

Industry Security Notice

Number 2011/01

Subject: ADVICE ON THE USE OF SOCIAL MEDIA AND NETWORKING SITES BY MOD CONTRACTOR STAFF

Introduction

1. The Ministry of Defence (MOD) is aware of the prevalence of social networking sites and their use by individuals. Whilst the MOD views the use of such sites as an important channel for social interaction and by no means wishes to restrict any individual's access to such sites, employees or associates of MOD contractors should be aware of the threats that their use can bring.

Issue

2. This advice is issued to assist MOD contractors' to inform their staff on the security issues surrounding their online presence, particularly the use of social media, both within the workplace and socially.

Action by Industry

3. The information in this Industry Security Notice should be disseminated as widely as possible within companies to ensure staffs are aware of the threats associated with the use of social media.

Background

4. Modern technology and media has provided individuals with new and valuable tools to enhance their personal and social lives, such as social networking sites including 'Facebook', 'Bebo', 'LinkedIn' and 'MySpace'; news and media sites; blogs and fora. Whilst these can actively enhance an individual's quality of life and provide a forum for the exchange of ideas there are attendant risks and vulnerabilities involved with their use.

5. Awareness within the defence contractor community of the traditional protective security measures associated with the protection of MOD information and assets is generally high, effective and well established. However, it is also vital to consider the more 'novel' forms of threat in order, not only to protect information assets but in particular a company's most valuable asset, its people.

6. The security of assets and personal information is valuable both in our working and personal lives, the compromise of which can rapidly make life difficult or in extreme cases, dangerous.

7. The MOD has no desire to discourage individuals from using these tools but we feel it is important that everyone should be fully aware of what information they need to safeguard in order to protect themselves, their families, their employers and the MOD information they have responsibility for. It is worth remembering that whether at work or home, MOD contractor staff are covered by the ambit of the Official Secrets Act.

The Threat

8. The information that is provided to social networking sites etc. is usually gathered and used for perfectly legitimate and harmless purposes. However, there are those who wish to gather personal and work related information for illegal, improper or illegitimate purposes. The majority of these wish to use information primarily to engage in criminal acts, such as identify theft, illegal immigration and financial fraud. There are however, other groups who wish to gain information for espionage or terrorist purposes or for use in adverse media reporting. In all cases it can involve a threat to a company, individuals, their families' safety, livelihood or in the wider world, MOD capabilities and operations.

9. The emergence of social media as part of an individual's daily life and the use of web based tools has greatly increased the level of vulnerability. The internet is available to almost everyone worldwide and once information is published it is impossible to retract. E-mails can be intercepted and once delivered the sender has no control over where an e-mail is forwarded.

10. The use of blogs and social networking sites is an area of particular concern as the security of such sites is often not well understood by users. Very often the default security settings allow everyone to see submitted information. Also there is usually minimal control over the security settings of those accepted as 'friends' so information shared with them may be more widely available than originally intended. The security of online blogs may also not adequately be controlled and supposed 'members-only' areas can easily be infiltrated by those with ulterior motives.

11. A worrying trend is the establishment of web based groups which are actively recruiting members based on the level of security clearance they possess, such as LinkedIn's 'DV – Use it or lose it' forum. As membership of such groups automatically identify a user as being in possession of a security clearance it may bring into question that individual's judgement and fitness to possess a clearance in so identifying themselves. The identification of such an individual would also provide valuable information to a hostile intelligence service and would enable them to potentially build up a picture of current projects by identifying those in certain fields who openly 'advertise' their level of clearance. The identification of individuals involved in certain areas of research may also be of interest to some single issue pressure groups and could lead to active targeting of the individual and/or their families.

What information is wanted?

12. Information is always at a premium in the criminal and espionage world. Identified below are the main categories of information that could be at risk.

- a). **Personal Information** - Items of information which can be used to take advantage of a company, individuals and their families can include:
- Full Names
 - Date/Place of Birth
 - Address
 - Telephone Numbers
 - National Insurance Number
 - Passport Details
 - Qualifications
- b). **Account Details** - Criminal groups, single issue pressure groups, hostile intelligence services or terrorist groups may also try to gain access to online or telephone accounts using information such as:
- Account Numbers.
 - Logins/User IDs.
 - Passwords.
 - PIN Numbers.
 - Memorable Phrases.
 - Security Questions.
 - Online Profile Details.
- c). **Company Information** - Competitors or hostile intelligence services, terrorist organisations, single issue pressure groups or media organisations may seek to gain sensitive details about a company, its business, and the physical details of its premises or security measures beyond that which is already in the public domain. Information such as this could enable the company premises to be targeted or lead to adverse or inaccurate media reporting. Contractors should warn employees to be wary about publishing details about the company, its work and facilities. Information that can be used by hostile elements includes:
- Company Name/Location.
 - Work Telephone/e-mail.
 - Position/Role.
 - Access to Protectively Marked Material or Assets.
 - Areas of expertise.

NOT PROTECTIVELY MARKED

d). **Operations** - If you are involved in directly supporting MOD operations, information protection becomes even more important and as a corollary information gathering attempts by hostile agencies or groups become more determined. Information that will be of interest to these groups includes:

- Operational Programme.
- Deployment Details.
- Capability Shortfalls.
- Casualty Details.
- Morale.
- Mission Specific Information.

Information such as this can be used by an enemy in countering our operations, putting lives and assets at greater risk. It may also damage our credibility with our allies and possibility lead to a withdrawal of their support.

How can information be protected?

13. There are a number of simple steps that a company and individuals can take to protect themselves and information when employees are online:

a). **Social Networks & Blogs**

- Understand and apply security settings, remembering to periodically check them to ensure that any provider initiated changes have not invalidated their security settings.
- Consider disabling functions such as Facebooks 'places I have checked into' to avoid giving away the users location.
- Choose online 'friends' carefully and be circumspect in the information shared with them.
- Only post items that would be acceptable to family, friends or colleagues.
- Do not post any personal information on social network sites etc that might be used by individuals for the purposes of identity fraud or other illegal activity.
- Make sure photographs do not unintentionally give away information that may need protecting, such as locations, passes, operational information, protectively marked or commercially sensitive assets or equipment, computer screens or documents.
- Do not give out unnecessary info registering with sites or blogging.
- Do not discuss planned or current operations or equipment deployments.
- On professional and technical forums avoid inadvertently giving out sensitive technical information.
- If submitting reviews for technical publications on sites such as Amazon be wary of indicating the level of your expertise.
- Individuals should not identify themselves as being an employee of a defence contractor, the type of work that they perform, or that they have been granted a security clearance.

NOT PROTECTIVELY MARKED

14. Finally, if you or your staffs become aware that sensitive information has been posted on the internet, immediately inform your Company Human Resources department or Security Officer as applicable so that appropriate action can be taken.

Further information:

15. Further advice and guidance may be found on the Information Commissioner and CPNI websites at:

<http://www.informationcommissioner.gov.uk/Youth/section3/intro.aspx>

<http://www.cpni.gov.uk/advice/Personnel-security1/Online-social-networking/>

Conclusion

16 The risks from online targeting have become greater as we increase the depths and complexities of our online lives. Blogging and the use of social network sites can be an effective way of communicating and networking with friends, family, professional contacts or colleagues and can be fun. However, it is important to remember that the information provided could be used by unscrupulous individuals against you or you family, your company, your colleagues and friends or the UK Armed Forces. Always remember when using these services to be cautious with whom information is shared. It is second nature to safeguard information when in work; make sure you act with the same diligence online or in any public fora.

Validity / Expiry Date: Until further Notice

