

Factsheet FS 2011-01

Secure on Social Networks

Social networks are interactive Internet applications that allow users to create a personal profile, share information and maintain contacts with other users. Examples are Facebook, Hyves, Twitter and LinkedIn. During the past few years, the popularity of social networks has grown tremendously. They have come to form an important part of our communication. Although social networks offer a useful and fun interactive platform for the exchange and provision of information, they also present various security and privacy risks.

This factsheet offers you an overview of the risks involved in participation in social networks. We also discuss three popular methods of attack, as well as a number of measures that facilitate more secure use of social networks.

Security risks on social networks

The growing popularity and increasing use of social networks has not gone unnoticed by malicious parties. They regard social networks as a convenient instrument for their practices.

There are four main reasons why social networks are attractive to malicious parties:

1. The large number of users
2. The availability of (personal) information
3. Mutual trust between users
4. Relatively weak security

As a result of the accessibility of social networks, malicious parties can create accounts just as easily as well-meaning users. Thus, it becomes (virtually) impossible to make a distinction between legitimate users and attackers. This creates at least the following risks:

- By participating in social networks, you run the risk of getting infected. A successful infection may give malicious parties control over your computer.
- You run the risk of providing malicious parties insight into your personal details (or those of your contacts), which they can subsequently exploit, e.g. for the purpose of identity theft.

Whilst these risks exist, it remains rather difficult to determine or provide an indication of the odds. Statistics about how often an attack is (successfully) carried out are rare and many cases only surface on an incidental basis.

Therefore we have to turn to other indicators, such as the ease with which a particular attack can be carried out along with what malicious parties can acquire through them. Both of these indicators return (indirectly) in the next section.

How do malicious parties operate?

By gaining insight into the methods of attack used by malicious parties, you will be better positioned to recognise and avoid attacks on social networks. The methods of attack used on social networks coincide in part with existing ways that are used to tempt users, like phishing and the distribution of malware. Attackers are also developing methods that are geared towards exploiting the environment of social networks, *rogue applications* being an example.

The most important facts:

- > Social networks are attractive to malicious parties because of:
 - the large number of users,
 - the availability of (personal) information,
 - mutual trust between users, and
 - relatively weak security
- > The two most important risks of social networks are:
 - Your computer can get infected with malware
 - Your personal data can fall into the hands of malicious parties
- > Malicious parties use existing as well as innovative methods of attack
- > As a result of the default user settings, your profile details are open to the public

Phishing

Social networks are used for various different purposes. An important example is their 'networking function': the ability to create new contacts as well as maintain existing contacts. Users share personal information to facilitate these networking activities.

Attackers can use this information to send users targeted phishing messages that look like a regular e-mail or personal message. These messages create the impression that they originate from the social network itself or have been sent by another party, such as a financial service provider or the tax office. As a result of their personal nature, these messages constitute a more refined method of attack; they increase the user's tendency to open and answer the message.

These spoof messages make it look like another user of the social network is sending you an invitation to form part of his or her network. The message will contain a link for accepting or declining the invitation, which once clicked will log you in on the social network. This offers attackers the opportunity to capture your login details.

Malware distribution

The distribution of malware (malicious software) such as viruses, Trojans and worms forms an important link in the chain of subsequent illegal actions. A computer that has been infected by malware can be used for other attacks and/or for the collection of personal information.

The distribution of malware through social networks usually takes place through malicious links that attackers include in their (e-mail) messages. This can occur as follows:

1. Attackers can exploit a hijacked user account to send messages.
2. Attackers can create their own (generic) profile and use it as a host for malicious links.

The first option offers the greatest likelihood of success, as it allows malicious parties to benefit from the mutual trust between users. The contacts of a legitimate user will be less alert to potential threats derived from his or her profile.

Attackers also use specific habits of social network users to spread their malware. An example is the use of abbreviated URLs. This provides attackers with a convenient way of hiding their mala fide links and to increase the victim's inclination to click on a URL of which the destination is impossible to check.

Rogue applications

The number of applications used on social networks continues to grow. Malicious parties also try to exploit this development, and their attempts are successful because they know how to cater to the needs of users of social networks. For this purpose they tend to develop rogue (malicious) applications. An example is the Profile Creeper on Facebook. This application purportedly allows you to check who has viewed your profile, but in reality comprises a survey scam. This rogue application is often offered to users in the following way:

"I just saw who STALKS me on Facebook! You can see who creeps around your profile too! [LINK]"
If you click the link to accept this application, the same message will be sent to all your contacts. This creates a chain reaction that increases the reach of the malicious application. However, that is only the

Account hijacking

Attackers can use login details from social networks to take control of or hijack your account. This allows them to abuse your list of contacts and the associated trust relationships.

The hijacking of an account is relatively easy since attackers only need your log-in details. Malicious parties are able to capture such log-in details through the use of existing methods, as indicated on the left.

Once attackers have obtained your login information, they will try to retrieve data from the contact list of your user account or spread malware among your contacts. They can also use your account to send spam.

Koobface

Koobface is an Internet worm that spreads itself by sending Facebook messages to the contacts ('friends') of an infected user.

Friends receive a message that directs them to an external website from which they are prompted to download an update for the Adobe Flash Player. When they download and execute this update, their system also becomes infected.

first stage of the attack. For the full installation of the application you are asked to fill out a questionnaire. Such questionnaires form a source of revenue for malicious parties.

Other risks

Other risks are primarily associated with the accessibility of shared (personal) data. The privacy settings for social networks are generally set to 'public' by default. This means that unless you manually change these settings, your profile and its contents will be publicly accessible. The information in your profile is often of a personal nature and it is undesirable that everybody is able to view it.

There is also a risk in sharing information (indirectly) related to your work or information on your employer on social networks. If you make this information public, a conflict might arise between your activities on social networks and your employer's (information provision) policy. The media has already featured a number of cases that show how participation in social networks can impact a user's professional life.

The general terms and conditions of social networks describe the way they handle your personal details. This includes the extent to which they are able to use and appropriate the content you publish. This creates possible risks for posts to which intellectual authorship rights might apply, such as research results, trademark rights, patent violations, etc.

Third Party Applications

The addition of third-party applications such as games and quizzes often allows third parties to gain access to certain parts of your profile.

This does not mean per se that the application contains malicious elements. Rather, third parties will use the information available in your profile to personalise other services, e.g. for the purpose of creating personalised advertisements.

Measures to promote more secure usage

Participation in social networks will always involve a degree of risk. The following tips will help you reduce your risk profile:

- Consult the general terms and conditions
As indicated earlier, social networks introduce a number of risks, particularly in the area of privacy. By reading the general terms and conditions of a website, you can make a well-considered decision regarding the possibility of signing up and disclosing your private details. Also make sure to read the updates; the general terms and conditions of social networks are modified on a regular basis.
- Limit the access to your profile to your friends and acquaintances
To prevent strangers from accessing your profile, it is important to limit access to people you know.
- Exclusively accept invitations from people you know and verify each invitation
In addition to connecting to your friends and business contacts, one of the most entertaining aspects of social network sites is that they allow you to make new acquaintances. Some people consider it an enticing challenge to link as many contacts as possible. However, an all too enthusiastic addition of new contacts may mean that you provide people who you do not know very well or even total strangers with access to your profile. Even if you limit access to your profile to known contacts, the linking of strangers involves the risk that your personal details fall into the hands of malicious parties. In case of doubt about an invitation, the best thing to do is to contact your acquaintance via mail or telephone to verify whether the invitation has indeed been sent by him or her. Namely, the possibility exists that another person is abusing the identity of your acquaintance on the social network.
- Be aware of what you publish
The risks of social networks discussed earlier are reinforced by the fact that it is very difficult to remove data from the Internet once it has been published. Add to that, the profile information that was visible to the public at a given time will often have ended up in the database (cache) of search engines like Google or may have been copied to other websites.
- Follow your employer's social media guidelines

Various employers have started to introduce guidelines for employees regarding their participation in social networks. Make sure you comply with these guidelines to avoid problems in the professional domain.

- Use strong passwords
To at least limit the risk of account hijacking, it is important to use strong passwords. Simple passwords can be cracked with greater ease by malicious parties. Also try to avoid the use of the same password where possible.
- Make sure your virus scanner is up-to-date
Antivirus software is able to detect the bulk of malicious software and notify you of its presence. This will allow you to block or prevent at least a number of these attacks.
- Install new software and browser updates in a timely fashion
Software vendors regularly make updates available that remedy newly identified vulnerabilities in your operating system or web browser. The installation of these updates will enhance your security status and may prevent attackers from exploiting known vulnerabilities.

Final remarks

The measures presented above are primarily focused on the reduction of risks, but do not entirely take them away. Therefore it is important to be aware of methods which can reduce the potential damage of a successful attack. If you do end up clicking on a link, for example, the best thing to do is to remove the link as soon as you can to prevent your contacts from clicking on it, to prevent the further distribution of the attack. A similar countermeasure can be carried out after you fall victim to account hijacking. This can be done through informing your contacts about the account hijacking. Simultaneously, you can, with the assistance of the social network, try to resolve the problem and regain control of your account.