

Executive Summary

Online Social Networks or Social Networking Sites (SNSs) are one of the most remarkable technological phenomena of the 21st century, with several SNSs now among the most visited websites globally. SNSs may be seen as informal but all-embracing identity management tools, defining access to user-created content via social relationships.

Since the commercial success of an SNS depends heavily on the number of users it attracts, there is pressure on SNS providers to encourage design and behaviour which increase the number of users and their connections. Sociologically, the natural human desire to connect with others, combined with the multiplying effects of Social Network (SN) technology, can make users less discriminating in accepting 'friend requests'. Users are often not aware of the size or nature of the audience accessing their profile data and the sense of intimacy created by being among digital 'friends' often leads to disclosures which are not appropriate to a public forum. Such commercial and social pressures have led to a number of privacy and security risks for SN members.

This paper emphasises the commercial and social benefits of a safe and well-informed use of SNSs. It also outlines the most important threats to users and providers of SNSs and offers policy and technical recommendations to address them.

Threats

- **Threat SN.1 Digital dossier aggregation:** profiles on online SNSs can be downloaded and stored by third parties, creating a digital dossier of personal data.
- **Threat SN.2 Secondary data collection:** as well as data knowingly disclosed in a profile, SN members disclose personal information using the network itself: e.g. length of connections, other users' profiles visited and messages sent. SNSs provide a central repository accessible to a single provider. The high value of SNSs suggests that such data is being used to considerable financial gain.
- **Threat SN.3 Face recognition:** user-provided digital images are a very popular part of profiles on SNSs. The photograph is, in effect, a binary identifier for the user, enabling linking across profiles, e.g. a fully identified Bebo profile and a pseudo-anonymous dating profile.
- **Threat SN.4 CBIR:** Content-based Image Retrieval (CBIR) is an emerging technology which can match features, such as identifying aspects of a room (e.g. a painting) in very large databases, increasing the possibilities for locating users.
- **Threat SN.5 Linkability from image metadata:** many SNSs now allow users to tag images with metadata, such as links to SNS profiles (even if they are not the owner/controller of that profile), or even e-mail addresses. This leads to greater possibilities for unwanted linkage to personal data.
- **Threat SN.6 Difficulty of complete account deletion:** users wishing to delete accounts from SNSs find that it is almost impossible to remove secondary information linked to their profile such as public comments on other profiles.
- **Threat SN.7 SNS spam:** unsolicited messages propagated using SNSs. This is a growing phenomenon with several SNS-specific features.
- **Threat SN.8 Cross site scripting (XSS), viruses and worms:** SNSs are vulnerable to XSS attacks and threats due to 'widgets' produced by weakly verified third parties.
- **Threat SN.9 SN aggregators:** these 'SNS portals' integrate several SNSs which multiply vulnerabilities by giving read/write access to several SNS accounts using a single weak authentication.

Executive Summary

- **Threat SN.10 Spear phishing using SNSs and SN-specific phishing:** highly targeted phishing attacks, facilitated by the self-created 'profiles' easily accessible on SNSs. SNSs are also vulnerable to social engineering techniques which exploit low entry thresholds to trust networks and to scripting attacks which allow the automated injection of phishing links.
- **Threat SN.11 Infiltration of networks:** some information is only available to a restricted group or network of friends, which should provide the first line of defence in protecting privacy on SNSs. However, since it is often easy to become someone's 'friend' under false pretences, this mechanism is not effective. On many SNSs it is even possible to use scripts to invite friends.
- **Threat SN.12 Profile-squatting and reputation slander through ID theft:** fake profiles are created in the name of well-known personalities or brands or within a particular network, such as a school class, in order to slander people or profit from their reputation.
- **Threat SN.13 Stalking:** cyberstalking is threatening behaviour in which a perpetrator repeatedly contacts a victim by electronic means such as e-mail, Instant Messenger and messaging on SNSs. Statistics suggest that stalking using SNSs is increasing.
- **Threat SN.14 Bullying:** SNSs can offer an array of tools which facilitate cyberbullying (i.e. repeated and purposeful acts of harm such as harassment, humiliation and secret sharing).
- **Threat SN.15 Corporate espionage:** social engineering attacks using SNSs are a growing and often underrated risk to corporate IT infrastructure.

Recommendations

The Virtual Group makes the following recommendations:

- **Recommendation SN.1 Encourage awareness-raising and educational campaigns:** as well as face-to-face awareness-raising campaigns on the sensible usage of SNSs, SNSs themselves should, where possible, use contextual information to educate people in 'real-time'. Additional awareness-raising campaigns should also be directed at software developers to encourage security-conscious development practices and corporate policy.
- **Recommendation SN.2 Review and reinterpret the regulatory framework:** SNSs present several scenarios which were not foreseen when current legislation (especially data protection law) was created. The regulatory framework governing SNSs should be reviewed and, where necessary, revised.
- **Recommendation SN.3 Increase transparency of data handling practices:** a review of the practices of SNS providers in Europe with respect to existing data protection law is recommended.
- **Recommendation SN.4 Discourage the banning of SNSs in schools:** SNSs should be used in a controlled and open way with co-ordinated campaigns to educate children, teachers and parents.
- **Recommendation SN.5 Promote stronger authentication and access-control where appropriate:** stronger authentication should be used in certain SNS environments. Additional authentication factors which could be used range from basic e-mail verification through CAPTCHAs^[51] and recommendation-only networks to physical devices such as mobile phones and identity card readers.

Executive Summary

- **Recommendation SN.6 Implement countermeasures against corporate espionage:** various steps are recommended for the prevention of social engineering attacks on enterprises.
- **Recommendation SN.7 Maximise possibilities for abuse reporting and detection:** SNSs should make it as easy as possible to report abuse and concerns. 'Report Abuse' buttons should be as ubiquitous as the 'Contact Us' option on classic websites.
- **Recommendation SN.8 Set appropriate defaults:** default settings should be made as safe as possible, and accompanied by user-friendly guidelines.
- **Recommendation SN.9 Providers should offer convenient means to delete data completely:** simple tools should be provided for removing accounts completely, as well as allowing users to edit their own posts on other people's public notes or comments areas.
- **Recommendation SN.10 Encourage the use of reputation techniques:** reputation mechanisms can act as a positive motivator towards good online behaviour.
- **Recommendation SN.11 Build in automated filters:** a legislative review into SNS filtering should be undertaken, with a view to SNS providers building filters into their sites.
- **Recommendation SN.12 Require consent from data subjects to include profile tags in images:** SNS operators should give users privacy tools to control the tagging of images depicting them.
- **Recommendation SN.13 Restrict spidering and bulk downloads:** SNS operators should restrict spidering and bulk downloads (except for academic research purposes).
- **Recommendation SN.14 Pay attention to search results:** data should either be anonymised, not displayed, or the user should be clearly informed that they will appear in search results and given the choice to opt out.
- **Recommendation SN.15 for addressing SNS spam:** similar techniques to those used for e-mail anti-spam reputation systems should also be developed to eliminate spam comments and traffic.
- **Recommendation SN.16 for addressing SNS Phishing:** the best practices for combating phishing on SNSs, which are promoted by the APWG, should be adopted.
- **Recommendation SN.17 Promote and research image-anonymisation techniques and best practices**
- **Recommendation SN.18 Promote portable Social Networks:** the economic and social implications of portable social networks should be addressed.
- **Recommendation SN.19 on research into emerging trends in SNS:** looking to the future, the group has identified some trends emerging in SNSs which have important security implications. More research should be carried out in the areas of mobile SNS, convergence with virtual worlds, misuse by criminal groups and 3D representation and online presence.