Australian Government
Department of Defence
Defence Science and
Technology Organisation

Network Security Risks of Online Social Networking in the Workplace

Anselm Teh

Cyber and Electronic Warfare Division

Defence Science and Technology Organisation

DSTO–GD–0772

ABSTRACT

More people are using Online Social Networks (OSNs) at home and in the workplace. To help us understand the risks associated with their use, this paper reviews notable literature regarding network security risks due to OSN usage. The literature states that there are many possible attacks that can be carried out using OSNs, including information gathering, phishing and JavaScript exploits. There are also a number of technical and non-technical methods available to manage these security risks, including awareness training and standard computer security measures such as the use of an antivirus program and firewall.

APPROVED FOR PUBLIC RELEASE

Published by

DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh, South Australia 5111, Australia

Telephone: 1300 DEFENCE
Facsimile: (08) 7389 6567

AR No. 015–771
November, 2013

APPROVED FOR PUBLIC RELEASE

Network Security Risks of Online Social Networking in the Workplace

Executive Summary

This report provides a review of notable literature on the network security risks of Online Social Network (OSN) usage in the workplace.

It contains summaries and reviews of literature including conference papers, journal papers, news stories, and blogs. We provide details of attacks targeted at the underlying technologies used by OSN platforms and describe preventative measures for mitigating the network security risk due to OSN use.

We provide descriptions of non-technical attacks (information gathering, phishing) and their applications (identity theft, leakage of sensitive information, social engineering, malware deployment), technical attacks (malicious JavaScript, malicious OSN applications) and their applications (performing unwanted functions, accessing private information, malware deployment) and preventative measures. These attacks can result in significant information about users being revealed to attackers.

We conclude from the literature that there are a number of non-technical and technical prevention measures that can be taken to reduce the security risk posed by the use of OSNs. These include: user awareness training; standard computer security and network security measures; and browser hardening.

THIS PAGE IS INTENTIONALLY BLANK

Contents

Tables

Glossary

API Application Programming Interface.

ATM Automated Teller Machine.

CAPTCHA Completely Automated Public Turing test to tell Computers and Humans Apart.

CSRF Cross-Site Request Forgery.

DDoS Distributed Denial of Service.

DoS Denial of Service.

FQL Facebook Query Language.

HTML Hypertext Markup Language.

HTTP Hypertext Transfer Protocol.

OSN Online Social Network.

PIN Personal Identification Number.

TOS Terms Of Service.

URL Uniform Resource Locator.

US-CERT United States Computer Emergency Readiness Team.

XML Extensible Markup Language.

XSS Cross-Site Scripting.

THIS PAGE IS INTENTIONALLY BLANK

1 Introduction

Online social networks (OSNs) have become popular in recent years. An Australian survey conducted by Sensis in 2011 found that more than half of Internet users surveyed had a presence on OSNs [1]. OSNs such as Facebook are accessible through a web browser and so can be used wherever there is an Internet connection—at home, at work, or on a mobile device. Although most users surveyed accessed OSNs at home, 22% accessed OSNs at work. In a survey of US college students, 56% said that they would not accept a job offer from a company that banned social media, or that they would join the company and find a way to circumvent the policy [2].

As more people are using OSNs, it is important to examine the security risks associated with their use. The purpose of this paper is to provide a review of the literature on the computer network security risks related to the use of OSNs in the workplace. This paper reviews research published in conference and journal proceedings, books and relevant work published on the Internet. This is not an in-depth summary of all possible risks, attacks and security measures associated with OSN usage, but a review of notable literature in the field.

2 Background

Zhang et al. [3] state that OSN platforms perform three main functions. The first function is to allow users to construct digital representations of themselves and display their connections with other users. OSN users can build digital representations of themselves using a *user profile*. This is a page that may contain user information, work and education history, personal interests and arbitrary information about the user. User profiles may also provide access to a list of the social connections a user has in the OSN. These ‘friend lists’ allow OSN members to navigate a user’s social graph and discover that user’s relationships with others.

The second function of an OSN is to support the maintenance and enhancement of pre-existing social connections [3]. OSN providers often make functionality available that allows users to further develop their social connections, such as message posting tools, instant messaging and media sharing. Third-party applications also provide socially interactive functionality such as playing games.

The third function of an OSN is to help users to forge new social connections based on common interests, location and activities [3]. OSNs promote the creation of new social connections by suggesting new people to connect to. OSNs also provide the ability to join user-created groups where users that share a particular interest can have discussions. A search function allows users to easily find people or companies by name, and users can also find people by traversing the social graphs accessible through friend lists on user profiles.

Examples of popular OSNs include:

- Facebook - a social networking platform focussed on socialising, sharing media and playing games[1]
- LinkedIn - a networking platform focussed on professional networking[2]

[1] https://www.facebook.com/

[2] http://www.linkedin.com/

- Twitter - a platform that allows users to broadcast short messages[3]
- MySpace - a similar platform to Facebook that has become less popular in recent years[4]
- Google+ - a similar platform to Facebook that was started by Google in 2011.[5]

It is important to examine the computer security risks related to OSNs because many young employees expect to be allowed access to social media at work. In a study commissioned by Cisco [2], 2,800 college students and young professionals were surveyed about their attitudes regarding social media and device flexibility at work. The results were that 33% of respondents would prioritise social media freedom, device flexibility and work mobility over salary in accepting a job offer, and 56% of students said that they would not accept a job offer from a company that banned social media, or that they would join and find a way to circumvent corporate policy.

To examine the risks associated with OSN use in the workplace, we must have an awareness of computer security. Schneier [4] and Wang [5] state that computer security has three aspects: *confidentiality*, *integrity* and *availability*. We summarise their definitions as follows:

- confidentiality - data cannot be read by unauthorised users
- integrity - data or software cannot be modified, deleted or fabricated by unauthorised users
- availability - attackers cannot block legitimate users from having reasonable access to their resources and services.

Wang [5] also mentions that network security also deals with a fourth aspect, non-repudiation. As non-repudiation is not important in OSN security literature, we will not focus on this aspect.

Confidentiality, availability and integrity are managed using access control measures [4]. Access control is implemented in various ways in different OSNs and generally allows users to control who can see, modify, or post messages on their profile—typically, the owner of the profile, the owner's friends, or the general public. Although all OSNs implement some form of access control, there are many ways that malicious users can gain access to OSN resources that they should not be able to.

Apart from the social networking platforms managed by commercial OSN providers, there are a number of software packages that provide collaborative functionality for corporate networks. Products such as Confluence[6] allow users to create and organise material in their own 'space', and allow other users to view it. Using a corporate OSN could allow improved information sharing between employees while ensuring that the information was stored on an internal network. This would provide some protection against users who do not have network access. However, the use of a corporate OSN would not remove the risk posed by allowing access to public OSNs. As the current OSN security literature does not examine security issues specific to corporate OSNs in detail, we do not discuss it in this paper.

In the following section we discuss how attackers can use OSNs to compromise the confidentiality, integrity and availability of information stored on OSNs and on computer networks where OSNs are used. The methods used to perform these attacks are examined in Section 4.

[3] https://twitter.com/

[4] https://www.myspace.com/

[5] https://plus.google.com/

[6] https://www.atlassian.com/software/confluence/overview

2.1 Motivation for Attackers

As mentioned earlier, computer and network security measures aim to provide data confidentiality, integrity and availability. Common attacks used to circumvent these measures include eavesdropping, password stealing, identity spoofing, Denial of Service (DoS) attacks and malware installation [5]; the information sharing culture of OSNs can be used to make all of these attacks more successful.

The aggregation of user data in an OSN is a valuable resource for attackers. OSNs can provide access to a wealth of personal and sensitive information about users. Attackers can use OSNs to extract information about a target's personal life, family, friends and workplace information; analyse extracted information to infer information about the target; or even make direct contact with the target or the target's friends to perform social engineering.

The OSN mechanisms that support information sharing can also be used maliciously. OSNs can be used to spread malicious links that lead to malware downloads or phishing sites, allowing an attacker to steal credentials or deploy malware. OSN profiles can be cloned to facilitate social engineering, giving an attacker a more trusted relationship with the victim. Attackers can develop malicious OSN applications that are easy to install and provide access to the victim's information. Due to the ease with which social connections and interactions are accepted in an OSN, malicious users may not even need to resort to complicated attacks in order to subvert the security measures of a target computer network. We examine the methods used to perform these attacks in Section 4.

As OSNs generate and store a lot of information, it is useful to understand what kind of data they produce. The following section categorises the types of data that can be extracted from an OSN.

3 Types of OSN Data

OSNs contain a large amount of data about users and their interactions. Bonneau et al. [6] categorise OSN data into three categories:

- profile data
- social graph data
- traffic data.

Profile Data refers to user-provided information that is displayed on a user's profile page. Examples include: full name, date of birth, location, and relationship status. This data includes information that can be used for social engineering or identity theft attacks.

Social Graph Data refers to a node graph where each user is represented by a node, and each social connection between two users is represented by a link between two nodes. This graph can reveal information about a user's home and work life, and provide other avenues that an attacker can use to extract information. A user's social graph may provide information about:

- friends

- family
- work colleagues
- club members.

Traffic Data refers to usage information accessible by social networking servers. This information includes:

- IP addresses
- length and frequency of sessions
- profiles visited [7]
- web browser information.

Traffic data could possibly be used to infer information about a user, but it is generally inaccessible to regular users. It may, however, be accessible in some form to employees of the social networking company or business partners of the company.[7] Although this type of information may be exploited by malicious insiders, it is generally inaccessible to other users. Bonneau et al. [6] state that traffic data can be considered low risk.

These categories suggested by Bonneau et al. provide a high-level partitioning of OSN data based on how the data is generated—user input, user interaction, or lower level communication. Schneier's taxonomy [8] is more relevant to everyday users as it addresses questions about who generated the data and who has control over it. Schneier's taxonomy consists of:

- *Service data* is data that a user gives to a social networking site in order to use it, for example, name, age and email address.
- *Disclosed data* is data that users post on their own pages, for example, blog entries, photographs, messages and comments.
- *Entrusted data* is data that users post on other users' pages. It is the same as disclosed data, but another user has control of it.
- *Incidental data* is data that other people post about a user. It is the same as disclosed data, but created by another user who has control of it.
- *Behavioural data* is data that the site collects about a user's habits.
- *Derived data* is data about a user that is derived from all the other data.

[7] For more information, see:
https://www.facebook.com/about/privacy/
https://www.google.com/intl/en_uk/+/policy/
http://www.linkedin.com/static?key=privacy_policy
https://twitter.com/privacy

We can see from both of these taxonomies that data extracted from OSNs can provide valuable information about a target. Some of this information is not even created by the target or under their control. Information gathering is important in any attack, and is vital to the success of social engineering and phishing attacks. The information available on OSNs could greatly aid the success of attacks against individuals or the companies that they work for. The following section provides examples and applications of attack methods that use OSN functionality.

4 Methods of Attack

OSNs provide a platform that can improve information sharing and social interaction. With this increased accessibility come a number of risks including information leakage and exposure to malicious code. This section will examine methods that attackers may use to exploit OSNs. Sections 4.1 to 4.3 cover attacks that use the inbuilt functionality provided by OSNs, and Sections 4.4 to 4.6 cover attacks that involve the use of malicious code to exploit vulnerabilities in the OSN platform.

4.1 Non-technical Attack Methods

OSNs provide functionality that allows users to search through OSN data. This section examines how this functionality could be used by malicious actors for their own purposes. A number of the methods mentioned in this section use computers to aid in information processing or performing repetitive tasks, but they do not involve the use of malicious code to exploit OSN vulnerabilities.

4.1.1 Information Gathering

OSNs are designed to allow users to easily find and connect to each other, and users are actively encouraged to create new social connections with people they might know. This essential social networking function requires all users to make some information publicly available, and thus this information can also be accessed by malicious users.

Zhang et al. [3] examined the design issues regarding security and privacy in OSNs and determined that there are inherent conflicts between the aims of social networking and the privacy requirements of its users. One of the main motivations for a user to join an OSN is to be able to easily share information and interact socially. The more information a user releases publicly the more they can benefit from their participation, but this may also lead to malicious attacks including stalking, spamming and phishing.

Many people use OSN sites without realising how much content can be seen by people outside of their ‘friend list’. Liu et al. [9] surveyed 200 Facebook users to determine whether the privacy settings of posted content matched the privacy expectations of the users who posted them. They found that privacy settings matched users’ expectations only 37% of the time. When the settings did not match, they almost always exposed content to a wider audience than expected. They also found that 36% of content is posted using the default privacy settings, but even when users modify these settings they only match the user’s expectations 39% of the time.

Users may also choose to share their personal information without understanding the risks involved in revealing it online. In [10], Polakis et al. use automatic harvesting techniques to extract profile information from publicly accessible Facebook, Twitter and Google Buzz[8] profiles. Table 1 shows five of the more common categories of publicly available information they harvested from 1,597 Facebook profiles.

Table 1: *Categories of profile information and the percentage of users that reveal them publicly in Facebook profiles [10]*

Category	Percentage of profiles
Current city	41.8
Hometown	38.8
Employers	24.9
College	24.5
High school	24.5

Sophos performed similar experiments on a smaller scale in 2007 [12] and 2009 [13]. These experiments involved using made-up information to create Facebook profiles and using these profiles to send friend requests to legitimate users. Because Facebook friends can access more profile information than the general public, any legitimate user that accepted a friend request might be revealing private information to an unknown party. Both experiments used newly-created profiles to attempt to befriend 200 people on Facebook. Of the people contacted, 41% accepted a friend request in 2007 and 46% in 2009. The Sophos researchers gained access to information such as:

- full date of birth
- email address
- college or workplace
- town or suburb
- family and friend data.

We can see that many people make important personal information available on their OSN profile page, and people who do not release their information publicly may allow attackers to view this personal information by accepting their friend request. Once a user has accepted a friend request from an attacker, the attacker has ongoing access to 'disclosed data' and 'incidental data' posted on the user's profile page. This information could be used maliciously in a number of ways including social engineering attacks, identity theft and password guessing. The malicious uses of this information are covered in more detail in Section 4.2.

Even if users try to keep important information out of their profile page, other users may inadvertently reveal this information by posting photos or making seemingly benign comments. For example, if a user 'Bob' keeps his real name and occupation out of his profile for privacy reasons, Bob's friend 'Alice' might post a photo of them together and comment that Bob was 'the best teacher in Canberra'. This would reveal Bob's location and occupation, and could even reveal his identity through automated facial recognition [3]. Lam et al. [14] examined the possibility of using this involuntary information leakage to infer the name of a social network account holder that did not reveal their name. In an analysis of approximately 600,000 profiles on a Taiwanese OSN

[8] Google Buzz was an unsuccessful OSN platform created by Google. They shut it down in 2011 [11].

called ‘Wretch’, the researchers could identify the first name of 72% and last name of 30% of the account holders. They could also identify the age of 15% of the users and school of 42% of the users. This method of inferring a user’s name and personal information is based on text processing and the application of a number of heuristics, so it is feasible that this method could be modified for English language OSNs. We can see that merely keeping information out of one’s profile may not be enough to prevent it from being discovered by a malicious party.

Because online communities often form around shared user attributes (for example, a user’s interests, school, or location) it may be possible for an attacker to infer information about victims even if they do not post this information on their profile page. Mislove et al. [15] observed that users are significantly more likely to be friends with others who share the same attributes, and that this often leads to communities of users that are centred around certain attributes. By analysing the Facebook profiles of Rice University students, the authors found that they were able to use community detection algorithms[9] to discover communities of users that share specific attributes. They found that if they had access to the attributes of 20% of the users in a community, they could infer the attributes of the remaining users with over 80% accuracy. Mislove et al.’s discussion shows that this result is dependent on the group of users and attributes under analysis; for example, Rice undergraduates were 4.49 times more likely to go to the same college as another user in their friend list compared to a randomly selected college, but 2.33 times more likely to study the same major.

It may also be possible to discover the identity of an OSN user through analysis of their browser history. Wondracek et al. [17] pointed out that by stealing the history from a user’s browser, an attacker could extract group membership information from the history and combine this with publicly available group membership data to uniquely identify the user. Although the use of a history stealing attack can be categorised as a technical attack, publicly available group membership information can be collected without the use of any exploits. Wondracek et al. applied their proposed method in a real-world experiment using the ‘XING’ social network. Out of 26 volunteers, 15 had a history that indicated group interaction and all 15 users could be uniquely identified. Although this attack shows that group membership information can be used to identify a user, it has the limitation that a user can only be identified if the user is a member of multiple groups, each group has a publicly available member list, the attacker has successfully stolen the user’s browser history, and group membership information can be inferred from the URLs (Uniform Resource Locators) in the browser history.

OSNs such as Facebook, Google+, LinkedIn, MySpace and Twitter generate revenue from advertising and may offer services such as ‘targeted advertising’. This allows an advertiser to focus on a subsection of the OSN user base based on their age, sex, interests and other profile information. This targeting is done through an intermediate layer so as not to reveal any personal user information to the advertiser. Korolova [18] found that Facebook’s targeted advertising tools could be manipulated to allow an attacker to infer personal information about a target. This was done by running multiple advertising campaigns while varying the set of target criteria. The criteria used in the proposed attack comprises a constant set of features extracted from the victim’s public profile and a varying feature that the attacker wishes to discover. When a match occurs the attacker can assume that they have discovered the correct value for the unknown feature. Korolova was able to correctly infer a friend’s age using prior knowledge of her education and workplace. The cost of finding out this information was a few cents and could feasibly be applied to more sensitive profile

[9] Community detection algorithms for node graphs aim to identify clusters or communities where many edges join vertices in the same cluster (in the case of OSNs, many users are friends with other users in the same community), and comparatively few join vertices of different clusters [16].

information. Korolova also proposed that information *not* provided in a user's profile could be inferred by targeting them with advertisements that they may be interested in (for example, 'Having marital difficulties? Our office offers confidential counselling'). Information about the target could then be inferred from the behavioural information associated with the target's response.

4.1.2 Phishing

Phishing attacks involve an attacker attempting to acquire sensitive information from a victim by impersonating a trustworthy entity [19]. A typical example of a phishing attack involves an attacker sending an email to a victim purporting to be an employee from their bank. The email may state that the victim's account has been suspended and that the victim needs to verify their identity by supplying their personal information, including their ATM Personal Identification Number (PIN) [20].

Phishing is now common on OSNs, and phishing methods are frequently used by attackers to try to gain access to a victim's login details. Phishing attacks commonly work by directing a victim to access an official-looking login page that harvests the victim's credentials. Once their credentials have been stolen, their account can be used to attack others. If the victim has reused these credentials on other sites, the attacker may be able to access these accounts as well.

An example of such an attack is as follows. The victim receives a message that seems to link to a humourous video. It redirects the victim to a site that appears to be a Facebook login page, but actually steals user credentials [21].

In a similar scam on Twitter, the target receives a message saying 'you look like you lost weight in this video'. The message contains a link to a page that appears to be the standard Twitter login page but is actually a malicious site that steals user credentials [22].

Phishing can be made even more effective by personalising the attack using information about the victim. This is called *spear phishing*. In [19], Jagatic et al. used information extracted from publicly accessible social networking profiles to perform a phishing experiment. The authors sent emails to two groups of students containing a link which redirected them to a site that asked for their university login details. One group received spoofed emails from their friend's email address, while the other group received emails from an unknown address within the university domain. The authors found that students were 4.5 times more likely to follow the link and enter their login details when the sender was someone they knew. When the results of the experiment were revealed to the students, many did not understand how the researchers had obtained information about their friends. This suggests that many users do not understand how much information they make available through their OSN profile and how it could be used against them.

4.2 Applications of Non-Technical Attacks

The non-technical attack methods mentioned in Section 4.1 can be used in a number of ways. This section lists some possible applications of these attacks.

4.2.1 Identity Theft

Identity theft commonly refers to the use of a victim's personal information to obtain assets such as credit cards and mobile phones in their name [23, p. 32]. As many people display information such as birth date, address and pet's name on their OSN profiles, attackers have easy access to much of the information needed to perform identity theft.

A type of identity theft specific to social networking involves the creation of a profile using the name and personal information of a victim. An attacker using this 'cloned profile' can then interact with acquaintances of the victim with an increased level of trust. Bilge et al. [24] demonstrated an automated way to clone a public social network profile. Their system provided the ability to extract profile information from public profiles, create new profiles using the same name and profile information but different email address, and send out friend requests to friends of the victim. Their experiment found that friend requests from cloned profiles had a success rate of 90%, while friend requests from unknown accounts had a success rate of 30%.

Identities may also be bought and sold illegally online. In [25] Brian Krebs described an illegal site that provides paid access to databases of illegally obtained information. A user can search these databases for specific information such as date of birth or Social Security number, and a successful search costs as little as $3 US. Packs containing hundreds or thousands of identities can be bought for as little as 9 cents per identity. These packs include information such as full name, email address, email account password, driver's license number, bank name and account number, employer name and number of years the individual has been in their current job. Identity theft can lead to severe personal difficulties and allow attackers to gain access to information that they would otherwise not have access to.

4.2.2 Leakage of Sensitive Information

Leakage of sensitive information can easily occur through social networking services. As OSN users become accustomed to regularly sharing information about themselves, they may reveal sensitive information without realising it. Employees may post sensitive information about certain projects they are working on, or mention concerns about the company's financial status or changes in structure. Social networks can also be used by malicious insiders as a way to export confidential information [26]. Once this information becomes public, it cannot be secured. Leakage of sensitive information is an obvious danger to the confidentiality of workplace information.

4.2.3 Social Engineering

Social engineering is the manipulation of an unsuspecting person into revealing confidential information or obeying instructions that they normally would not [27, p. 121]. The availability of background information about the victim is important in a successful social engineering attack. This information is used to create a believable pretext to justify any questions asked or requests made by the attacker.

Information found on social networks can be used to infer detailed information about a company, including organisational charts, technology used, and employee groups and interests. This information can then be used to target an employee or group in order to custom-design a scenario for a social engineering attack [28].

The DefCon 18 social engineering contest consisted of a number of contestants using social engineering techniques to extract potentially useful information from businesses. The results from the two-week information gathering process showed that Facebook and LinkedIn were amongst the resources used by almost every contestant. Facebook was useful as employees from target companies often had publicly accessible accounts. LinkedIn proved to be the most useful resource, allowing contestants to build complete organisational charts and extract information about key employees [28]. These results show that OSNs can be extremely useful to prospective social engineers.

4.2.4 Malware

Malware can be introduced onto target computers through phishing scams in OSNs. Phishing messages may include links to malicious sites or even contain malicious code that is executed by the browser.

An attacker typically entices a victim to navigate to a malicious site by creating a phishing message containing information about topical issues (e.g. the death of Whitney Houston [29], free gifts [30], or OSN account information [31]). The message might provide a link to a video, picture, or website, and when the user navigates to this address the browser automatically downloads a malicious executable. URLs may be obfuscated through the use of a URL shortening service—these are used to shorten long URLs by providing an alternative short URL that redirects the browser to the desired site. This process can hide the fact that the short URL does not lead to the site that the user expects [32]. Phishing scams that download malware have been found on Facebook, Twitter and MySpace [33] [34] [35].

The Koobface worm is a well-known example of malware that spreads via phishing messages and has been found on multiple OSNs. It works by tricking a user into downloading malware, which, when installed, turns the victim's computer into a *zombie*—a computer under the control of the attacker. When the malware is installed on multiple computers, the attacker can control many of them at the same time. This zombie network is called a *botnet*. Thomas and Nicol [34] used a zombie emulator to communicate with servers controlling the Koobface botnet to analyse the infection cycle of the malware. The cycle begins when the victim receives a phishing message from one of their contacts. This message is sent from a compromised or fraudulent account and contains a short URL provided by a message shortening service. Clicking on the link triggers a series of browser redirections which aim to subvert security measures that block blacklisted URLs. The victim's browser then accesses a site that appears to be a YouTube or Facebook page that is actually a malicious page served by a compromised machine. The page content tricks the victim into downloading a malicious file appearing to be an Adobe Flash update, and once the victim installs this malware their machine becomes a zombie. The victim's zombie machine may then be used to create fake OSN accounts, acquire new friends, spam the victim's contacts and create blog accounts to act as redirectors. The application also tricks victims into solving CAPTCHAs[10] by making them believe that their computer would restart if they did not. Koobface has spread through Facebook, MySpace and Twitter networks [34] [35], and variants exist for Mac OSX [37] and Windows [38].

Malware may be used to steal information, steal credentials, deny services to the user, or control a target computer and use it to perform illegal activities. If attackers are able to deploy malware

[10] CAPTCHAs are programs that generate and grade tests that humans can pass but computer programs cannot [36].

onto a victim's computer, they may also be able to use this computer as a 'pivot point' to access other computers on the network. Once malware is active on a target machine, it could compromise the confidentiality, integrity and availability of information on the network the target machine is connected to.

4.3 Summary

OSNs provide functionality to allow easy searching of data and sharing of information. This functionality can be used for information gathering and phishing attacks, which could result in identity theft, the leakage of sensitive information, social engineering attacks, or malware downloads.

4.4 Technical Attack Methods

Attacks that use OSNs are not restricted to using legitimate OSN functionality to perform malicious acts. Like other web-based applications, OSNs may be vulnerable to JavaScript-based attacks. Attackers may also write malicious OSN applications that can access OSN resources with the privileges of the victim. This section examines the use of technical attack methods to exploit OSN vulnerabilities.

4.4.1 Malicious JavaScript

JavaScript is a scripting language supported by most modern browsers [39, p. 3]; this portability is ideal for authors of malicious JavaScript code. JavaScript-based attacks exploit vulnerabilities in a site's code or the user's browser in order to execute code. Facebook, Twitter, and MySpace have all been affected by JavaScript *worms*—pieces of malicious code that spread themselves through a computer network, in the case of OSNs by using Cross Site Scripting (abbreviated as XSS) or Cross-Site Request Forgery (CSRF) exploits, explained further below.

An XSS attack is the injection of JavaScript code into a vulnerable website. When a victim accesses the site, the code is executed in their browser. On OSN sites, this injection could be done in numerous ways:

- posting a link containing the JavaScript exploit on the vulnerable site [40]
- injecting the exploit into a compromised page [41]
- sending the victim a link containing the exploit that accesses the vulnerable site [42]
- stating that the victim should copy and paste the exploit code into their address bar in order to win a prize [43].

XSS vulnerabilities can allow the attacker to execute arbitrary JavaScript code and can be used to perform malicious actions such as stealing HTTP cookies stored on a victim's browser. Authentication cookies contain information that allows users to access their account without re-entering their credentials. Stealing these cookies may allow an attacker to perform transactions using the victim's account.

CSRF attacks use the victim's browser context to perform HTTP requests. This means that if a user is logged in to a site, a request made by the browser will be performed with the user's permissions. A website would be vulnerable to this sort of attack if it relied on HTTP cookies alone to confirm the requestor's identity. More secure authentication processes, such as those that use a cryptographic "nonce"[11], would not be susceptible [44].

One recent Twitter CSRF exploit provides a link to a web page containing malicious JavaScript code that posts a status update using the victim's browser context [45]. Another CSRF vulnerability, found on Facebook, allows an attacker to arbitrarily change many settings for any user. This vulnerability has since been fixed [46].

4.4.2 Malicious OSN Applications

OSNs such as Facebook, MySpace, and Google+ commonly allow third-party developers to provide functionality through OSN applications. These applications use Application Programming Interfaces (APIs) provided by the social networking platform to access user information and provide a personalised service. When OSN applications are installed, they must request permission from the user to access or manipulate user information. This may include access to profile information, friend lists, or the ability to publish messages on the user's message stream. Users must accept this permission request before the application can be installed.[12] Any user information extracted by the application is protected by a Terms of Service (TOS) agreement between third party developers and the OSN service providers [47].

Although many OSN services nowadays provide a fine-grained means of controlling access to profile data, it is the application developers who specify the required permissions to let users install an application. The relationship between application developers and users grants the developers a high level of access to a user's profile; developers may have more access than friends, even though users may know little about the developer [47].

Although OSN service providers monitor their network for suspicious application activity, it is not possible to completely prevent malicious applications entering the marketplace. Facebook is the most popular service that has been affected by malicious applications. A well-known malicious application is the 'Secret Crush' worm, which claimed to be able to reveal the identity of users that had a crush on the victim. To install the application, the victim had to forward an application invitation to five of their friends. Once the application was installed, the victim was prompted to install a 'crush calculator', which turned out to be an adware[13] application [48].

4.5 Applications of Technical Attacks

The technical attack methods mentioned in Section 4.4 can be used in different ways. This section lists some of the possible applications of these attack methods.

[11] A "nonce" is a one-time token used in a transaction. See [44] for more details.

[12] An example of OSN permissions can be seen at the following URL https://developers.facebook.com/docs/reference/api/permissions/

[13] An adware program is designed to launch advertisements. For further information, see https://www.securelist.com/en/glossary?SSL=1&letter=65#gloss153599593

4.5.1 Perform Unwanted Functions

XSS exploits like those mentioned in Section 4.4.1 allow attackers to execute JavaScript code using the victim's permissions. This could lead to a number of unwanted results, including redirection to a malicious website, the posting of unwanted messages on the victim's message stream, or the theft of cookies containing login information.

CSRF exploits can allow an attacker to successfully perform HTTP requests to a vulnerable site using the victim's permissions. This could include banking sites and result in unwanted transactions.

Malicious applications can perform functions such as spreading throughout the victim's friend network, or generating unwanted traffic. A recent example is a Facebook application that presented itself as an official application [49]. This application posted messages on victims' walls to inform them that Facebook was closing down its unused accounts. Users were asked to verify their activity by installing a malicious Facebook application called 'Confirm your activity - Official Application'. The application requested permission to access basic information, the ability to post messages to the victim's wall, and access to the victim's data when the application was not in use. Once the application was installed, it posted a message to the victim's wall, prompting their friends to download the malicious application. A simple malicious OSN application such as this can be effective against a user who does not know how to recognise it.

Academic investigations into malicious applications show that they can be operated like a botnet to perform a Distributed Denial of Service (DDoS) attack. Athanasopoulos et al. [50] created a Facebook application that displayed pictures from the National Geographic website every time it was clicked by a user. The application also had an undisclosed function that loaded pictures from a victim site into a hidden HTML 'iframe' element every time the application was clicked. It was installed by nearly 1,000 different users from different countries in the days after its release and generated a peak bandwidth of 6 Mb/s at the victim host. The authors calculated that with a more popular application which had 1–2 million users, the victim host could have to cope with traffic of 24 Mb/s on average. This paper shows that it is easy to create a malicious application, make it available through an OSN like Facebook, and have it spread quickly.

4.5.2 Access Private Information

Many popular Facebook applications request access to private data that they do not need. Because of this, users are accustomed to accepting unnecessary permissions requests in order to install applications. In a study of 150 popular Facebook applications, Felt and Evans [47] found that over 90% of them had unnecessary access to private data. Of the 14 applications that processed the data as part of their functionality, four clearly violated the Facebook TOS.

Applications may also be able to access social graph information even when they have not been installed by users. Bonneau et al. [6] examined Facebook Query Language (FQL) to see how it could be used to gather user information. They found that applications with no registered users could use general FQL queries to gather social graph data. By repeatedly performing queries, it was possible to extract friendship graphs that might otherwise be private. Users must opt out of the Facebook Platform in order to be hidden from FQL queries, but less than 1% of users do so [6]. As the Facebook Platform is required in order to use third-party applications, users that opt out of the platform would have reduced functionality.

4.5.3 Deploying Malware

JavaScript exploits and malicious applications are both able to spread links to malicious websites. If a user downloads malware by accessing a malicious link, the malware could perform any number of functions, including gaining control of the victim's computer.

4.6 Summary

XSS and CSRF have been used in the past on MySpace, Twitter, and Facebook to create worms and spread links that could lead to malware downloads. Malicious applications that can spread through friend lists and be used to collect private profile data have also been found on Facebook. JavaScript exploits and malicious applications can be used to compromise the confidentiality and integrity of data stored on an OSN, disrupt the availability of services through DoS attacks, and deploy malware on a target machine.

Table 2 provides a summary of the attacks discussed in this section.

4.7 Security of OSN Providers

A successful attack against an OSN provider could expose users' information no matter how secure their settings were. According to the literature on OSN security, OSN providers such as Facebook, Twitter, and Google+ have not yet been successfully attacked. Twitter and Facebook have suffered service outages due to purported DDoS attacks [51,52], but these outages would be an inconvenience for users rather than pose a security risk. In June 2012, LinkedIn confirmed that password hashes belonging to their users were found in the wild. LinkedIn stated that they found no evidence of a data breach and that they were investigating the matter. They have since increased the security of their password databases [53].

Google, the company that created the Google+ platform, has been successfully attacked in the past. In an attack in 2010 a Google employee in China was sent a malicious link as part of a phishing attack. This attack lead to the automatic downloading of malware onto the victim's computer and the theft of proprietary code [54,55].

Drawing from these examples, we can say that there is some risk that an OSN provider could be successfully attacked and that information could be stolen.

We discuss how OSN providers could improve the security of their platforms in Section 5.2. The next section covers non-technical measures that can be taken to mitigate the risks of OSN use in the workplace.

5 Preventative Measures

This section examines some proposed methods to mitigate the risks of using OSNs at work. Section 5.1 looks at possible non-technical measures, while Section 5.2 examines technical measures.

Table 2: *Overview of OSN attacks*

	Information Gathering	**Phishing**	**XSS**	**CSRF**	**Malicious OSN Applications**
Types of attack	manual browsing web crawling OSN API manipulation	spam spear phishing	redirection cookie theft worm arbitrary JavaScript functions	arbitrary HTTP requests	unwanted OSN functions
Applications	information aggregation information analysis identity theft social engineering spear phishing	scams steal credentials deliver JS exploits deploy malware	unwanted OSN functions malware deployment	exploit vulnerable websites malware deployment	information stealing DDoS

5.1 Non-technical Preventative Measures

Awareness training and the defining of acceptable use policies are widely recommended as preventative measures against OSN-based attacks [26, 48, 56–58]. This section covers some of the areas that employees should be familiar with and that security policies should cover.

Being aware of possible risks may help OSN users to safeguard information about their company, co-workers and work program. Apart from OSN administrators, only users can control the type and amount of information they have that is available to the public.

In [28], Hadnagy et al. pointed out that companies are only as secure as their weakest employee. When contestants in their social engineering competition failed to extract information from one employee in a company, they could often call a different person in the company to extract the information they needed. These results support the idea that awareness training is important for all employees, including the lowest level of employees within an organisation. When Jagatic et al. [19] performed phishing attacks on around 1700 university students, they found that the attacks were less successful on the students that majored in a technology subject than those that majored in other subjects.

Researchers from IT Governance [59], a company that creates information technology and information security products, suggest that awareness training for OSN security should cover:

- different types of data and the risks associated with their loss
- privacy controls
- reputation considerations
- the risks of downloaded content.

As mentioned in Section 4.1, profile information and messages posted on OSNs can be used for malicious purposes. Name and email address information can be used for phishing, personal information and social graphs can be used for social engineering and spear phishing, résumés and information such as ‘mother’s maiden name’ can be used for identity theft, and work-related information could be gathered for use by an employer’s competitors [59]. If users understand how their information can be used maliciously, they can consider the risk involved before posting anything [58].

Employees can better control the information stored on their OSN profiles if they understand the privacy settings available. OSNs may provide the functionality for users to change the visibility settings of their data, activate or deactivate their account, or delete their account. Information in a user’s profile can be made visible to different subgroups of people; visibility settings typically include: private (user only), friends only, public, or a combination [59]. For example, most of the information posted on a Facebook profile is available to ‘friends of friends’ by default [26], while a user’s birth date is only accessible to friends [59]. An OSN may change its default privacy settings over time, in which case awareness training can become out of date.

Employees should consider the possible risks to their reputation before posting anything [60]. OSNs are designed to allow users to share information easily, and once information is posted it can be difficult for a user to completely remove it.

Awareness training should include scenario-based exercises and cover simple points such as using OSN settings to restrict information access to certain groups, limiting the posting of personally identifiable information and professional information, thinking carefully before accepting any friend requests, and displaying caution regarding forwarded links [57, 58]. Parsons et al. [58] mention that training programs are more likely to be successful if the learning is personal, meaningful, and enforced. Further awareness training could include providing active assessments of employees' social networking exposure and providing reports containing personal profile analyses and possible risks [57].

5.2 Technical Preventative Measures

There are many defensive measures that can be taken to reduce the risk of attack through OSN sites. Many technical papers focus on improving weaknesses by altering the OSN platform, but there are a number of client-side measures that can be taken to reduce the impact of a malicious attack. This section covers technical preventative measures mentioned in the literature.

All papers agree that to protect computers in any network, standard computer security measures should be taken. Software patches and anti-virus signature definitions should be kept up to date and firewalls should be used to control traffic in and out of the network [58, 61]. Web traffic filtering should be used to block known malicious sites and reduce the chance of data leakage [59, pp. 46–50], and JavaScript and other active content should be blocked or restricted to trusted sites [61, pp. 36–40]. An application layer proxy should be used to inspect traffic for anomalous data, and intrusion protection and traffic monitoring systems should be used to detect anomalous traffic [26, 61].

One measure that is not discussed in detail in the OSN security literature is ensuring that web browsers are using secure settings; for example, Firefox can be set to alert the user whenever a website attempts to redirect it to a different site. Other Firefox settings suggested by the United States Computer Emergency Readiness Team (US-CERT) include displaying warnings when sites try to install add-ons, set cookies, or download files; setting the default download action for all file types as 'Save to Disk'; disabling Java; and blocking JavaScript using the 'NoScript' plug-in [62]. The US-CERT site also provides suggestions for hardening Internet Explorer and Safari web browsers. The SANS Institute also provides browser hardening suggestions and links to configuration files for Internet Explorer and Firefox that can be downloaded and applied [63].

Cole [26] mentions security measures tailored for workplaces that use OSNs. These measures include specifying an approved list of OSN applications and monitoring OSN traffic for signs of abuse, using modern firewall technology to block the traffic from certain Facebook applications, and using directory services to associate specific Facebook functions with different user groups. These measures could allow OSN traffic to be managed differently depending on the user.

To enable users to monitor the information they release publicly, Luo et al. [64] propose the use of web crawlers to actively extract information from users' OSN profiles. These crawlers could be deployed on multiple OSNs to examine the aggregated information a user has posted across these networks. The information could then be analysed and compared with the user's desired privacy level, and action could be taken if a mismatch occurred. Although this proposal sounds feasible, it would require the use of web crawlers on multiple OSNs. As this breaches the TOS of OSNs such as Facebook[14], it could not be implemented legally.

[14] https://www.facebook.com/legal/terms

A number of papers propose the implementation of 'virtual private social networks' to give users control over the profile information seen by others. The basic idea proposed is that each user in the private network has a profile that is populated with false information. A separate mechanism is then used to replace the false information with real information when a member of the private network accesses it. Conti et al. [65] propose a method where the real details of each user in a private network are kept in XML (eXtensible Markup Language) files on each member's local computer. A Firefox plug-in is then used to swap the false information in a profile with real information when OSN pages are accessed. Luo et al. [66] propose a similar method where real user data is encrypted and kept in a central repository and retrieved when needed. Guha et al. [67] propose a method where each field in a user's profile is replaced with information from another user's profile. These relationships are stored in a dictionary and can be accessed by authorised users. The methods described above have the advantage of being able to use the functionality of OSN platforms while retaining privacy for users, but they also add overheads such as dictionary management, word replacement using JavaScript, and, in [66], access of a remote repository each time a profile element needs to be looked up. These methods also prevent users outside the private network from finding users in the network, and do not fully address the issue of sensitive workplace information being posted in comments.

As mentioned earlier, many technical papers recommend that OSN providers do more to secure their platforms. Bonneau et al. [6] provide a number of recommendations including suggesting that OSNs should limit the number of mechanisms they provide to access user data, and that 'friend-of-friend' sharing should be eliminated. Athanasopoulos et al. [50] suggest that OSNs need to redesign their APIs to ensure that applications are constrained in the ways they can interact with the Internet. They also suggest that every application should run in an isolated environment to constrain their interactions with other hosts. These suggestions provided by Bonneau and Athanasopoulos would improve user privacy, but would also restrict information sharing. As OSNs make money from user information, they would not benefit by implementing a restrictive policy.

Felt and Evans [47] suggest that OSNs should manage the privacy of users that install third-party applications by providing an API that only allows profile information to be seen by users in approved groups. Developers must then create applications that perform functions using a limited, anonymous social graph. This method could support a range of OSN functionality without compromising profile information, but requires OSNs to update much of their API.

Nagy and Pecho [68] suggest a number of ways that OSNs could reduce malicious activity. They suggest that OSNs restrict the creation of new accounts by requiring an invitation from an existing account holder, implement a 'total-friends' constraint, and deploy software agents that control a dummy profile to monitor activity. However, restricting the creation of new accounts and constraining the number of friends a user has are impractical suggestions as they could restrict the activities of legitimate users and the growth of the OSN. Dummy accounts that monitor malicious activity are already used by anti-virus companies to gather information on current threats, but using software agents to interact with users could be an invasion of privacy and may even appear to be phishing attacks to a suspicious user.

OSNs benefit from a large user base and access to user information. OSNs such as Facebook, LinkedIn, MySpace and Twitter generate income by providing access to their user base for advertising and content delivery services. A large user base is therefore more attractive to advertisers as it allows them to disseminate their advertisements to a wider audience. Detailed user information is also enticing to advertisers, as it allows better targeted advertisments which may have a higher success rate [18]. Hence methods that restrict the growth of the user base are unlikely to be adopted.

5.3 Summary

There are a number of non-technical and technical prevention measures that can be taken to reduce the possibility of security breaches due to OSN use. As OSNs can be accessed wherever a web browser and Internet connection are available, the only prevention measure that can be applied in the workplace and which still relevant outside of work is awareness training.

In the workplace, computer security risks can be mitigated through non-technical measures such as awareness training and the implementation of security policies related to OSN usage, and technical measures such as antivirus usage, firewall usage, regular software updating, traffic filtering and blacklisting, and applying browser hardening settings.

OSNs generate revenue from their access to a large user base and access to user information. Methods of improving security that constrain their user base and discourage users from sharing information would be detrimental to their revenue stream, and it therefore seems unlikely that these methods would be adopted.

6 Conclusion

OSNs provide a platform to support socialising and the sharing of information, and are becoming increasingly popular. Although OSNs can improve knowledge sharing and strengthen relationships [58], there are many risks to consider.

A typical OSN profile contains a large aggregation of data—some not created by the owner of the profile—which can be mined for information. This data is valuable to malicious parties and could provide enough information to make inferences about other parts of the profile owner's life. Even if users endeavour to keep any information out of their page that they feel is sensitive, it could be unwittingly posted there by one of the owner's friends.

Many attacks that take place in OSNs are the same as attacks that take place through email, such as phishing scams and malware deployment. When used successfully in OSNs, they can compromise the confidentiality, integrity, and availability of data stored in an OSN or on the computer it is being accessed from. Although OSNs have security teams that screen posts and third-party applications for malicious content, it is not possible for all malicious activity to be blocked from OSN sites—this can be seen from the regular reports of OSN scams detailed in antivirus company blogs.

A number of technical and non-technical preventative measures can be implemented to mitigate the risk of using OSNs at work, with the most obvious one being an awareness program to familiarise employees with specific dangers and acceptable use policies. The added benefit of an awareness program is that it can also protect employees away from work.

References

1. *Sensis Social Media Report: What Australian people and businesses are doing with social media* (2011) Technical report, Sensis. URL – `http://about.sensis.com.au/ignitionsuite/uploads/docs/sensis%20social%20media%20report.pdf`.

2. *The New Workplace Currency - It's Not Just Salary Anymore: Cisco Study Highlights New Rules for Attracting Young Talent Into the Workplace - The Network: Cisco's Technology News Site* (n.d.). URL – `http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=532138`.

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

4. Schneier, B. (2000) *Secrets & Lies: Digital Security in a Networked*, Wiley Publishing.

5. Wang, J. (2009) *Computer Network Security*, Higher Education Press and Springer.

6. Bonneau, J., Anderson, J. & Danezis, G. (2009) Prying data out of a social network, *in International Conference on Advances in Social Network Analysis and Mining, 2009. ASONAM '09.*, pp. 249 –254.

7. *Information we receive and how it is used* (2011) *Facebook*. URL – `https://www.facebook.com/about/privacy/your-info`.

8. Schneier, B. (2010) A taxonomy of social networking data, *Security Privacy, IEEE* **8**(4), 88.

9. Liu, Y., Gummadi, K. P., Krishnamurthy, B. & Mislove, A. (2011) Analyzing Facebook privacy settings: user expectations vs. reality, *in Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, IMC '11, ACM, New York, NY, USA, p. 61–70. URL – `http://doi.acm.org/10.1145/2068816.2068823`.

10. Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T. & Markatos, E. P. (2010) Using social networks to harvest email addresses, *in Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, WPES '10, ACM, New York, NY, USA, p. 11–20. URL – `http://doi.acm.org/10.1145/1866919.1866922`.

11. Honan, M. (2011) RIP Google Buzz, *Gizmodo*. URL – `http://www.gizmodo.com.au/2011/10/rip-google-buzz/`.

12. *Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves* (2007) *Sophos Press Releases*. URL – `http://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx`.

13. *Facebook users at risk of "rubber duck" identity attack* (2009) *Sophos Press Releases*. URL – `http://www.sophos.com/en-us/press-office/press-releases/2009/12/facebook.aspx`.

14. Lam, I., Chen, K. & Chen, L. (2008) Involuntary information leakage in social network services, *in Proceedings of the 3rd International Workshop on Security: Advances in Information and Computer Security*, IWSEC '08, Springer-Verlag, Berlin, Heidelberg, p. 167–183. URL – `http://dx.doi.org/10.1007/978-3-540-89598-5_11`.

15. Mislove, A., Viswanath, B., Gummadi, K. P. & Druschel, P. (2010) You are who you know: inferring user profiles in online social networks, *in Proceedings of the third ACM international conference on Web search and data mining*, WSDM '10, ACM, New York, NY, USA, pp. 251–260. URL – http://doi.acm.org/10.1145/1718487.1718519.

16. Fortunato, S. (2010) Community detection in graphs, *Physics Reports* **486**(3–5), 75 – 174. URL – http://www.sciencedirect.com/science/article/pii/S0370157309002841.

17. Wondracek, G., Holz, T., Kirda, E. & Kruegel, C. (2010) A practical attack to de-anonymize social network users, *in IEEE Symposium on Security and Privacy (SP)*, pp. 223–238.

18. Korolova, A. (2010) Privacy violations using microtargeted ads: A case study, *in IEEE International Conference on Data Mining Workshops (ICDMW)*, pp. 474 –482.

19. Jagatic, T. N., Johnson, N. A., Jakobsson, M. & Menczer, F. (2007) Social phishing, *Commun. ACM* **50**(10), 94–100. URL – http://doi.acm.org/10.1145/1290958.1290968.

20. Wisniewski, C. (2011) Bank phishing emails increasing, promising bonuses and activation, *nakedsecurity*. URL – http://nakedsecurity.sophos.com/2011/11/02/bank-phishing-emails-increasing-promising-bonuses-and-activation/.

21. Cluley, G. (2011) Facebook phishing: Can you spot the difference?, *nakedsecurity*. URL – http://nakedsecurity.sophos.com/2011/06/03/facebook-phishing-spot-the-difference/.

22. Cluley, G. (2011) Look like you lost weight in this video? it's a Twitter phishing attack, *nakedsecurity*. URL – http://nakedsecurity.sophos.com/2011/08/04/look-like-you-lost-weight-in-this-video-its-a-twitter-phishing-attack/.

23. Anderson, R. (2008) *Security Engineering*, 2nd edition edn, Wiley.

24. Bilge, L., Strufe, T., Balzarotti, D. & Kirda, E. (2009) All your contacts are belong to us: automated identity theft attacks on social networks, *in Proceedings of the 18th international conference on World wide web*, WWW '09, ACM, New York, NY, USA, p. 551–560. URL – http://doi.acm.org/10.1145/1526709.1526784.

25. Krebs, B. (2011) How much is your identity worth?, *Krebs on Security*. URL – https://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/.

26. Cole, E. (2010) *Enabling Social Networking Applications for Enterprise Usage*, SANS. URL – https://www.sans.org/reading_room/analysts_program/palo_alto_networks_12_2010.pdf.

27. Wilding, E. (2006) *Information Risk and Security*, Gower.

28. Hadnagy, C. J., Aharoni, M. & O'Gorman, J. (2010) *Social Engineering Capture the Flag Results*, Social-Engineer.org. URL – http://www.social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf.

29. Cluley, G. (2012) Warning: Whitney Houston autopsy video links on Facebook aren't what they seem, *nakedsecurity*. URL – `http://nakedsecurity.sophos.com/2012/02/15/whitney-houston-autopsy-video-links-facebook/`.

30. Cluley, G. (2012) Free Amazon.com gift card promotion is a Facebook scam, *nakedsecurity*. URL – `http://nakedsecurity.sophos.com/2012/01/23/free-amazon-com-gift-card-facebook-scam/`.

31. Cluley, G. (2012) Sigh.. no, Facebook is not ending on march 15th 2012. hoax spreads quickly, *nakedsecurity*. URL – `http://nakedsecurity.sophos.com/2012/02/13/facebook-not-end-march-15/`.

32. Tanase, S. (2009) Short URLs, big problems, *Securelist*. URL – `https://www.securelist.com/en/weblog?weblogid=208187741`.

33. Cluley, G. (2010) Cross-platform boonana trojan targets facebook users, *nakedsecurity*. URL – `http://nakedsecurity.sophos.com/2010/10/28/cross-platform-worm-targets-facebook-users/`.

34. Thomas, K. & Nicol, D. (2010) The Koobface botnet and the rise of social malware, *in 5th International Conference on Malicious and Unwanted Software (MALWARE)*, pp. 63–70.

35. Cluley, G. (2008) Facebook and MySpace malware, *nakedsecurity*. URL – `http://nakedsecurity.sophos.com/2008/08/04/facebook-and-myspace-malware/`.

36. Google (n.d.) What is a CAPTCHA?, *ReCAPTCHA*. URL – `https://www.google.com/recaptcha/captcha`.

37. Krebs, B. (2010) Koobface worm targets java on mac OS x, *Krebs on Security*. URL – `https://krebsonsecurity.com/2010/10/koobface-worm-targets-java-on-mac-os-x/`.

38. Symantec (2010) W32.Koobface, *Symantec*. URL – `http://www.symantec.com/security_response/writeup.jsp?docid=2008-080315-0217-99`.

39. Flanagan, D. (2006) *JavaScript: The Definitive Guide*, 5 edn, O'Reilly.

40. Cluley, G. (2010) Twitter 'onMouseOver' security flaw widely exploited, *nakedsecurity*. URL – `http://nakedsecurity.sophos.com/2010/09/21/twitter-onmouseover-security-flaw-widely-exploited/`.

41. Cluley, G. (2009) Mikeyy attack hits twitter users - a bad 24 hours for web 2.0 security, *nakedsecurity*. URL – `http://nakedsecurity.sophos.com/2009/04/12/mikeyy-attack-hits-twitter-users-bad-24-hours-web-20-security/`.

42. *Cross-site Scripting (XSS)* (2011) *OWASP - The Open Web Application Security Project*. URL – `https://www.owasp.org/index.php/XSS`.

43. Wisniewski, C. (2011) Facebook explains pornographic shock spam, hints at browser vulnerability, *nakedsecurity*. URL – `http://nakedsecurity.sophos.com/2011/11/16/facebook-explains-pornographic-shock-spam-hints-at-browser-vulnerability/`.

44. Blatz, J. (2011) CSRF: attack and defense. URL – https://www.mcafee.com/us/resources/white-papers/wp-csrf-attack-defense.pdf.

45. Cluley, G. (2010) WTF? Twitter gets the goat as viral message spreads, *nakedsecurity*. URL – http://nakedsecurity.sophos.com/2010/09/26/wtf-twitter-goat-viral-message-spreads/.

46. Cluley, G. (2010) Embarrassing privacy flaw found on facebook, *nakedsecurity*. URL – http://nakedsecurity.sophos.com/2010/05/19/embarrassing-privacy-flaw-facebook/.

47. Felt, A. & Evans, D. (2008) Privacy protection for social networking APIs, *in Web 2.0 Security and Privacy*.

48. Steve & Mansfield-Devine (2008) Anti-social networking: exploiting the trusting environment of web 2.0, *Network Security* **2008**(11), 4 – 7. URL – http://www.sciencedirect.com/science/article/pii/S1353485808701272.

49. Cluley, G. (2011) Facebook is closing all accounts today? nope, it's a viral rogue application, *nakedsecurity*. URL – http://nakedsecurity.sophos.com/2011/04/08/facebook-is-closing-all-accounts-today-nope-its-a-viral-rogue-application/.

50. Athanasopoulos, E., Makridakis, A., Antonatos, S., Antoniades, D., Ioannidis, S., Anagnostakis, K. & Markatos, E. (2008) Antisocial networks: Turning a social network into a botnet, *in Information Security*, Vol. 5222 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, pp. 146–160. URL – http://dx.doi.org/10.1007/978-3-540-85886-7_10. 10.1007/978-3-540-85886-7_10.

51. van Buskirk, E. (2009) Denial-of-Service attack knocks Twitter offline, *Wired*. URL – http://www.wired.com/business/2009/08/twitter-apparently-down/.

52. Arrington, M. (2009) DDOS attacks crush Twitter, hobble Facebook, *TechCrunch*. URL – http://techcrunch.com/2009/08/06/ddos-attacks-crush-twitter-hobble-facebook/.

53. Mills, E. (2012) LinkedIn confirms passwords were 'compromised', *CNET News*. URL – http://news.cnet.com/8301-1009_3-57448465-83/linkedin-confirms-passwords-were-compromised/.

54. *Operation Aurora* (n.d.) *McAfee*. URL – http://www.mcafee.com/us/threat-center/operation-aurora.aspx.

55. Markoff, J. (2010) Cyberattack on Google said to hit password system, *The New York Times*. URL – http://www.nytimes.com/2010/04/20/technology/20google.html.

56. Gao, H., Hu, J., Huang, T., Wang, J. & Chen, Y. (2011) Security issues in online social networks, *Internet Computing, IEEE* **15**(4), 56 –63.

57. Lenkart, J. J. (2011) *The Vulnerability of Social Networking Media and the Insider Threat: New Eyes for Bad Guys*, Masters, Naval Postgraduate School, Monterey, California.

58. Parsons, K., McCormac, A. & Butavicius, M. (2011) Don't judge a (Face)Book by its cover: A critical review of the implications of social networking sites, *DSTO Technical Report*.

59. IT Governance Research Team (2009) *How to Use Web 2.0 and Social Networking Sites Securely*, IT Governance Publishing.

60. Park, M. (2009) Legal issues to consider for web 2.0, *in Inspecht HR Futures Conference*, Melbourne, Australia.

61. Timm, C. & Perez, R. (2010) *Seven Deadliest Social Network Attacks*, Syngress Seven Deadliest Attacks, Elsevier.

62. Crowley, C. (2009) *Preventing Incidents with a Hardened Web Browser*, SANS. URL – `https://www.sans.org/reading_room/whitepapers/bestprac/preventing-incidents-hardened-web-browser_33244`.

63. Dormann, W. & Rafail, J. (2008) *Securing Your Web Browser*, US-CERT. URL – `https://www.us-cert.gov/reading_room/securing_browser/`.

64. Luo, B. & Lee, D. (2009) On protecting private information in social networks: A proposal, *in IEEE 25th International Conference on Data Engineering, 2009. ICDE '09.*, pp. 1603–1606.

65. Conti, M., Hasani, A. & Crispo, B. (2011) Virtual private social networks, *in Proceedings of the first ACM conference on Data and application security and privacy*, CODASPY '11, ACM, New York, NY, USA, p. 39–50. URL – `http://doi.acm.org/10.1145/1943513.1943521`.

66. Luo, W., Xie, Q. & Hengartner, U. (2009) FaceCloak: an architecture for user privacy on social networking sites, *in Proceedings of the 2009 International Conference on Computational Science and Engineering - Volume 03*, CSE '09, IEEE Computer Society, Washington, DC, USA, p. 26–33. URL – `http://dx.doi.org/10.1109/CSE.2009.387`.

67. Guha, S., Tang, K. & Francis, P. (2008) NOYB: privacy in online social networks, *in Proceedings of the first workshop on Online social networks*, WOSN '08, ACM, New York, NY, USA, p. 49–54. URL – `http://doi.acm.org/10.1145/1397735.1397747`.

68. Nagy, J. & Pecho, P. (2009) Social networks security, *in Third International Conference on Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09.*, pp. 321 –325.

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION DOCUMENT CONTROL DATA	1. CAVEAT/PRIVACY MARKING

2. TITLE Network Security Risks of Online Social Networking in the Workplace	3. SECURITY CLASSIFICATION Document (U) Title (U) Abstract (U)
4. AUTHORS Anselm Teh	5. CORPORATE AUTHOR Defence Science and Technology Organisation PO Box 1500 Edinburgh, South Australia 5111, Australia

6a. DSTO NUMBER DSTO–GD–0772	6b. AR NUMBER 015–771	6c. TYPE OF REPORT General Document	7. DOCUMENT DATE November, 2013

8. FILE NUMBER 2012/1114135/1	9. TASK NUMBER 07/348	10. TASK SPONSOR CIOG	11. No. OF PAGES 24	12. No. OF REFS 68

13. URL OF ELECTRONIC VERSION `http://www.dsto.defence.gov.au/publications/scientific.php`	14. RELEASE AUTHORITY Chief, Cyber and Electronic Warfare Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SOUTH AUSTRALIA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS

No Limitations

18. DSTO RESEARCH LIBRARY THESAURUS

Social Network
Phishing
Identity Theft
Security

19. ABSTRACT

More people are using Online Social Networks (OSNs) at home and in the workplace. To help us understand the risks associated with their use, this paper reviews notable literature regarding network security risks due to OSN usage. The literature states that there are many possible attacks that can be carried out using OSNs, including information gathering, phishing and JavaScript exploits. There are also a number of technical and non-technical methods available to manage these security risks, including awareness training and standard computer security measures such as the use of an antivirus program and firewall.