www.enisa.europa.eu

FAQs to the report “Online as soon as it happens ”

Why has ENISA conducted this report and 'what is the reason for ENISA looking specifically at mobile social networking?

The social networking phenomenon has registered an exceptional growth trend and there has been a widening in terms of users’ profiles involved in such activity. This phenomenon is rapidly evolving not only in relation to the audience, changing its demographics, but also in relation to the way the audience itself can experience social networks. Besides traditional computer-based access, users are now able to access social networks through their mobile phones.

How many social networking users are there?

Of the around 283 million European users, 211 million of them, aged 15 and older who accessed Internet via a home or work computer in December 2008, visited a social networking site. The growing popularity of social networks has determined an increasing demand to access them via mobile phone. It has been estimated that in 2011 the number of mobile social network users worldwide will be 554 million, corresponding to 13.3% of mobile phone subscribers, with a growing trend for 2012: 803 million users, corresponding to 18.8% of mobile phone subscribers. In Europe, in 2012, the number of users will be 134 million meaning that one out of five mobile phone subscribers will use the mobile device to access a social network.

The AR community members also expressed interest for the mobile social networks topic. 15 members of the AR community contributed to this paper in a number of ways (suggestions, reviews, observations etc.).

What social networking sites are being accessed via mobile phones?
The most popular social networking sites accessed via personal computer are also the leading ones being used over mobile phones. Facebook represents the vast majority of social networking's active reach on mobile phones and it has been the most visited site in at least four European countries: the UK, Italy, Spain and France.

What are the privacy issues involved?
Besides the services and opportunities offered, social networks are not exempt from risks affecting users' privacy, personal and professional life. Social networks are exposed to a higher level of risk than, for example, professional social networks since users, in general social networks, often share much more information about themselves than in professional social networks. Privacy issues can arise from three different types of attackers; third parties, other users and platform providers.

Third parties may gain fraudulent access to personal data published on a user profile or by stealing or finding a lost mobile, which can cause severe privacy issues. Access by a third party can also occur without violating any technical rules and is due basically to the privacy profile level which is not set properly by the user.

Other users also have the same potential as third parties to cause privacy issues. It is possible in fact to leave comments on the personal profile of other community members or to tag a picture portraying the user without his consent. This is why it is also important to agree with friends and peers on the rules to be followed when using and accessing social networks in order to ensure secure personal data processing.

Platform provider has full access to user data, collecting for example the user's IP address and browser type and the information provided is available in search results across the network and to third-party search engines.

What are the major risks and threats related to MSNs?
The growing popularity of the social mobile phenomenon creates significant opportunities for business and personal purposes but also exposes its users to security risks and threats. The report points out the major risks and threats of mobile social networking services, e.g. identity theft, corporate data leakage and reputation risks.

Identity theft in mobile social networks is one of the most important threats as its consequences may affect the reputation and privacy of the user. Identity theft can be easily carried out in different ways by since the attacker will be

able to take full control of the user's account. The attacker can then publish comments in the name of the legitimate user, change the current password and e-mail address to permanently take control of the account or by using the compromised account to spread malicious software. The 'forgery' of a user's identity can have a very serious impact on his personal life and reputation at work.

Corporate data leakage means accidental disclosure of corporate sensitive information. This can appear due to the fact that users discuss and share their experiences, including work ones, on social networking sites, and users posting professional information on their business profile could have these posts distributed to their Facebook or Twitter accounts. The real-time spread through social mobile of corporate data can cause serious damage to organisations as well as social network users, who can be affected by this threat as a result of unauthorised posts or photographs in real time, which can affect their privacy and reputation at work.

Two examples are:

- **UK- Data leakage for airlines companies**
  In 2008, Virgin Atlantic airlines investigated allegations that its staff posted rude comments on Facebook that criticised the cleanliness of the company's fleet and of its passengers. The 13 members of the Virgin Atlantic staff have been dismissed for their behaviour. Later, a similar episode involved the British airlines check-in staff based in Gatwick who posted on Facebook messaging saying that travellers are 'smelly' and that operation's at Heathrow's Terminal 5 are 'shambolic'. An investigation was launched after the episode.

- **Italy – Professor's fake profile on Facebook**
  A fake profile of a University professor in Turin was created on Facebook. The professor wanted to create his own Facebook page but he found out that someone else had already registered him, creating a profile with very offensive features, affecting his reputation. The episode was immediately reported to the public prosecutor in Turin for the necessary investigation and measures to be taken.

What are ENISA's recommendations?

ENISA believes that users' awareness is the first line of defence regarding their privacy and security of their data. This report aims to provide a set of recommendations for raising the awareness of SNSs users and in particular of social mobile users of the risks and the possible consequences related to their improper use.

Besides pointing out the risks and threats of mobile social networking services, the report also gives 17 ‘golden rules’ on how to combat these threats. Some of these rules are

- Remember to log out from the social network once your navigation is over.
- Do not to allow the social network to remember your password (this function is called ‘Auto-complete’).
- Do not mix your business contacts with your friend contacts.
- Report immediately stolen/lost mobile phone with contacts, pictures, or personal data in its memory
- Set the profile privacy level properly.

For report:
http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens

For press release:
http://www.enisa.europa.eu/media/press-releases/instantly-online-17-golden-rules-for-mobile-social-networks

For further details, contact:
Isabella Santa, Senior Expert Awareness Raising. ENISA,
awareness@enisa.europa.eu
Ulf Bergström, Spokesperson, ENISA
press@enisa.europa.eu, Mobile: +30 6948 460143