The Social Network: Be on the safe side!

Since the 1990s, when the US government relinquished control over the Internet, we have lived in an era that may rightly be called "The Era of The Internet".

The Internet offers a broad variety of activities: communication, purchase of goods and services, entertainment, general web-surfing and many others. But one of the most popular activities on the Internet in recent years has become *Social Networking.*

Social Networking is a process of socialising through the Internet. A social networking website is a platform that builds and supports groups of individuals, interconnected by common interests. Users may share ideas, opinions, photographs and videos, find old and new friends, join communities of people with similar interests, and all these for FREE!

There is a wide range of social networking websites: Facebook, Twitter, MySpace, Flickr, LinkedIn and dozens of others. The number of social network users is growing exponentially every year, as well as increasing the time that each user spends on social networking. Thus, Facebook alone, which is currently leading the industry of social networking, has more than 500 million users worldwide and half of them are logged on to the website every day [1].

Social networking has evolved into the main way of communication in the 21st century and brought new opportunities. But new opportunities came at a price! The price is the new, previously unknown, threats and vulnerabilities.

The purpose of this article is to give some information about the social-network-related threats and some hints on how to socialise online with minimal risk. Awareness of threats is the first step on the way to secure social networking. Being well-informed about the risks on social networks and being armed with knowledge about possible risk mitigation measures will enable users to take appropriate precautions for self-protection and will help to adopt secure online-behaviour.

Due to the nature of social networks, users publish sensitive information, including full name, date of birth, phone numbers, photographs, information about tastes, experience and relationships. Thus, sensitive information becomes easily accessible to a great number of people. Therefore, the main concern on social networks is privacy.

Who can misuse your private information on social networks?

Different parties may gain access to your personal information online, both legally and illegally:

1) Platform providers. Despite privacy settings some providers may have access to private data.

2) Third Parties. A third party may gain access to personal data by breaking into a social network website. Personal information may simply be available to the third party due to the lack of attention to privacy settings.

3) Other Users. Other users may maliciously use data posted by an author or they may publish information or upload photographs that will portray the author in an undesirable manner.

Identity Theft

Identity theft is one of the most important threats on social networks. Identity theft is the use of victim's private information by a criminal in order to conduct certain actions on the victim's behalf (open bank accounts; get credit cards, loans, state benefits and documents such as passports and driving licenses; post offensive and false information). A malicious user (misuser) may steal an identity through the theft of login credentials or a mobile device that has been used to access a network. Identity theft may lead to financial losses and reputation damage. Below are some recent examples of identity theft on social networks.

In Spain in 2009, multiple identity theft happened, aimed at celebrities. Well-known people found profiles opened in their name on a social networking website with comments and opinions affecting their reputation [2].

In Greece in 2009, a man created a fake profile of his ex-girl-friend with nude photographs. The woman reported the misuse and the fake profile was removed [2].

In the UK, a businessman found a fake profile created in his name on Facebook. The profile contained false information about the victim's sexual orientation and political views. The businessman took the case to the High Court where the malicious user was ordered to pay damages [2].

Data misuse

Some active users of social networks have their profiles publicly accessible. Other users accept unknown people to be their friend on social networks, so they expose information of varying degrees of sensitivity to strangers. All sensitive information may be misused for identity theft, phishing emails or malicious software particularly targeted at the profile owner.

As a user of online social networks, you may get a phishing email that contains a lot of personal information. The misuser may pretend to be an acquaintance from last years holiday, discuss the resort and the hotel you stayed at. Later the misuser may send you an email asking for financial help as he/she is in a difficult situation; for example, alone in a foreign country with no money as the purse and credit cards are stolen.

You may get phishing emails from a fake social network provider, asking to reset your password or reveal some sensitive information. The above are only the most standard examples of data misuse. Misusers are very creative and regularly change patterns.

A user may be confronted unexpectedly, for example at the job interview, with information that he/she has published in the public domain. A future employer may look through a user's profile and photographs on the social network. Seeing a job candidate's binge drinking photographs or rude and offensive comments on a wall will hardly improve chances of the employment.

Other people and Organisations

Everyone must be aware of how his/her comments and photographs portray organisations and people involved.

In 2008, Virgin Atlantic airlines dismissed 13 employees for posting negative comments about the company's customers on Facebook [2].

In May 2009, an Italian nurse published on her Facebook profile photographs taken at her workplace in an intensive care unit. On some photographs, patients were visible. An investigation was conducted to establish privacy violations. Another Italian nurse published a

photograph of a drunken patient and posted some offensive comments. The nurse was suspended.

Mobile devices

Social networking is rapidly getting mobile. More than 200 million active users are currently accessing Facebook through mobile devices. These users are twice as active on Facebook as non-mobile users [1]. Most mobile devices are used to store sensitive personal information, e.g. photographs and videos. Therefore, the loss of mobile device may lead to a sensitive information leakage and to far-reaching consequences, including serious financial and reputation damage.

Legislation

There are various legal documents that regulate different aspects of private information protection.

European Convention on Human Rights
http://conventions.coe.int/treaty/en/Treaties/Html/005.htm
Declares and protects Human Rights and Freedoms in Europe.

Defamation Act 1996
http://www.legislation.gov.uk/ukpga/1996/31/contents
Regulates issues related to defamation or malicious falsehood.

Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents
Regulates the processing of information relating to individuals, including obtaining, holding, use or disclosure of such information.

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents
Regulates rights of privacy, as a part of an individual's private and family life.
In 2002, Naomi Campbell sued a newspaper in the High Court for publishing her private photographs. Campbell received damages of £3,500, on the grounds of violation of the Human Rights Act and the Data Protection Act.

10 Basic Privacy and Security Rules on the Social Networks

1) Use all available technical tools to protect your privacy on a social network. Be familiar with the social network privacy rules and use privacy settings knowledgeably (information about privacy settings on Facebook: http://www.facebook.com/privacy/explanation.php). Reset you password regularly.

2) Do not reveal to strangers any sensitive information such as full name, date of birth, address, phone number, mother's maiden name, etc.

3) Be careful with the information you are posting about yourself (comments, photos, videos). Consider how this information portrays you, as you may be faced with it in the future.

4) Choose your friends. Accepting someone as a friend will lead to revealing sensitive information. You are not obliged to accept anyone as a friend. You may refuse or ignore the request from an unknown user.

5) Do not post offensive comments about other people. Do not post photographs and videos of other people without their consent.

6) Be aware of the social network-related policies within your organisation. Make sure that photographs taken at your work place do not affect the organisation's confidentiality and do not break security rules.

7) Protect mobile devices that you use to access social networks and store sensitive information. Do not leave them unattended. Do not save sensitive information on them without a good reason. Use security features on mobile devices.

8) Be careful when accessing a social network through public-access locations. Do not access social networks from non-trusted locations. Do not ever save your credentials on public computers.

9) Be aware of phishing emails. Remember, website provider would not ever request you to send sensitive information by email. Never follow links in an email - log on to a networking website by typing a URL.

10) Be familiar with the legislation. You may seek protection and compensation if you became a victim of a privacy violation.

None of the rules on their own could provide complete security to personal information. For example, privacy settings on a social network may give a user a sense of security. But if, at the same time, the user ignores other rules and, for example, accepts strangers as friends and saves login credentials on the public computers, then the sense of security is false. Only consistent compliance with all rules will help to avoid most of the threats on social networks.

The main advice for secure social networking is to be thoughtful about the actions you undertake online and use social networks in an intelligent manner. Remember that any social network is a public place.

Make sure that your family and friends are aware of the threats on social networks. Protect your close ones by making them aware.

The idea of information sharing is a cornerstone of Social Networking, but this great idea may be easily misused. It is a task for everyone to find an individual balance of active socialisation

online and privacy. Luckily, there are plenty of ways to protect yourself and to ensure your privacy.

Be aware. Be safe. Happy networking!

References:

1. http://www.facebook.com/press/info.php?statistics, accessed on 26th March 2011
2. Promoting information security as a cultural and behavioural change. 2010