

Busy Reader Guide for Managing The Risk From Online Social Networking





Introduction

Online social networks (OSNs) are popular interactive applications which allow users to create a personal profile and build and maintain links with other users. They are accessible from personal computers and personal electronic devices (PEDs) such as mobile phones, and their use can offer significant business benefits. However, the speed of development of these applications and the focus on user-generated content means their use can carry significant risks.

This busy reader guide is intended for a senior readership to assist in assessing the risks posed to the business by the use of Internet-based social networking sites and provides strategic guidance on managing the risk associated with their use. It also advises all users of the risks posed by the use of OSN applications. More detailed information on risks and control measures is provided in CESG Good Practice Guide 27 – *Managing the risk from online social networking*.

Risks to consider

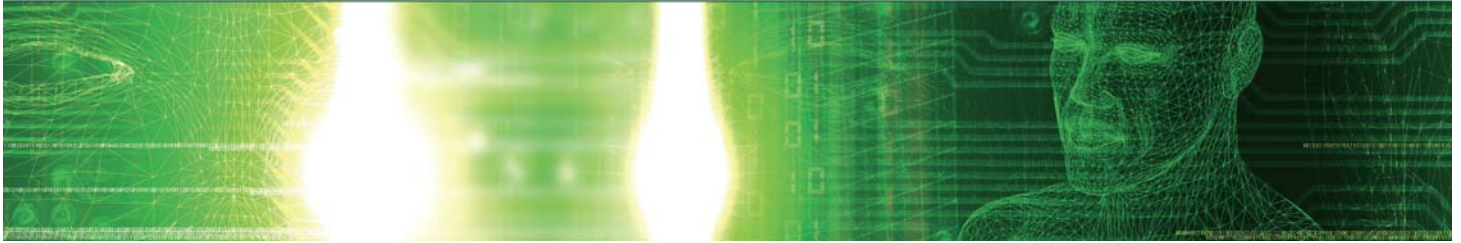
Disclosure of personal data - the publication of personal information on OSNs can make users susceptible to identity theft. It can also result in takeover of other accounts, such as online bank accounts, as users often include the answers to security or password reminder questions on their OSN profiles. There may be data protection issues, as some OSNs 'own' the data posted on them and make it available to others for a fee – this is detailed in the terms and conditions.

Personal safety and cyberharassment - information posted on OSNs, such as a home address and family details, may be used to target individuals for attacks in the real world. Some sites can also be updated with a user's real-time location. OSNs provide a forum for hostile behaviour online, and employers have a duty of care to ensure staff are not subjected to such harassment or bullying in the workplace.

Phishing – this is the process of attempting to acquire sensitive information, such as login or credit card details, by masquerading as an entity with the right to have that information. OSNs are increasingly being used for phishing attacks in two ways: to deliver the attacks, and to research information about an individual so attacks can be specifically targeted at them and hence more likely to succeed.

Social engineering – this is the manipulation of individuals into performing actions or divulging information, for example login details to a corporate IT system. Convincing attacks require a good knowledge of the individuals and the organisation they work for, which can often be obtained from OSNs.

Reputational damage, corporate liability and release of sensitive information – OSNs enable rapid content sharing. However, once information is published on the internet it is in the public domain and essentially impossible to recall. Individuals may publish views which embarrass an organisation or are



interpreted as being those of the employer, especially if they detail their job description or employer in their profile. Organisations have vicarious responsibility for the actions of their employees on corporate IT systems. OSNs also provide a medium through which sensitive information may be published. Unclassified information posted on OSNs may also become more sensitive due to the effects of aggregation.

Timewasting/bandwidth issues - employees may make excessive use of OSNs for private purposes during work time. In addition, some features of OSNs (such as the ability to host videos) can be bandwidth-intensive.

Malicious code – ‘Malware’ and links to malicious websites spread rapidly across OSNs and malware is increasingly being written to specifically target the sites. The rapid rate of development of these sites can also be to the detriment of security and they are frequently found to have vulnerabilities which make them more prone to malware attacks. It is also possible for third parties to develop applications for most OSNs. These are not generally checked prior to launch, so can contain malicious code. For more information, see the busy reader guide - *Protection from malicious code*.

Advice

By far the most effective way of reducing the risks posed by OSN usage is educating users about the risks and safe practice. The corporate security policy should include an online code of conduct for staff detailing

regulations for OSN usage from corporate IT systems, including any technical or policy controls on the amount of time or bandwidth used on these applications. Security controls to guard against malicious code should be applied, and the following advice given to users:

1. Customise privacy settings to ensure your private information is only viewable to people you know.
2. Do not post sensitive or personal information, regardless of privacy settings.
3. Only form links with people you know or have been introduced to by someone you trust, be wary of strangers who make contact.
4. Do not click on links unless you have a good reason to trust the source. To avoid becoming the victim of phishing attacks, do not follow links from emails but type the URL into the browser bar or use a saved URL if navigating to a favourite site such as a bank or online store.
5. Use good passwords, not dictionary words or strings of letters or numbers. Do not re-cycle passwords or use the same passwords for multiple accounts.
6. Do not disclose sensitive information about employer or job online. Where possible maintain separate professional and personal online personas.

UNCLASSIFIED

The copyright of this document is reserved and vested in the Crown.

IA
CESG
B2h
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

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

© Crown Copyright 2010. Communications on CESG telecommunications systems may be monitored or recorded to secure the effective operation of the system and for other lawful purposes.

UNCLASSIFIED