, see Figure 12 from google image. In this case, the attacker sends spam to user. Once the user click the web link given in the spam, the user would fall into the trap of phisher. The user would turn to be a victim after he give some of his personal information on the fake website, see Figure 13.



Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.
Before you are able to use the new login system, you will be required to update your account.
Click here to update your account online now.

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

Update your Facebook account

This message was intended for dave@askdavetaylor.com.
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

Figure 12: Phishing attack based on spam with Facebook

To avoid phishing attacks, we can take following actions:

Keep devices clean. Use the latest operating system, software, web browsers, anti-virus protection and applications, to fight against viruses, malware, and other security threats.

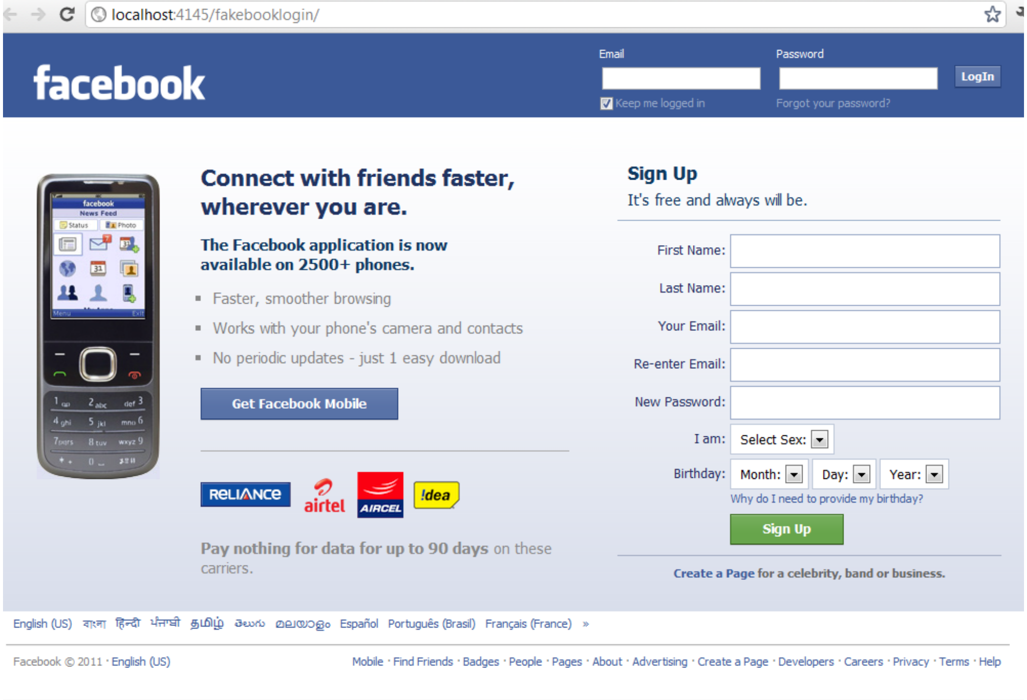
Before posting sensitive information on SNS, check the security of the website.

Never reveal personal information in an email, and do not respond to SPAM with suspicious web links.

Be careful about the website's URL. A lot of malicious SNS look like the legitimate sites, while the URL might use a different domain or apply variation to spell domain name.

If uncertain about whether an email request is legitimate or not, contact the organization to verify directly. Contact the organization using information provided on an account statement, not information provided in an spam.

Check available information about known phishing attacks from the Anti-Phishing Working Group. Also remember to report the sured phishing attempts to the Anti-Phishing Working Group, to help updating new information in their database.



localhost:4145/fakebooklogin/

Connect with friends faster, wherever you are.

The Facebook application is now available on 2500+ phones.

- Faster, smoother browsing
- Works with your phone's camera and contacts
- No periodic updates - just 1 easy download

Pay nothing for data for up to 90 days on these carriers.

Sign Up

It's free and always will be.

Create a Page for a celebrity, band or business.

facebook
Email
Password
LogIn
☑ Keep me logged in
Forgot your password?
Get Facebook Mobile
RELIANCE
airtel
AIRCEL
!dea
First Name:
Last Name:
Your Email:
Re-enter Email:
New Password:
I am: Select Sex:
Birthday: Month: Day: Year:
Why do I need to provide my birthday?
Sign Up
English (US) বাংলা हिन्दी ਪੰਜਾਬੀ தமிழ் తెలుగు മലയാളം Español Português (Brasil) Français (France) »
Facebook © 2011 · English (US)
Mobile · Find Friends · Badges · People · Pages · About · Advertising · Create a Page · Developers · Careers · Privacy · Terms · Help

Figure 13: Fake Facebook Site for Phishing Attack

## 3.7 Pharming Attacks

In [GS07], author calls pharming attacks such phishing attacks that are carried out without a lure. Pharming attack is more advanced than phishing attack while both of them basically use fake SNS to get users' personal information. Pharming attacks do not rely on spam to trap users.

Pharming attack is defined as attack aiming to redirect a website's traffic to another malicious website. The pharmers would apply malware such as viruses, trojans and spyware to perform pharming attacks. In [SP07], we have five common pharming attack technical methods:

***Malwares*** — Pharmers could deploy malware onto users' computer system to intercept visit requests to SNS, and redirect user to the fraudulent SNS which the pharmer has set up.

***Domain Hijacking*** — a pharmer might hijack a SNS by using techniques of domain slamming and domain expiration, then the pharmer could redirect all legitimate network traffic to a fraudulent site. The pharmer would submit domain transfer requests and switch from one domain to another in domain slamming. Then the domain holder with new registrar could change the routing operations to redirect network traffic to a differently illegitimate server. For domain expiration, the domain names are leased for fixed periods. The failure of leasing process management could probably lead to a legitimate ownership transferred to a pharmer.

***DNS Cache Poisoning*** — DNS servers will cache the queries made by the users for a fixed amount of time. The caching process is done to reduce response time for frequently used domains for better user experience. Pharmers could poison the DNS cache by inserting malicious IP address mapping, by replacing users wanted SNS with fake websites.

***Hosts File Modification*** — Most operating systems store files locally. The hosts file has a mapping list which maps from the domain name to the corresponding IP address, for example the URL of www.facebook.com maps to IP address of 173.252.120.6. Pharmers can by modify the host lookup files with malicious mapping utilizing the operating system vulnerability. In this case, they could map www.facebook.com to 170.200.100.6 which is the IP address of a fake website in real case.

***Static domain name spoofing*** — The pharmer would take advantage of slightly wrong spellings or misspellings of domain names which could trick users to visit the malicious website. For example, a user want to access www.facebook.com, while a pharmer may direct the user to www.facebok.com which is a fake website of the pharmer. The pharmer builds the fake website with one letter missing from the legitimate address to trick the user into believing the address is genuine.

Let us view an scenario of pharming attack based on DNS cache poisoning, see Figure 14 from google image. To understand how pharming attacks work, we explain the pharming attack step by step:

Step 1: An attacker exploits vulnerabilities of a DNS. The attacker would poison the DNS cache and change valid entries.

Step 2: The victim originally wants to visit www.nicebank.com.

Step 3: The victim queries the DNS server to resolve the website.

Step 4: The poisoned DNS resolve the website to a malicious fake website and victim is redirected to www.n1cebank.com.

Step 5: The victim actually visits the fake website of attacker, and he is unaware of the pharming attack. The victim would leave personal information to the attacker.

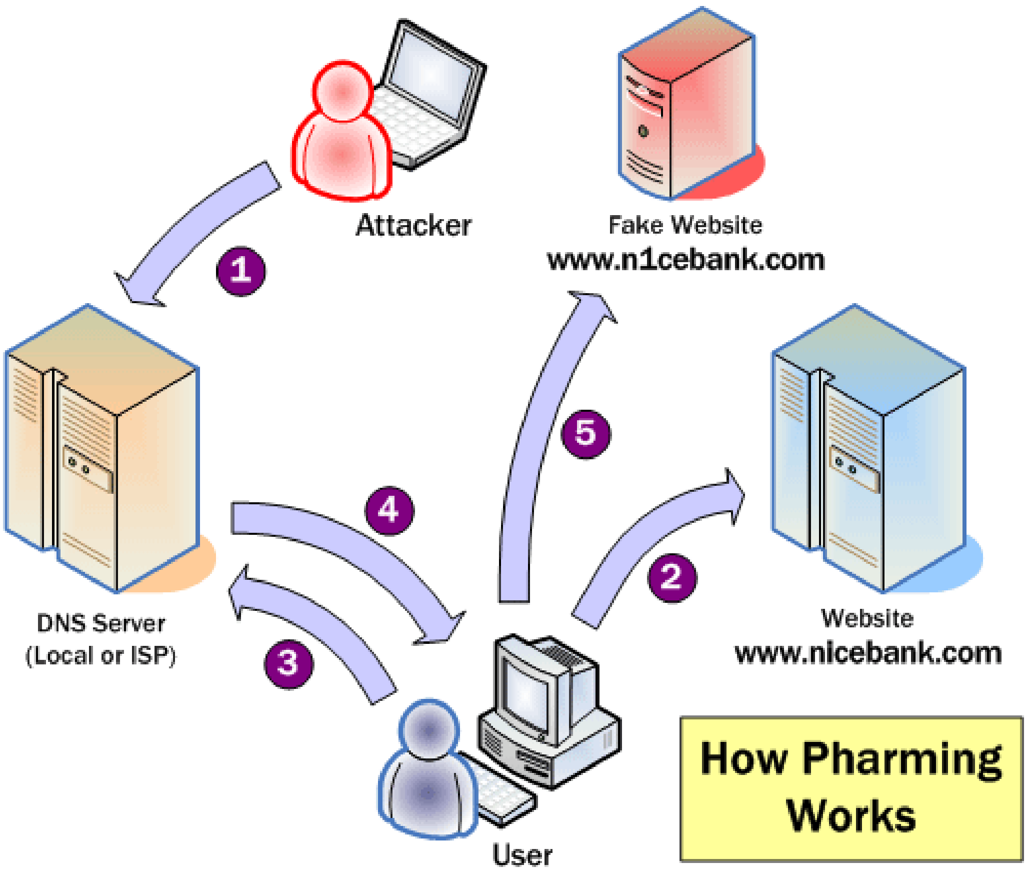


Figure 14: How pharming attacks work

# 4 Requirements for security and privacy on SNS

Users' data must be protected wherever it exist, in databases application or other places. To ensure the security and privacy on SNS, we have some basic requirements for each component on SNS and control power over SNS.

Firstly, SNS's security is critically important, concern all kinds of attacks to strengthen the reliability of management. We also need to do intensive testing. Secondly, there should be good information ethics, to strengthen the protection awareness of user information security, improve the user information security management systems and processes, detailed user privacy protection clause, publish security access guidelines, alert the users to protect personal information on sites' prominent position. For data collection and use of personal information, set more restrictive rules, to clear the purpose of data collection and use of user information. For information involved personal privacy and property, set higher level security measures, strict management of enterprise staffs' access and use of user information.

From our view, the security and privacy are dependent on individual user, service provider, third-party organizations and governmental organization.

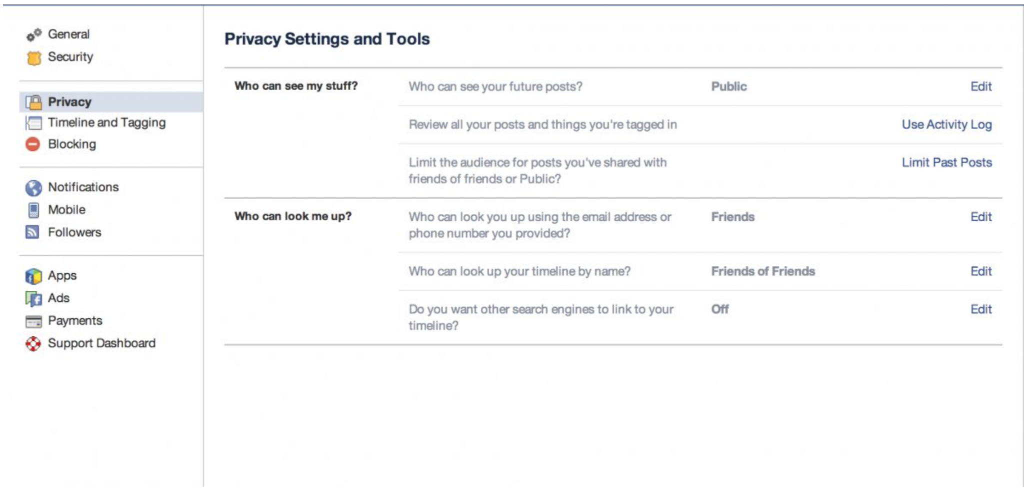
## 4.1 Users' action

In information-technology-based networking environment, user awareness of information security is quite important. Information security depends on several capabilities, including awareness of information security, information security knowledge, information ethics and information security capabilities and other specific content.
Prosperity and development of social networks rely on trust between users. Most SNSs require users to register with real names, providing a high accuracy of user information. Additionally, the contact list are basically real friends in living, and the information security awareness of users would be not sufficient. In many cases, users will easily revert some seemingly fraudulent information from friends, which tend to make the hackers succeed. For those users interested in social networks, they frequently post bits of their daily life, and to upload a lot of photos and videos to share with other users, and these actions produce a high risk of information leakage.
Users' ability to self-protection for information security have to be improved. Many social networking site's privacy settings are very cumbersome, and many users do not very well carry out privacy settings. For example, with the use of friend search function and access to certain users' personal information, bad intentioned people can find some users' personal information, which is visible outside when combined with search engine.

Some users are using a mailbox registered to a number of social networking services. They even generally use the same username and password on each SNS such as Facebook, Twitter and Youtube. Once one of the websites account is disclosed, it will lead to a chain reaction and bring harm to other SNSs.

Concerning security and privacy issues when using SNS, individual users need to improve their knowledge about information security and privacy. To avoid being the victims of cybercrime, the users should take some precautions. Below are some helpful and useful tips:

Configure privacy settings carefully, ensure that only those people you trust have access to your profiles and the information you post. Restrict the ability for others to post information on your pages, to protect against cases where others post some junk information or malicious links. The default settings for some sites might allow anyone to see our information or post information to our page. We can take Facebook as an example, see Figure 15 from google image.



Privacy Settings and Tools

| | | | |
|---|---|---|---|
| Who can see my stuff? | Who can see your future posts? | Public | Edit |
| | Review all your posts and things you're tagged in | | Use Activity Log |
| | Limit the audience for posts you've shared with friends of friends or Public? | | Limit Past Posts |
| Who can look me up? | Who can look you up using the email address or phone number you provided? | Friends | Edit |
| | Who can look up your timeline by name? | Friends of Friends | Edit |
| | Do you want other search engines to link to your timeline? | Off | Edit |

Figure 15: Facebook privacy setting

Choose SNSs carefully. Review SNS's privacy policy carefully. We can evaluate the site and ensure we understand the privacy policy. Some sites might share users' information, such as preferences, email addresses and phone numbers. If a SNS's privacy policy is badly designed or can not properly protect our information, we can refuse to use the site.

We need to ensure that any computer we use to connect to a SNS has proper security measures in place. Keep using and maintaining firewall, anti-virus software and anti-spyware software. Furthermore, keep these applications and operating system updated and patched now and then.

Be cautious about installing some specified applications. Some SNSs provide the third-party applications, such as games. Keep in mind that SNS might have no quality control or review of these applications and these applications might get full access to our account and the information we share. Malicious applications can access our data to interact with our friends on our behalf and to steal and misuse our personal data. Only install applications which come from trusted, well-known sites. Once we no longer need to use an application, remove it. Installing some applications may modify our security and privacy settings by default.

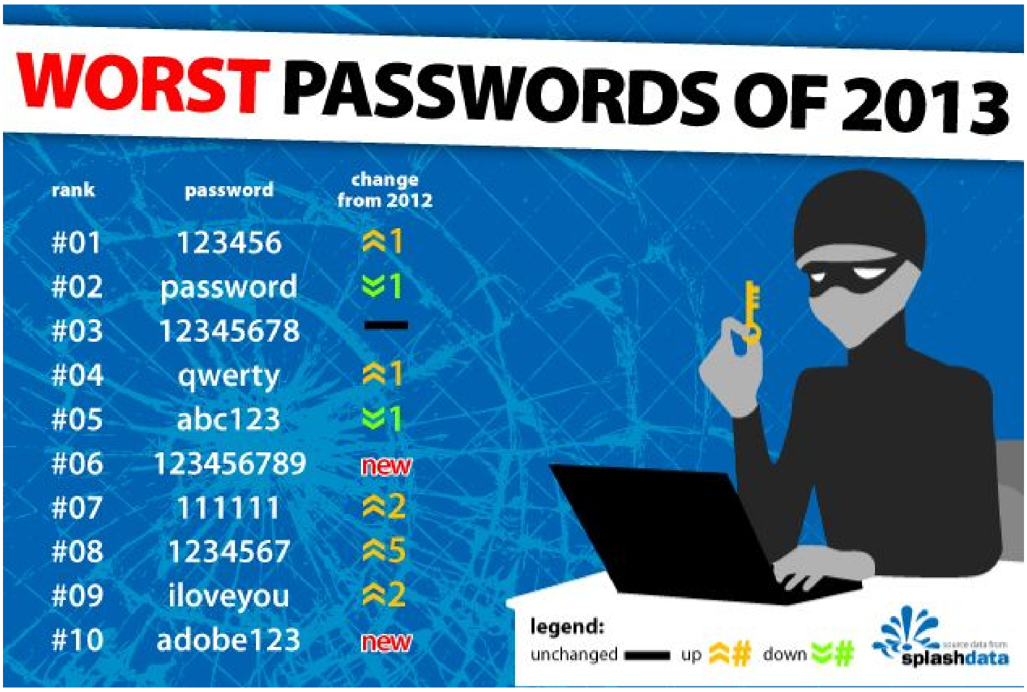
Avoid giving away email addresses or phone numbers of our friends. Never allow SNSs to scan our email address book or contact book. When we join a new social network site, we might be required to enter our email address and password to check if our contacts are on the same network. The site might use this information to send email messages to everyone in your contact list, which leads to large amount of spam.

Be cautious about specified links. If a link looks suspicious, seems too good to be true, never try to click on it even if the link is from our most trusted friend's page. Friend's account might have been infected or hijacked and now be spreading malware.

It is preferable habit to use our personal bookmarks or type the address of SNS directly into our browser. If we click a link to a fake social networking site through spam or another website, we might be entering our account name and password into the fake site, and then our personal information could be stolen.

If we are going to request to delete our account, first remove all of the data. Make sure that the account be deleted, rather than deactivated.

Use strong and unique passwords. Short, simple and naive password are easy to be guessed by computer software. We have some examples of bad passwords during the year of 2013, in Figure 16 from google image. Using the same password on all accounts increases the vulnerability of these accounts if one becomes compromised. Use different passwords for different accounts, and never use a password you use to access your organizations network on any personal sites you access.



WORST PASSWORDS OF 2013

| rank | password | change from 2012 |
|---|---|---|
| #01 | 123456 | ⇑1 |
| #02 | password | ⇓1 |
| #03 | 12345678 | — |
| #04 | qwerty | ⇑1 |
| #05 | abc123 | ⇓1 |
| #06 | 123456789 | new |
| #07 | 111111 | ⇑2 |
| #08 | 1234567 | ⇑5 |
| #09 | iloveyou | ⇑2 |
| #10 | adobe123 | new |

legend:
unchanged — up ⇑# down ⇓#
source data from
splashdata

Figure 16: Worst Passwords in 2013

Professional hackers can break into our accounts and send some messages which look like they're from our friends, but actually aren't. If we suspect that a message is fraudulent, use an alternate way such as phone call or e-mail to contact your friend to check out. If the message is really from a hacker, tell our friend soon.

Carefully select "friend" and groups we join on SNSs. The more "friends" we have or groups you join, there are more people who have access to our information. Sometimes the identity thieves might create fake profiles in order to copy our information. Once we add the fake friend, part or all of our profiles could be viewed which leads to private information leaking.

Do not assume privacy on a SNS. We should not share our confidential information for neither personal nor business use. We should only post information we are comfortable to display for a complete stranger.

Do not post your personal information which makes you vulnerable, such as your address, schedule and routine. Do not announce that you are on vacation or away for an extended period of time. The bad guy might choose to break into our house after seeing our post.

Think twice before make post on SNSs. Before posting information or comments, remember to use discretion. Once we post some information on SNSs, it will be viewed potentially by everyone and may not be able to be retracted afterwards.

Remember to delete the meta data when posting pictures. The meta data might contain the date and time of the picture.

## 4.2 Service providers' action

In the case of user information being compromised, the social network business has been increasing. Originally a social network business should take responsibility and obligation for principal information security. However in practice, most social networking companies are not deeply aware of the importance of user information security, do not fully fulfill the responsibility to protect the security of users information. While they use to lure and mislead users by games reward, they get priority access to new features and other ways, to encourage users to fill in the user's real information, including name, gender, age, home address, e-mail address, education, experience, phone number.

On the other hand, SNS's service provider did not often pay attention to security. The service provider of SNSs do not spend adequate funding for the construction of professional security management team, hence they have no ability to prevent attacks. These service providers designed privacy protection entirely to facilitate enterprises to develop business, and they ignore the user's information security risks. We can take renren.com of China as an example. Although renren.com has complete privacy control strategy for relevant data of user information, still this strategy can not be utilized. Attackers can view user's profile to obtain user information. If the user sets appropriate privacy control strategy, most users have been unable to access the user's profile information, but they still are able to use user's friends list information.

According to highly interactive features social networking sites have, attackers can find the relationship through the interaction between different users, so-called social network virtual personal networks. In this case, although attackers can not directly target user's account to obtain user information, but interact through social networking sites, attackers can perform an indirect penetration attacks to friends account. Once get the account information of users' friends, attackers not only can browse the target users' personal information, they can also send private messages or spam to users' friends for phishing attacks.

SNSs usually have privacy policies on their website, such as "Terms of Use", "Conditions of Service" or "Terms and Conditions". The agreement provides them of policies of ownership, dissemination, usage, privacy, delete and change of data.

Some SNS users simply avoid talking about sensitive issues such as information security protection, ownership and legal disclaimers part of questionable validity. Social networking companies will provide user information to the user who decide to use third-party companies. These third-party companies may collect users' information without liability.

In fact social networking companies neither inform users of third-party companies nor get the user's consent to run third-party applications. These SNS companies violate the right to information and the user's choice, and they are not able to completely exempt from duty and obligation.

SNS's service providers must understand what is the sensitive data and what is the extent to limit the disclosure of specified sensitive information. They should keep updating security policies with data growing in volume, variety and velocity. SNS's service provider need to build strong defence against all kinds of attacks. SNS's service provider also need to supervise the third-party applications inserted on SNS
.

For SNS service providers, in order to maintain security of SNS, they have to fulfill basic implementations, such as information security management system, infrastructure security, access control management, data encryption, network security monitoring etc.

***Information Security Management System*** — ISMS is a system which SNSs could use to establish information security policies and objectives within an overall or a specific range, and accomplish these goals. It is the result of direct management activities, it is expressed as a collection of policies, principles, goals, methods, procedures, checklists and other elements.

ISMS is to establish and maintain standards of information security management, it requires SNSs to establish Information Security Management System by determining the scope of the information security management system, development of information security policy, a clear management responsibility for risk assessment based on the selection of control objectives and control methods.

Once ISMS is established, it requires SNS to operate according to the system rules, and maintain the effectiveness of system operation. An ISMS should require organization to establish and maintain a documented information security management system, which should elaborate the protected assets, organizational risk management approach, control objectives and control manner and extent to ensure needed. In ISMS, we have four phases: plan, do, check and act, see Figure 17 from google image.

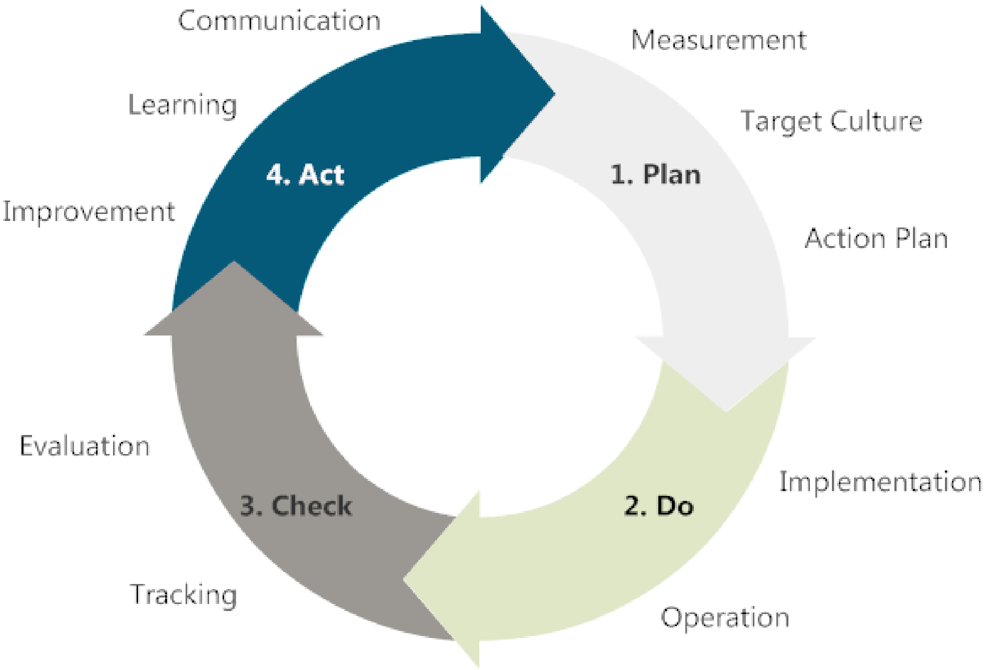


Figure 17: Four phases for ISMS

Plan phase is based on risk assessment, legal requirements, SNS's own business operations need to determine the control objectives and control manner. Planning phase is to ensure the correct establishment of the scope and detail level of ISMS, identify and evaluate all of the information security risks and develop appropriate treatment plans for these risks. At planning phase, all important activities must be documented for future traceability and control for changes.

For planning phase, we need to fulfill the following requirements: establish the required scope of ISMS and the processes of system's environment; arrange strategic and organizational information security management environment; identify the scope of the information assets; ensure information security risk assessment criteria and level of assurance required.

Within an SNS, security policy is about to give guidance on how to manage information assets, protection and distribution rules, instructions, the basic of ISMS. Information security policy of SNS and management methods, would provide direction and support for SNS's information security management.

Furthermore, SNS need to determine the assessment methodology of information security risk, and determine the criteria of risk level. Assessment methodology should be established within ISMS range, fulfill information security requirements, meet the requirements of laws and regulations, taking effectiveness and efficiency into account. We need to establish a risk assessment document. In the document, we choose to explain risk assessment methods, why the methods are suitable for security requirements and business environment, also present techniques and tools used, and the reasons of using these technologies and tools.

SNS also require ISMS within the control of information assets; to identify threats to those assets; identify possible vulnerabilities, and the potential impact on these assets because of the confidentiality, integrity and availability loss.

At the plan phase, we need to make some assessments: Assess the business impact due to security failure according to the potential impact of asset confidentiality, integrity or availability of loss; assess the real possibility of failure according to the main threats associated with the assets, vulnerability and their influence and control of the current implementation; determine the risk level based on the established criteria of risk level.

For different information security risks that have been identified, SNSs may need different analysis. If the risk to meet SNS's risk acceptance policies and guidelines, SNS could deliberately and objectively accept the risk. For an unacceptable risk, SNS can consider to avoid the risk or transfer risk. For the inevitable risk transfer, we should take appropriate security controls to reduce it to an acceptable level.

SNS should select and document control objectives and control method, in order to reduce risk to acceptable levels.

Do phase is the implementation of selected security controls. For this phase, we need an appropriate priority to manage the operation, execute the selected control of the planning stage to deal with information security risk.

For those considered as acceptable risks, we do not need to take further actions. For unacceptable risks, we need to implement the chosen control, which should be synchronized with the risk management plan prepared in the planning phase. Successful implementation of the program requires effective selection of formulated method, assignment of responsibilities and segregation of duties, and to monitor these activities in accordance with formulated ways.

After unacceptable risk get reduced or transferred, there will be some residual risk. For this residual risk, risk control needs to ensure that undesirable effects and damage are quickly identified and properly managed. In order to run ISMS and all security controls for this phase, we also need to allocate appropriate resources (people, time and money).

SNS need to ensure the synchronization of awareness and control activities, arrange training on information security awareness, and exam the training results, in order to ensure they remain effective and real-time.

Check phase takes compliance checking based on policies, procedures, standards, laws and regulations for the implementation of security methods. Checking is a critical phase for ISMS. Checking is the stage to analyse operating results and seek opportunities for improvement. If SNS find a control action unreasonable or insufficient, it is necessary to take corrective action to prevent the information system staying at an unacceptable risk status. SNSs should adopt a variety of ways to check ISMS is running well and its performance monitored.

The management process at check phase includes the following:

1. Run the implementation procedures and other controls, rapidly detect errors in the processing; quickly identify failures and destruction of ISMS; enable administrators to confirm executed safety activities to achieve the expected results manually or automatically; determine actions to be taken to deal with security breaches in accordance with business priorities; study other SNSs' own security experience.

2. Generally review the effectiveness of ISMS; collect the results of security audits, incidents and suggestions, and get feedback from all shareholders and other interested parties on a regular basis effectiveness of ISMS review.

3. Assess the residual risk and the level of acceptable risk; pay attention to orga-

nizational, technical, internal changes in the business objectives and processes, as well as external changes identified threats and social habits, regularly review that residual risk and the acceptable risk level is reasonable.

4. Review the implementation of management procedures to determine the adequacy of established safety procedures, compliance with standards, as well as whether to work in accordance with the intended purpose.

Act phase will take corrective and preventive actions to achieve continuously improvements according to the results of ISMS audit, management review and other relevant information. After the plan, do, and check phases, SNS's act phase must draw a conclusion of the plan: whether it should continue with the old plan or abandon the old plan and start a new plan.

Measuring ISMS to meet the performance and security policy and objectives. SNS need to recognize the improvement of ISMS and effective implementation. Take appropriate corrective and preventive actions. If necessary, revise ISMS, to ensure that the revised ISMS achieve the desired objectives.

Corrective action means that SNS shall determine actions to eliminate the process of the implementation of ISMS, operation and use does not comply with the plan, and prevent recurrence. So corrective action has requirements for SNS: identify the nonconformity of ISMS implementation and operation process; find the cause of nonconformity; evaluate to ensure that the actions which do not meet the requirements do not recur; take required corrective actions to implement ISMS; record the effective actions taken.

Preventive action is that SNS shall determine action to eliminate the cause of potential nonconformity to prevent its occurrence. Preventive actions should appropriately adapt to the effects of the potential problems. Preventive action's requirements are the following: identify potential nonconformity and the related causes; identify and implement the necessary preventive actions; review preventive action taken; record the result of preventive actions; identify the changed risk and pay attention to the risk changes.

***Infrastructure security*** — Vulnerable infrastructure devices put network security at risk. Secure network infrastructure are foundational to the security of users' data. Vulnerable infrastructure potentially open the door to attacks that can compromise SNS's security defences.

All devices connected to the network, including core routing and switching, wireless, and firewalls, need periodic assessments in order to protect the integrity of SNS's infrastructure. As new devices are added to the network, they must be integrated

Table 5: Access Control Basic

| ***Types*** | ***Descriptions*** |
|---|---|
| Authentication | Ensure access is only granted to authorized users, groups, and services. |
| Authorization | Restrict the actions and views permitted by any particular user, group, or service. |
| Accounting | Record who accessed the device, what occurred, and when for auditing purposes. |

into SNS's security system to meet policy and compliance requirements.

***Firewall*** — Firewall offers a network security system which could control the incoming and outgoing network traffic according to the fixed rules. A firewall typically builds a barrier between a trusted, secured internal network and unsecured, untrusted external network or Internet. Firewall permit remote access to a private network by logins and secured authentication certificates.

Firewalls are often categorized as software-based firewall and hardware-based firewall. Software-based firewall runs software on general purposed hardware. Hardware-based firewall will filter traffic between two or more networks.

Software firewalls are installed on personal computer and we can customize it. Software firewall offers us some control over its protection features and functions. Software firewall will prevent attackers to get access or control our computer.

Hardware firewalls could be a stand-alone product. And they could also be found in broadband routers. Hardware firewall is an important part of network set-up and computer system.

***Access Control Management*** — Access control refers to security features that control who can access resources in the SNS system. The service provider need to build a good security model for controlling access to users data, and for controlling access to administrative functions. see Table 5.

Access control systems could complete tasks of authorization, identification, authentication, access approval and accountability. We have several popular types of access control models, see Table 6.

***Data encryption*** — Data, often referred to as plaintext, is encrypted using an encryption algorithm and an encryption key. This process generates ciphertext that can only be viewed in its original form if decrypted with the correct key. Decryption

Table 6: Access Control Models

| ***Types*** | ***Descriptions*** |
|---|---|
| Mandatory Access Control | Security clearance of users and classification of data (as confidential, secret or top secret) are used as security labels to define the level of trust. |
| Discretionary Access Control | The owner decides who is allowed to access the specific data sources, and what privileges they have. |
| Role-Based Access Control | Access policy determined by the system, not by the owner of the data. |
| Identity-Based Access Control | Use network administrators to manage activity and access more effectively based on individual needs. |
| Organization-Based Access control | allows the policy designer to define a security policy independently of the implementation. |
| Responsibility Based Access control | Information is accessed based on the responsibilities assigned to an actor or a business role. |
| Attribute-based Access Control | Access rights are granted to users through the use of policies which combine attributes. |

is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.

Data encryption technology can be applied associated with firewalls. It is used to improve the security and confidentiality of SNS systems and users' data. Data encryption technology is one of the main techniques to prevent private data leaked and used externally. Data encryption is technically implemented by both software and hardware.

General data encryption can be implemented at three levels of communication: link encryption, node encryption and end-to-end encryption.

For some communication links between two network nodes, link encryption provides security for data transmitted over the Internet. For link encryption, all messages are encrypted before transmission, each node decrypt the message received and encrypt again for next link, and then transmit. Before reaching its destination, a message may have to go through a lot of transmission of the communication links.

Since the messages are decrypted and re-encrypted at each intermediate transmission node, all data in link including routing information shows in the cipher text form. Thus, link encryption hides the source and destination of the message to be transmitted. With technology of filling and padding characters, we can encrypt data without transmitting, so that the frequency and length characteristics which messages can be masked, thereby preventing traffic analysis.

At a network node, link encryption provides security only on a communication link, with the messages in plain text format, so all nodes must be physically secure, otherwise they will leak plaintext content. However, it is quite costly to provide encryption hardware and a safe physical environment for each node.

Node encryption provides higher security for network data, and it is similar to link encryption in operation mode: both provide security for the transmission of messages in the communication link; both decrypt and re-encrypt messages at the intermediate node. Since all transmitted data is encrypted, the encryption process is transparent to the users.

However, node encryption does not allow messages to be presented in plain text format. Node encryption firstly decrypted the received message, and then use a different key for re-encryption. This process conduct a security module on the node. Node encryption requires the header and routing information transmitted in clear text format, so that the intermediate node can get information about how to handle the messages. Therefore, this method is fragile against attackers who use traffic analysis.

End-to-end encryption allows data transmission from the source to the destination always exist in ciphertext format. In the end-to-end encryption, the message will not be decrypted before reaching the destination. Because the message in the transmission process are protected, even if a damaged node does not make message leak. End-to-end encryption system is cheaper and more reliable than link encryption and node encryption, and it is easier to design, implement and maintain. End-to-end encryption also avoids the synchronization problem inherent in other encryption systems, since each packet is encrypted, packets are independent so that a message packet transmission errors that occurred does not affect the subsequent message packet. Moreover, from the user's security needs, end-to-end encryption is more natural. Individual users may prefer to use this encryption method, so as not to affect other users on the network, this method requires only the source and destination nodes be confidential.

End-to-end encryption systems do not allow to encrypt the destination address of the message, since each node which the message through need this address to determine where to transmit the message. Because of end-to-end encryption method can not cover up the source and the end of the message, it is fragile in preventing an attacker from traffic analysis.

***Network Security monitoring*** NSM is the collection, analysis and escalation of indications and warnings to detect and respond to intrusions.

## 4.3 Third-party organizations' supervision

It is worth noting that, most SNSs have highly cooperation with third-party application providers. SNS offers open programming interface to third-party applications, and third-party applications can obtain the user's personal information. Third-party applications run the applications on their own servers. It is difficult to obtain effective supervision on these third-party applications. So it is necessary to make more protection rules of users information security for third-party applications providers, push these providers to comply with rules to protect user information security.

Cooperation with third-party SNSs is another important way to reduce user privacy leakage. It also makes better user privacy protection, reducing the risk of privacy disclosure. In the current network environment, third-party websites or third-party programs will require the user to apply the general authorization, user could agree to the site or program to obtain user information. Therefore, we need to push third parties to the premise of the program achieving its function, and supervise the flow of information strictly. We must also strengthen the audit of third-party applications, ensuring that these applications promptly eliminate safety hazards for the user to provide security.

In June 2012, Baidu, renren, Tencent, Sina, Microsoft, Alibaba Group and Netease companies founded Internet Security Working Group in China in accordance with relevant laws, regulations. Internet Security Working Group is voluntary industry composition, non-profit consortium, and does not have legal personality. It is based on equality, mutual benefit, common development, complementary advantages, seek common ground under the principle of co-sponsored formation. The purposes of the working group include: work together to help users improve security awareness; exchange technology, sharing information; give full play to the overall effect; improve security through industry collaboration, software and services; protect the majority of Internet users; defence network security threats; and jointly promote the industry cooperation, enhance Internet security.

## 4.4 Governmental organizations' supervision

With the increasing of cybercrime, we have more crime cases against security and privacy of user information on SNS. On the other hand, the related laws are not robust and can not cover all aspects of the cybercrime.

The governments need to make detail research on cybercrime on SNS, and publish specified law against them. Thus powerful punishment could be good judgement on the attackers against SNS. The government needs to make legislation for users' information security on SNSs. SNSs need some specified rules, clearly define boundaries of personal information security, users' rights and obligations.

The government should also set up special agencies for network users' information security, to develop a unified network authentication system, supervising SNS, give "business license" to the qualified SNSs. These agencies also need to periodically check the level of privacy protection for the licensed sites, and make suitable rates by posting different levels of badges or tokens. This assessment is clearly visible to all users, indicating the extent of trusted sites as a way to promote the site to strengthen self-management.

In addition, both competent authorities and SNS industry associations, should make full use of the news media widely to publicize the importance of network security to protect user information, take the initiative to educate users and help users understand the various laws and regulations.

# 5 Solutions to security and privacy issues

Development of SNS provides new ways to interact with other registered users, but SNS also face new challenges to protect user information security. Information security of SNS is a major issue to be solved immediately, we must deal with it seriously developing better SNS and other internet applications. If handled carelessly, there will be serious blows to the confidence of users to participate in SNS, affecting the healthy development of the Internet economy.

On the one hand, policy makers, regulators, and social networking companies should fully understand the importance and necessity of the user information security protection and accelerating the user information security laws and regulations promulgated in the field of social networking. Social networking companies had better improve safety management level, and enhance the user's information security literacy to improve information security situation, to address and combat these potential risks, and to maintain and maximize the benefits and effectiveness of social networks to promote the SNSs.

On the other hand, the evolution of the SNS is with the development of an application, the future of the Internet will definitely have a more attractive, more rich, innovative applications. We must firmly grasp the phenomenon evolving information security and content, make efforts from technical and management aspects, ensure information security on SNS.

We have generally two types of solutions combined: technical solutions and regulatory solutions. Technical solutions apply different Internet technologies to solve problems based on technical skills. While in some cases, technical solutions are not efficient to solve the problems. Then regulatory solutions will be the supplement of technical solution. Regulatory solution apply different regulations to limit unwanted problems for security and privacy issues on SNS.

## 5.1 Technical solutions

Technically, we can apply many types of methods for security and privacy issues of SNS, such as Virtual Private Network, Platform for Privacy Preferences, Hippocratic Databases System, Cryptographic protocols, Data Anonymization, Data Perturbation, Data Randomization, Data Condensation. We will give detailed descriptions about these methods.

***Virtual Private Network*** (VPN) — VPN functions aim to establish a private network over a public network, using encrypted communication [FH98]. VPNs are widely used nowadays. VPN gateway applies encryption for the packet and packet destination address to enable remote access. In order to maintain data communications security, communication process between VPN server and client are encrypted. With data encryption, data can be considered to be securely transmitted over a dedicated data link which looks like a private network, but in fact VPN using a common link on the Internet, so called VPN virtual private networks, which essentially is the use of encryption technology in the public Internet package a data communication tunnel.

There are many ways to achieve VPN, and the commonly used methods are the following:

1. VPN server: In large LAN, VPN can be implemented by building VPN servers at the network center.
2. Software VPN: VPN can be implemented through a dedicated software.
3. Hardware VPN: VPN can be implemented by dedicated hardware.
4. Integrated VPN: Some hardware devices, such as routers, firewalls, are equipped with VPN functions. It is worth nothing typically, however, that generally hardware devices which have VPN functionality are more expensive than those do not have VPN functionality.

Nowadays, we apply some common VPN technologies as listed below: 1. Multi-Protocol Label Switching (MPLS) VPN is based on Multi-Protocol Label Switching technology. MPLS simplifies core routers' routing method by using traditional routing label switching realization of IP virtual private network. MPLS takes advantage of the Layer 2 switching and Layer 3 routing technology with a very good performance in solving major problems of VPN, service classification and traffic engineering. Therefore, MPLS VPN interconnection in the settlement enterprise, providing a variety of new business operators are increasingly optimistic, it has become an important means of providing value-added services in the IP network operators.

2. SSL VPN is HTTPS-based VPN technology, working between the transport layer and application layer. SSL VPN leverages the SSL protocol which provides certificate-based authentication, data encryption, and message integrity verification mechanism and there to establish a secure connection for the communication between the application layer. SSL VPN is widely used in Web-based secure remote access for users' remote access to internal network provides security guarantees.

3. IPsec VPN is based on IPsec protocol VPN technology to provide security from the IPsec tunnel protocol. IPsec is an end-to-end IP-based communication mechanisms which is designed by the IETF to ensure data security. VPN is Internet data transmission providing a high-quality, interoperable, and cryptology-based security guarantee.

***Platform for Privacy Preferences*** (P3P) — P3P is developed by the World Wide Web Consortium, and it is one of the most well-known Web privacy technologies [RC99] [CLM+02]. P3P could offer users automated matching between user preferences and privacy policies . P3P allows SNSs to declare the intended use of the information that SNSs collect when users browse the websites pages. The original purpose of P3P is to grant users more control over their personal information.

P3P is a collection of privacy protection recommendation standards. P3P is designed to provide privacy protection for Internet users. There are more and more

SNSs collecting user information during users' access. P3P aims to reduce possible privacy violations such as arising personal information's collection.

The standard operation of P3P is the following: the website should tell the users about SNS's privacy policy, the types of gathered information and to whom this information willl be provided, how long the information will be retained and how the information is used. SNS users have right to view the privacy report of the SNS which support P3P, and decide whether to accept the cookie or whether to use the SNS.

***Hippocratic Databases System*** — The primary goal of a database system is to provide an environment that is both convenient and efficient to use in retrieving and storing information [GJK08].

Current database systems basically have ability to manage persistent data and support accessing a large amount of data efficiently. Database systems need the following capabilities: support at least one data model; Support certain high-level languages that allow the user to define the structure of data, access data, and manipulate data; transaction management, the capability to provide correct, concurrent access to the database by many users at once; access control, the ability to deny access to data by unauthorized users and the ability to check the validity of the data; resiliency, the ability to recover from system failures without losing data.

Hippocratic database have the capabilities of current database systems. Furthermore, Hippocratic databases share statistical databases with the goal of preventing disclosure of private information. Additionally Hippocratic databases are secured.

Hippocratic databases have ten principles based on the privacy regulations and guidelines: purpose specification, consent, limited collection, limited use, limited disclosure, limited retention, accuracy, safety, openness and compliance.

***Cryptographic protocols*** — A wide variety of cryptographic protocols are used to protect data confidentiality, integrity, and authentication [NJ05]. Encryption is the conversion of digital data into another format, called ciphertext, which cannot be understood by anyone except authorized users. Modern encryption protocols could play a vital role in the security assurance of SNS system as they can provide not only confidentiality, but also authentication and integrity. Data integrity ensures the origin of data can be verified, and it can proof that the content of data have not been changed.

Cryptography is classified into symmetric cryptography and asymmetric cryptography.

Symmetric cryptography use the same key to encrypt and decrypt data. The most widely used symmetric-key cipher is Advanced Encryption Standard(AES), which was originally created to protect government classified information. Symmetric-key encryption is much faster than asymmetric encryption, while the sender must exchange the key used to encrypt the data with the recipient before the recipient can decrypt it. Asymmetric cryptography could securely distribute and manage huge amounts of keys. For optimised security, most cryptographic processes choose to use a symmetric cryptography to encrypt data efficiently, and use an asymmetric cryptography to exchange the secret keys.

Asymmetric cryptography is also known as public-key cryptography, which uses two keys: one public and one private. These two keys are different but mathematically linked. The public key can be shared to public, whereas the private key must be kept secret. Rivest-Shamir-Adleman(RSA) cryptosystem is the most widely used asymmetric cryptography. One key is used to encrypt data and the opposite key is used to decrypt data. Public-key cryptography provides not only confidentiality, but also the integrity, authenticity and non-repudiation for data and electronic communications of SNSs that use digital signatures.

Cryptography is one of the most effective network security technology. An encrypted network, not only can prevent unauthorized users wiretapping and network, but also be effective to deal with malicious software.

***Data Anonymization*** — Data anonymization [AP04] [AY08] refers to a method where before data sharing, data collectors hide or generalize partial information in the original data, thus making data finally released out cannot provide enough information about the identity, such private data in the information will not be able to correspond to the real and personal information linked, reasoning that privacy information about the person, providing privacy protection.

There are various anonymization technologies which could help SNS users to prevent data collection by blocking or hiding potential identify information such as IP addresses and cookies. Anonymization is an effective way to realize the protection of privacy. The basic idea of data anonymization is to make change to data, normally by generalizing or hiding data. After the change, the raw data has been transformed to other form.

***Data Perturbation*** — Data perturbation will replace the original data with some part of synthetic data [LKR06]. After replacement, the statistical information computed from the perturbed data does not differ from the statistical information computed from the original data to a larger extent. Data perturbation can be done by applying additive noise, data swapping or synthetic data generation.

The perturbed data do not correspond to real-world data owners, so the attacker cannot perform the sensitive linkages or recover sensitive information from the released data. Thus the individual data in the perturbed data are meaningless to the attackers.

Although data perturbation technology does not allow reconstructing the original data, data perturbation is only used for data distributions.

***Data Randomization*** — For data randomization, the data is scrambled in such a way that even the central part of the system cannot tell with probabilities better than a pre-defined threshold, whether the data from a customer contains truthful information or false information [Evf02] [KDWS05]. The information received from each individual user is scrambled and if the number of users is significantly huge, the aggregate information of these users can be estimated with good amount of accuracy. This is very useful for decision-tree classification since decision-tree classification method is based on aggregate values of a data set, rather than individual data items.

The data collection process of data randomization is carried out by two phases.

The first phase: the data provider randomize the original data and transmit the randomized data to the data receiver.

The second phase: the data receiver reconstructs the received randomized data with a reconstruction algorithm.

Data randomization is relatively simple and does not require knowledge of the distribution of other records in the data. Hence, data randomization can be implemented at data collection time.

The weakness of data randomization technique is that it treats all the records equal irrespective of their local density. This leads to a problem where the outlier records become more susceptible to adversarial attacks as compared to records in more dense regions in the data.

We still have an effective solution for the weakness of data randomization technique: add some noise to data. However, this reduces the utility of the data for mining purposes as the reconstructed distribution may not yield results in conformity of the purpose of data mining.

***Data Condensation*** — Data condensation uses condensed statistics of the clusters to generate pseudo data. In data condensation, we would construct constrained clusters in data set and then generate pseudo data from the statistics of these clusters. We construct groups of non-homogeneous size from the data, such to guarantee that each record lies in a group whose size is at least equal to the anonymity level.

Subsequently, pseudo data is generated from each group so as to create a synthetic data set with the same aggregate distribution as the original data.

Data condensation can be effectively used for classification problems. The use of pseudo-data provides additional protection, as it becomes difficult to perform adversarial attacks on synthetic data. Furthermore, the aggregate behaviour of data is preserved, making it useful for a variety of data mining purposes.

Data condensation uses pseudo data rather than modified data, hence it could help gain better privacy preservation as compared to other techniques. Further more, the pseudo data has the same format as the original data so that data condensation can work without re-designing data mining algorithms. In case of data stream problems where the data is highly dynamic, data condensation is very effective.

While, if we transform huge amount of data into a single statistical group entity for data condensation, the results will be affected since large amount of data is lost in the data condensation process.

## 5.2 Regulatory solutions

On solutions based on the legislative or industry self-regulation, we are just relying on external forces to regulate social networking companies to improve the level of protection of users' information security. Social networking companies carry out SNS business for the needs of users and collect a lot of information, hence the majority of social networking companies need to deeply realize the importance of user information security, make more efforts for increasing information security and management.

We have two types of regulatory solutions: self regulation and mandatory regulation solutions. Self regulation needs the information holders voluntarily regulate themselves to guarantee data privacy. Mandatory regulation refers to legislation aimed at protecting users' privacy on SNS.

### 5.2.1 Self Regulation

Self regulation is an alternative solution if mandatory regulation of SNS privacy protection is absent. Self regulation is also self discipline of information holders. The information holders consist of individual users and SNS companies.

Individual users should be aware of their own actions on SNS. They might post some personal information of other users on SNS, which could lead to information leakage and could offer help to intended attackers who want to use personal information. Even worse, some individual users are potential attackers of personal information on SNS. For these users, self discipline could still help to control their behaviours on SNS and avoid improper actions developing to be crime. Self regulation of individual users is not certified.

For SNS companies, they generally adopt different privacy rules in handling their users' information. Self-regulated privacy policies of SNS companies can be certified. This certification is a formal process to assert to users that a SNS's claimed security and privacy policy is well implemented on website.

Trusted, well-known third party is usually responsible for certifying security and privacy policies. Upon request, these third-parties check a given SNS's practices with its security and privacy policy. To approve SNS's privacy policy, they need to check many kinds of actions of SNS: what type of information to be collected, who collects it, how information will be used, whether it is shared, detail privacy policies, and security measures etc. Different third-parties might have different requirements in order to approve a given site. If and only if the trusted party makes sure that the SNS does fulfill its privacy policy, it delivers a certificate of good conduct that the SNS can display on its website, typically in the form of a trust seal.

The purpose of a trust seal is to provide the users with assurance of merchant verification by a third party and ensure that the SNS pass security checking and privacy is well protected. We have many trust seals already, and these popular trust seals are TRUSTe, BBBOnline, and GeoTrust etc, see Figure 18 from google image. After typing address of secured website, we will connect to a secured website with trust seal, we can see the green address bar from the browser, see Figure 19 from google image.

One important thing for the third-party is that frequent checking for the website are mandatory to ensure SNS companies do not change the policies secretly. Furthermore, third-party have to pay attention to the website using fake Trust Seal.

Industry self-regulatory mechanism is an indispensable link for secured information security system. The United States has a typical national model with network privacy protection through industry self-regulation. United States model has four ways for protection, namely constructive industry guidelines, network privacy certification program, technical protection mode and the safe harbor proposals. We can take network privacy certification program as an example. If people see Trusted certification mark of a well-known third-party certification organization, then it indicates that the site has taken some measures to protect the personal information on the

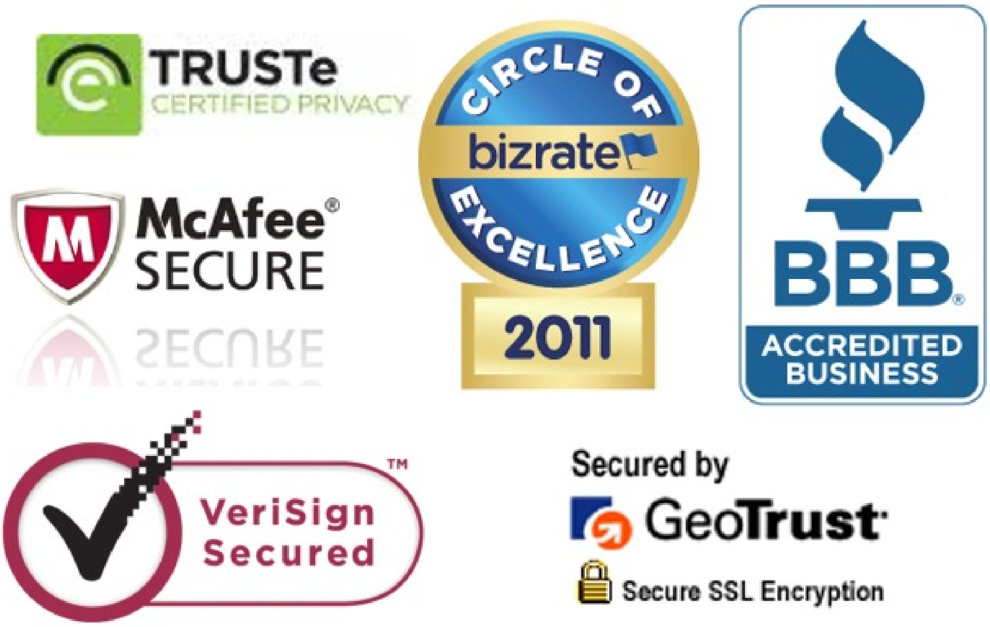
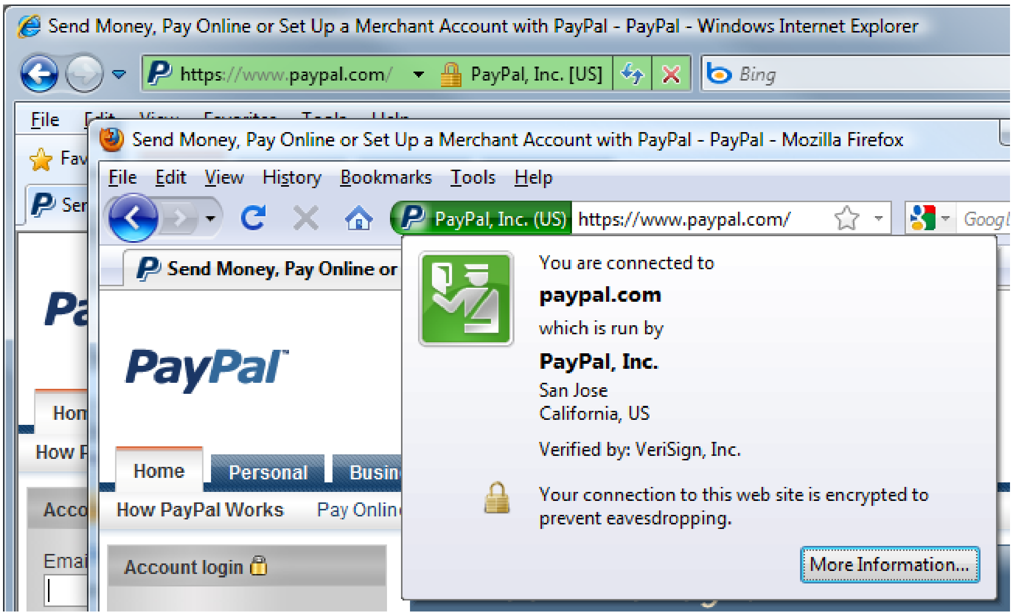


Figure 18: Some Popular Trust Seals


Send Money, Pay Online or Set Up a Merchant Account with PayPal - PayPal - Windows Internet Explorer
https://www.paypal.com/
PayPal, Inc. [US]
Bing
File
Send Money, Pay Online or Set Up a Merchant Account with PayPal - PayPal - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
PayPal, Inc. (US)
https://www.paypal.com/
Send Money, Pay Online or
PayPal
Home
Personal
Busin
How PayPal Works
Pay Onlin
Account login
More Information...

You are connected to
**paypal.com**
which is run by
**PayPal, Inc.**
San Jose
California, US
Verified by: VeriSign, Inc.

Your connection to this web site is encrypted to prevent eavesdropping.

Figure 19: Secured website with Trust Seal normally have a green address bar

website, and you can be assured to use the site.

Industry self-regulation is an important responsibility of industry associations. SNS industry associations could help to achieve self-discipline of SNS. So, if we can use the power of SNS market associations, we could have a greater possibility to manage SNS industry, to promote industry self-regulation, and assist the government market regulation such that to improve SNS market governance. Both government regulation and industry self-regulation will help to regulate SNS market.

### 5.2.2 Mandatory Law

Self regulation is helpful to correct malicious actions on personal data of SNS, however self regulation is not always sufficient. In [Cul00], author finds out whether users' information privacy can be protected through self-regulation, and the study suggests that an effective self-regulatory regime for information privacy has yet to emerge, legislation is required. We have to take advantage of mandatory law for more efficient reactions to cybercrimes.

Governments in many countries have established legislation in order to protect users information on SNS. In fact, most privacy-related laws were enacted in response to particular events or needs for a specific industry. The security policy will define what people can do with network components and resources and what they can not do.

Government need to regulate companies for proper data collection. Companies doing this are SNS companies and third-party applications service companies. The legislation must have basic requirements for companies' actions with data collection: SNS companies should have a legal and clearly defined purpose to collect users' information; SNS companies must disclose their purpose to the users whom are information sources of collection; Permission to use information is specific to the original purpose; SNS company is allowed to keep the data only to satisfy that purpose; if the company needs to use the information for another purpose, it needs to apply for a new information collection.

The author [SZ99] indicate that implementation of The Identity Theft and Assumption Act, will empower law enforcement, consumer protection agencies, and the public to combat identity thieves and deter such conduct as society continues to see the expansion of advanced technology. The Identity Theft and Assumption Act was the first law to criminalize identity theft at the federal level. In addition to making identity theft a crime, this act provided penalties for individuals who either committed or attempted to commit identity theft and provided for forfeiture of property used or intended to be used in the fraud. This law created a very broad definition of identity theft including misuse of different forms of information, including name, Social Security number, bank account number, password, or other information linked

Table 7: Defined Identity Theft Actions in Identity Theft and Assumption Deterrence Act

| ***Defined Actions of Identity Theft*** |
|---|
| Producing false identification |
| Possessing an identification document that you know was stolen |
| Possessing five or more pieces of identification that are not your own |
| Transferring identification that has been stolen or produced unlawfully |
| Assessing a false identification document with the intent to defraud United States |
| Manufacturing, owning, or transferring a machine or device that can be used to produce false identification |
| Processing an identification document that looks official but you know was not provided from an authorized source |
| Possessing five are more pieces of identification that are not your own with the intent to give them to someone else |
| Manufacturing owning or transferring a machine or device that can be used to produce false identification with the intent that it will be used to make more of that device |

to an individual other than the one providing it. The act defined identity theft's action, see Table 7 from wikipedia.

In order to prevent malware attacks, we also have many laws. Among them Computer Misuse Act and Computer Fraud and Abuse Act are often applied. Computer Misuse Act of 1990 introduced three criminal offences, see Table 8 from wikipedia.

The Computer Fraud and Abuse Act essentially indicates that, whoever intentionally accesses any protected computer to obtain information without authorization or exceeds authorized access, shall be punished under the Act. CFAA define 7 types of criminal offences, see Table 9 from wikipedia. Attempts to commit these crimes are also criminally punishable.

In order to prevent spam attack, we have CAN-SPAM Act from 2003. The CAN-SPAM Act's full name is: Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003. CAN-SPAM Act is good response to the growing

Table 8: Criminal Offences defined in Computer Misuse Act

| ***Criminal Offences defined in Computer Misuse Act*** |
|---|
| Unauthorised access to computer material |
| Unauthorised modification of computer material |
| Unauthorised access with intent to commit or facilitate commission of further offences |

Table 9: Criminal Offences defined in Computer Fraud and Abuse Act

| ***Criminal Offences defined in Computer Fraud and Abuse Act*** |
|---|
| Trafficking in passwords |
| Compromising confidentiality |
| Threatening to damage a computer |
| Damaging a computer or information |
| Accessing to defraud and obtain value |
| Trespassing in a government computer |
| Obtaining national security information |

number of spam attacks. In the law, legitimate businesses and marketers are required to be conscientious about their mailing actions. The CAN-SPAM Act also define misinterpretations and fraudulent practices which should be regarded as criminal offences, see Table 10 from wikipedia.

Legislation could also play an essential role in anti-phishing. In March 2005, United States introduced the Anti-Phishing Act mainly against phishing online. The Act would punish the attackers who criminalize Internet scams involving fraudulently obtaining personal information. Anti-Phishing Act proposes that attackers who execute phishing and pharming attacks or use information gained by online fraud to commit crimes such as identity theft, will be fined of up to 250000 dollars and prison up to five years.

In cooperation with Anti-Phishing Act, The United Kingdom introduced the Fraud

Table 10: Criminal Offences Types defined in CAN-SPAM Act

| ***Criminal Offences Actions*** |
|---|
| Sending multiple spam emails with the use of a hijacked computer |
| Sending multiple emails through Internet Protocol addresses that the sender represents falsely as being his/her property |
| Trying to disguise the source of the email and to deceive recipients regarding the origins of the emails, by routing them through other computers |
| Sending multiple spam emails via multiple mailings with falsified information in the header |
| Using various email accounts obtained by falsifying account registration information, in order to send multiple spam emails |

Act in 2006. The Act states that a general offence of fraud could lead to a maximal ten-year prison sentence, and it is forbidden to develop or possess phishing kits with the intention to commit fraud. The Fraud Act gives a statutory definition of the criminal offence of fraud, it defines fraud in three classes: fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. The Fraud Act strengthen legal arsenal against phishing with Anti-Phishing Act.

In Modern digital world, internet technology has upgraded so fast and the technologies used for cybercrime also increase and upgrade. The approach of protecting security and privacy through mandatory laws is no longer as effective as it was in the past. Legislation is often far behind the new developments of SNS technologies and the legislation systems are not fast enough to cover the security and privacy issues on SNS. Additionally, laws are generally specific in each country. It means different countries might have different law against the same cybercrime. Furthermore, even the similar laws have differences in details.

In this situation, the governments had better to cooperate to make the international law and guidelines. Each government should found specific agency to study the security and privacy on SNS, do research work on all kinds of cybercrime on SNS and understand how those attacks against personal data are made. The agency then have an idea to prepare the related law: how to define the cybercrimes, what conduct to the cybercrimes, and what punishment made to the related case etc.

We could consider the current situation in China, where the network showed a rising trend in crime associated with the user's privacy in the form of diverse cybercrime, while Chinese government do not have perfectly relevant laws. Laws governing the protection of personal information have not yet been perfectly introduced.

Although we have many laws related to the protection of personal information, still we lack specific legislation. Imperfect law, on one hand can not put identity theft under effective sanctions, reducing the cost of illegal activities; on the other hand, due to the big cost of protecting rights, victims who face information leakage and other violations often chose to keep silence and make a concession. Therefore, we should accelerate the development of relevant laws and regulations.

# 6 Conclusion

In this thesis, we firstly outline the background of SNSs, including the history and security and privacy issues of SNSs.

Secondly, we display the potential attacks to SNSs, such as passive attacks, active attacks, malware attacks, identify theft attacks, spam attacks, phishing attacks and pharming attacks. We also present that how each type of attack is performed.

Thirdly, we present the basic requirements to maintain the security and privacy of SNS from four different angles: individual users, service providers, third-party supervision and governmental supervision. From each angle, we show what actions are needed to be taken and how to perform them effectively.

Lastly, we show some actual solutions used to secure SNSs, by both technical and regulatory means. For technical solutions, privacy preserving data mining means are most popularly applied for current SNSs. For regulatory solution, we indicate that both self-regulation and mandatory legislation are needed.

# 7 Acknowledgment

This thesis project is prepared for my master graduation. I would like to express my special appreciation to Timo Karvi for supervising me patiently in the thesis work. And I want to thank Dr. Valtteri Niemi for supporting my thesis work.

# References

AP04 Aggarwal, C. C. and Philip, S. Y., A condensation approach to privacy preserving data mining. In *Advances in Database Technology-EDBT 2004*, Springer, 2004, pages 183–199.

AP08 Aggarwal, C. C. and Philip, S. Y., *A general survey of privacy-preserving data mining models and algorithms.* Springer, 2008.

AY08 Aggarwal, C. C. and Yu, P. S., On static and dynamic methods for condensation-based privacy-preserving data mining. *ACM Transactions on Database Systems (TODS)*, 33,1(2008), page 2.

BC09 Becker, J. L. and Chen, H., *Measuring privacy risk in online social networks.* Ph.D. thesis, University of California, Davis, 2009.

bE07 boyd, d. m. and Ellison, N. B., Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13,1(2007), pages 210–230. URL `http://dx.doi.org/10.1111/j.1083-6101.2007.00393.x`.

BHI$^+$08 Brown, G., Howe, T., Ihbe, M., Prakash, A. and Borders, K., Social networks and context-aware spam. *Proceedings of the 2008 ACM conference on Computer supported cooperative work.* ACM, 2008, pages 403–412.

BL09 Bhattacharya, P. and Lawrence, J. C., Network security monitoring system, January 27 2009. US Patent 7,483,972.

BS03 Bayardo, R. J. and Srikant, R., Technological solutions for protecting privacy. *Computer*, ,9, pages 115–118.

CLM$^+$02 Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M. and Reagle, J., The platform for privacy preferences 1.0 (p3p1. 0) specification. *W3C recommendation*, 16.

CS09 Cormode, G. and Srivastava, D., Anonymized data: generation, models, usage. *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data.* ACM, 2009, pages 1015–1018.

Cul00 Culnan, M. J., Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing*, 19,1(2000), pages 20–26. URL `http://dx.doi.org/10.1509/jppm.19.1.20.16944`.

DB00 Dhillon, G. and Backhouse, J., Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43,7(2000), pages 125–128.

DJ09 Dowling Jr, D. C., International data protection and privacy law. *Practising Law Institute (available online at www. whitecase. com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_ IntlDataProtectionandPrivacyLaw_ v5. pdf)*.

Doy11 Doyle, C., *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.* DIANE Publishing, 2011.

ERB03 Eltoweissy, M. Y., Rezgui, A. and Bouguettaya, A., Privacy on the web: Facts, challenges, and solutions. *IEEE Security & Privacy*, 1,6(2003), pages 0040–49.

Evf02 Evfimievski, A., Randomization in privacy preserving data mining. *ACM Sigkdd Explorations Newsletter*, 4,2(2002), pages 43–48.

FH98 Ferguson, P. and Huston, G., What is a vpn?, 1998.

FPT14 Franchi, E., Poggi, A. and Tomaiuolo, M., Information attacks on online social networks. *Journal of Information Technology Research (JITR)*, 7,3(2014), pages 54–71.

GJK08 Grandison, T., Johnson, C. and Kiernan, J., Hippocratic databases: Current capabilities and future trends. In *Handbook of Database Security*, Springer, 2008, pages 409–429.

GKKM07 Ghinita, G., Karras, P., Kalnis, P. and Mamoulis, N., Fast data anonymization with low information loss. *Proceedings of the 33rd international conference on Very large data bases.* VLDB Endowment, 2007, pages 758–769.

GL04 Gouda, M. G. and Liu, X.-Y. A., Firewall design: Consistency, completeness, and compactness. *Distributed Computing Systems, 2004. Proceedings. 24th International Conference on.* IEEE, 2004, pages 320–327.

GS07 Gupta, M. and Sharman, R., Pharming attack designs., 2007.

Gun11 Gunatilaka, D., A survey of privacy and security issues in social networks. *Proceedings of the 27th IEEE International Conference on Computer Communications. Washington: IEEE Computer Society*, 2011.

HCSS14 He, B.-Z., Chen, C.-M., Su, Y.-P. and Sun, H.-M., A defence scheme against identity theft attack based on multiple social networks. *Expert Systems with Applications*, 41,5(2014), pages 2345 – 2352. URL `http://www.sciencedirect.com/science/article/pii/S0957417413007860`.

HDL+90 Heberlein, L. T., Dias, G. V., Levitt, K. N., Mukherjee, B., Wood, J. and Wolber, D., A network security monitor. *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on.* IEEE, 1990, pages 296–304.

Hon12 Hong, J., The state of phishing attacks. *Communications of the ACM*, 55,1(2012), pages 74–81.

KDWS03 Kargupta, H., Datta, S., Wang, Q. and Sivakumar, K., On the privacy preserving properties of random data perturbation techniques. *Data Mining, 2003. ICDM 2003. Third IEEE International Conference on.* IEEE, 2003, pages 99–106.

KDWS05 Kargupta, H., Datta, S., Wang, Q. and Sivakumar, K., Random-data perturbation techniques and privacy-preserving data mining. *Knowledge and Information Systems*, 7,4(2005), pages 387–414.

LAE+04 LeFevre, K., Agrawal, R., Ercegovac, V., Ramakrishnan, R., Xu, Y. and DeWitt, D., Limiting disclosure in hippocratic databases. *Proceedings of the Thirtieth international conference on Very large data bases-Volume 30.* VLDB Endowment, 2004, pages 108–119.

LKR06 Liu, K., Kargupta, H. and Ryan, J., Random projection-based multiplicative data perturbation for privacy preserving distributed data mining. *Knowledge and Data Engineering, IEEE Transactions on*, 18,1(2006), pages 92–106.

LP02 Lindell, Y. and Pinkas, B., Privacy preserving data mining. *Journal of cryptology*, 15,3(2002), pages 177–206.

Mal14 Malina, L., Privacy preserving cryptographic protocols for secure heterogeneous network, 2014.

MGA12 Malik, M. B., Ghazi, M. A. and Ali, R., Privacy preserving data mining techniques: current scenario and future prospects. *Computer and Communication Technology (ICCCT), 2012 Third International Conference on*. IEEE, 2012, pages 26–32.

MJB11 Madejski, M., Johnson, M. L. and Bellovin, S. M., The failure of online social network privacy settings.

MT05 Marshall, A. M. and Tompsett, B. C., Identity theft in an online world. *Computer Law & Security Review*, 21,2(2005), pages 128 – 137. URL `http://www.sciencedirect.com/science/article/pii/S0267364905000683`.

NJ05 Nadeem, A. and Javed, M. Y., A performance comparison of data encryption algorithms. *Information and communication technologies, 2005. ICICT 2005. First international conference on*. IEEE, 2005, pages 84–89.

NWM10 Nosko, A., Wood, E. and Molema, S., All about me: Disclosure in online social networking profiles: The case of facebook. *Computers in Human Behavior*, 26,3(2010), pages 406–418.

OAW12 O?connell, M. E., Arimatsu, L. and Wilmshurst, E., Cyber security and international law. *International Law Meeting Summary, Chatham House*, 2012.

RC99 Reagle, J. and Cranor, L. F., The platform for privacy preferences. *Communications of the ACM*, 42,2(1999), pages 48–55.

RHW$^{+}$08 Rieck, K., Holz, T., Willems, C., Düssel, P. and Laskov, P., Learning and classification of malware behavior. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, Zamboni, D., editor, volume 5137 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2008, pages 108–125, URL `http://dx.doi.org/10.1007/978-3-540-70542-0_6`.

RKK$^+$13 Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S. and Dabbish, L., Anonymity, privacy, and security online. *Pew Research Center.*

RKK14 Rizi, F. S., Khayyambashi, M. R. and Kharaji, M. Y., A new approach for finding cloned profiles in online social networks. *Int. J. of Network Security*, 6.

SKV10 Stringhini, G., Kruegel, C. and Vigna, G., Detecting spammers on social networks. *Proceedings of the 26th Annual Computer Security Applications Conference.* ACM, 2010, pages 1–9.

SP07 Srivastava, T. V. and Purcell, J., Phishing and pharming–the deadly duo. *Sans Institute.*

SS94 Sandhu, R. and Samarati, P., Access control: principle and practice. *Communications Magazine, IEEE*, 32,9(1994), pages 40–48.

SW09 Siponen, M. and Willison, R., Information security management standards: Problems and solutions. *Information & Management*, 46,5(2009), pages 267–270.

SZ99 Saunders, K. M. and Zucker, B., Counteracting identity fraud in the information age: The identity theft and assumption deterrence act. *International Review of Law, Computers & Technology*, 13,2(1999), pages 183–192.

TCJ10 Tan, P.-N., Chen, F. and Jain, A., Information assurance: Detection of web spam attacks in social media. *Proceedings of Army Science Conference, Orland, Florida*, volume 20, 2010.

VBF$^+$04 Verykios, V. S., Bertino, E., Fovino, I. N., Provenza, L. P., Saygin, Y. and Theodoridis, Y., State-of-the-art in privacy preserving data mining. *ACM Sigmod Record*, 33,1(2004), pages 50–57.

VSVS04 Von Solms, B. and Von Solms, R., The 10 deadly sins of information security management. *Computers & Security*, 23,5(2004), pages 371–376.

WJC99 Wesinger Jr, R. E. and Coley, C. D., Firewall providing enhanced network security and user transparency, April 27 1999. US Patent 5,898,830.

WK08 Wang, Y. and Kobsa, A., Technical solutions for privacy-enhanced personalization. *Intelligent User Interfaces: Adaptation and Personalization Systems and Technologies: IGI Global.*

WWDF12 Willey, L., White, B. J., Domagalski, T. and Ford, J. C., Candidate-screening, information technology and the law: Social media considerations. *Issues in Information Systems*, 13, pages 300–309.

ZBW12 Zilpelwar, R. A., Bedi, R. K. and Wadhai, V., An overview of privacy and security in sns. *International Journal of P2P Network Trends and Technology*, 2,1(2012).

ZSZF10 Zhang, C., Sun, J., Zhu, X. and Fang, Y., Privacy and security for online social networks: challenges and opportunities. *Network, IEEE*, 24,4(2010), pages 13–18.