

NOT PROTECTIVELY MARKED

**SCOTTISH  
CRIME &  
DRUG  
ENFORCEMENT  
AGENCY**



**Scottish Business Crime Centre Liaison Unit**

**Bulletin 02/2011**

**Social Networking Risks and Smart Phones**

**May 2011**

© Copyright SCDEA 2011. All rights reserved.

NOT PROTECTIVELY MARKED

## **Introduction**

This bulletin is issued by the Scottish Business Crime Centre Liaison Unit (SBCC) of the Scottish Crime and Drugs Enforcement Agency (SCDEA). It is devised with the aim of bringing about preventative or remedial action. We recommend you use this bulletin to compliment existing knowledge and support ongoing improvements to protection of your business and staff.

The SCDEA promote effective business crime information/intelligence sharing between the SCDEA and the Scottish business community. Our aim is to reduce the harm caused by serious organised crime and to make Scotland a hostile environment for serious organised criminals.

## **Social Networking**



Social networking websites have become highly prevalent in today's society with individuals exposing their daily lives and personal details on the internet. Websites such as Facebook and Twitter have recently come under huge media coverage and legal argument surrounding their website content and the subsequent disclosure of publishers' identities.

Social networking websites, by design, encourage users to publish details of their movements, intentions, personal details and photographs, giving scant disregard to the possible criminal intentions of others. There is a much misaligned status to the acquisition of a high number of 'friends' or 'followers'.

These sites promote and encourage the acceptance of any friend or follower requests. Many such requests may be from unknown persons and once "befriended" may access additional personal details posted by the user. It is the responsibility of the account owner to moderate their own security settings to ensure only appropriate information can be accessed by persons known personally to them.

A substantial amount of personal information can be available through open source research (information that is freely and publicly available on internet) e.g. employment, social status or family. This information can be invaluable to serious and organised criminals impacting both personally on an individual and to commercial environments.

Social networking information shared by individuals or their friends and/or relations can be collated by criminals to build an accurate picture of a person's life exposing them to:

- **Threats**
- **Blackmail**
- **Extortion**
- **Kidnap**
- **Identity theft**
- **Stalking**

Would you expect your bank manager to advertise their home address online? What about an employee openly discussing sensitive business matters on social networking site? Regard should also be given to what family members post online.

The integrity of your corporate information and the safety of your staff are potentially at risk. The financial sector including cash centres and cash transit, government, law enforcement, military and security are obvious professions where the risk is greater but **any business** could be exploited if there is profit to be made.

It is recommended that any information posted on the internet is perceived as accessible to all internet users throughout the world, regardless of website security settings.

**To safeguard personal and business security it is encouraged that**

- **users ensure a high level of security is afforded to any social networking websites used by them**
- **Only appropriate persons known personally should be accepted as 'friends' or 'followers'**
- **Information and images posted are moderated and no inappropriate information is posted that may be detrimental to the integrity of either an individual user or commercial business.**

## Smart Phones



A smart phone is a mobile phone that offers computing capability and internet connectivity. They utilise an operating system similar to computers and allow users to run multiple applications (apps) such as access to email, editing / read business documents / schedules and internet usage and social networking on the move. These applications can (often unknowingly) access and download sensitive data held on these devices and also identify a user's location by means of inbuilt GPS ability to geolocate the user.

It is now common for marketing services to exploit user's lack of security e.g. sending them a notification when in close proximity to a coffee or fast food chain. Through Facebook and other services, users can now use smart phones to 'check in' at locations they visit displaying the details for all to see, exposing lifestyle patterns.

Geotags may be automatically embedded in images taken with smart phones revealing the location of where the photograph or video was taken. When posted on the internet to a social media site such as Twitter, Facebook or YouTube the exact location of the image and type of device used, could be available to any one viewing the image.

Such features may be unknowingly and automatically active having been set to a default position of 'on' unless disabled by the user, as result individuals often share too much information inadvertently.

Additionally, poor device security settings and use of open or free Wi-Fi zones add to the vulnerability of both devices and sensitive and personal data.

**Recommendations:**

- **Consider which applications you allow access to your smart phone GPS function**
- **Be aware of the default settings for web services and devices used**
- **Exercise caution when utilising open or free Wi-Fi zones**
- **Never assume internet security settings of personal devices offer same protection as those within secure workplace network**
- **CHECK YOUR SECURITY!**

For further information on ecrime, free downloads please go to:

[www.ecrimescotland.org.uk](http://www.ecrimescotland.org.uk)

For further information and examples, including how to disable automatic GPS geotagging, please go to the US Army web site at:

<http://dmna.state.ny.us/members/geotagging.pdf>

The SCDEA welcomes feedback regarding this and any other bulletin produced by the SBCC Liaison unit. If you have any queries, suggestions or are seeking advice on other matters please do not hesitate to contact us using the details below:

**Scottish Business Crime Centre Liaison  
Scottish Intelligence Co-ordination Unit  
Scottish Crime and Drug Enforcement Agency**

**Direct dial: 01506 524 548**

**Email: [SICU-DESK@scdea.pnn.police.uk](mailto:SICU-DESK@scdea.pnn.police.uk)**

**[www.sdea.police.uk](http://www.sdea.police.uk)**

**[www.sbcc.org.uk](http://www.sbcc.org.uk)**

### **Our Vision**

To protect Scotland's communities from serious organised crime

### **Our Mission**

Working every day for the people of Scotland - dismantling serious organised crime

### **Our Organisational Values**

Trust, Commitment and Respect

#### Disclaimer

*Whilst every care has been taken in developing and compiling this document, the SCDEA accepts no liability for any loss or damage caused, arising directly or indirectly, in connection with reliance on its contents.*

*This is a government document that has been graded as **NOT PROTECTIVELY MARKED**. There are no specific requirements for storage or disposal and it can be considered as safe for wide distribution within your organisation. This can extend to its use for training or awareness programmes for staff. However, unless otherwise specified, this information is not intended for general public dissemination and should not be included on public facing websites, external mailing lists, social media or other outlets routinely used by you to deliver information to the public. We therefore request that you risk manage any onward dissemination in a considered way.*

© SCDEA 2011