symantec™ | Security Response

The Risks of Social Networking

Candid Wüest
Senior Software Engineer

Contents

Abstract

Social networks are an inherent part of today's Internet and used by more than a billion people worldwide. They allow people to share ideas and interact with other people, from old friends to strangers. This interaction reveals a lot of information, often including personal information visible to anyone who wants to view it. Hence privacy is often a key concern by the users. Since millions of people are willing to interact with others, it is also a new attack ground for malware authors. They are spreading malicious code and sending spam messages by taking advantage of the users' inherent trust in their relationship network. This paper will illustrate and discuss the most prevalent issues and threats targeting different social networks today.

1 Introduction to social networks

The Internet has become a central point for information-sharing in today's world. A strong part of the so-called Web 2.0 is represented by social networks. They are a great place for people to meet friends or discuss ideas with like-minded people. In simple terms, a social network is an interconnected network of individual entities which share a mutual interest and gain a method of interaction or information sharing through the service.

Social networks come in many different facets. Some are strong in a particular geographic location like Orkut in Brazil, VKontakte in Russia, or Mixi in Japan. Others are well known globally, like Facebook and Twitter. Depending on the user base, there are specialized or focused groups—LinkedIn and Xing have a business-oriented focus—enabling

people to share business contacts and job offerings. Other networks specialize in keeping in touch with your old friends from high school.

As one of the main purposes of social networks is to find other people, all major networks provide search functionality with different criteria. Users can search for local friends by restricting the query to a single town, for co-workers by searching for a company name, or for like-minded people by searching for their favored artist. There are also independent meta search engines like Yasni or 123people, that will search a given name in multiple networks and return all results in one central place.

Social media has become more established with enterprises as well. A survey that Symantec conducted revealed that 95% of the asked companies do not block access to social network sites.[1] Part of this is no doubt because of the rush of businesses to adopt social networking into their own marketing efforts. It can also keep your employees happy—32% of people surveyed would not want to work for a company that prevents them from accessing a social networks at work. On the other hand, IT departments are often worried by social media. 84% of CIOs and 77% of system administrators asked are concerned about the security risks of their end users using social networks at work. Some companies are thinking of blocking the access to social networks completely instead of discussing the needs with their employees and making them aware of the risks. It is very difficult for administrators to prevent users from visiting social networks from work laptops while at home or when using company smart phones. Therefore it's probably best to include it in the risk scenarios and create a realizable usage policy.

1.1 Common examples

1.1.1 Facebook

Facebook is currently one of the most active social networks used globally. In July 2010 Facebook announced that they have over 500 million registered users. The network allows users to create profile pages where they can present themselves, sharing pictures and anything on their mind. Facebook also allows various applications to be used inside the network, ranging from fortune cookies to multiplayer games.[2]

1.1.2 MySpace

MySpace is a classic social network where people can exchange messages and ideas. It offers easy integration with music and hence is often used by independent musicians to present their own work.[3]

1.1.3 Mixi

Mixi is the most widely used social network in Japan. It has around 20 million users engaged in community exchanges. As with similar social networks, users can send and receive messages, present themselves on their own profile page and engage with like-minded people in community groups.[4]

1.1.4 Orkut

Orkut is a global social network operated by Google. It is very popular in Brazil and India. Like many other social media outlets, it allows users to meet new friends and maintain existing relationships by posting update messages and personal pictures.[5]

1.1.5 Twitter

Twitter is a micro blog service. At the beginning of 2010 it held more than 75 million registered users. Each user can post short messages of up to 140 characters on his or her account. Other users can then subscribe or follow that person's page and receive their update messages. In the middle of 2010 Twitter handled around 750 messages per second, or around 65 million messages per day, with a steep growth rate.[6]

2 Spamming in social networks

Spam is one of the most classic attacks of all time and we have seen it adapt to new technologies multiple times—from email spam, to instant messaging spam, to in-game spam. Of course social networks have not been

left out by spammers. With social networks continuing to add millions of users to their overall user base, crafty spammers are taking advantage of the popularity of these networks to design new spamming techniques week after week. Since nearly all of those services allow users to send messages to each other for free, it provides an easy entry point for spammers.

Some networks only allow messages to be sent if both users are connected. To bypass such restrictions dummy accounts are generated by the attackers and thousands of friend requests are automatically sent in hope that some will accept them. Once accepted the attacker can start sending spam messages. Even the friend connection request allows for short messages to be sent within it, without any previous connection between the users.

Of course, the use of compromised accounts is a common practice for spamming. Using previously phished account credentials adds to the credibility of the message, as the receiver does know the compromised identity and might be more willing to open the message as a result. It is easy for an automated script to take a previously posted message from the compromised user account, add spam text, and resend it to all the connected contacts. Other variations like commenting other people's pictures or sending invitations to bogus events are other ways of sending messages to a larger audience.

Unfortunately in every place where people can write normal information, spammers will try to place advertisements. We have seen spam messages in direct messages, status updates, comments on videos, contact requests, etc. Some methods will even generate multiple messages on different channels. For example, if a user sends out event invitations on Facebook, the user will receive a notification message within Facebook, but also an email notification, unless the user has explicitly disabled notification emails.

Many communities have implemented CAPTCHA tests that must be solved when too many messages are sent. This should stop, or at least slow down, automated messaging spam. Unfortunately most CAPTCHA implementations have been broken and there are even services that use manual labor work to solve them successfully. Furthermore, attackers often have the option of using multiple accounts in parallel until each of them is blocked by the daily message limit. Most social networks offer a feature to report messages as spam and get them blocked in the future, which only helps if the attacker doesn't switch user accounts frequently.

Twitter has drastically improved their internal spam detection and filtering in 2010, bringing the spam message portion down to 1%, from 10% in 2009.[7] With 65 million tweets per day that still means 650,000 are spam, but it is much better than the 90% spam rate that we currently encounter with email.[37]

In addition to the spam inside the social networks, the brand reputations of social networks are often misused in order to boost the credibility of bulk mails sent outside of the social network. For example, spoofed emails claiming to come from the support center, notifying users about new friend requests or password resets, have made their way through the Internet. Since people are used to receiving contact requests from forgotten friends they often do not fully inspect the message, instead clicking the link in the notification email. Some contain links to malicious websites, others use the old, but still working, approach of attaching a malicious attachment with a Trojan, as seen in figure 1.

Figure 1

Trojan.Bredolab spoofed email

Date: Tue, 27 Apr 2010 13:40:55 +0530 [04/27/10 10:10:55 CEST]
From: Facebook Service <login@facebook.com>
Subject: Facebook Password Reset Confirmation! Customer Support.
Part(s): Facebook_document_Nr1527.zip [application/zip] 28 KB

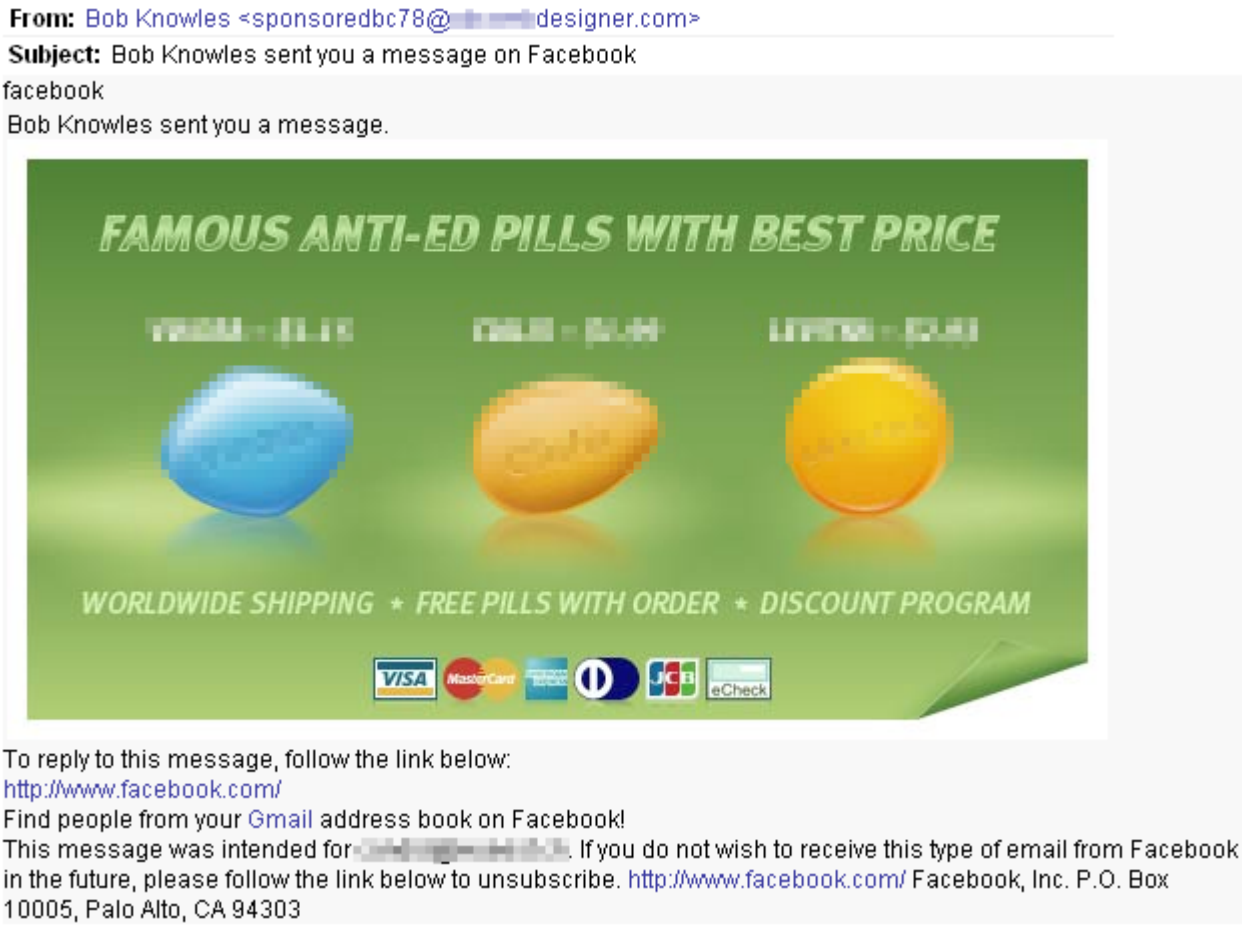
```
Dear user of facebook,

Because of the measures taken to provide safety to our
clients, your password has been changed.
You can find your new password in attached document.

Thanks,
Your Facebook.
```

Figure 2

Spam mail spoofing Facebook message



2.1 Targeted spam

Social networks are a huge resource for spammers. Most networks allow for automated access with scripts, which can then crawl the whole network for email addresses that could be used for spamming. It even goes a step further—such scripts can not only extract the email address of a target, but also the real name and some context data, such as hobbies or other things of interest. This opens the door for very personalized spam emails to be generated. Take the following hypothetical example. If my MySpace profile indicates that I have a pet rabbit called Luca, then I might be more willing to click on a spam mail that offers me cheap rabbit food, as it affects me personally. If the origin of a spam email is listed as a friend's name and the message addresses the user correctly with his full name, then the user might be more inclined to open and read the message. Subject lines that contain the name of the city a user lives in are far more likely to be clicked on than the usual gibberish. All this information is public knowledge and can be easily retrieved from social networks.

In August 2010 Facebook suffered from a bug that allowed anyone to see the real name and even the profile picture behind a given email address, as the login mask provided exactly this information if someone tried to login without a password. This enabled anyone, including spammers, to enrich a list of given email addresses with corresponding full names. Issues like this make targeted spam feasible with little overhead. (The above issue has since been fixed.)

3 Social engineering threats

3.1 Placing baits in social networks

We have observed many variations of search engine optimization (SEO) attacks, even SEO image poisoning has recently been pushed again. The idea is simple, utilize keywords and links in such a way that the sites are ranked very high and appear in the first search results. Similar attacks can also happen in social networks. Most social networks allow visitors to see what is trendy and hot at the moment. For example Twitter lists the top trending topics on its home page. This makes it easy accessible for attackers, who can automatically grab hot keywords and include them in their spam messages to get a better listing. Some attackers even started manipulating benign Twitter messages before forwarding. The attackers search for new messages that contain hot keywords. This could be a message about a questionable offside goal in the latest football match, with a shortened URL linking to a corresponding news article. The fraudster then takes this message, replaces the original shortened URL with his or her own link that points to a malicious site, and re-tweets the message. This makes it nearly impossible for normal visitors to distinguish between good and malicious messages. Hence the chances are relatively high that an innocent user who is searching for something will stumble upon the malicious link.[8]

Figure 3

Tweets with links to malware

Of course we also see typical enticing messages offering links to videos of naked celebrities or cracked software tools being spammed out in the hope that someone will find and click on them.

3.2 Follower scams

As the importance of social networks has grown, so has the pressure on people to get as many friends or followers as possible. In some social circles, social acceptance is partially based on the number of connections in social networks. School kids are especially focused on this—the more online friends you have, the more popular you are. This need has also been noticed by scammers and we have seen friends and follower scams appear on the Internet.

Some websites offer free services where you have to hand over your account name and password and they will in turn ensure that you acquire many new followers per day. Obviously it is a bad idea to share your password with strangers, since you cannot control what will be done with your account. In most cases it is also against the terms and conditions of the social network. Most of these services will simply take the account and start using it to send unrelated spam messages to all the connected friends, which is surely not what the user wanted. Even those services that do generate new followers often just cross-link the users that have given out there password or use auto-generated bot accounts to follow these users. Another technique is to auto follow thousands of users or send thousands of friend requests to random people and hope that some will accept them and follow the user back. Some people are even charging for such services as can be seen in the advertisement shown in figure 4.

Figure 4

Twitter followers advertisment

In May 2010 a Turkish Twitter user accidently discovered an undocumented feature in Twitter that allowed users to force others to follow them. It was a very simple trick: issue the command "accept" followed by a user name forcefully added that user to a follower list without asking his or her permission. Within minutes of discovering this, people all over the world started adding celebrities as their followers. Eventually Twitter reset the follower count temporarily to zero while they cleaned up and patched the attack.[9] This lead to a few funny remarks by prominent Twitter users who noticed that their follower count had dropped to zero.

Figure 5

Ashton Kutcher tweeting about his zero-follower status

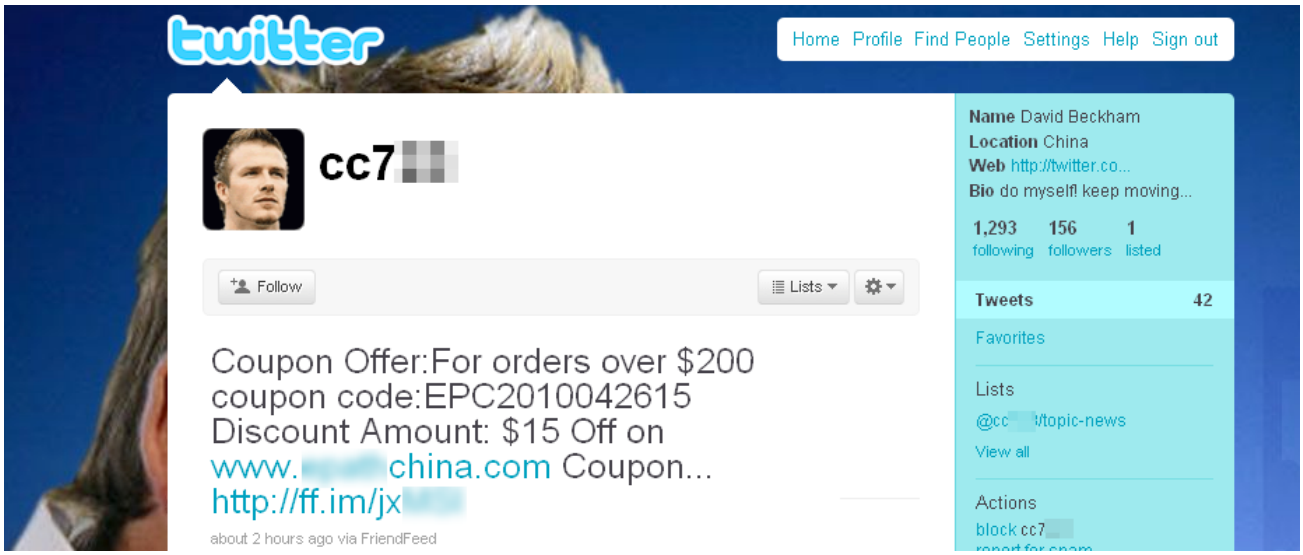
3.3 Impersonation of celebrities

We have seen a few fake profiles of celebrities that have been created on various social networks. Unfortunately there is little stopping someone from registering a new account under the name of a celebrity and using a publicly available photo as a profile picture. There is generally no real authentication that links a virtual profile to a real-life identity. Thus as long as the posted messages sound credible people will think it is the official account. Such a fake account can then be used to spread misinformation and rumors or to attract new followers that can later be spammed. Sometimes the fake accounts are actively promoted by subscribing to hundreds of random users in the hope that a few of them will be curious enough to connect to the new admirer. These accounts usually contain only a few messages, all consisting of advertisement links. Some other fake celebrities' accounts

have apparently been used to successfully get in contact with real celebrities, posing as their friends. Depending on how close those two persons stand it might be possible to boost some credibility by referencing some alleged meet up at a premier party, allowing to possibly elicit some personal secrets.

Figure 6

Fake David Beckham profile with spam messages



Some services have introduced verified accounts. Twitter has confirmed the identity behind some of their accounts and displays a "verified account" message on those profile sites. But this is far from being applied to every prominent account and of course they cannot guarantee that it really is that specific person sending the messages.

Unfortunately history has shown us that sometimes the chosen passwords of official accounts are guessable. In other cases vulnerabilities in the service allow attackers to access other user's accounts without knowing the password. In either situation, a successful account hack often results in messages being sent under the user's account name. This happened at the beginning of 2009 when a handful of celebrity Twitter accounts got hijacked and absurd messages were posted on their accounts.[10]

Figure 7

The Verified Twitter account of Bill Gates

3.4 Impersonation of friends

In nearly all social networks impersonation is a real issue for everyone. As we discussed earlier there are multiple ways a password could be disclosed unintentionally. Phishing attacks and local information-stealing Trojans are currently the most common causes. Once an attacker obtains the password of an account he can start to send out messages or update the profile status. These update messages often include links to other malicious sites in order to get more account passwords. As the message seems to come from a friend's account people tend to trust it. This inherent trust, and the usual curiosity, leads to a high click rate on those malicious links, making the attacks very successful. Users should be aware that even messages coming from confirmed friends might have been auto-generated by malware. Therefore do not blindly click on links in messages and be vigilant, especially when asked to log in or download further content, such as video players.

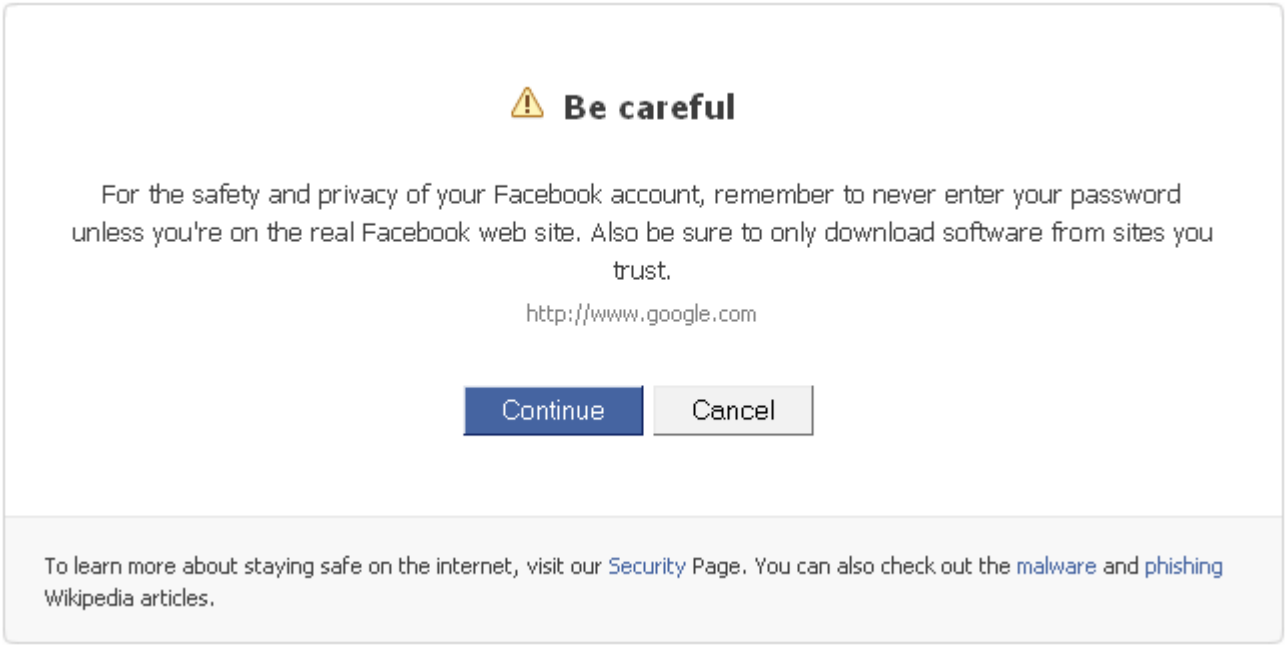
3.5 Koobface

The W32.Koobface worm has been one of the first large malware attacks, targeting social networks for years, and it is still wide-spread and active today. It is very successful as it uses clever social engineering attacks and counts on the link-opening behavior of social media users.[11]

The current variants send direct messages from infected users to all their friends in Facebook and other networks, but it is also capable of updating status messages or adding text to profile pages. The posted link will be passed through Facebook's official forwarding service which autogenerates a warning message before redirecting the user to the second URL, as seen in figure 8. The attackers probably speculate that the people are used to these warning pages and will click continue anyway. This does not deter many users from clicking on the link.

Figure 8

Redirection warning from Facebook

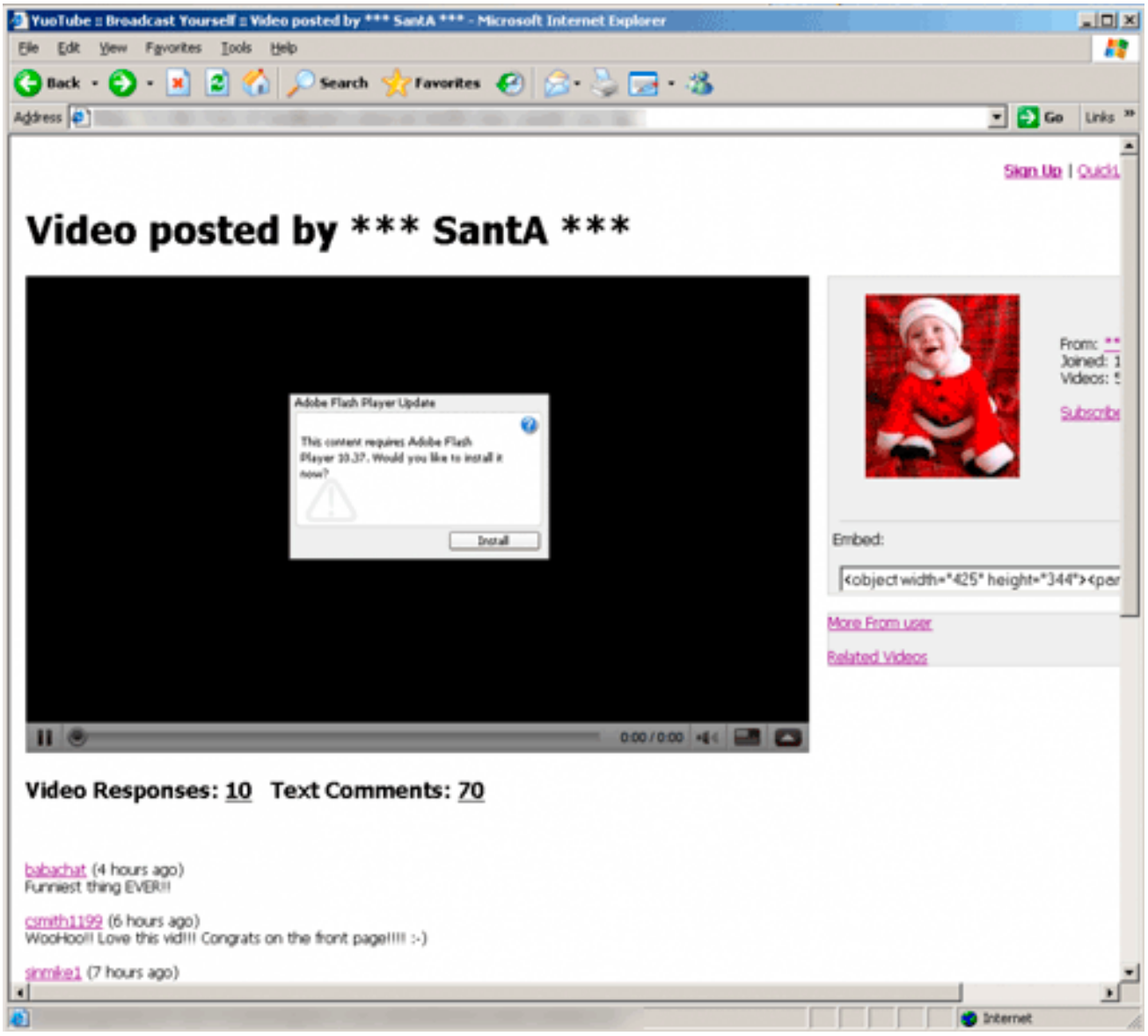


Newer variants of Koobface are not only spreading on Facebook, but also on other social networks including MySpace, Hi5, Bebo, Tagged, Netlog, Fubar, LiveJournal, Twitter, and Friendster. The bait schema used usually follows a simple pattern. A user receives a personal message or reads a post on a social media site. The message will state something funny and interesting about an alleged video and contains a link to a fake YouTube site. When clicking on the spoofed YouTube site the user is prompted to download and install a setup executable for the latest video player in order to play the video.

This of course is the Koobface Trojan, which will infect the computer. The fake video sites are served from infected machines and captured servers, but the attackers are also trying out new things, like sharing an image of the video on Google's Reader which then points back to the malware. In order to make the spoofed video site more convincing, the link in the message can pass a unique id which is then used to load the spoofed friends name and photo from the social network site. This looks very convincing when embedded in the video site, just like the friend actually posted the "interesting" video.

Figure 9

Fake YouTube site created by W32.Koobface



Once installed, the Trojan will download further components and start searching for access credentials to various social network sites. Besides its main routine of propagating through social networks, the command and control server can advise the Trojan to download other modules to the client. Example can include a small Web server to host the fake video site, a DNS changer, or an installer for a misleading application. Even a CAPTCHA breaker component has been seen downloaded to compromised computers, asking the victim from time to time to solve a CAPTCHA for the attacker, disguised as some sort of Windows validation check. This enables the Trojan to bypass any anti-bot security measures and still automatically spam out new messages. Of course the list of available modules also contain a classic information-stealing component that will steal passwords and send them back to a drop server.

The misuse of infected user's accounts makes it simple for the Koobface gang to succeed, since not only do they not have to create fake accounts, they get a list of connected friends with an inherent level of trust for free. This makes the enticing messages very convincing and lets the threat spread like wildfire through the social network. It is not always easy for the social network provider to successfully apply filters on such content, as some media

types are often shared across different networks, like photo sites and video sites. This makes it harder to control content that is just embedded. In addition, some variations on the messages and different links bring in an element of randomization.

Similar malware, albeit not as sophisticated as Koobface, has targeted other social networks. JS.Frienren is a worm that attacks the RenRen network, which is popular in China. Analogous to W32.Koobface, once installed it searches for cookie credentials and, if found, sends a message with a malicious link to all the user's friends. When a user clicks on this link a malicious Flash movie opens the malicious script to start the infection loop again.[12]

3.6 Phishing

It should come as no surprise that since social networking sites use user name and passwords for logging in, those services are also susceptible to phishing attacks. Just like with phishing attacks on banks, social networking phishing comes in many different flavors. We have seen the traditional spoofed emails claiming to be from the social network service offering some update or contest. In order to see the update the user needs to follow a link and log in, thus handing over his credentials to the attacker. The linked page is a fake copy of the original login page, focused on stealing user account credentials. There are also other social engineering tricks at work where the user is presented with a link to an interesting picture and the question "Is this you on this photo?" Like before, the landing page is a phishing page that intends to steal the passwords.[13] Currently the amount of phishing lures for community sites is relatively low at 3%, when compared to 78% targeting the financial sector. This clearly is because the profits for phished bank accounts are much higher. In addition, the creation of dummy accounts on social networks is rather simple and can be used to generate accounts for spamming.[14]

Some of the scams try to relate themselves to the official service by offering some additional service. On Twitter there were rumors about a service called "Twitviewer" that would allow anyone to find out who is reading their messages without following. All you needed to do is provide the user name and password of the account to them. As you've probably guessed, once the account was handed over it is misused to send out the same promotion messages that the user fell for in the first place. The scam did indeed appear to reveal follower names, but they were just randomly selected users that hadn't necessarily visited the profile.[15]

Similar phishing attacks have been observed on other social networks. Figure 10 shows a screenshot of a phishing site using a Brazilian carnival theme to lure Orkut users into revealing their password. Whenever a user logs in to a service and enters a password he or she should double check that it is the original website beforehand and not a spoofed one, such as verifying the exact URL location and checking if the page is using SSL for communication. Additionally anti-phishing protection features from the browser or security software suites can help minimize the risk even further, since some attacks are difficult to spot manually.

Figure 10

Orkut phishing site using a Brazil carnival theme

3.7 Advanced fee scams

By design, social communities are an interesting target field for advanced fee scams, also referred to as 419 scams. Since people willingly disclose a lot of private information, a scammer can easy identify possible victims that will fall for the scam and adjust the motives that the chosen social engineering trick will exploit. These types of scams typically come with a nice matching story that will present the victim some enormous benefit with apparently no strings attached. Later the scammer will inform the user about some unforeseen problem and will need a small amount to be paid up front. After the money is paid the attacker disappears, along with the promised benefits.

In 2009 we noticed a cleverly executed 419 scam targeting Facebook users. The attacker was searching for new DJs in Facebook groups and started contacting them. Since disc jockeys use the social network to promote themselves and their work, it is easy for an attacker to identify such people. In this specific case the cover story was that the scammer pretended to be a dance club owner in Miami who was searching hot, new talent to play at his club. He offered the disc jockeys round trip airplane tickets, five star hotel accommodation, and 4,000 dollars for spinning records over six nights. The catch was that the scammer wanted a small deposit, to ensure that the DJ would not bail out at last minute.

The two targets we talked to remained skeptical. Before the young DJs agreed to pay the money, they requested a signed contract and to provide for the travel arrangements beforehand. They spoke personally with the scammer on the phone and even contacted the hotel and the airline to receive independent confirmation that their tickets had been booked. With this assurance, they transferred the money through Western Union, as requested by the scammer, since he claimed to be traveling at the moment. A day later he disappeared with the money and the travel arrangements were canceled. A typical advanced fee scam, but with the help of social networks it was easy for the attacker to identify a lot of possible victims and to repeat the same scam multiple times. This example shows that the revealed personal information can be a gold mine for scammers.[16]

3.8 Misusing information from the social network

The information that is found in social networks can also be misused in attacks outside of the service. The following sections illustrate a few examples of possible attacks.

3.8.1 Resetting passwords

Many Web services, not only social networks, allow users to reset their password if they can't remember it. Sometimes all that is needed is the user name and the correct answers to a few security questions. These security questions are filled in by the user during registration and are used as a basic verification process. Unfortunately the typical questions are not so hard to answer. The answers to questions like: "What is the name of your pet?", "Where did you go to primary school?", or "What is your date of birth?" can be extracted from social network profiles with little effort. This allows an attacker to answer the assumed security question correctly and reset the account. Once the account is compromised it might be used to harvest other useful information or to spam connected friends.

People should be advised not to use the standard security questions, as these answers are not hard to guess given the information stored on online profiles. It's best to create your own personal question where possible or, even better, use secure passwords and to store them in a central password safe application.

3.8.2 Befriend someone to get information

Some penetration testers have been reported to use social networks to break into larger enterprises. Obviously the same attacks could be used by malicious attackers. The idea is to search the suitable social networks for employees of the determined target. This is often easy as business networks allow you to restrict searches by company names and enable the attacker to link email addresses and user names to specific companies. Using the information from the different employee profiles returned, a plausible fake account can be created. The attacker then sends a friend request with some bogus cover story to a promising account. The cover story could be the attacker is a new worker from the branch office or perhaps simply a shared interest in a listed hobby. Even

if the user is smart enough not to publicly reveal sensitive company information he or she might be lulled into a false sense of security over time by small talk and regular conversations.

Once the attacker is sure that the built-up level of trust is high enough, he or she might start asking for specific information, like internal server names, project names, or even have the newly won friend open an infected document or visit a prepared website that will drop a back door onto their computer. Thus the shared information acts as an initial identifier for the attacker to select people from a targeted group. I agree that social engineering does not work that well with all user groups, but the social network will provide a large list of possible candidates that the attack can be tried upon.

The same applies to fake accounts that are created just to gain the trust of someone. A recent example of this was demonstrated in July 2010 with a fake profile named Robin Sage that was actively pushed to request connections to random people, which most people accepted without having any idea who the fictitious woman was. Just the fact that she was connected to some mutual friends was enough to convince the people to add her. By the end of the experiment the fake identity was connected to hundreds of people from various organizations including military, government, and security companies. In some cases the fake account even received access to sensitive information, job offers, and gifts.

3.8.3 Revealing reconnaissance data

Another mistake that we observed several times is that employees reveal seemingly uncritical technical information to the public without knowing it. This could be a Twitter comment stating that the user is fed up configuring a particular firewall product at work or a status message indicating that the user finally found a way around a Web proxy product being used, and is now able to post to his profile again. An attacker can use this product information to learn about the security software that is used by the user or the company. Knowing what they are up against makes it easier to search for vulnerabilities in this particular setup. Therefore, never make too specific posts about what security software you are using to protect yourself.

4 Applications & widgets in social networks

Some social networks allow active content to be embedded in the form of applications or widgets. These applications can then interact with the user and his group of friends. A simple example would be a daily joke application, which posts a new humorous joke to the user's profile site every day for the user and the user's friend's amusement. More complex applications are also possible, like multiplayer games or photo rotation albums.

Each social network has its own ways of implementing applications and embedding active content. Some allow remote code to be included, which poses a great risk as it is harder to control what will be loaded. Larger networks have created their own APIs, which allows developers to access specific information from the user's accounts. Unfortunately, that sometimes allows them to covertly access some information or even attack users or other applications. The following sections show some examples of attacks that we observed.

4.1 Examples

4.1.1 Example 1 – Never Text Again

In July 2010 around 300,000 people fell for a shady application in Facebook. Suddenly more and more personal profiles started showing a message with the following text:

> *I am shocked!!! I'm NEVER texting AGAIN since I found this out. Video here: http://bit.ly/[REMOVED] - Worldwide scandal!*

Figure 11

Social engineering posts on Facebook

Analyzing the click statistics for this specific short URL revealed nearly 300,000 clicks.

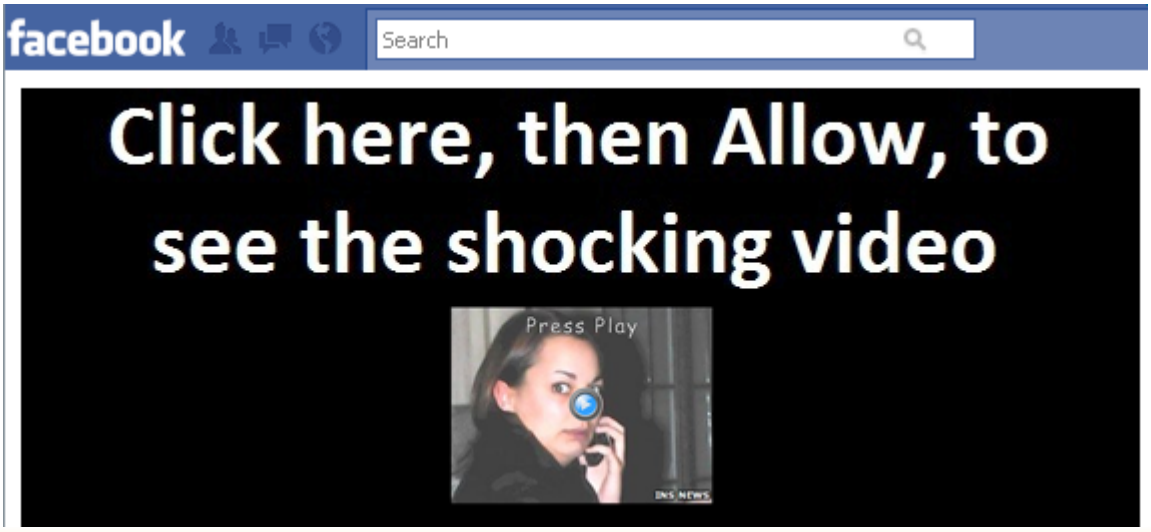
If an inquisitive user clicks on the shortened link he or she is redirected to a rogue Facebook application. The names and URLs of the application vary. For example:

- http://apps.facebook.com/wonttextagain/
- http://apps.facebook.com/nevertxtingagain/

The list of application names grows and grows. This is because Facebook bans such applications as soon as they are discovered, but the malware author reregisters them under a new name in order to keep the attack working.

Figure 12

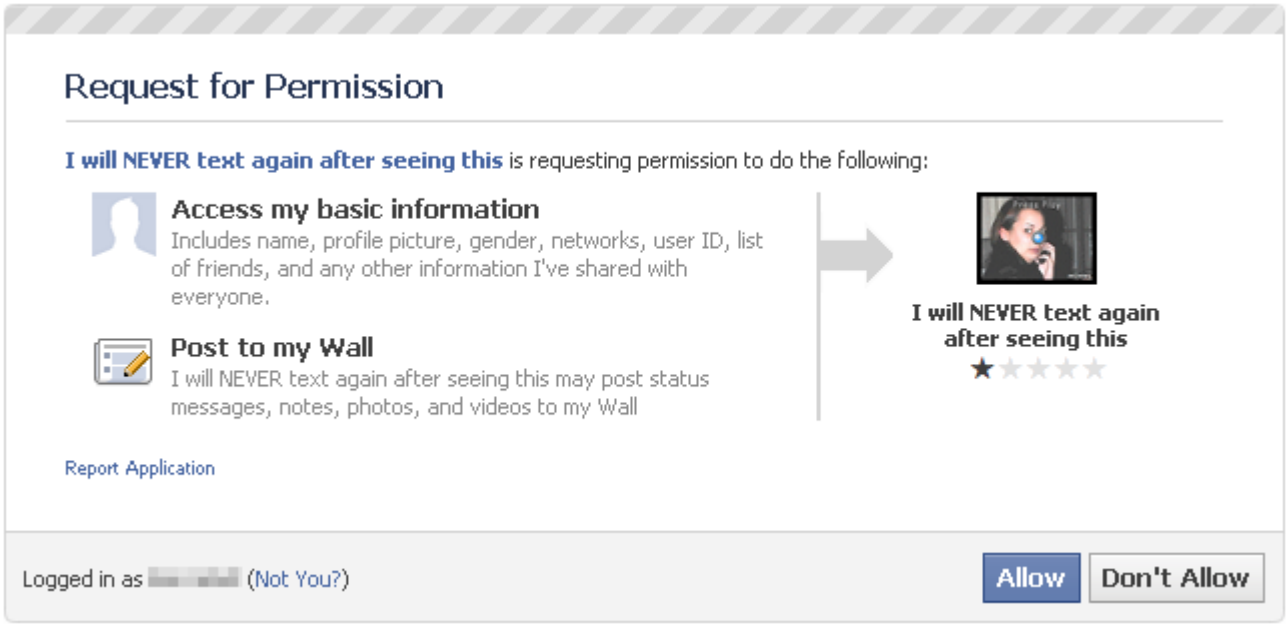
Malicious Facebook application install page



Clicking on the Facebook application starts the application installation process. In order to fulfill its shady business the application requests some elevated privileges from the user, as seen in figure 13.

Figure 13

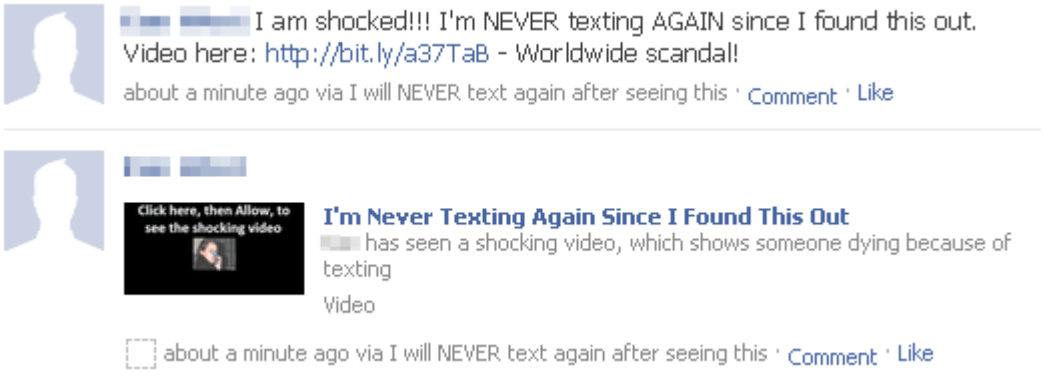
Facebook application permission dialog



It should be bluntly obvious that something strange is going on. Since when does a simple video application need to read your personal information and have the ability to post to your profile site for you? It is hard to say how many of the users that clicked on the first link and ended up at the permission screen actually granted the application the requested privileges. The only thing that is certain is that there were quite a few of them, as only this explains why so many profiles have this updated status message. This is because the rogue application will start reposting the enticing message that the user fell for in the first place, restarting the loop again.

Figure 14

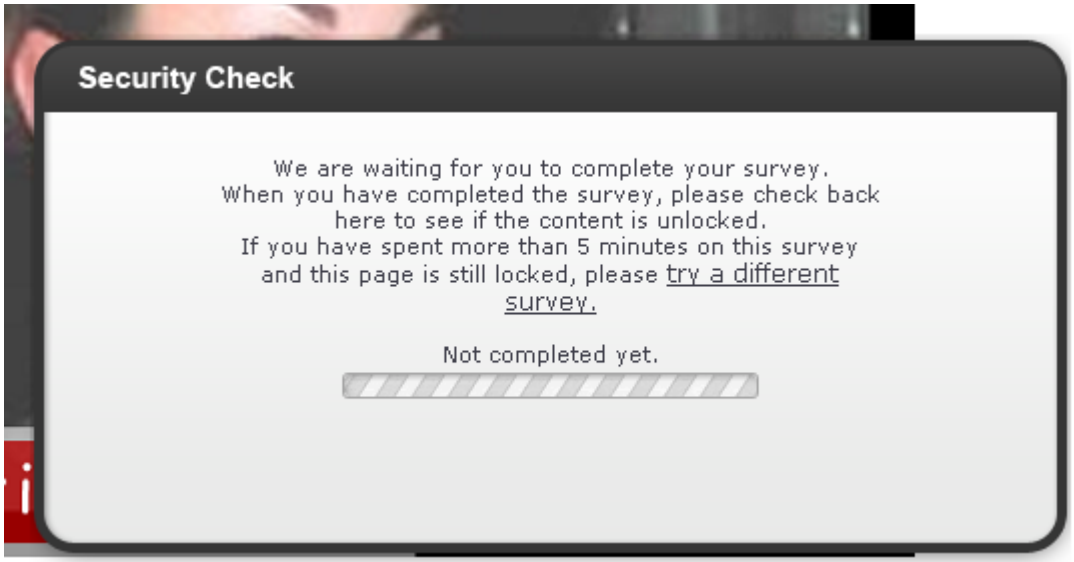
Automatically posted Facebook message by malicious app



The poor, tricked user does not even get to see the promised video now, as he or she is asked to fill out a survey under the disguise of a security check. The survey choices range from overpriced ringtone subscriptions to spyware toolbars. No matter how many surveys are filled in, the user never manages to see any video playback. So it seems that the main purpose is to trick users into subscribing to some of the offered premium content services.

Figure 15

Fake security check notification from a malicious application



Luckily in this case it is easy to clean up an infected profile. A user can go to the application settings tab of his profile and search for the offending application. A click on the "X", followed by a confirmation, will remove the application and stop it from sending messages. Unfortunately, all the personal information that might already have been sent can obviously not be retracted.

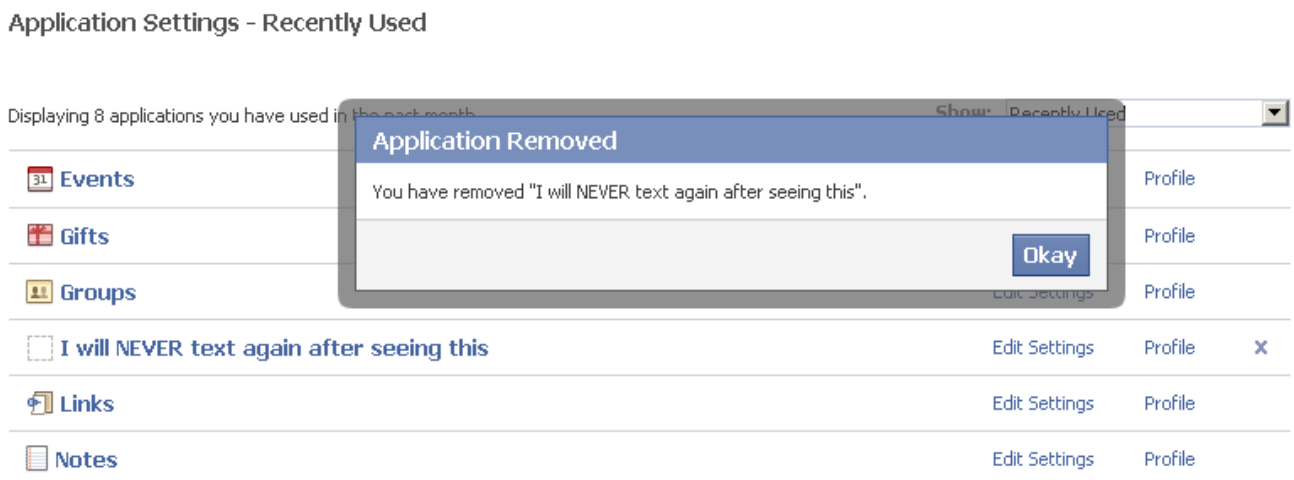
If in doubt which of the installed applications posted the message on your profile, check below the offending message. The applications name might be shown in the context, similar to this:

posted a minute ago via [NAME OF THE APPLICATION]

Unfortunately it is also possible to post messages without revealing this piece of information.

Figure 16

Application settings removal confirmation page



4.1.2 Example 2 – Candid Camera Prank

A very similar attack appearing on Facebook in the summer of 2010 used the message in figure 17 as bait.

Figure 17

Social engineering message and picture posted by malware

Like before, if a user clicked on the linked video they would be forwarded to one of many malicious application sites. The application requests the permission to post on the user's profile site. Once permission is granted, it forwards the same provocative message to all the different channels. After that, the user is asked to update their FLV player in order to see the video. For this a small pop-up box is generated with the usual social engineering text:

> *Your FLV Player seems to be out of date. Please update your FLV Player in order to proceed. Please click the Continue button now and wait a few seconds.*

By clicking the update link the user is redirected to a site where a file called FLVDirect.exe is downloaded. As you might have guessed this is not a video player application, but a Trojan horse that will download more malware on to the user's computer. We have seen this attack repeated with a long list of different subject lines. Nearly every week there is a new scam flooding through one of the social networks. Therefore if you see a similar message, regardless if the message was posted by a close friend of yours, if it asks you to install a Facebook application or even download a file from a website and run it just to see a video, you should cancel. The chances are high that this is just another wave of the described attack happening.

4.1.3 Example 3 – Quiz

More and more often we come across suspicious text quizzes on social networks like Facebook. Some third-party providers offer the possibility for anyone to easily create text quizzes. Typically it's a quiz with a few multiple choice questions, to find out which movie character the user would be or what his or her dream vacation would be like. The user who wants to create such a quiz just fills in the questions and the answers and the application does all the rest for him. Unfortunately the quiz requests privileged access from any user who wants to fill it out. After completion it asks him to send a link to a few friends before presenting the results. This way it spreads fast and the original creator gets information links from users all over the network.

4.2 Application leading to unrelated malware

There can also be pitfalls with legitimate applications. A lot of the most popular applications on Facebook are games. Besides the usual card games and arcade classics, simulation games (sometimes referred to as social games) are very trendy and enjoyed by many users. This means the user can have his virtual fish tank, his little tropical island, or a down-to-earth farm to look after. FarmVille is a very popular example with currently more than 60 million active users per month. The user can grow virtual crops and berries and harvest them to earn experience points and coins. These in turn can be used to buy cattle or equipment to help get bigger harvests and so on. Achievements can be published on the user's profile to show everyone how good a farmer they are. Just as in real life, it takes a while for the plants to grow and become ready for harvesting. This ensures that the user will come back often to check on the progress and generates a certain bond. For those who do not want to wait there is also a possibility to buy in-game coins with real money from a credit card.

For the impatient ones that do not want to spend real money either, there are lots of websites offering cheat tools for the game. These "helper tools" are often just standard Trojans that will not help in the game at all, but covertly steal passwords and other information from the user. This shows that social games can drive people to websites that offer alleged helper applications, which are in fact malicious programs. It's better to stay away from such tool offers.

4.3 Vulnerabilities in applications

Besides the things an application is allowed to do—which already may include harvesting personal information—it might also introduce new weaknesses to a user's profile. There have been a few cases where vulnerabilities in Facebook applications where found that allowed attacks on user's private data. Most often these where XSS or CSRF attacks, which can lead to serious data breaches.[19] But we have also seen reports of vulnerabilities that allow permissions—that have been granted to a legitimate application—to be sent on to a malicious application.[20] Therefore any installed application can constitute a security risk either by doing mischief on its own or by being used as a weak entry point.

4.4 What applications can do

Most social networks allow applications to have a wide variety of access to user data through different interfaces. Some provide documented APIs that allow specific access to pieces of information. This can also include granular access on a permission basis so that the user can decide which access to grant to the application. Depending on its type, the application can be anchored deep within the social network and melded within the user interface. Alternatively, it could just interact on a loose level, displaying some partial information on a different website.

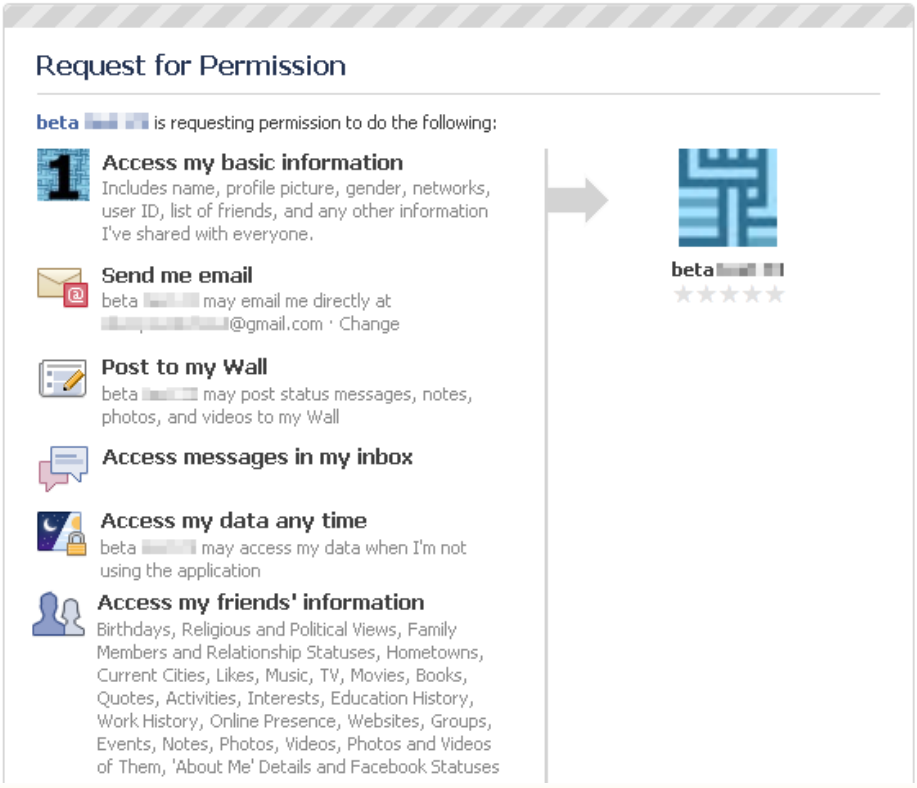
As an example, Facebook has two basic application types. First, there are social plug-ins, which allow the integration of basic Facebook features onto any website. Canvas applications, which do interact with the profile, can send update messages or open a new page, which in turn can contain nearly anything.

The "Like" button that allows people to inform others about the existence of a page is an example of a social plug-in.[21] The other applications can, to some extent, load code from remote websites and execute it.

In spring 2010, Facebook changed their underlying API and authentication process, making it more visible for the user what data an application is allowed to process. Before accessing any non-public information from an account, the application needs to acquire the extended permissions to do so.[17] This means the application needs to ask the user for permissions, as seen in Figure 18. Depending on the needed information, there is some granularity available for the allowed action. Once this permission is granted by the user, the application can do whatever it wants with this information. The user can revoke the privileges and disable applications at anytime from the application settings menu, but all information that was accessed until that point could already have been transferred.

Figure 18

Permission request page of test application, designed by author



Since the summer of 2010 Facebook requires any new developer to confirm their identity either by the help of a working mobile phone number or a credit card number.

This is done in order to combat anonymous developers registering dummy accounts for malicious applications.[18] Unfortunately this does not make it impossible to register anonymous accounts with anonymous phone numbers which are still available in some countries.

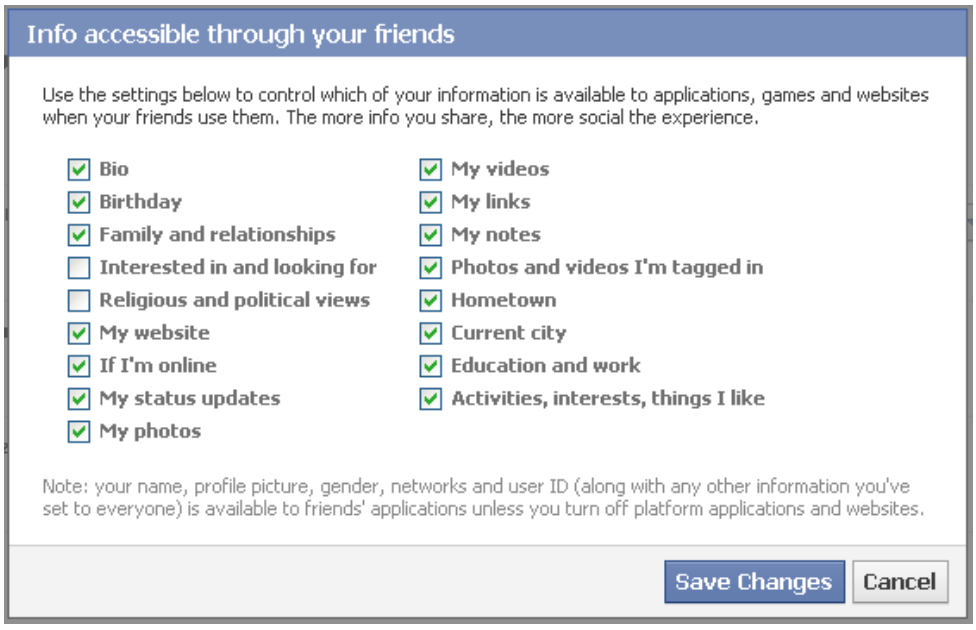
Here is a selected list of some of the things an application can get permission for:

- **Access the public information**—This includes the user's name, profile picture, list of friends, and all other public parts of the profile.
- **Access the profile information**—This includes any additional information, such as birthday, favorite movies and books, etc.
- **Send email**—This means sending direct emails to the registered email address.
- **Access posts in the News feed**—This allows the application to read the posted messages.
- **Access family and relationships information**
- **Access photos and videos**
- **Access friends' information**—This includes their details, birthdays, etc.
- **Access the data at any time**—This means the application can access the data even if the user is logged out and not using the application at that moment.
- **Post to the wall**—Add new message posts on the user's behalf

These examples demonstrate that an application could get access to nearly all information that a user entered in their profile, given that the user grants the permission to do so. Since the applications are allowed to load remote scripts, it is not possible to conclusively say what does happen to the user information and how it is processed. An application could easily store all the accessible information on an offsite database and use it later. Of course there are regulations by Facebook on what an application is officially allowed to do, to which a developer needs to agree. Nevertheless, users should read the permission request windows carefully and verify if that application really needs to access those pieces of information. After all, it is to protect their private information.

Figure 19

Default friends application access permissions



In addition, an application can request offline access privileges from a user. If they are granted the application can access the user information at any time, regardless of if the user is actually interacting with the application or even logged into Facebook. This access only gets revoked if the application is explicitly removed by the user under his application settings. It is also worth mentioning that some of the non-public information, which is only available to your friends, might also be accessed through applications that your friends use. This means that if one of your friends grants an application full rights, it can also access and process your information, even when you have set it to "friends only". In order to prevent this, a user must modify his application access settings of his account. By default, the applications of friends have access to all the information that is shared, except religious and political views, and some interests.

5 Content threats

5.1 Infected profile sites

Fortunately the owners of the big social networks have learned over the years to lock down the content that users can post or upload as much as possible. But sometimes someone finds a bug in the implementation, or a case that was not considered, that still allows the uploading of malicious content. One of the most dangerous cases is if it is possible to include arbitrary remote content. This allows an attacker, among other things, to embed web-attacking toolkits inside profile sites, generating a massive drive-by download attack against everyone viewing the infected profile. Social media sites can also be used as staging place for malware. For example, a malicious binary hidden in a legitimate photo that was uploaded, or BASE64, encoded as a weird-looking comment, could interact with malware. Those later modifications do not directly pose a threat to the user visiting the profile site, as they lay there dormant. However, they can obviously be misused by a remote Trojan to update itself. In general, most often when we see infected profiles or status pages they contain malicious scripts, as discussed in Section 5.3 or malicious links as shown in Section 5.2.

5.2 Malicious links

Since users control the content of their own profile they can add malicious content to the pages. One of the most obvious attacks is to redirect the user to an external malicious site which is fully controlled by the attacker. The posts can be made deliberately on specially registered dummy accounts or unwillingly by script attacks. The user redirection can be achieved by social engineering tricks with promising sounding links or by embedding active content like iframe tags, JavaScript, or Flash videos that redirect the user automatically. The social engineering attack is very hard to block for the social media provider, since it is hard to distinguish from regular posts. Each link has to be followed through to ensure that it points to harmless content. Some providers have started to use publicly available URL blacklists in order to block certain URL posts. We at Symantec have recently release a free application for Facebook that automatically scans links posted on the profile or news site. It uses our Norton Safeweb technology to scan each link for malicious content.[22] Some other network providers use a intermediate redirecting site that warns the user that they are now leaving their page and that the target site is not controlled by them. The final redirected website might contain anything from advertisements for fake products, to misleading applications, phishing sites, or even drive-by download attacks.

5.2.1 URL shortening services

URL shortening services have been around for years. Today it is usually a short domain name combined with an injective function key lookup redirection system. This allows a user to create a short URL out of any given long link. This makes it easier to share as there is no line break and it fits well into short messages too. There are a few hundred shortening service publicly available. Most services are free to use and available to everyone. Some were created in conjunction with applications or browser plug-ins. One of the obvious concerns with such services is that they obfuscate the destination of the link. This makes it impossible for a user to distinguish between shady and trustworthy links as they do not see its destination. Fortunately many of the popular services allow to either see a preview of the destination or a statistic page with the number of hits so far.

For example, if you receive the following Bit.ly short URL: http://bit.ly/XuX9i you can append a plus sign at the end of the URL, which will then open a preview page when visited that explains more about the target page. In this case this would be: http://bit.ly/XuX9i+

Many of the available services use public blacklists to prevent malicious links from being shortened. Unfortunately this is often just reactive and still allows previously unknown malicious links to be used for attacks. In addition multiple redirections and appended random arguments can obfuscate the links even more. Currently the monitored level of malicious links behind shortened URLs is still below 1%.

5.3 Script threats

Most social networks provide an API that can be used to access the functionality directly from a script. This is widely used by third-party applications that, for example, allow you to update your status from a smartphone or similar device. This method of access can also allow an attacker to build automated scripts that can harvest any available information he or she wants or to have worms that replicate across the network.

5.3.1 Manual script attacks

One of the simplest attack classes that we have seen on social media are the manual script attacks. Manual because the victim is asked to copy and execute the script manually. Therefore quite a few interaction steps are needed. One example is the “find your facebook twin” scam on Facebook. A few hundred thousand people apparently liked the idea and posted the message with a link on their profile. If a user clicks the link he or she will be asked to follow a few simple instructions. In this case the instructions are:

1. Click the Like button (This will generate an entry on the user’s profile site.)
2. Press CTRL+C
3. Press ALT+D
4. Press CTRL+V
5. Press ENTER

Figure 20

Manual script attack first step instruction

Following the instructions step-by-step will copy hidden JavaScript, focus on the users URL bar, paste the JavaScript, and then execute it. By doing so, the script is able to use the current logged in session to send messages to all the user’s friends, asking them to repeat the cycle. Even if someone follows through until here, no twin pictures are posted yet. The user is asked to click on a few surveys in order to get to the application. The surveys are usually quizzes or brain teasers and often require the user to subscribe to an expensive subscription for their mobile phone. During our tests we were unable to determine if there is really a twin finder application at the end of the tunnel.

Similar scams make even less efforts to automate and hide the action. After asking a user to Like and share the enticing message on their profile, they are asked to post the message five times anywhere on Facebook. After this the usual expensive surveys are asked to be completed as kind of a CAPTCHA test to prove that the user is not a robot.

Figure 21

Posted scam messages with links to manual script attacks

Another very similar attack was active on Google's Orkut in June 2010. Users where tempted with the chance of getting free mobile phone call credit by following a few simple instructions. All they had to do was to copy some obfuscated JavaScript into their address bar and run it, obviously while logged into Orkut. As before, this resulted in messages being posted on behalf of the unknowing user.

Figure 22

Manual script attack instructions

The one thing that all those attacks have in common is that the user is more or less voluntarily spreading the information further to his friends. No vulnerabilities in the service are exploited. Even thought the observed tricks mainly tried to fool users into subscribing to expensive mobile phone goodies, the same tactics could be misused to redirect users to infected websites. Some attackers have started to add advertising banners to each of the steps, generating further cash flow for them.

Users should always be very skeptical when asked to complete a few manual commands, especially if it is not clear what the purpose of the command is. Also pay attention when entering your real address or real mobile phone number anywhere and read the fine print. In some countries doing so might already be enough consent for someone to bill you for a service.

5.3.2 Cross-site scripting (XSS)

Cross site scripting (XSS) attacks are a common type of injection attack. There are a variety of ways an attacker can inject or embed custom scripts in a legitimate website that he does not fully control. Is he or she able to upload a status message that can contain script tags? A user that visits the prepared site or follows a specially crafted link will then land on the specific site where the injected script from the attacker will be sent back as a part of the legitimate site. This allows the script from the attacker to be executed in the visitor's browser from within the vulnerable site. This script can then abuse the trust that the user has in a benign website and potentially steal session cookies or start cross-site request forgery attacks (CSRF).

In April 2009, Twitter was hit by a couple of XSS worms. One of these, later dubbed Mikeyy, did not cause any direct damage or download other malware, but it definitely kept a lot of people busy and is a good example of the potential of such attacks. What had happened was that someone found a XSS vulnerability in one of the attributes in the cascading style sheets (CSS) of the Twitter profile sites. The user was allowed to modify some of the color values of the profile's CSS. Unfortunately a malicious user could send unexpected characters for the color value, resulting in custom code being executed by the browser. Instead of a simple style tag, as shown below, the attacker was able to submit a closing tag for the style element followed by a script element that pointed to his remote malicious script.

Normal tag:

```
<style type="text/css"> a { color: #0000ff; } </style>
```

Modified tag with embedded script code:

```
<style type="text/css"> a { color: #

</style>mikeyy:) "></a><script src=http://mikeyylolz[REMOVED].com/x.js> </script>
```

Using this hole it was possible to load a small bit of JavaScript code that would execute whenever someone would view an infected profile. As people usually are logged into the service when they are browsing other profiles, the script can misuse the session and infect their own profile with the same malicious script, spreading from profile to profile. Further, the worm started posting messages under the victims name, such as "Mikeyy I am done..." and "Twitter please fix this, regards Mikeyy". These messages could have easily contained short links to malicious websites. The statistics from some of the short URLs used shows that one attack was clicked by more than 18,000 users. In June 2010, another serious XSS attack hit Twitter. This time it was an unfiltered name field for custom Twitter applications that allowed the injection of scripts. Fortunately the discoverer just created a Matrix-style screensaver example on his profile site, but did not misuse it to spread a worm.

Besides spreading worms, XSS attacks are often used to steal a user's session cookie by reflecting it. Alternatively, the attacker may use it to include remote content. It can allow for the creation of phishing sites under the real domain, sending credentials back to the attacker. Normal anti-phishing toolbars will not detect these phishing sites.

5.3.3 Cross-site request forgery (CSRF)

The CSRF attacks exploit the trust that a website has in the browser and its request. Whenever a request comes from a user's browser with a valid session, the Web server will accept the request and process it. The Web server has no way of knowing if the request was deliberately made by the user or if a hidden script on a website issued the command covertly in the background, without the user noticing it. Since most people are constantly logged into their favored social places and do not log out, this is an immense target for CSRF attacks. Such an authenticated session can be misused by scripts on maliciously crafted websites or scripts planted by XSS attacks. Those sites can then issue commands—like adding a new friend or posting a comment on his or her behalf—which will be accepted because the current user is logged in. To the social network it looks like the user clicked a button with this action. This includes possibilities for propagating worms.

An older example, which happened on MySpace in 2005, is the well-documented "Samy is my hero" incident. Samy, a user of MySpace, had figured out ways to bypass the content filter that was in place for publishing content on profile pages. Among other things he discovered that he could place JavaScript in CSS tags without getting filtered. By obfuscating his JavaScript he was able to perform various actions including reading out the content of the current page and creating new HTTP POST requests. This was already enough to generate a kind of worm. The script he developed launched as soon as someone viewed an infected profile, just like a common XSS attack does. It then performed new requests that added the user as a friend. The worm then appended the string "but most of all, samy is my hero." to the heroes section of the profile, along with its own code so that it could propagate further. This enabled it to spread very fast, and infected more than 1 million users in less than 20 hours. In the end, this led MySpace to temporarily shut down their service for maintenance and cleanup.[23] Similar attacks are still possible on some social networks and we see the trend of mass infection increasing, such as with malicious Facebook applications, as discussed in section 3.

To minimize the risk, people should always properly log out of any service when they are finished using it. For some networks it might be cumbersome to log in every five minutes. In those cases smart security solutions can help mitigate the risk.

5.3.4 Clickjacking

Clickjacking and click fraud is not new phenomena, but get a new twist when applied to social networks. The principle behind these attacks is that users can be tricked into clicking on things that they do not see or are aware off. Usually an invisible frame is loaded, along with some content, and laid over a simple game, or something similar, that gets the user to click multiple times at specific places. While a user thinks they have clicked somewhere in the game, they actually click on the invisible layer and actually start some other action. This could be a submit button that gets executed. Small JavaScript snippets can ensure that the invisible button is always below the mouse pointer when the user starts clicking. This allows the attacker to perform any action that requires a few simple clicks. If the user is logged into a service at the same time, then something like a CSRF attack with manual interaction can occur. This means the user could get tricked into clicking on an invisible button to change his privacy settings or sharing all his photos on his social network account. From updating status messages to changing a user's profile setting—everything is possible. Even CAPTCHAs could be integrated and passed to the user for solving.[24]

On Facebook, "Likejacking" did emerge as a combination of clickjacking and the "Like" feature in Facebook. The Like button enables the user to reference back to a specific site outside of Facebook with one simple click.[25]

In one case, posted messages contained enticing text such as "Try not to laugh xD" or "The Prom Dress That Got This Girl Suspended From School." followed by a link. If a user clicked on any of the links seen on the profile sites of infect-

Figure 23

Clickjacking example with two layers

ed friends, they got redirected to a website with the only visible content being “click here to continue” written in bold letters. Of course clicking anywhere on the page triggered an invisible Like button, which then updated the user’s status message with the same text as seen in the first clicked message. The same principle was used with an image of uncle Sam, which asked the user to click on two colored spots in sequence, which again shared and published the malicious link to all friends. This allowed the threat to spread to thousands of profile sites with little effort. Even thought it did not directly do any damage, similar attacks could include malicious URLs with drive-by download attacks. Some of the newer versions started to include advertisements that would generate revenue when a user viewed them.

It is not trivial for users to protect against such clickjacking attacks. Besides using up-to-date security software, users can also use browser plug-ins, such as NoScript, that will detect some of the invisible frames. For the owner of websites, there are a few techniques that can be applied in order to ensure that their website is not displayed in an invisible frame. Some of these techniques are described in a paper from Stanford University.[26]

For instance, Facebook implements some of these methods to ensure that the “Share” button is not used inside a hidden iframe tag. If the page detects that it is loaded in an iframe tag it will replace its content with a simple logo and a link that when clicked opens the main page in a new window. This prevents from clickjacking attacks. Despite this fact we still saw some clickjacking attacks in Facebook in August 2010. They obviously failed on hijacking the share button, which suggests that the user of the malicious script did not properly test it or that he just bought it off the black market and did not know how it works exactly. Unfortunately the like-jacking attack still works, as the Like button is allowed to appear in iframe tags. The attacks that we have observed often try to use the mobile versions of the social network page as they are simpler to parse and often do not contain the same level of security mechanisms.

6 Social aspects

It is beyond the scope of this paper to cover all the social aspects that come with social networks, but it is important to point out that there is a certain danger from non-technical issues in social networks. Sadly enough several cases have occurred where people used the network to threaten and intimidate other users, which range from blackmailing them, to release intimidating pictures to the public profile, to mobbing or cyber bullying by sending hateful messages, often to younger users.

Another issue is stalkers who use social networks to closely follow the personal lives of their victims and terrorize them in real life. Some networks have now started to cooperate with organizations that protect potential victims. Facebook responded to a British child protection organization and introduced a report button in 2010 that can be used to report questionable behavior or abuse. Other networks like MySpace have had such reporting functionality for quite some time.

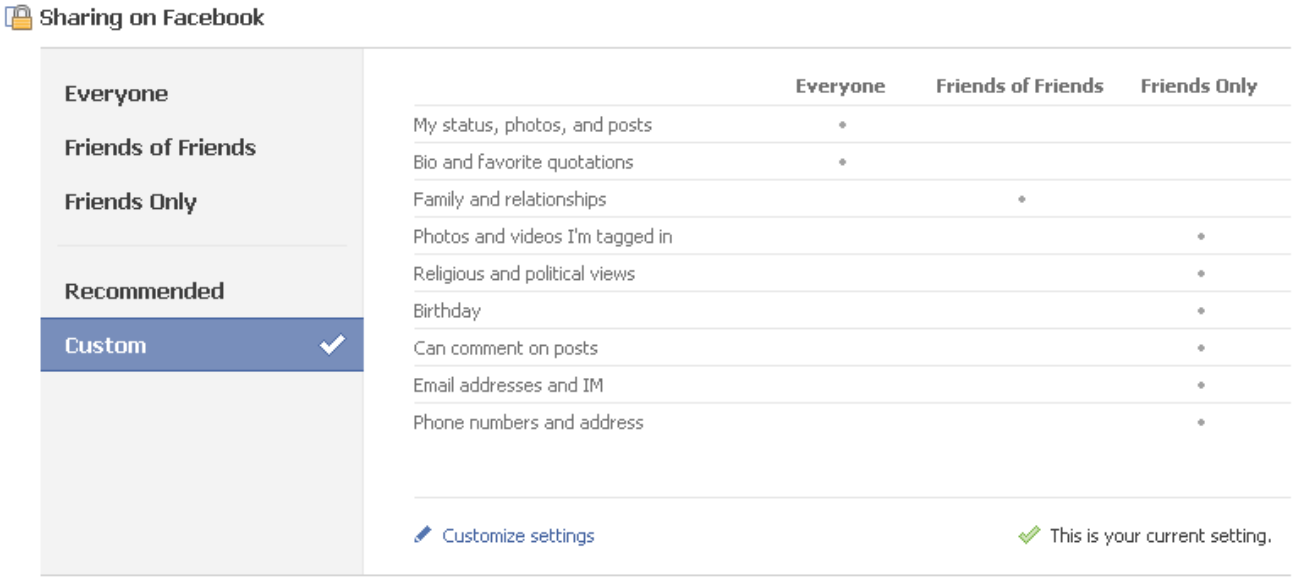
7 Design issues

7.1 Privacy

As we elaborated above, privacy is one of the main concerns of social network users. It is up to the user how much private data he or she is willing to share with the world. Depending on the information that is posted, it does make sense to restrict the access to the invited group of friends or similar. Most social networks allow a user to set different privacy settings for confirmed friends in contrast to public strangers. In some cases, a user can decided to share his private email address with all his connected friends but keep it invisible for someone just browsing his public profile. For example, Facebook distinguishes three groups of visitors: direct “friends”, the “friends of friends”, or “everyone”. For a list of different information pieces the user can decide how far he wants to share that information, as seen in figure 24.[27] The default sharing setting, “everyone”, is pretty liberal and shares a lot of information. Many users might not be aware of this and would probably like to adjust their privacy settings.

Figure 24

Facebook privacy settings



Twitter on the other hand allows its users to protect their tweets/messages. This means once enabled all future messages will only be seen by users that have been confirmed as friends. The privacy settings also allow a user to disable if others can find them by searching for their email address. This makes it harder to link a Twitter account to a known email address.

It is also important to keep in mind that some social networks state in their EULA that they will reserve the right to use and even sell all the material that you upload. It is clear that some need the rights because the content is shared in the network, but others might be sharing some information with third-party companies. The permissions granted would theoretically include using your photo for a commercial ad without telling or paying you anything. Fortunately, we are currently unaware of any case where this has happened.

Often users are not even aware of the amount of information that they are actually sharing publicly, or think that it is not easy to access this information in larger quantities. In July 2010 a Canadian engineer used a simple crawler script to access publicly available information on Facebook. He was able to get access to 170 million user records before he stopped. Obviously he could have downloaded even more than just the real names and the URL of the profile. Information like this can be of great interest to spammers and attackers.

No matter which social network you use, make sure that you check the privacy settings and if necessary, modify them to your needs where possible. It is always an act of balance between participating by sharing information and preserving your own privacy.

7.1.1 Deleting data & accounts

Once a message is posted it is nearly impossible to remove it completely from a social network. Especially since it might already have been forwarded to others and been reposted again. Twitter provides a button to delete messages individually. But since there are quite a few aggregation services, the message might already have been forwarded or archived by third parties who are unaware of the delete action. Basically, once something is posted to the Internet it can no longer be deleted for sure. Therefore it is better think twice before posting something in the first place. Facebook users can go to their profile page, and when they hover over a post, a Remove button will appear, allowing them to delete the post.

If you want to delete your full account it is often not as straight forward as with single messages. On Facebook you can deactivate a profile from the settings page, which will keep all the data in place, but simply switch the

profile invisible to others. This way it can be reactivated at any time later. If you really want to delete a Facebook account you need to log into the account and visit the delete page, which can be found in the FAQ of the help center.[28] The account will then be deactivated for two weeks and if during that time no further interaction is made it will be removed. Unfortunately, this includes automated log-ins from affiliate sites that the user might still have in his browser cache. So it might be a good idea to clear the browser history and cache, to ensure that he or she does not accidently log in, cancelling the deletion process completely.

7.2 Information disclosure

It is clear that since one of the main purposes of a social community is to share information, some information will be disclosed to others. However, the users are sometimes not aware of the shared information or its implications. The following sections will elaborate on a few examples.

7.2.1 Revealing location data

People like to socialize and share what's on their mind. This includes, by nature, information that might be misused. One of the attributes that is often overlooked is the location data that is passed along. Many people are broadcasting information about exactly where they are, which is not an issues per-se, but this information can obviously also be misused for stalking or other shenanigans. Some services like FourSquare focus on the geographical location that people are at a given moment. In FourSquare, people can check-in at different locations. The more often they check in, the higher their ranking for that place raises. That way people can see other users who are at the same restaurant or concert. Even thought FourSquare allows a user to limit what information is publicly displayed, there is always the chance that there are design flaws. In June 2010 someone discovered that even if the user disables the option to be shown on location sites, it was still possible to enumerate the checked-in users and identify who was there.[29] Twitter also offers the option to add a location tag directly to each message that is sent and in August 2010 Facebook added a utility called Places, which allows user to share their location and tag other users that are at the same place. This indicates that location aware services will increase in the future.

Another user group which should be a bit more sensitive on revealing geographical locations is the armed forces. Sending status update messages back to the loved ones at home revealing the troop power and current location is probably not a wise idea. But even something as simple as uploading some pictures from a dessert can reveal information, as many cameras automatically embed metadata into pictures. This can be a simple time stamp or GPS coordinates if it is a newer model. Therefore it does not come as a surprise that many military forces have banned the use of social media completely, or at least trained their users not to share too much information, since there were already a handful of cases where location information was leaked.

Besides showing where users are located at a given time, it obviously shows where they are not, for example, at home or in school. So theoretically speaking a tech-savvy burglar could find out when people are not at home, find their home address, and then break into their homes. To illustrate this point further, a group created a website called PleaseRobMe.com which listed people that had updated their profiles with messages like "I'm away for two weeks on vacation" etc. It is debatable if this scenario is too farfetched. In a less damaging way, it would not be a wise idea to mark your location as "at the cinema", when you told your boss you are at home lying in bed sick. There have already been some cases where people have been fired because their boss was following the posts of people taking sick days and then exposing them.

7.2.2 Revealing identity

In some groups, social networks can be directly linked to Internet users on other platforms and since they provide a real name, also identify a user behind an anonymous action.

In Xing a registered user can see who visited his or her profile page even if that person did not add him or her as a friend or send any messages. Just merely reading the profile page while logged in is enough for leaving a trace. Unfortunately this can be misused with CSRF attacks. A user with malicious intent can add an invisible frame or link to any unrelated website he or she controls and link it to his or her own Xing profile site. Whenever someone visits that Web page while logged into the social network they will leave a trace in the logs. The site owner

can then correlate his or her Web server log file with the reported visitors from his or her Xing profile page and potentially identify the real identity of the visitor.

Some researchers have brought this one step further by fingerprinting someone's social network connections. For example with the CSS attribute of links called "visited" and a small bit of JavaScript code an attacker can identify if a user has recently been on a predefined URL. This method can be used to iterate through multiple sites and identify which of the social networks are being used by the user. Depending on the type of social network, it can also reveal the home profile site of the user or give a strong indication on who the user actually is. There has been an attack that uses affiliations to different groups to determine the intersection of the groups and predict the user's identity.[30] Obviously such an attack requires some previously gathered information on the groups available on the network, as well as some backtracking after the connection is identified. However, it shows that in some cases it is possible to identify a visitor of a given website if he or she is a social media user. In some cases it is even a feature offered by the platform itself. Facebook offers a feature called instant personalization which is currently enabled for all users by default. This allows some pre-approved third party sites to identify the user that is visiting their website without having them to log in. The site can access the public data on the users profile in order to adapt its service.

7.3 Insecure frameworks

Since social network platforms are getting more and more complex it is not astonishing that from time to time some vulnerabilities in their frameworks are discovered. The severity ranges from accessing private information of other users to modifying other user's accounts.

In May 2010 Facebook experienced a privacy glitch. Ironically, the bug was in the privacy settings tool itself. It allowed a user to test out his modified privacy settings by previewing how his profile looks to another person. This kind of provided a read-only access to someone else's account. Unfortunately this also included the chance of seeing private chat conversations or pending friend requests that the other person had.[31]

Another example is SchuelerVZ. A partner network of StudiVZ, it is a popular social network in Germany, with more than 5 million users, mostly school kids. In May 2010 a student created a crawler that was able to export the data of 1.6 million user accounts in a few days, sometimes using design bugs to discover the group affiliation of protected user accounts.[32] This issue had followed multiple data leaks. In October 2009 three incidents became publicly known. In one of these cases attackers were able to read information from private accounts by using the power search function—even when a user locked his birthday on his profile site, a search for his birthday would still list his account in the results. A combination of automated queries for every possible combination and correlation allowed then to read out all the desired information from protected profiles.[33]

In a small incident that occurred on Facebook in 2010 after publishing a code update, an unknown number of private messages were sent to the wrong person's inbox. Users didn't know if the message was received by the right person or if it landed somewhere else.[34]

Another conceivable attack type is SQL injections, where an attacker would find a way to pass his or her own SQL queries to the linked database. These attacks can be very devastating as they might reveal user accounts with passwords, emails, and all the other sensitive information.

Even when leaving aside all the attacks against vulnerabilities in the code base, there are external attacks than can interfere with a social network's services. In August 2009 Twitter learned this the hard way, when it was hit by a massive distributed denial of service (DDoS) attack that took the whole web service offline for a few hours. Facebook was under attack at the same time, but was able to keep its service working.[35] Such DDoS attacks do not compromise the privacy of user data, but it does limit the availability of the social network. Since some services have become dependent on social media news, this can have a serious impact for them.

All the above-mentioned security issues have been fixed by the corresponding social networks. These are just a few examples illustrating that it is not impossible for an attacker to find a vulnerability to automatically read out any information from a given social network, regardless of their privacy settings.

7.4 Misuse as control structure

Given the well-distributed architecture of social networks, their good Internet connections make them a primary candidate for botnet control. Especially as such commands could blend into the regular social network traffic seen at any major site. The following sections discus some methods that we have seen used in the wild.

7.4.1 Botnet control over status messages

There have been attempts to misuse social networks as a command and control structure for botnets. This does not come as a surprise, especially after several ISPs have been shut down in order to eradicate botnets. The botnet creators have been searching for more robust means of controlling their assets. Since social networks are well distributed and usually have fast Internet connections, they are a prime candidate for a command structure.

Trojan.Whitewell is one such bot, periodically checking the mobile version of a predefined Facebook account. The attacker can submit a new post to the profile in order to have the bot download and run a file from an URL or contact a web server to get new commands.[36]

Similar ideas have been tested on Twitter, where the bot downloads the latest messages from a predefined Twitter account. The messages where all BASE64 encoded URLs that point to online resources where the bot could download an update. We have also seen a simple Twitter bot creator tool that will generate a bot that will check for commands in clear text on selected accounts.

Figure 25

Bot Twitter account with encoded commands

It should be pointed out that this setup does not necessarily provide further resistance against shutdowns, since the social network service provider can simply disable the accounts or filter for specific posts. Of course the attacker can always create new accounts, but the bots already distributed will not be able to get these updates.

Some attackers noticed this single point of failure as well. KreiosC2 is a good example of a proof-of-concept bot that uses social networks for control channels in a more sophisticated way. The bot can be bound to commands in natural language submitted by any user account or find commands embedded as comments in uploaded JPEG files. This makes it much harder to block and filter out all the commands for the service provider. We see that most of the current attempts at using social networks as a command and control structure are of a very basic nature. However, it would be possible to use the infrastructure for covert channels in a more sophisticated way.

7.4.2 Information sharing

Besides using social networking profiles as command structures, they can also be used for storing updates or dropping off information. Just think of a Trojan that downloads a binary update from a predefined profile. To make it harder to trace, the updates could be embedded in a media file, such as a picture. The updated Trojan could then send its gathered data as encrypted text updates, such as local passwords, back to another profile. If the information is obfuscated enough it could blend into the normal expected traffic and be accessed from anywhere.

8 Best practice tips

8.1 Be skeptical

Social networks can be a useful source for business information, as well as for newsworthy updates from your friends. But they also contain a lot of useless information. Generally speaking, you should treat anything you see online with a high degree of skepticism. Do not believe everything you read, be it financial advice, breaking news, or tips on free giveaways—especially if it involves clicking a link or installing an application. If someone asks you for money in advance, it might be a scam.

8.2 Check privacy policies & settings

All major social networking services have specific privacy guidelines and rules that are published on their websites. Make sure you understand them, even though they may be tedious to read, as they likely explain if your information is shared with other parties. Some services offer the ability to restrict your privacy settings for specific groups, such as allowing you to share pictures with your friends only and not everyone. Make good use of these settings.

8.3 Good passwords

Use good, strong passwords. (Your birth date or "123456" are not good passwords.) If possible, the password should contain letters and numbers, as well as special characters. If you can't remember complex passwords, either use a passphrase as hint or use any of the available password management utilities that can securely store them for you. Do not choose a password that can be guessed by the information that you have published on your account site. This includes friend's names, favored movie stars, or pet names.

8.4 Protect the password

You should never share your password with others. This includes services that promise to help you get more friends or something similar. Do not lose control of your password. If you enter your password, ensure that you are on the real website and not a phishing scam page that just looks like the original site. Should you suspect that you have fallen for a phishing attack and your account has been compromised, use a clean computer to log into the original service and change your password.

8.5 Be thoughtful

Always think twice before posting something. Keep in mind that once you posted it, even to a close group of friends, you no longer have control over where it will be reposted and who might read it. These things can come back to haunt you when you search for a new position in the future. Consider if you really need to publish the full information. This includes posting too many personal details, such as phone numbers or work-related things. Furthermore refrain from forwarding virus hoax or exaggerated warning messages that will confuse more than help other users. Be nice and respectful to others—do not post hate messages about others, since you would not want to receive them yourself.

8.6 Be wary

People on the Internet are not always who they claim to be. The celebrity who you are following might just be another fan, and the supposed co-worker from another office might just be someone doing reconnaissance on your enterprise. Not everyone that claims to be your friend is your friend.

8.7 Stay updated

Always ensure that the software you use is up-to-date. Not only does this include the operating system and web browser, but also third-party plug-ins, such as PDF viewers. Install all the latest patches and hot fixes from the official site and automatically check for newer available versions through the software.

8.8 Stay protected

Some of the newer attacks are very sophisticated and are sometimes hard to spot for an untrained eye. Use comprehensive security software to protect against these threats.

9 Conclusion

Social networking communities are an inherent part of today's Internet. People love using them to stay in contact with friends, exchange pictures, or just to pass the time when bored. Companies have also discovered social media as a new way of targeting their customers with relevant information. With user groups with hundreds of millions of members, there are always some black sheep with malicious intent. We have seen many worms spread through social networks. In most cases they have used social engineering tricks to post enticing messages on behalf of an infected user. Curious friends who follow the link will also get infected with malware and unwillingly spread the message further. Unfortunately many people will click on nearly any link that they see posted and add anybody to their private network that asks, without knowing who really is behind it. This inherent trust, especially in messages coming from friends that have had their account compromised, makes it easy for attacks to succeed, regardless if it is a phishing attack, a spam run, or a malicious worm spreading through automated scripts.

History has shown us multiple cases where the privacy of a user was breached, either by gaps in the underlying framework or by embedded applications that have leaked information. But many users do not even shore up the privacy settings provided by the network itself and are unaware of the risks that come with sharing too much personal information. Often they will post sensitive information—down to their own password—for everyone to see.

Social networks definitely can be fun, but users should be aware of the risks and behave with the needed level of skepticism, just like anywhere else.

10 References

1. http://www.symantec.com/connect/blogs/social-media-can-t-live-it-can-t-live-without-it
2. http://www.facebook.com
3. http://myspace.com
4. http://www.mixi.jp
5. http://www.orkut.com/
6. http://blog.twitter.com/2010/02/measuring-tweets.html
7. http://blog.twitter.com/2010/03/state-of-twitter-spam.html
8. http://www.zdnet.com/blog/security/cybercriminals-hijack-twitter-trending-topics-to-serve-malware/3549
9. http://gizmodo.com/5535536/the-real-story-behind-twitters-ridiculous-follow-bug
10. http://techcrunch.com/2009/01/05/either-fox-news-had-their-twitter-account-hacked-or-bill-oreilly-is-gay-or-both/
11. http://www.symantec.com/security_response/writeup.jsp?docid=2008-080315-0217-99
12. http://www.symantec.com/en/uk/security_response/writeup.jsp?docid=2009-082405-1354-99&tabid=2
13. http://www.symantec.com/connect/de/blogs/phishing-facebook-continues
14. http://www.symantec.com/business/theme.jsp?themeid=threatreport
15. http://www.symantec.com/connect/de/blogs/twitter-used-bait-phish-personal-information
16. http://www.symantec.com/connect/de/blogs/hey-mr-dj-don-t-put-record
17. http://developers.facebook.com/docs/authentication/permissions
18. http://developers.facebook.com/blog/post/386
19. http://theharmonyguy.com/2009/10/09/the-month-of-facebook-bugs-report/
20. http://theharmonyguy.com/2010/04/10/facebook-platform-vulnerability-enabled-silent-data-harvesting/
21. http://developers.facebook.com/plugins
22. http://apps.facebook.com/nortonsafeweb/
23. http://namb.la/popular/tech.html
24. http://www.symantec.com/connect/de/blogs/clickjack-baddie-whack
25. http://developers.facebook.com/docs/reference/plugins/like
26. http://seclab.stanford.edu/websec/framebusting/framebust.pdf
27. http://blog.facebook.com/blog.php?post=391922327130
28. https://ssl.facebook.com/help/contact.php?show_form=delete_account
29. http://www.wired.com/threatlevel/2010/06/foursquare-privacy/
30. http://www.iseclab.org/papers/raid2010.pdf
31. http://eu.techcrunch.com/2010/05/05/video-major-facebook-security-hole-lets-you-view-your-friends-live-chats
32. http://www.coresec.de/lenaml/lenaml.pdf
33. http://www.heise.de/security/meldung/SchuelerVZ-Datenlecks-auch-geschuetzte-Informationen-ausgespaeht-843963.html
34. http://techcrunch.com/2010/03/01/facebook-code-testing-bug/
35. http://www.wired.com/epicenter/2009/08/twitter-apparently-down/
36. http://www.symantec.com/connect/de/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today
37. http://www.messagelabs.com/intelligence.aspx

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

About the author

Candid Wüest is a Senior Software Engineer in Security Response, based in Zürich, Switzerland.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com