



# Security Guide to Social Networks

Trend Micro, Incorporated 

 By: David Sancho  
Senior Threat Researcher

A Trend Micro White Paper | August 2009

## TABLE OF CONTENTS

- INTRODUCTION .....3
- PRIVACY IN A CONNECTED WORLD: DATA MINING IN SOCIAL NETWORKS .....4
- CREATING LARGE NETWORKS .....6
- WHEN CODE BREAKS .....8
- BEST PRACTICES .....9
- REFERENCES .....10



## INTRODUCTION

Social networking sites are websites designed for human interaction. They enable users to meet others; keep in touch with them; and share experiences, feelings, and opinions. They are all built on a similar foundation—the user builds a network of contacts bound by an element of trust. The user then creates content for his/her friends and, in turn, accesses the content they have created. This content can include such diverse things as holiday pictures, interesting links, latest news, opinions, comments, and mood updates.

The potential for mischief and malicious activities arises when one or more of those contacts breaks your trust. When that happens, a number of things can go wrong such as:

- Your contact's account was compromised and somebody else is using it.
- You added somebody to your network that you thought you knew but, in fact, you did not.
- You added somebody you thought was trustworthy but he/she turns out not to be.
- Insufficient use of privacy controls caused you to share data with people you never intended.

This document will cover the most common areas of attack using social networks and will recommend ways of minimizing risks. The goal of this paper is not to stop you from participating in social networks but to enable you to use them more safely.

## PRIVACY IN A CONNECTED WORLD: DATA MINING IN SOCIAL NETWORKS

Social networks contain a wealth of personal information. People share their date of birth, email address, home address, family ties, and pictures. Some of that information would not be valuable by itself but having a clear picture of everything about a person can give attackers ideas and information required to perform other attacks such as credit card fraud or identity theft. Any real-life targeted attack can be made much more effective through access to additional information about the intended victim.

In addition to this, underground forums sell personal information. Your data can be mined and stored somewhere in the dark corners of the Internet waiting for a criminal to pay the right price for it. Criminals can use this information to obtain birth certificates/passports/other documentation and fake real-life identities. Some countries have looser controls than others, but in general, identity theft is something that already happens regularly.

Other data that is of interest to criminals include email addresses, physical addresses, dates of birth, and affiliations:

**Social networks contain a wealth of information. These include:**

- Date of birth
- Email address
- Home address
- Family ties
- Pictures

- Email addresses are entered into databases that are later used for spam campaigns. Email addresses that come from social networks can be further categorized to improve the impact of the campaign—race, age, country and other factors can be used as filters in such a database so that its market price is higher than just any normal email address database. Email addresses can also be of great value in spear-phishing campaigns where they are often used as sender addresses. Spear-phishing is a very targeted phishing attack so using a known contact from a “friends” list adds credibility to the malicious email and increases the chances of success for the criminal.
- Real-life addresses are often shared in social networking sites and they too can be used to amass mailing databases for advertising purposes in a similar way as described above.
- TrendLabs researchers have reported prices of personal information ranging from US\$50 per stolen bank account credentials to about US\$8 per million email addresses. This last figure is likely to be much higher if it involves fresh addresses coming from a social networking site. [1]
- Date of birth data is used by different companies to confirm people’s identities over the telephone. Criminals do not have databases but they do have tools to automate “date of birth” searches in social networking sites. This proves that there is a demand for this information as a complementary piece in order to perpetrate certain types of fraud.
- Another factor that exacerbates this massive data-leakage potential is a user’s public profile. When users set their information to be accessible without logging in to the social networking site, that informa-

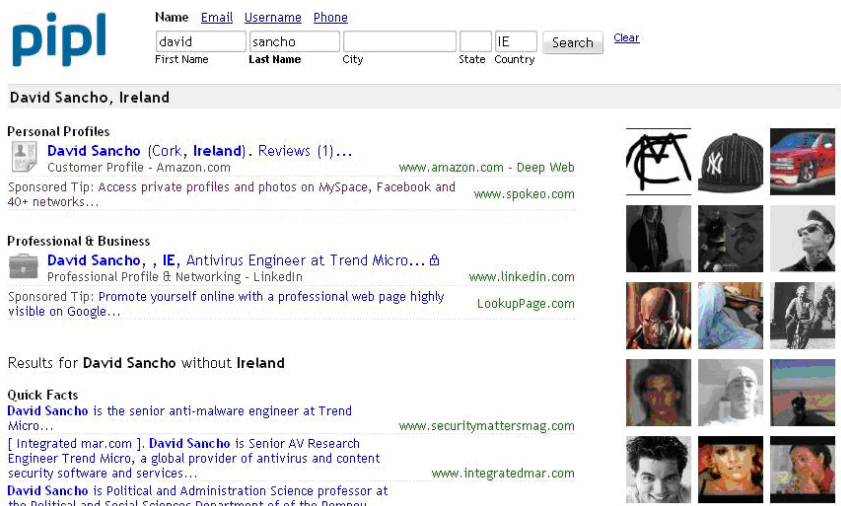


Figure 1. Sample pipl profile page

tion can be indexed in search engines or any other archive. There are social networking search engines that can search all available data about any name in a certain region. This makes the lives of stalkers, fraudsters, or any other attacker much easier. Not only do *Google* and other crawlers gather publicly available information but there are also meta-search engines like *pipl.com* specifically designed to search social networking sites and other sources to gather all sorts of information, from your name and the names of your friends to all the holiday pictures from three years ago that you already forgot you published online.

In July 2009, the wife of a high-level government executive in the United Kingdom published personal data in a social networking site. This garnered a lot of attention, not for the confidentiality of the content but for the lack of awareness there is about the accessibility of your online content. There is also another issue at play here, which is the fact that once you publish any picture online, you lose control over it as people leech and republish it on places you do not even know. In this case, news sites were some of the first to republish the infamous family pictures originally shared by the said executive's wife. [2]

It is worth mentioning the fact that Human Resource (HR) departments are already utilizing information on social networks' public profiles to know more about job candidates. A certain online recruitment website reports that 20% of employers use social networking sites to run searches on job applicants and 68% use search engines like *Google* and *Yahoo!* to check on candidates. [3] Although this common practice is not strictly illegal, it might be ethically questionable.

## CREATING LARGE NETWORKS

Social networking sites not only facilitate interacting with personal and professional contacts but also locating them in the first place. They are intended for both connecting and reconnecting people. It is fairly simple for miscreants to create a large network of contacts by using any number of underhanded techniques such as:

- Creating a fake celebrity profile and allowing people to add them to their contact lists.
- Creating a duplicate of somebody's profile and re-inviting all of their friends.
- Creating a profile, adding themselves to a medium-sized group or community, and inviting a number of members of the group (universities, schools, etc.). Then joining a second group and starting again.
- Creating a female profile and publishing a pretty picture of "herself" then letting people add him/her to their lists. A lot of people use social networking sites to meet their partners online and many of these sites have specific tools to facilitate this.

There are a number of strategies that allow an attacker to break the circle of trust and get into people's contact lists. A lot of social network users do not realize that their contact lists really is a circle of trust and by adding somebody they do not know—celebrities included—they are opening their data to untrusted parties.

Some sites do not have privacy controls in place, or the ones they have do not protect all user data. Even if they do have comprehensive privacy controls, the user is often not obligated to select who can access his/her data and is often dissuaded from using the available controls because they appear too complex or time-consuming. Many users simply do not bother to configure these controls, be it for laziness or lack of knowledge. This means that whether by the site's design or the user's lack of interest, personal data is needlessly exposed to strangers, search engines, and the wider online world.

So, what can an attacker do with a large network of contacts in a social networking site?

One obvious possibility is advertise. By writing/commenting on people's profiles or sending private mail, the attacker can distribute links advertising websites and products. If this strategy is done subtly, it can work relatively well, although usually this will be too much effort for any attacker. Contacts will quickly notice that the posts are covert advertising and will delete/block the attacker altogether. The same can be accomplished by private Web messaging, which all social sites allow but it is similarly ineffective for the same reasons stated above. These kinds of social networking spam runs are usually of a very limited duration and come from pay-per-click or pay-per-action affiliate-based online marketing schemes.

▶ So what can an attacker do with a large network of contacts in a social networking site? One obvious possibility is advertise. The second possibility is collect contact information such as email addresses or telephone numbers. The third possibility is phishing and/or malware installation.

The second possibility is the collection of contact information such as email addresses or telephone numbers. Those social sites that display your friends' contact information can be used to amass working email databases along with phone numbers or other data that can serve to better target future spam, phishing, and vishing (voice phishing) campaigns. There are people amassing large contact databases, which are later sold to spammers, scammers, and credit card fraudsters. The value of such a database is measured on the quality of the data. Older email databases have been spammed over and over so the addresses might have been abandoned or accounts closed altogether. The more valuable email databases include fresh working emails such as the ones you can find in social networking sites. This kind of data is not only useful for conducting campaigns but also has value in itself and can be sold through the underground economy.

The third possibility is for phishing and/or malware installation. Imagine this scenario—the attacker creates a phishing page identical to *Facebook's* login page. Then they change their status line to "check this funny video I found yesterday" and a link to the fake page. When people click the link, they are presented with a fake *Facebook* login page, which they use to "log in" again, perhaps thinking that somehow their session had timed out. At this point, the attacker has the victim's username and password but the attack does not end there. After "logging in," the fake page displays a funny video that

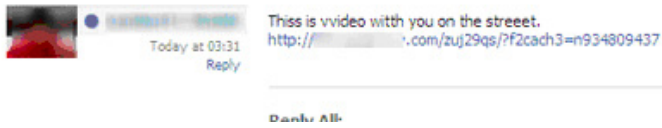


Figure 2. Sample malicious Facebook personal message

pening and, as has always been the case with malware attacks, they will continue to get more and more complex as users become increasingly careful with the links they click.

This is the real danger of social and community-based sites—users trust their contacts to not send bad links, to not to try to infect their computers and take good care of their personal data. Once the trust is broken any of those situations can happen at any time.

The real finesse comes from masking those bad links as if they were good. A normal user will probably have no problem clicking on a *youtube.com* link coming from an online contact but might be more careful with a *badsite.org* link. Enter URL shorteners. These online redirection services purposely hide a URL in order to make it shorter. Masked malicious URLs do not look dangerous before clicking on them. After that click, though, it is often too late. These shortening services are so widely used that people do not think twice before clicking one of them, even without knowing what lurks behind. URL shorteners are a security concern and should be taken very seriously.

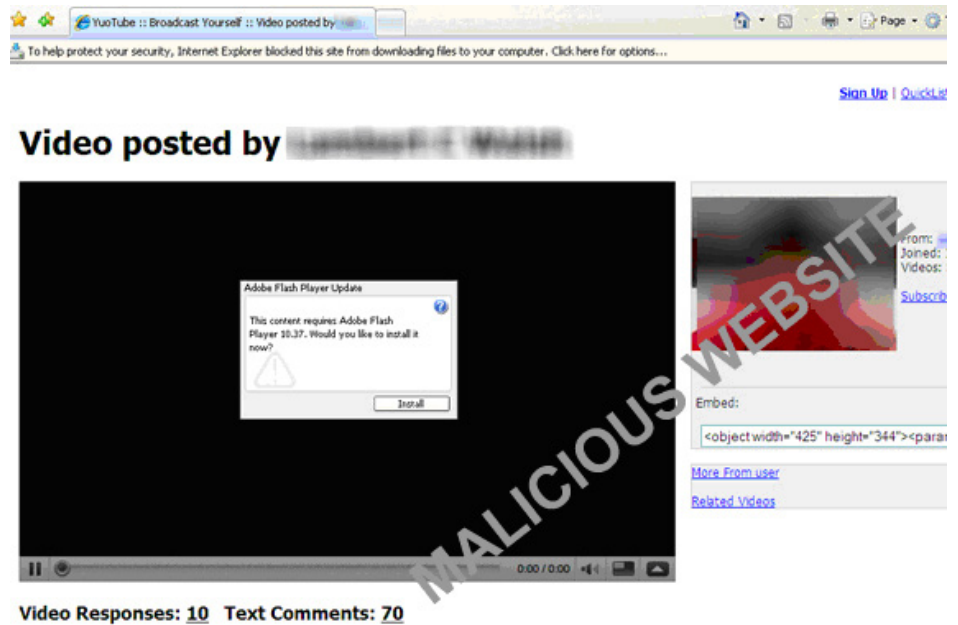


Figure 3. Sample malicious video linked to a Facebook personal message

exploits a browser vulnerability and installs a Trojan in the background. This is not a hypothetical scenario but a high-level description of the activities of the malware known as “KOOBFACE” that have been successful spreading on a number of social networks. This is already hap-

## WHEN CODE BREAKS

Another attack vector is the exploitation of programming flaws in websites. These Web pages have been made by humans and they can have errors that could compromise the site's security measures. This has happened a number of times to well-known social networking sites and will likely happen again in the future. In these occurrences, all users are at risk. Poorly thought-out security, weak administration practices, or badly written code can all help an attacker to gather your data or help them stage a bigger attack against any number of users.

There have been instances of security flaws on *Facebook* that allowed anybody to access the “basic information” data of any user, no matter what their security settings were. [4] This attack was released by casual users after *Facebook* ignored the users' warnings for a few days. No great knowledge was needed in this case to exploit a security weakness.

*Twitter* has had “cross-site scripting” attacks performed against it. In these cases, the attackers could change the *Twitter* status of any user accessing the attacker's account. This meant that the bad guys could make you tweet bad links so your *Twitter* followers would be at risk of being infected. [5]

*MySpace* was attacked in 2007 by a JavaScript that would copy itself to the viewer's profile along with a piece of text—“Samy is my hero.” This was caused by a security flaw that could have caused the victim to run any other command like redirecting the page to a malicious website. Thankfully, the young man who discovered the flaw and created the worm only wanted to have more friends added to his profile. [6]

These three examples are not the only cases of security flaws on social networking sites. In fact, such flaws are identified frequently. News about such security holes are released every month and are a concern for all affected websites and their users. Since their solution is out of the user's hands, it is difficult or impossible to do anything about them.

Social networking sites keep adding to their security controls and refining their existing ones but, as in any development project, they also continue to innovate on their platforms and add exciting new features. These new options need to keep up with the security features or they too will suffer from security weaknesses. This is a cat-and-mouse game where the privacy and data security of the users are at stake.

▶ Social networking sites keep adding to their security controls and refining their existing ones but, as in any development project, they also continue to innovate on their platforms and add exciting new features. These new options need to keep up with the security features or they too will suffer from security weaknesses.

## BEST PRACTICES

Social networking and community-based online services offer great fun and many benefits, both to individual users and to organizations. Users can reestablish contact with old school friends, find activity or even life partners, create art, and make new friends. Companies can leverage them to build their brand, get invaluable information about what their customers really think, and fix problems as they arise, among many other value-adding activities. However, social networking sites can also be a source of personal information leaks. They can also become a malware attack vector when not used cautiously.

There are ways to manage the risks. For starters, **you should only publish information that you are perfectly comfortable with, depending on what you want to accomplish.** In a dating site, you will want to state your age but not your exact birthday. Likewise, in a site where you plan to meet your high school friends, your year of graduation is probably the most important thing and date of birth will not be something you need to share at all. This may sound logical on a security standpoint but many people do not give it a second thought when opening their accounts.

The second recommendation is to **add only people you trust to your contact list.** Every time you receive a request from somebody to be your contact, ask yourself if you really trust that this person will keep your data safe and if their intentions are legitimate. If you are going to use the social network to meet new people and therefore plan to add unknown persons, set up a special email address and minimize the amount of personal information you share. In this case, **avoid clicking on unexpected links coming from them and never fully trust any of those contacts.**

As my good friend Rik Ferguson always says, the rule of thumb for this is asking yourself "Would I give this information to a stranger over the phone?" If the answer is "no," then you should not be posting it online, as they amount to the same thing. Wise words, Rik.

### The following are ways to minimize risks in social networks:

- You should only publish information that you are perfectly comfortable with, depending on what you want to accomplish.
- Add only people you trust to your contact list.
- Avoid clicking unexpected links coming from people you do not know.
- Never fully trust anyone you do not know that well.

## REFERENCES

- [1] <http://us.trendmicro.com/us/trendwatch/current-threat-activity/underground-economy/index.html>
- [2] <http://www.dailymail.co.uk/news/article-1197562/M16-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html>
- [3] <http://www.onrec.com/newsstories/17612.asp>
- [4] <http://www.scmagazineus.com/Facebook-bloggers-reveal-way-to-peek-at-private-profiles/article/138867/>
- [5] [http://blogs.computerworld.com/twitter\\_stalkdaily\\_mikeyy\\_xss\\_worm](http://blogs.computerworld.com/twitter_stalkdaily_mikeyy_xss_worm)
- [6] <http://www.betanews.com/article/CrossSite-Scripting-Worm-Hits-MySpace/1129232391>

### TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).

### TREND MICRO INC.

10101 N. De Anza Blvd.  
Cupertino, CA 95014

US toll free: 1 +800.228.5651  
phone: 1 +408.257.1500  
fax: 1 +408.257.2003

[www.trendmicro.com](http://www.trendmicro.com)

