enisa
European Network and Information Security Agency

Social Networking

2008

What is Social Networking?

Social networking is a powerful mixture of human social instincts and web 2.0 technology. It may be seen as an informal but all-embracing identity management tool, defining access to personal information via social relationships.

The essential elements of a social networking site (SNS) include tools for:

- posting personal data into a 'profile' and user-created content;
- personalized interaction with online friends (e.g. blogs); and
- defining social relationships which determine who has access to data, who can communicate with whom and how.

SNS users often do not behave according to the size or nature of the audiences accessing their data due to the sense of intimacy of being among 'digital friends'. This can lead to a 'digital hangover' – disclosures that cannot be forgotten in the morning. Moreover, commercial pressures in an industry estimated to be worth about €10B, encourage design and behaviour which increase the number of users and connections ('viral' techniques). This can magnify security problems and dilute privacy in the development process.

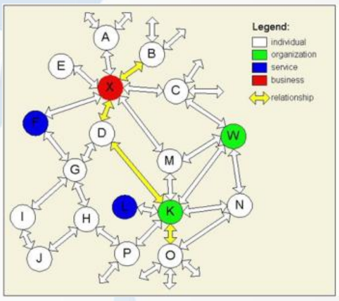

Figure 1: relationships in a SNS

ENISA's work on SNS

ENISA has gathered input from social networking experts into a report to raise awareness about the risks related to SNS and recommendations on how to manage them. The aim is not to deter people from using social networking but rather promote a safer environment for users and reduce large-scale security problems which also affect network providers and governments.

If used correctly, social networking can enhance data privacy over and above more established mechanisms such as blogs. If not, however, it provides a dangerously powerful tool in the hands of spammers, unscrupulous marketers and others who may take criminal advantage of users.

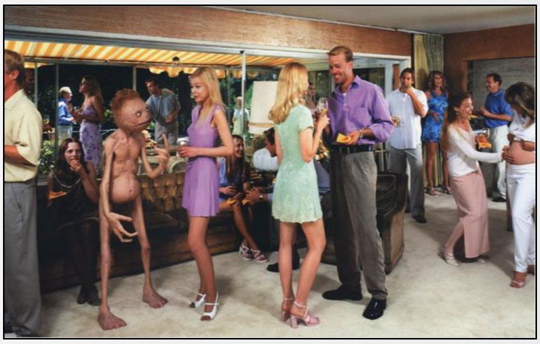

Figure 2: the digital cocktail party

What actions are needed to improve social networking?

ENISA has issued recommendations on four levels aimed at improving SNS security.

Users of SNS can take actions to ensure protection of personal data. They should always consider the consequences of material, particularly images, before posting online. Imagine the audience which might realistically access the data and learn about (and use) the privacy settings available on social networks. Accepting default settings is not enough.

ENISA recommends **enterprises** to develop a SNS usage policy for staff which takes into account the possible uses of SNS data for social engineering attacks. Firms should also educate employees about so-called 'spear-phishing' attacks.

ENISA urges **governments** to review legislation and its interpretation in the context of social networking. There are many issues which need clarification including, for example, deletion of user-generated content or image-tagging by third parties.

Governments should promote awareness raising programmes for safer social networking. Banning SNS in schools is not a solution as this policy deters children from seeking help in case of problems. SNS also offer adults the means to learn the skills needed to mentor and monitor young people in this area. SNS can be a valuable educational resource. Government's role should be, therefore, to promote transparency about the handling of data collected via SNS and support research and initiatives which encourage recent innovations on secure portability on SNS which discourage so-called 'lock-in'.

SNS **providers** play a critical role in ensuring security on their sites. They should promote safer usage in real-time by posting security information on SNS. They also need to increase transparency of data handling practices. Abuse of data should be straightforward to report and data easy to delete completely. These actions are not comprehensive, however. There are numerous other issues which providers must address to improve the SNS environment.

A complete overview of ENISA's recommendations can be found at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

Latest developments

Work is ongoing in the fight to improve security on SNS. Data portability, one of ENISA's key recommendations, is a recent development which could help break the "Hotel California" effect ("*you can check out, but you can never leave*") which underlies many of the security problems. Several key SNS providers have recently rolled out features in this area.

Users can also be empowered as owners of a 'social graph' which can move between sites, while maintaining security and privacy. Further research is needed on image-anonymisation, in other words how to post images which are less revealing, while still fulfilling their purpose. Other issues requiring investigation include security of mobile social networks where location data is more common; convergence with virtual 3D worlds; and criminal misuse of SNS.

If used carefully, social networking need not be avoided. ENISA aims to promote the benefits of a safe SNS environment. People need to be sensitised to the risks of entering such sites but also the actions they can take to manage these risks.

I want to know more…

Please visit our website regularly (http://www.enisa.europa.eu), or email us at info@enisa.europa.eu. Additionally, ENISA has produced a video clip on social networking sites which can be downloaded at:http://www.enisa.europa.eu/pages/position_papers.htm.