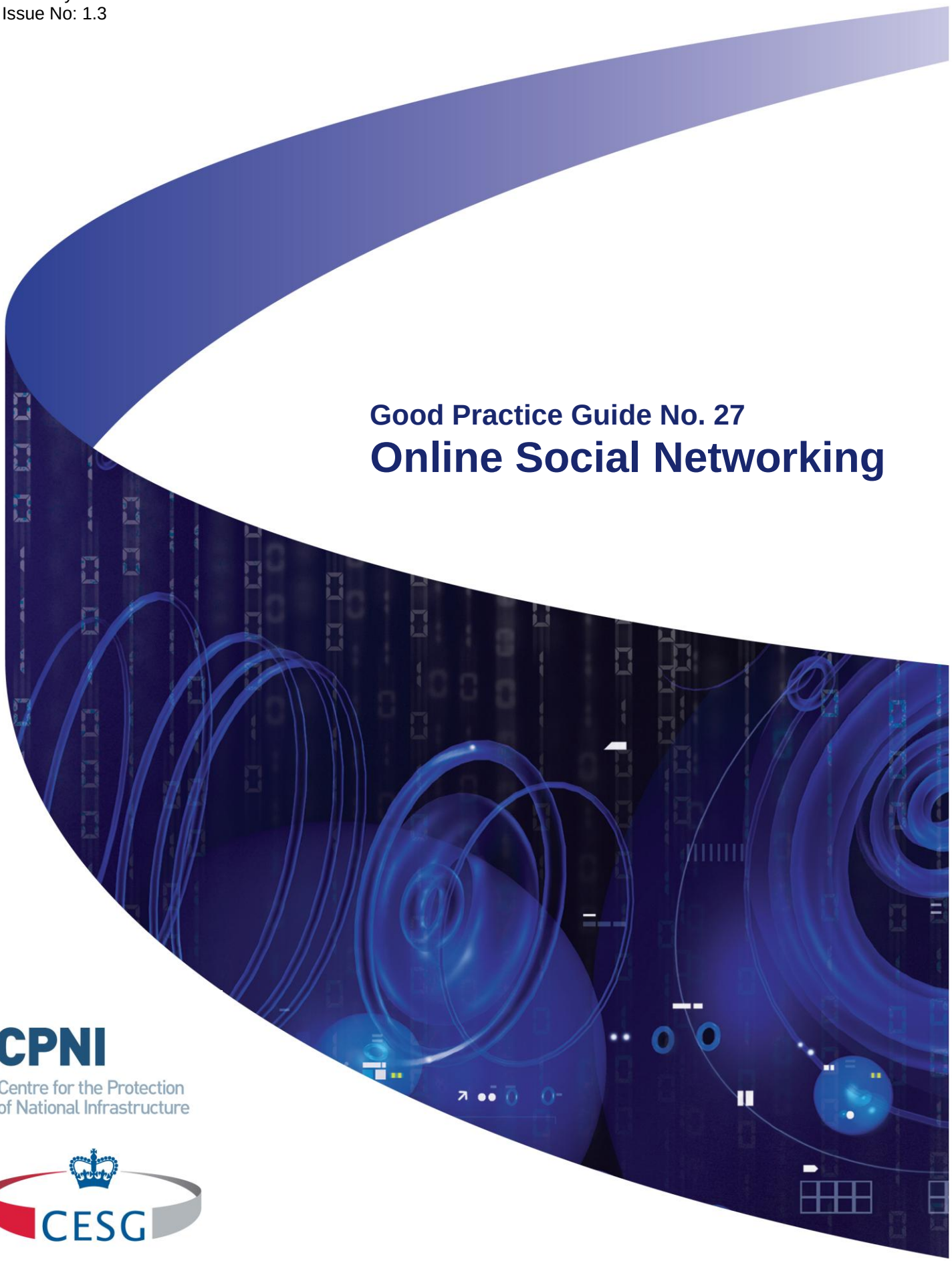
February 2014
Issue No: 1.3

Good Practice Guide No. 27

Online Social Networking



CPNI
Centre for the Protection of National Infrastructure

CESG
NATIONAL TECHNICAL AUTHORITY FOR INFORMATION ASSURANCE

Good Practice Guide No. 27

Online Social Networking

Issue No: 1.3
February 2014

Document History

Version	Date	Comment
1.0	July 2010	First issue
1.1	Sept 2010	Minor updates
1.2	February 2014	Updated
1.3	February 2014	Minor update

Purpose & Intended Readership

This Good Practice Guide (GPG) has been developed in collaboration between CESG (the National Technical Authority for Information Assurance) and the Centre for the Protection of National Infrastructure (CPNI)[1] to help assess and reduce the risks posed by the use of online social networking sites. It is intended to support those who work in Information Assurance (IA) and IT security officers involved in information and security risk management. This guidance also provides information for line managers, corporate security policy makers and HR practitioners who may be involved in managing cases regarding the inappropriate use of Online Social Networks (OSNs) in breach of corporate processes. It may also be useful for those involved in Knowledge and Information Management.

Executive Summary

Online social networking and microblogging have become very popular, and offer significant business benefits to organisations. However, their use poses risks both to the data on the IT system used to access the sites, and to the users of the sites and the organisations they work for.

The risks associated with OSN usage can be divided into three main categories:

- Risks caused by content posted on OSNs
- Risks caused by social interactions on OSNs
- Risks caused by OSN-derived malware, phishing and spam

Threat actors are increasingly using OSNs to target individuals and specific groups for both online and offline attacks. Such targeted attacks are much harder to spot and therefore more likely to be successful. This is exacerbated by the fact that many people are more relaxed online than they would be in face-to-face communication.

Crucially however, the realisation of many of these risks is dependent on user behaviour. Educating users to raise awareness of the risks and promote good practice is therefore crucial to ensuring that these sites can be used safely.

It is recommended that organisations seek professional advice, especially in areas of employment law and IT practice discussed in this document, when implementing or amending procedures to take account of the risks posed by OSNs.

Appendix A contains a sample end user guide which organisations may distribute to staff or use as a model for their own guidance, providing it is consistent with the results of their risk assessment. A glossary of terms is also provided.

[1] CPNI is the government authority that provides advice on protecting the country's essential services, facilities and networks from terrorism and other threats.

Aims and Purpose

Many organisations have an increasing business need to use online social networks. This guide details the risks associated with the use of these applications, and gives guidance on how they can be used safely. The risks posed by the use of online social networks are not purely related to IA, but also threaten other aspects of security. This guide therefore aims to provide a holistic view of the risks and appropriate countermeasures relating to all aspects of the safe usage of OSN technologies. This should enable organisations to carry out a full risk assessment (for organisations bound by the SPF, this will be an IS1&2 (reference [b]) risk assessment), make an informed decision and formulate their own policy on whether and how to use these applications. This GPG will help organisations bound by the SPF (reference [a]) to meet their obligation under Mandatory Requirement (MR) 9.

This guide does not aim to duplicate existing published material, and, where relevant, references are used to direct readers to detailed published guidance on particular topics. In particular, it should be read in conjunction with CESG Good Practice Guide No. 7 (GPG 7), Protection from Malicious Code (reference [c]) and CESG Good Practice Guide No. 8 (GPG 8), Protecting External Connections to the Internet (reference [d]). Readers are also strongly advised to consult CPNI's advice on personnel security (available at http://www.cpni.gov.uk/advice/Personnel-security1).

Changes from the Previous Issue

The most significant changes in this complete review of content are:

- Updates relating to current social networks
- Incorporating Digital Strategy and Civil Service social media guidance
- Updated statistics and examples
- Removal of less relevant content (e.g. bandwidth issues)

Feedback

CESG Information Assurance Guidance and Standards welcomes feedback and encourage readers to inform CESG of their experiences, good or bad in this document. Please email: enquiries@cesg.gsi.gov.uk

Contents

Chapter 1 - Introduction 4
What are OSNs? 4
Why are OSNs relevant to my organisation? 5
What risks are associated with OSNs? 6
Chapter 2 - Threat 7
The threat 7
Threat actors 7
Chapter 3 - Vulnerabilities and risks 9
Risks associated with different types of social networking 9
Content-related risks 9
Risks related to social interactions on OSNs 13
Risk of OSN-derived malware, phishing and spam 14
Chapter 4 - Security controls 17
Overview 17
Control measures recommended for individuals using Internet-based ESNs 17
Control measures recommended for ISN usage 26
Control measures recommended for use of public and bespoke ESNs by organisations 28
Appendix A: End User Guide 31
End User Guide 32
References 36
Glossary 38

Chapter 1 - Introduction

Key Principles

- Online Social Networks (OSNs) are interactive web services which allow users to create a personal profile and build and maintain links with other users. They can be either public, Internet-based applications or internal organisational networks
- OSNs may be used by individuals to maintain personal or professional relationships, and by organisations for public engagement or service provision
- Many of the risks associated with the use of OSNs arise from the fact that much of the content on these sites is user-generated

What are OSNs?

1. Online Social Networks (OSNs) are predominantly Internet-based services which allow individuals to create a profile containing personal information and interact with other users. In 2013, 83% of households had Internet access and 73% of UK adults used the Internet on a daily basis; 61% of the population used a mobile device to do so (reference [e]). Social networking continues to grow within the UK: 57% of the population aged 16 and above use social networks, ranking the UK as the second-highest across Europe. There is significantly greater engagement in the younger age groups (reference [f]).

2. A large number of OSNs are now available, offering a wide and varied range of features. Most public sites (also known as 'External Social Networks' or ESNs) are free to use. Although most ESNs are Internet-based, it is possible to interact with some via other means, for example most popular ESNs can now be accessed via applications on mobile phones. Most ESNs have variable privacy settings, enabling users to alter the aspects of their profile which are visible to other users and the public.

3. Microblogging sites, of which the most popular in the UK is Twitter (reference [g]), enable users to publish 'microblogs' which are typically less than 140 characters (on Twitter these are known as Tweets). Around a quarter of all Twitter posts contain URLs, and due to the strict character limit on posts these are often shortened, so the real URL is hidden from users until they load the page.

4. Social bookmarking sites offer users the ability to create personalised interest boards, which are shared with the public. Pinterest is one popular such service, where users create 'pinboards' of images relating to or inspired by their interest, adding comments if they wish; other users can add their own comments and 'repin' these images into their own profiles. If images are 'pinned' by being copied and uploaded to the site, the originator can no longer control their use.

5. Virtual worlds, websites for recruitment/CV, genealogy, dating, photograph and video sharing (such as Flickr and YouTube) and general bookmarking are

outside the scope of this document. However, many of the risks and control measures associated with these sites are similar to those of ESNs.

6. Many large organisations have also set up their own 'Internal Social Networks' (ISNs) to promote communication and collaborative working. These are closed networks, often hosted on the organisation's own servers or the servers of an external provider as opposed to being Internet-based, which are accessible only by members of the organisation. They may be integrated with other collaborative tools such as wikis and document sharing applications.

Why are OSNs relevant to my organisation?

7. The popularity and widespread availability of OSNs means they represent a valuable tool for a wide variety of Governmental and non-governmental organisations. Social networks, among other social media tools, offer an effective and inexpensive method to engage with many users, in line with the 'Digital by Default' approach established in the Government Digital Strategy (reference [h]). Further advice on using social media and improving access can be found in Social Media Guidance for Civil Servants [i]) and the Digital by Default Service Standard (reference [j]).

8. There are three main ways organisations are likely to use OSNs:

   a. Use of public ESNs by individuals for:

      i. Business purposes – individuals contacting suppliers, partners, colleagues etc. A common example of this might be the use of LinkedIn to build professional contacts.

      ii. Personal purposes – keeping in touch with family and friends on corporate systems during breaks. Staff are also likely to use ESNs from outside the organisation's accreditation scope, such as from home computers physically outside the organisation, or from personal mobile devices either physically inside or outside the organisation, for this purpose.

   b. Use of ISNs for business purposes.

   c. Use of public or bespoke ESNs for purposes of public engagement, advertising or service provision by the organisation (e.g. for public consultation on new policy, to distribute public information or for recruitment). Organisations may set up profiles on existing ESNs to represent the organisation or a key individual within that organisation (such as an MP or press officer). These may be accessed and edited by multiple employees. Alternatively, some organisations have launched their own ESNs for public engagement.

9. The type of OSN being used will determine where the OSN lies in terms of the accreditation scope. An ISN owned by an organisation would normally fall within the accreditation scope, unless it is provided by another project, in which case it will be in the analysis scope.

What risks are associated with OSNs?

10. Like many Web 2.0 collaborative technologies, although the potential benefits are great, use of the technologies inherently carries greater risks than traditional web browsing. These risks largely come from the fact that the content on OSNs is predominantly user-generated. Verification of the source of the content on these sites is difficult, if not impossible. Damaging and/or inappropriate content can also be published and disseminated easily.

11. Increasingly users of social networks access their profiles via mobile devices, often using a mobile 'app' provided by the social network or third party developer. Devices and apps rarely have little more than limited security functionality, which could make users more vulnerable to attack. In addition, users tend to be less guarded when using mobile devices, being more likely to share information, trust other users and quickly adopt new technologies. In the past year, half of all Internet-using adults have been the victims of cyber crime or harassment, with the average cost of such crime increasing by 50% in one year (reference [k]).

12. The risks are not only from the social networking user, but also those they have connected to through the social network and what the network provider can ascertain about them through data mining and extracting statistical groupings across the large number of users.

13. These risks can jeopardize the Confidentiality, Integrity and Availability of the data on the IT system or device being used to access the OSN. However, the risks are not solely related to information assurance. OSN usage could potentially also undermine personnel safety, organisational reputation and the safety of the public who interact with an entity via these services.

Chapter 2 - Threat

Key Principle

- Individuals or organisations who place information on OSNs may put themselves or the organisations that employ them at risk from a range of threats. The threats are varied and threat sources can range from individuals with a grudge through to foreign governments

The threat

14. The following illustrates the types of threat sources from IS1 & 2 (reference [b]) that, potentially, could maliciously take advantage of OSN usage. The relevance of each of these will depend on the individual or organisation in question:

    a. Commercial competitors
    b. Criminal groups
    c. Disaffected employees
    d. Foreign Intelligence Services
    e. Hackers
    f. Journalists
    g. Members of the public
    h. Single issue groups
    i. Terrorists

Threat actors

15. The following table presents the IS1 & 2 (reference [b]) threat actor types that are deemed most likely to be relevant in the context of online social networking. Individual organisations should make their own assessment of how relevant each of these, and the other threat actor types detailed in IS1 & 2 (reference [b]), are during their own risk assessment.

Threat Actor Type	Description
Normal User	A normal user would be an employee accessing an ESN. They may post content to the site or inadvertently infect the corporate IT system with malicious code derived from an Internet-based ESN. In the context of ISNs, a normal user would be any user with an account on the ISN. They could be coerced by a threat source into releasing sensitive information which is available to them via the ISN.
Privileged User	A privileged user would be an IT administrator (or other employee with high levels of privileges on the corporate IT system) using an online social network. They may post content to the site in the same way as a normal user. However, should the system become infected with malicious code it will have more privileges available to it. In the context of ISNs, a privileged user would be responsible for managing the ISN and would have access to all the accounts on the network. He may be coerced by a threat source into releasing sensitive information posted on the ISN or providing the threat source with access to the ISN.
Indirectly Connected	An indirectly connected threat actor in this context would be other Internet users who are not members of the organisation. For example, it could be another user of the Internet who views or uses personal information on the site to carry out identity theft or for the purposes of social engineering, or a criminal who uses the sites to launch phishing attacks or propagate malware.
Service Consumer	A service consumer in this context would be another user of the OSN. They may intentionally or unintentionally post links to phishing sites or malware on a profile or site.
Service Provider	A service provider could be an OSN provider, who may unintentionally incorporate vulnerabilities during development, or aggregate and filter information and user groups using data mining techniques. It could also be the developer of a third party application, who could, intentionally or unintentionally, use the application to spread malware or harvest user data.

Table 1 – IS1 threat actors

Chapter 3 - Vulnerabilities and risks

Key Principles

- There are three key vulnerabilities associated with OSNs - the publication of content on these sites, the social interactions between users, and their ability to be used to spread malware, aid phishing attacks and spam
- Each of these vulnerabilities give rise to a myriad of risks, however a key feature of most of these risks is that they are dependent on user behaviour – when considering the risks of OSN use, the user really is the main threat

Risks associated with different types of social networking

16. When conducting a risk assessment, the type and context of the OSN concerned should be considered, as this will determine how great the risk is. For example, the level of risk associated with posting content will obviously depend on the public accessibility of the social network.

Content-related risks

17. The first vulnerability is the ability to post inappropriate content on OSNs, and there are a number of risks which arise from this. The OSN profile page encourages the publication and sharing of personal information and opinions. In general, people are more relaxed about what they will post online than what they will say offline. Social networks and microblogging sites are also designed to enable content and comments to be published frequently, quickly and easily.

18. Once content is posted on the Internet, it is essentially impossible to completely delete it. Internet content is cached frequently by search engines so preventing publication of potentially damaging content is much more effective than subsequent removal. Moreover, attempts to remove content after publication can backfire and make the original information more widely known.

Identity theft

19. As already discussed, OSNs allow users to create a profile containing personal details. Some of the information users can post, such as date of birth and home address, is commonly used in identity verification and may therefore be used by criminals for the purpose of identity theft. In addition, many of the answers to common security questions, such as ‘pet’s name’ and ‘name of my first school’ can be found on OSN profiles. It should be noted that identity fraud within the UK was estimated to cost £3.3bn in 2013 (reference [l]).

20. Although many users would not intentionally make such information public, there is a general misconception regarding the public nature and amount of privacy afforded by OSNs. Information can also be pooled from multiple sources on the Internet and this can be made easier by specialised search engines such as 123people.co.uk, which search and aggregate information from multiple social networks.

Photograph-related risks

21. The ability to upload and share photographs is a key feature of many OSNs, and most social networks also offer an image annotation functionality, which enables users to 'tag' their contacts in the photographs they upload. OSNs can therefore provide a comprehensive collection of photographs of an individual. Photographs can also be geo-tagged (by location) and may contain other information in the background, such as car registration plates, house numbers, and images of sensitive material such as military equipment or maps, which may pose a security risk.

Physical safety

22. Information posted on OSNs may result in risks to personal security, as it could be used by threat actors to target individuals for attacks in the 'real world'. Users may post their address, details of their family and their whereabouts on OSNs. Individuals working in sensitive or controversial roles, such as serving members of the military, may be particularly at risk.

23. In addition, most OSNs and microblogging sites can be now be accessed and updated from GPS-enabled mobile devices. Many OSNs have facilities or third-party applications which use the GPS data from a mobile device to post an individual's real time location on the site. Location-based social networks, such as Foursquare, enable users to 'check-in' to their current locations and can see who else is nearby or has been there recently. Depending upon the users' settings, these location notifications can be immediately publically published and potentially used to locate currently empty properties (reference [m]). The publication of detailed plans and locations has been linked to a number of burglaries, and the insurance industry has suggested that users of ESNs may pay 10% higher insurance premiums in future (reference [n]).

Social engineering

24. OSNs may be used by those wishing to conduct research in order to undertake social engineering attacks, which require the threat actor to have knowledge of the target(s) and/or the organisation they work for. This can often be obtained from social networking profiles, especially those on professional networking sites such as LinkedIn, which often contain a large amount of detail about an individual's position, skills and responsibilities. Information about the internal structure and organisation of a department or company can also be obtained from groups or networks of employees (reference [o]).

25. Social engineering may take the form of spear phishing or whaling attacks. Social networking sites generally require an email address for the sign-up process. If a corporate email addresses is used, it may be harvested and used for phishing or targeted malware attacks against the organisation. Further information about social engineering and online reconnaissance can be found in CPNI's guides (references [p] and [q]).

Reputational damage and corporate liability

26. One of the main features of many OSNs is the ease with which content can be posted. Although this can be advantageous, it does increase the likelihood that some content may be posted without being properly checked, which could potentially damage the reputation of an organisation. Such a post may be deliberate (made, for example, by a disgruntled employee), accidental (an individual may express a personal opinion which, because of their position in a particular organisation, is interpreted as the official line of that organisation), or due to lack of clarity (something may be posted which contains a mistake, or could be misinterpreted). The risk of this happening does not stop when an employee goes home at the end of the day or even leaves employment permanently.

27. Employers bear ultimate responsibility for their employees' activities when using corporate IT systems. Organisations are therefore at risk of litigation resulting from the actions of their employees on both internal and external social networks. Use of sites must also comply with the Data Protection Act 1998 (relevant for any sites which collect or handle personal information), and, for public bodies, with the Freedom of Information Act 2000 and Public Records Act 1958 (relevant where ISNs and ESNs are used for business purposes). Due to the public nature of these services, users should familiarise themselves with the Attorney General's advice regarding the potential to commit contempt of court. Civil servants are also required to adhere to the Civil Service Code, or relevant regional or service code.

28. It is also worth noting that users have no control over advertising when using public OSNs, so a profile may be displayed adjacent to advertising which could be considered inappropriate. For example, an advertisement for a health supplement displayed on the same page as a health provider's profile may be construed as endorsement of the product.

Release of sensitive information

29. OSNs provide a forum through which sensitive or Protectively Marked information may be inappropriately shared or published. This may be deliberate, or inadvertent, e.g. by data aggregation. For example, a single comment about the problem a technical member of staff and OSN user has had with a server at work that day may not be damaging, but several months-worth of such comments may potentially combine to reveal a lot of information about the IT architecture of that organisation, which may make the organisation more susceptible to electronic attack.

Cyberbullying, cyberstalking and cyberharassment

30. OSNs not only provide a forum for bullying and harassment, but can also be used by cyberstalkers to identify and target their victims as they can provide personal information such as an individual's address, schedules and real-time location as discussed earlier.

31. There have been incidents where perpetrators have set up false profiles of the victim on OSNs, or published defamatory or embarrassing comments or content claiming to come from the victim to damage his or her reputation. There have been year-on-year increases in convictions (including jail terms) for defamation or harassment via social media, with public attention drawn regularly to widely-reported high-profile cases. In June 2013 the Crown Prosecution Service issued guidelines regarding prosecutions involving social media (reference [r]).

ID Hijacking/profile squatting

32. Related to the above is the possibility of identity hijacking. This occurs when an individual sets up a profile in the name of an individual or organisation without their permission. OSN users generally assume that profiles are created by the individual they represent; and rarely check with the person in the real world that this is the case. False profiles can either be produced for the purpose of slander, harassment or reputation damage; or in order to gain access to private profiles of the contacts of the individual being impersonated, or to extort information or money from other users.

Hijacked accounts

33. Account hijack (also known as 'account takeover') is a growing problem, increasing by 53% in one year [s]). It occurs when a threat actor obtains the login details of a user, sometimes via a successful phishing attack, a bulk dictionary attack if the password is weak, or covert malware compromise. Some sites, such as Twitter, have now stopped account holders choosing the most common passwords, but most still rely on users to select good passwords. A study of 32 million stolen OSN passwords which were posted on the Internet found that 1% of users had 123456 as a password, and 20% of users had selected one of the most common 5000 passwords (reference [t]).

34. Although the potential consequences of password theft are wide ranging and relate to content, social interactions and malware, they will be discussed together here. Hijacked accounts may be used:

    a. to propagate malware, spam or phishing attacks;

    b. to access personal information from the user's account and those on their contact list;

    c. for financial gain. A common scam is for a criminal to hijack an account and send messages to the user's friends claiming to be stranded and request money. With the information available on many OSN profiles these requests can sound very realistic; or

    d. to damage the reputation of an individual or organisation. If an organisation or a representative of an organisation sets up an official profile on a social networking site and it is hijacked, inappropriate content, links or malware may be posted in its name.

Inappropriate or offensive content

35. As discussed, one of the main features of OSNs and other Web 2.0 applications is that they feature user generated content. It is therefore possible that users may inadvertently access inappropriate or offensive content, placed by others on these sites. Employers may have a duty of care to protect their staff from this type of material. Most OSN providers have mechanisms by which offensive content can be reported for removal.

Disclosure of personal information due to website development faults

36. Several faults have been discovered in social networking sites which have resulted in more user data being publicly available than set by the user or agreed in the terms and conditions. Although most sites are quick to correct such problems once they are found, it is important to note that such instances do occur relatively frequently, and as a result it is not possible to guarantee that privacy settings applied by the user will always be enforced.

Third party applications

37. Many OSNs have now released their Application Programming Interface (API) to enable developers to write applications for the site. These applications run on servers owned and controlled by the developers, and have no assurance or provenance. When users download or sign up to use these, a significant amount of personal data is often shared with the developer even if it is not required for the application to function. Some applications or quizzes, such as ones which reveal news headlines from the day a user was born and publish this on their homepage, may also reveal personal information.

Terms and conditions

38. OSNs have terms and conditions, including a privacy policy, which state what they can and cannot do in terms of sharing user data with third parties, and what happens to information and accounts which are deleted. In some cases, any data posted becomes the property of the OSN, and some sites, such as LinkedIn, will sell this data to third parties.

Risks related to social interactions on OSNs

39. A key feature of OSNs is that they enable people to maintain and develop personal and/or professional contacts. However, this feature is also a vulnerability which can result in several risks if users fail to follow safe usage practices.

Lack of discrimination regarding contacts

40. Most users are less discriminatory about who they will add as a contact on an OSN than they would be in real life. This is important as, depending on a user's privacy settings, much more of the personal information on their profile may be available to their contacts than to the public.

41. Studies continue to demonstrate that at least some OSN users are fairly indiscriminate when it comes to adding users as friends. This means users may be sharing personal information with people they do not know. It is highly unlikely that most people would be this indiscriminate with their personal information offline, supporting the theory that many users have different attitudes and behaviours online and offline.

Lack of control over postings by other users

42. A user may be very careful not to post anything inappropriate, however they cannot control what their contacts post. Birthday greetings can reveal exact dates of birth and comments on work may disclose sensitive information about individuals who work in sensitive roles.

Aggregation of data

43. The popularity of many social networks allows effective data mining across their user population, which has been used to identify user characteristics despite enabling security features and using caution in what they have posted. Certain characteristics (e.g. a user not naming his employer) can become a marker which differentiates him from the majority of other users in a particular locality. 'Open Source Intelligence' (OSINT) tools such as Maltego collate data across many publicly available sources and have been used to identify some social network users as government workers, with enough additional publically-available information to potentially launch a successful spear phishing attack (reference [u]).

Risk of OSN-derived malware, phishing and spam

44. Given their huge popularity, the growing number of malware, phishing and spam attacks which specifically target OSN users is unsurprising. In addition, there are specific vulnerabilities relating to the development of OSNs which make them more prone to malicious code attacks. User behaviour on these sites also makes them ideal for these types of attack. Reports indicate that the average cost per victim of cyber crime continues to increase, with one estimate at 50% increase between 2012 and 2013 levels (reference [k]). CESG's GPG 7 (reference [c]) covers malware in some detail, so this section will only aim to discuss methods of malware propagation specific to OSNs. It is not intended to provide a detailed discussion of types and functionality of malware.

Phishing attacks using OSNs

45. Phishing attacks were originally delivered as untargeted mass email campaigns, but have recently become more sophisticated and targeted. Instead of sending mass emails or messages, phishers use social engineering techniques to target individuals, via information gleaned from OSN profiles. One study estimated the world-wide growth in the number of users receiving phishing messages at 87%, with a three-fold increase in daily phishing attacks within the UK (reference [v]).

46. Attacks are also increasingly being delivered as messages on social networking sites. Hijacking of OSN accounts means they often appear to come from an individual's friend or contact, so they are trusted far more than an unexpected email would be. The URLs are often obfuscated (they may be shortened, lengthened beyond recognition, or made to look like the authentic site through HTML encoding), so they may appear to be genuine but actually link to a malicious site. Equally, an appealing photo or image of text could be used to induce a user to click on an undisguised malicious link, or to connect to a malware server – and then naively share the lure with other users. This problem is exacerbated by the fact that some phishing attacks are launched specifically to steal a user's OSN login information, which then enables the attackers to hijack accounts and send URLs purporting to be from trusted sources, and to access private information for use in phishing attacks.

47. Several phishing worms have also been designed to target social networks, often targeting the most popular services. Microblogging sites such as Twitter have been the target of several phishing worms. The common use of shortened URLs in microblogs means that it is not easy to see what a URL actually links to. Many users are now so accustomed to clicking on shortened URLs that they do not expect to recognise the URL or consider the trustworthiness of links.

Spam

48. OSNs are increasingly being used to propagate unsolicited messages, or spam, which usually contain advertising. Although not generally harmful, spam can result in traffic overload on sites, and reduce their usefulness. Spam filters on OSNs are generally not as effective as those used for email accounts. Shortened URLs can also bypass some spam filters.

Socially distributed malware

49. Malware written specifically to target users of OSNs remains at a high level. The fact that users tend to acquire a large number of contacts makes malware spread rapidly around OSNs. Many users will automatically trust content or links which appear to come from a contact, and links to external websites are commonly shared on OSNs, often in obfuscated forms. These factors combine to enable cybercriminals to direct users to infected sites without raising suspicion. For example, the Koobface worm was first observed in 2008 on Facebook and Myspace, and there are now versions which target many other social networks.

50. Microblogging sites also frequently contain links to malware, often disguised in shortened URLs. URL shortening is popular with online criminals, who take advantage of the fact that users are accustomed to the format, and the inherent trust relationship which exists between users of OSNs.

51. Once again, if a site or profile set up to represent an organisation hosts malware, or links to sites containing malware, this could cause considerable damage to that organisation's reputation and public trust in it.

Malware derived from third party applications

52. As discussed previously, the APIs for most popular OSNs are publicly available, allowing anyone to create applications for them. Some are developed by large, reputable organisations but the vast majority are developed by individuals. These applications are not generally tested by the OSN prior to release on the site, so could potentially contain malicious code. Most users implicitly trust applications hosted on OSN platforms. For example, the Secret Crush/My Admirer application spread rapidly around Facebook in 2008. It enticed users to download adware by telling them they have an admirer and promising to reveal their identity once they had downloaded it.

Application development vulnerabilities

53. As with many Web 2.0 applications, the rapid pace of development and the interactive nature of OSNs, and their focus on user-generated content, combine to increase their susceptibility to certain types of security vulnerability. Examples of these include Cross-Site Scripting (XSS) vulnerabilities and Cross-Site Request Forgery (CSRF) attacks.

Chapter 4 - Security controls

Key Principles

- Selection of appropriate security controls and risk mitigation will depend on an organisation's own risk assessment, which should take account of the threat to that organisation and the vulnerabilities associated with the type of OSNs being used
- In general, the most effective security controls are user education and training to raise awareness of the risks and promote good practice

Overview

54. Although it is not possible to eradicate all risks associated with using OSNs, it is possible to substantially reduce them. It is therefore up to organisations to determine, depending on their risk appetite and the likely business benefit, whether to use OSNs, and if so, what type of OSNs they will use, and how they will use them.

55. The main ways organisations are likely to use OSNs can be divided into three: use of ESNs by individuals, use of ISNs by individuals, and use of ESNs (either public ESNs or bespoke designed Internet-based social networks) by organisations. As discussed in Chapter 3, the vulnerabilities described apply differently to the three uses. The recommended security controls will therefore be presented in three corresponding sections.

56. Where Internet-based OSNs are utilised, the security controls listed here assume that the relevant security controls described in GPG 8 (reference [d]), have been applied.

Control measures recommended for individuals using Internet-based ESNs

57. Organisations have several options regarding the use of ESNs, such as Facebook, Twitter and LinkedIn, from their IT systems – they can choose to:

    - Block access to ESNs from corporate IT systems altogether (this may be achieved by technically blocking access to the sites or blocking via a combination of policy and protective monitoring for enforcement)
    - Permit access to only those sites which have perceived business benefit and/or only to those users with a business need to access them
    - Permit access with limited functionality using a specialised device such as a secure web gateway
    - Permit access to all such sites

58. Although blocking access to ESNs may appear to be the most secure option, it should be recognised that many members of staff will access ESNs from outside the organisation, or even from mobile devices within the organisation. This will therefore not remove all risk. Some users may also attempt to use

tunnelling proxy servers to circumvent the block. Organisations may also choose to use social media to engage with their customers (references [h] and [i]). Technologies such as more advanced secure web gateways with fine-grained control of features (e.g. read-only access) may enable appropriate control of social networks within the organisation.

59. If access to ESNs is permitted, the most effective methods of reducing the risks from these technologies are not technical, but behavioural, and it is vital that users are given training on how to use them safely. As many people use OSNs at home, they are likely to use them in the same way if these applications are introduced in the workplace, without considering the different types of information risk or threat sources they are facing in this environment unless they are made aware of the risks. A model end user guide is provided in Appendix A. This may be given directly to staff or modified to reflect departmental policies or as a result of a risk assessment.

60. Protective monitoring strategies will ensure any incidents are detected (for more information see CESG Good Practice Guide No. 13 (GPG 13), Protective Monitoring (reference [w]) and CPNI's ongoing personnel security advice published at www.cpni.gov.uk/advice/Personnel-security1/Ongoing-measures.

61. More information on safe usage of OSNs by individuals can be found online, for example at www.getsafeonline.org and www.fightcyberstalking.org.

62. Table 2 provides the key control measures to protect against the risks posed by an individual's use of ESNs:

Advice	Details	Risks mitigated
Advice to mitigate risks relating to CONTENT		
Limit content posted	• Limit the amount of information users post on OSNs to that which is necessary. For example, it is often not necessary to post full dates of birth and addresses. • Unless there is a strong business case to do so, individuals should not post work-related material on an OSN. • Users should ensure they have not used password reminder questions on other websites, such as banking sites, or offline, to which the answer can be found on an OSN. • As information about an individual posted on different social network profiles and websites can be aggregated, the impact of all of the information about an individual present on the Internet should be considered, not just that found in a single profile.	• Large reduction in risk of identity theft if personal details are not posted. • Reduce risk of information being used to deduce passwords for other accounts. • Reduction in risk of targeted phishing, spear phishing and whaling attacks. • Reduce material available for social engineering attacks.
Maintain separate personal and professional personas	• Advise users to use separate accounts for personal and professional purposes where possible. • If it is not practical to use entirely separate profiles for professional purposes, use 'friend list' features (available on many OSNs, these enable contacts to be grouped into different user-defined categories) to segregate contacts into professional and personal contacts and customise privacy settings to determine what each group can see. • Mandate against signing up with, or publicising, work email address on personal profiles (N.B. may be difficult to enforce).	• Personal opinions not interpreted as official line. • Informal personal comments are less likely to be associated with the organisation the user works for, and so are less likely to damage the reputation of the organisation. • Reduce personnel security vulnerabilities – information on an OSN is less likely to be used to target an individual due to their job. • Email addresses cannot be harvested and used for spear phishing/whaling attacks against an organisation.
Issue guidance on online job	• If the risk assessment shows there is a significant	• Reduced risk to personnel or operational security as makes it

Advice	Details	Risks mitigated
descriptions	personnel or operational security threat as a result of staff declaring their employer or job title on public OSNs, guidance should be issued to advise them how to identify themselves to avoid individuals having to develop their own, possibly flawed, 'cover-story'. • Advise staff in these roles not to form or join overtly work-related networks or groups, or indicate that they know colleagues 'through work'. • Such staff should be advised to inform close friends and family, who are aware of their work, exactly what it is appropriate to discuss online.	harder for threat actors to identify and target relevant individuals.
Use privacy settings	• Encourage users of ESNs to decide what information they want to be viewable to whom, and adjust the privacy settings accordingly. N.B. for reasons described above privacy settings cannot be completely relied upon to protect personal information, but they will be effective the majority of the time.	• Reduced risk of identity theft. • Reduced risk of targeted phishing, spear phishing and whaling attacks. • Reduced risk of effective social engineering attacks based on OSN-derived information. • Mandating privacy settings in the acceptable usage policy will reduce the risk to personnel or operational security, however it will be very difficult to enforce, especially for personal profiles.
Consult site terms and conditions	• Users should read the terms and conditions of sites with which they have accounts to check what the provider can do with user information. If the terms and conditions are considered to be inappropriate, the user can choose to restrict the information they add to their profile or close the account.	• Personal information not unknowingly distributed to third parties.
Online acceptable behaviour policies/codes of conduct	• Produce acceptable online behaviour policies/codes of conduct or make it clear that pre-existing policies apply to behaviour online and on corporate IT systems. For example, the civil service code, which outlines the values expected of all civil	• Reduce the risk of reputation damage or litigation resulting from employees making inappropriate comments about the organisation, or related topics, online or on the corporate IT system.

Advice	Details	Risks mitigated
	servants, is applicable online as well as offline.	
Monitor public spaces on personal OSN profiles	• Advise users to monitor any public space (such as a Facebook 'wall' or an Orkut 'scrapbook') on their profile page and remove inappropriate comments or postings if required.	• Inappropriate material will be removed quickly and will be less likely to damage the reputation of the individual or the organisation they work for. Although the content will not be completely deleted it will be harder to access and much less likely to be found accidentally.
Raise awareness of techniques used by online criminals	• User education to raise awareness of common scams designed to procure personal or login information, and social engineering techniques. • Training programmes can help employees be made aware of how social engineering works and the value of the information they hold. Employees who may be particularly vulnerable to social engineering attacks – those in customer facing roles, for example, or those with access to important assets, such as IT administrators – may be considered for additional training.	• Reduced risk of account being hijacked (both OSN and other accounts, such as online bank accounts). • Reduced risk of successful social engineering attacks against the organisation.
Password security	• Ensure accounts on ESNs are protected by good passwords – avoid dictionary words or strings of consecutive numbers or letters (such as abcdef, 123456 or qwerty), use a mixture of letters and numbers. • Do not use the same password for multiple accounts or re-use passwords on different systems (e.g. a user should not use the same password to protect an OSN account and corporate IT system). • Do not store passwords (or use the 'remember me on this computer' option on sites) on devices, especially mobile devices which are liable to be stolen, such as smartphones and tablets.	• Reduced risk of accounts being hijacked. • Reduced risk of account hijack resulting in compromise of other accounts or systems.

Advice	Details	Risks mitigated
Check for ID hijacking/profile squatting	• Users can run regular searches on their own name. This can be done via traditional search engines, by searching the most popular ESNs or search engine aggregator services such as 123people. • Any incidence of ID hijacking should be reported to the site immediately so the profile can be removed. • There are personal online identity management services available, which will search the Internet and social networking sites for any mention of a particular name or keyword. Some are free whereas others are subscription based. One of the most popular is provided by naymz.com, a professional ESN similar to LinkedIn.	• Limit damage done by ID hijacking. • Online identity management services enable tracking of professional and/or organisational reputations online.
Bandwidth usage limitation or time-based access controls	• Impose a bandwidth limit on traffic from OSNs or time-based access controls on the sites.	• Prevent denial of service of other business critical functions as a result of excessive bandwidth usage for OSNs.
Limit functionality of OSN	• Employ a network access control device such as a secure web gateway to limit the extent to which users can interact with the allowed social networks.	• Prevent inappropriate information sharing.
Embed information legislation for public bodies	• Public bodies must ensure any use of OSNs for business purposes is compatible with their responsibilities under the Public Records Act 1958 and the Freedom of Information Act 2000.	• Ensure legal requirements for keeping public records are met.
Advice to mitigate risks relating to SOCIAL INTERACTIONS		
Consider contacts on OSNs	• Users should consider who they are adding as friends/contacts and avoid adding people they do not know unless there is a valid reason for doing so. In particular, avoid accepting unexpected requests from unknown users by default – investigate the request first. • If the user needs to form links with people he/she does not know well (e.g. to build new professional	• Reduced risk of divulging personal information to strangers. • Reduced risk of social engineering attacks resulting from infiltration of professional networks.

Advice	Details	Risks mitigated
	contacts), it is advisable for them to limit the amount of personal information they share. On some sites, such as Facebook, this can be done by customising the privacy settings for different classes of contacts.	
Modify privacy settings in relation to large groups or networks	• Users joining large groups or networks where not everyone is a close friend/contact should consider adjusting their privacy settings to modify what other members can see.	• Reduced risk of giving away personal information to strangers. • Reduced risk of social engineering attacks resulting from infiltration of professional networks.
Guard against account hijack	• Enable and make use of secure communications (e.g. https) where available. • If a contact acts suspiciously, sends unexpected links, or requests money it is advisable for users to check with them "offline" to ensure it really is them. • Users should be wary of emails purporting to come from OSNs asking them to log in, and should check any links in such emails carefully. • Users should also be alert for signs that their own accounts may have been compromised – some sites have "account management" features which detail when a user last logged on, so it is possible to check whether the account has been accessed by someone else in the interim. Other warning signs include alterations to profile pages, new people on contact lists, and finding that password(s) do not work. • If an account has been compromised, change the password, report the compromise to site administrators and warn contacts.	• Reduced risk of falling victim to financial fraud, loss of personal data or malware/phishing attacks as a result of a contact's account being hijacked. • Reduced risk of a user's account being hijacked as a result of interception or a successful phishing attack. • Early detection of compromised accounts will limit any potential damage to their contacts and own reputation.
Advice to mitigate risks relating to MALWARE, PHISHING and SPAM		
Apply anti-malware security controls	• Security controls designed to combat the risk from malicious code should be applied to all systems	• Reduced risks posed by OSN-derived malware.

Advice	Details	Risks mitigated
	with connections to Internet-based OSNs, including mobile devices. For more details see GPG 7 (reference [c]) and CESG Good Practice Guide No. 10 (GPG 10), Remote Working (reference [x]).	
Phishing awareness and user education	• Awareness and user education on the problem of phishing scams on OSNs. Warn users to be wary of all messages or applications which ask them to reveal personal details. • In addition to limiting the amount of personal information published by users, encourage them to be aware of what information they have published. • If messages or emails claim to contain links to sites where a user regularly logs in, it is safer to either type the address into the address bar or use a saved URL (such as from the favourites tab on a browser) to access the site to minimise the risk of logging on to a fake site. • Users should be particularly wary of shortened URLs. • The impact of successful phishing attacks can be minimised by avoiding password re-use.	• Raising awareness of phishing attacks will reduce the likelihood that users will be susceptible to them. • If users are aware of what personal information they have made public, they are less likely to be susceptible to targeted phishing attacks using that information. • Typing an address, or using a saved URL, instead of clicking on links, will reduce the chances of users being lured to fraudulent sites. • URL expansion and preview services should be used to check shortened URLs; these verify the final destination of abbreviated URL links from the various URL-shortening services. • Unique passwords ensure that a successful phishing attack can only compromise a single account.
Limit privileges on accounts used to access OSNs	• If access to Internet-based OSNs is permitted from an IT system, privileges for normal users on that system should still be limited to those which are necessary. For example, blocking the download of executable files from the Internet for normal users is strongly recommended unless there is a clear business reason not to do so. • Limit access to ESNs to accounts without administrator privileges.	• Reduce risk of users inadvertently installing or running malicious code. • Limiting access to accounts without administrator privileges may limit damage from malware.

Advice	Details	Risks mitigated
Restrict use of third party applications	• If there is no perceived business benefit, the use of third party applications on OSNs could be restricted.	• Reduced risk of deriving malware from third party applications. • However, such a ban may be hard to enforce.

Table 2: Key control measures to protect against the risks posed by an individual's use of ESNs

Control measures recommended for ISN usage

63. The risks posed by the use of an organisation's own ISN are substantially lower than the risks posed by content posted on public ESNs. Organisations concerned about the potential risks associated with ESNs, but who feel that staff may benefit professionally from the use of social networking tools, may therefore choose to set up their own ISN. However, doing this will have cost implications, and it will also limit the people who can join – e.g. colleagues and suppliers in other organisations will not be able to join the ISN – which may reduce the business benefits. It should also be remembered that organisations are responsible for the actions of their employees on internal corporate IT systems, so acceptable use and behaviour policies are still important. These control measures should be contained within the organisation's policy on acceptable usage of the ISN.

64. Readers are advised to consult their legal advisors to fully understand their particular legal situation.

65. Table 3 provides the key control measures to protect against the risks posed by the use of ISNs:

Advice	Details	Risks mitigated
Advice to mitigate risks relating to CONTENT. Also consider the following from Table 2: Password security, online acceptable behaviour policies/codes of conduct, embed information legislation for public bodies		
Limit content posted	• Limit the amount of information users can post on the ISN to that which is necessary for professional purposes. • Advise users to avoid giving additional personal details.	• Reduced risk of identity theft and personnel security vulnerabilities if information is leaked outside the ISN.
Define maximum security classification of data which can be posted on an ISN	• ISNs which are to handle information with high security classification should be accredited to this level and the maximum protective marking of any information should be clearly displayed on this site.	• Reduce risk of sensitive information being released via publication on an ISN.
Legal issues regarding website development	• Where sites collect or publish personal information, ensure the system complies with the Data Protection Act 1998. • Public bodies must ensure compliance with the Freedom of Information Act 2000 and Public Records Act 1958. • Ensure sites do not infringe copyright legislation. • Comply with Disability Discrimination Act when designing all websites (the Office for Disability Issues offers introductory information on their website: http://www.odi.dwp.gov.uk).	• Ensures sites are legally compliant and accessible. • The Information Commissioner's Office and Intellectual Property Office have more information on compliance with the Data Protection Act and copyright legislation; refer to http://www.ico.org.uk and http://www.ipo.gov.uk for further information.

Table 3: Key control measures to protect against the risks posed by the use of ISNs

Control measures recommended for use of public and bespoke ESNs by organisations

66. Although in many ways these control measures overlap with those for individuals using Internet-based ESNs, there are some key differences. For example, organisations are not at risk of identity theft in the same way as individual users. However, there are additional risks when an organisation launches either a profile on a public ESN or its own ESN, such as the damage which would be done to the reputation of the organisation if the profile or site were associated with the propagation of malware.

67. Readers are advised to consult their legal advisors where appropriate.

68. Table 4 provides the key control measures to focus on to protect against the risks posed by the use of public or bespoke ESNs by organisations:

Advice	Details	Risks mitigated
Advice to mitigate risks relating to CONTENT. Also consider the following from Table 2: Consult site terms and conditions, raise awareness of techniques used by online criminals, password security, online acceptable behaviour policies/codes of conduct, embed information legislation for public bodies.		
Policy and guidance on social media usage	• Organisations should develop a clear policy on the use of social media (including OSNs) for professional purposes. There are several examples of good practice in this area available from inside Government and from Industry. • Identify a central individual or group who can be responsible for monitoring and recording OSN usage by the organisation. This role may be best performed by a member of the corporate communications or digital engagement team.	• Clear guidance on how technologies are to be used reduces risk of reputation damage by publication of misleading or incorrect information, promotes a coherent corporate image and maximises business benefit. • Co-ordinating use of social media will allow sharing of good practice and monitoring of the organisation's online presence (official or unofficial).
Legal issues regarding website development	• Where sites collect or publish personal information, ensure the system complies with the Data Protection Act 1998. • Public bodies must ensure compliance with the Freedom of Information Act 2000 and Public Records Act 1958. • Ensure sites do not infringe copyright legislation. • Comply with Disability Discrimination Act when designing all websites (the Office for Disability Issues offers introductory information on their website: http://www.odi.dwp.gov.uk).	• Ensures sites are legally compliant and accessible. • The Information Commissioner's Office and Intellectual Property Office have more information on compliance with the Data Protection Act and copyright legislation; refer to http://www.ico.org.uk and http://www.ipo.gov.uk/ for further information.
Check for ID hijacking / profile squatting	• Organisations should run regular searches on their own name. This can be done via traditional search engines or by searching the most popular ESNs. • Any incidence of ID hijacking should be reported to	• Early detection will limit damage done to an organisation's reputation by ID hijacking. • Online identity management services also enable tracking of professional and/or organisational reputations online.

Advice	Details	Risks mitigated
	the site immediately so the profile can be removed. • The use of personal online identity management services should be considered if this is a particular concern. These will search the Internet and social networking sites for any mention of a particular name or keyword. Some are free whereas others are subscription based.	
Advice to mitigate risks relating to MALWARE – Consider the following from table 2: Apply anti-malware security controls, limit privileges on accounts used to access OSNs, restrict use of third party applications.		
Use standalone PCs /airgapped systems to access Internet-based OSNs	• If the risk to the Confidentiality, Integrity and Availability of data on system from malware is considered too high, standalone PCs separate networks can be used to access OSNs.	• Any malicious code will not infect the main IT system. • Need to consider the business implications of doing this – potential cost is one disadvantage. It may be impractical if data needs to be transferred between the standalone PCs and main system regularly or quickly, as secure processes will need to be put in place for doing this, such as a sheepdip system to scan for malware. The practicality will also be determined by how frequently and widely OSNs are used, e.g. it is much more feasible if access is required infrequently or by a limited number of staff, than if many staff need regular access.

Table 4: Key control measures to focus on to protect against the risks posed by the use of public or bespoke ESNs by organisations

Appendix A: End User Guide

The following End User Guide is provided as a model which organisations can use to produce guidance for staff. Depending on the organisation and the outcome of the risk assessment it may be copied directly or modified to suit a Department's requirements and acceptable usage policy. It does not remove the need for organisations to produce their own risk-based policies on OSN usage.

End User Guide

Introduction

Internet-based social networking sites, such as Facebook, LinkedIn, and Twitter, are popular applications which allow individuals to create a profile containing personal information and interact with other users. However, there are many risks associated with the use of these sites. Fortunately, many of these risks can be substantially reduced by following safe usage practices. This user guide is aimed at users of Online Social Networks (OSNs) and outlines the main risks and safe ways of using these sites.

Risks

1. Publishing personal information on your OSN profile may make you susceptible to identity theft. Dates of birth, full names and home addresses are key pieces of information for identity fraudsters. Many users also publish the answers to common security or password reminder questions (such as 'my first school') which can put other accounts, such as online bank accounts, at risk of account takeover. Some sites 'own' any data posted on them, and may reserve the right to sell your details to third parties – check the terms and conditions/usage policy.

2. Posting some information can also put your personal safety at risk. For example, your address, phone number, details of your schedules and plans and information about your family could be used to target you for attacks. Location based information can be posted on social networks, especially from GPS-enabled mobile devices, which tells others exactly where you are. Burglars may also use information on social network profiles, such as holiday plans or new purchases, to plan burglaries.

3. Phishing attacks, where a criminal masquerades as an entity with the right to request sensitive information such as a bank, are increasingly being delivered on social networking sites instead of by email. Profile pages are also being used to research information about an individual so attacks can be specifically targeted at them and hence more likely to succeed. Many phishing attacks are being launched with links to fake login pages for social networks to obtain users' login details and hijack their social networking accounts.

4. Most social networking sites provide an informal environment where it is easy to share views and update content. However, some users have damaged their career or the reputation of their employer by making inappropriate comments. Remember that, depending on privacy settings, your posts may be visible to all your contacts, networks and groups, or even other users and search engines.

5. Social engineering involves manipulating people into performing actions or revealing information they should not, for example their login details for the

corporate IT system. In order to do this, perpetrators need information about the individuals and/or the organisations they work for. This can often be obtained from social networks, especially if colleagues have set up groups based on their workplace and declared that they know each other 'from work'.

6. Social networking sites can be forums for bullying and harassment online (known as cyberbullying, cyberharassment or cyberstalking). Attackers may also use these sites to identify or target their victims due to the large amount of personal information some users post. Such incidents may take place online only or may spill over into other areas of life.

7. Account hijacking is a growing problem on social networking sites. Criminals obtain users' login details from phishing attacks or by 'dictionary attacks', which involve trying the most common passwords. Once they have access to a user's account, criminals may use this to propagate malware or spam or obtain personal information from the compromised account and people on that user's contact list. A common scam is for a criminal to hijack an account and send messages to the user's friends claiming to be stranded and request money.

8. Malicious code ('malware') spreads rapidly around Online Social Networks. Beware of links posted on friend's profile pages or sent to you in messages – if their account has been hijacked or they have been infected by malware it may not have been put there by them. In addition, many URLs are now 'obfuscated', meaning the full address of the website cannot be seen until the link is clicked on. This is often done to shorten long URLs so they can appear in character limited posts, such as on microblogging sites like Twitter.

9. Third party applications are usually written by independent developers, not by the social network provider. Although they can often be useful or fun, and most are safe, they are not checked or certified by the social network before launch. Some have included malicious code or links to malicious sites. Application developers may also be granted access to some of a user's personal information when they use the application.

Stay safe

10. Don't post more personal information than is necessary. For example, other users probably don't need to know your date of birth or home address – if you do need to give such details to any of your contacts, it is wise to give them to individuals offline or in private messages. Consider the security implications of posting details of your exact, real-time location. Share online safety guidelines with friends and family so they also can follow best practice (such as Get Safe Online's Get Safe Top 10) and keep your community safer.

11. Check your privacy settings. Who can see your profile information? It is worth taking the time to understand each setting control and making a proactive decision about who you want your information to be visible to? Many sites allow you to classify your contacts (e.g. 'friends' and 'professional contacts') and set

independent privacy controls for each. If you are a member of large groups or networks it may be wise to restrict what other members of these groups can see. Do you want your profile indexed in search results on the site or even on Internet search engines such as Google?

12. Choose your friends carefully! Social networking sites can be a great way of making new contacts, but beware of giving away too much personal information to people you do not know. If you do have individuals on your contact list you do not know well, consider restricting what they can see using your privacy settings. In addition, watch out for suspicious or unusual activity or language from your friends, as this may be a sign that their account has been hijacked.

13. Be cautious when using third party applications. Remember they could contain malware, or link to sites containing malware. Be particularly wary if you are prompted to install an update to another program when trying to use an application – this is a common trick used to install malware on a user's computer. It may also be possible to control what information is passed on to the developers of third party applications using your privacy settings.

14. Read the terms and conditions of any sites you sign up to. Ensure you are aware of who owns data posted on the site and what the owners of the site can do with your data.

15. Think about any information you post relating to your job or employer. Is the information in any way sensitive? Would it be of interest to competitors or journalists? In addition, information can become more sensitive by virtue of aggregation. Be especially aware of this when using professional networking services. Once information is posted on the Internet it is essentially impossible to completely delete it. Social network profiles are often not as private as users believe – be very wary about venting frustrations about work in public comments, as it is highly likely your colleagues or boss may see them. If at all possible, maintain separate personal and professional personas online.

16. Also consider whether your occupation may make you a target for any form of attack or harassment, or whether publicising your occupation may threaten the effectiveness with which you or your colleagues can do your job. If this is the case, limit the personal information you post and what you say about your work. If in doubt, ask your employer for advice. If it is inadvisable to discuss your work online, let your close friends and family know via another means outside of the OSN so they can avoid inadvertently saying something inappropriate.

17. To avoid becoming the victim of phishing attacks, do not click on obfuscated URLs unless you are very sure of the source. Use URL expansion and preview services to verify the safety of URLs in abbreviated links before clicking on them. If the link is to a site you visit regularly, such as your bank or an online store, type the URL or use a bookmark to ensure you are accessing the

genuine site. Security tools offered by certain sectors such as online banking and retailers may assist in guarding against certain types of attack.

18. Guard against hijack of your own social networking accounts – if you click on a link which asks you to log in to the site, type the site URL or use a bookmark to ensure it is the correct site and not a phishing scam. Signs of account hijack include passwords not working and activity or logins on your account at times when you weren't online. If your account is hijacked, change your passwords and warn your contacts that your account has been compromised.

19. As is good practice for all Internet usage, ensure the computer used to access these sites has anti-virus software running and that virus definitions are up to date. Also ensure that software running on the computer (such as the operating system and programmes such as Adobe Flash, Java and Adobe Acrobat) are up to date with the latest patches and updates.

20. If accessing social networking sites from your own computer, access them from an account with user privileges only, not administrator privileges. This will minimise the privileges available to any malware which is downloaded and so may limit the damage it can cause.

21. Use good passwords for all online accounts:

    a. Use a mixture of upper and lowercase letters, numbers and special characters; avoid dictionary words or strings of letters and numbers such as qwerty, 12345678, or abcdefg.

    b. Do not use the same password for more than one account – doing this means that compromise of one password will compromise multiple accounts. Never use the same passwords for Internet accounts and corporate IT systems.

    c. Change passwords regularly.

    d. Avoid storing passwords on computers (this includes using the 'remember me' function on sites), especially when using mobile devices (smartphones, tablets etc.) which are at high risk of theft, as theft of the device may lead to account compromise.

References

[a] HMG Security Policy Framework. Available at: http://www.cabinetoffice.gov.uk

[b] HMG IA Standard No. 1 & 2, Information Risk Management, Issue 4.0, April 2102 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.

[c] CESG Good Practice Guide No.7, Protection from Malicious Code, Issue 1.1, October 2012 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.

[d] CESG Good Practice Guide No.8, Protecting External Connections to the Internet, Issue 1.0, March 2009 (Not Protectively Marked). Available from the CESG IA Policy Portfolio.

[e] Internet Access – Households and individuals, 2013 – Office for National Statistics; http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2013/stb-ia-2013.html

[f] Social Networking: The UK as a Leader in Europe – Office for National Statistics; http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/social-networking--the-uk-as-a-leader-in-europe/sty-social-networking-2012.html

[g] Top Sites in United Kingdom; http://www.alexa.com/topsites/countries/GB

[h] Government Digital Strategy, November 2012; http://publications.cabinetoffice.gov.uk/digital/strategy

[i] Social media guidance for civil servants, May 2012 – Cabinet Office and the Home Office; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62361/Social_Media_Guidance.pdf

[j] Digital by Default Service Standard; https://www.gov.uk/service-manual/digital-by-default

[k] 2013 Norton Report: Cost per Cybercrime Victim Up 50 Percent; http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01

[l] Annual Fraud Indicator 2013, 6 June 2013, National Fraud Authority; https://www.gov.uk/government/publications/annual-fraud-indicator--2

[m] Raising awareness about over-sharing; http://pleaserobme.com/why

[n] Using Facebook or Twitter 'could raise your insurance premiums by 10pc'; http://www.telegraph.co.uk/finance/personalfinance/insurance/7269543/Using-Facebook-or-Twitter-could-raise-your-insurance-premiums-by-10pc.html

[o] Dating coach shows how to get classified military intel using social engineering; http://www.theverge.com/2013/8/4/4585994/hacking-people-is-easy-a-dating-coach-shows-how-easy-it-is-to-get-classified-intel

[p] Social Engineering: Understanding the Threat, CPNI. Available from www.cpni.gov.uk.

[q] Online Reconnaissance, CPNI, May 2013. Available from www.cpni.gov.uk.

[r] Guidelines on prosecuting cases involving communications sent via social media, The Crown Prosecution Service.; http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/index.html

[s] Fraud increase driven exclusively by identity crime; www.cifas.org.uk/fraudtrendstwentytwelve

[t] The Imperva Application Defense Center White Paper on Consumer Password Worst Practices. Available at www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

[u] "Who is tweeting from the NSA's parking lot?"; http://www.computerworld.com/s/article/9232476/Who_is_tweeting_from_the_NSA_39_s_parking_lot_

[v] The Evolution of Phishing Attacks: 2011-2013; http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf

[w] CESG Good Practice Guide No.13 – *Protective Monitoring*, Issue 1.7, October 2012. Available from the CESG IA policy portfolio.

[x] CESG Good Practice Guide No.10 – *Remote Working*, Issue 2.2, September 2012. Available from the CESG IA policy portfolio.

The CESG IA policy portfolio is available from the CESG policy website (http://cesgiap.gsi.gov.uk) and the CPNI partner extranet (http://protect.cpni.gov.uk/cps/rde/xchq/cpniextranet/hs.xsl). CPNI guidance on personnel security can be found at http://www.cpni.gov.uk/advice/Personnel-security1/.

Glossary

Account hijack – a situation where a user's login details are obtained and used to access their account, without their permission.

API – Application programming interface. A set of protocols implemented by a software program to enable interaction with other software.

Botnet – A network of computers ('software robots' or 'bots') connected to the Internet that are controlled remotely and interact to accomplish some distributed task. Malicious software often compromises machines without a users knowledge and turns the machine into a bot.

Cyberbullying, cyberstalking and cyberharassment - The use of the Internet or other electronic means to support deliberate hostile behaviour that is intended to harm others. The three terms are used somewhat interchangeably, although cyberbullying often refers to such actions perpetrated by or towards children whereas cyberharrasment and cyberstalking describe incidents directed at adults. This may take place solely on the Internet, or may be linked to incidents offline.

CSRF – Cross-site request forgery. CSRF attacks work by tricking a user's browser into making third-party requests to websites without the user's knowledge. As the user has already authenticated themselves to the site, the site carries out the requested transaction – which could involve revealing login details, authorising a credit card transaction, or transferring money.

Denial of Service – the prevention of authorized access to a system resource or the delaying of system operations and functions. This may result from either accidental or malicious causes.

ESNs – External social networks. Internet-based public social networks, may be open to anyone to join or may have certain criteria for membership.

ID Hijacking/profile squatting – the setting up of a profile purporting to belong to another individual without their permission.

ISNs – Internal social networks. Organisation-specific closed social networking sites accessible only by members of the organisation.

Malware – Malicious software. Software designed to infiltrate or access a computer without the consent of the user.

Mashup – an application that combines data or functionality from two or more sources to create a new service.

M**obile devices** - personal electronic devices, such as laptop computers, tablet computers and mobile phones.

OSNs – Online social networks. Applications which allow individuals to create a profile containing personal information and interact with other users.

Phishing – the fraudulent process of attempting to acquire sensitive information such as login and credit card details by masquerading as an entity with the right to have that information in an electronic communication.

Privacy settings – Most OSNs have modifiable settings which allow users to alter how much of their personal information is available to their contacts, other users, third party applications and search engines.

Sheepdip – a computer which is isolated from the main IT system and is used to screen incoming media or devices for viruses, malware, etc.

Social media – Applications which focus on the creation and exchange of user-generated content. In contrast to the 'one-to-many' dissemination of content with traditional websites, they enable 'many-to-many' style collaboration.

Social engineering - Social engineering refers to the techniques and tactics used to extract information from people, often without them realising they are being duped. This may be business information, such as financial market details and corporate financial information, or personal information.

Social network aggregators - 'mashups' which display information from accounts on multiple OSNs and combine several profiles for a user into one single profile.

Spear phishing - highly targeted phishing attacks against an individual or specific group of individuals, such as members of an organisation, employees of a company, or users of a particular website. The attacks generally take the form of a message which appears to come from someone with whom the target already has an established relationship. The aim of such attacks is to gain specific data or access to systems which only these individuals can provide.

Threat actor - A person, or group of people who are in a position to exploit a vulnerability. The threat actor is a person who actually performs an attack or, in the case of accidents, will cause the accident. For more information, see HMG Information Assurance Standard No. 1, available from the CESG IA policy portfolio.

Threat source – the person or organisation that desires to breach security and ultimately will benefit from a compromise in some way.

URL-shortening – the process by which a website is made available from a very short URL in addition to the full URL. Shortened URLs are particularly popular in microblogs where there is a strict character limit.

Virtual worlds - computer-based simulated environments in which users can interact with each other, such as World of Warcraft and Second Life.

Web 2.0 – the 'second generation' of collaborative, interactive, information-sharing, user-centric web applications, on which most social media services are based.

Whaling - phishing attacks which specifically target high profile individuals or senior members of organisations or companies.

Worm – An independent programme which replicates across network connections. In contrast to a virus, it can generally do this without an external stimulus (such as a user pro-actively running an infected file).

XSS – Cross-site scripting. XSS vulnerabilities enable users to inject client-side script into web pages which are then viewed by other users, without it being properly sanitised. Injection of malicious content in this way can be used for many purposes, including bypassing normal access controls and gaining access to a user's cookie or other information.

CESG's Good Practice Guides are issued by the UK's National Technical Authority for Information Assurance with the aim of informing intended recipients of the general security issues they should consider in their approach to information and communications technologies. They are not a replacement for tailored technical or legal advice on specific systems or issues. GCHQ/CESG and its advisers accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed upon this Guidance

IA
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Fax: +44 (0)1242 709193
Email: enquiries@cesg.gsi.gov.uk