CPNI
Centre for the Protection of National Infrastructure

SOCIAL NETWORKING AND ONLINE SECURITY

A SUMMARY OF GOOD PRACTICE

December 2013

Introduction

For many people, having a presence online is a normal part of day to day life and may be a necessary aspect of doing business. There are some practical steps you can take to keep safe online and ensure that only the information you want to broadcast is made available.

Step 1 – Understanding your "digital footprint"

You leave a digital footprint whenever you interact in a digital environment (e.g. browsing the internet, using a mobile phone, smart TV, or on-line gaming) or when anyone posts information about you into a digital environment, such as on Facebook or LinkedIn. It is normal to have a digital footprint, in fact it is difficult to avoid, and not having one can make you stand out more.

Part of staying safe online is familiarising yourself with your digital footprint. For example, try searching for yourself on **Google** or **pipl.com** to see how much information about you is available on the open internet. Having done so, you can then take steps to eliminate information that you do not wish to be available, or restrict who can easily access this information.

Step 2 – Managing your information online

Here are some practical considerations you should go through when managing your online profile and safeguarding your private information.

- **Online registration** – How much information do you have to give when you sign up for a new account? How much of this information will then enter the public domain? When signing up for a new account on social media or business networking sites, consider entering the minimum amount of real information necessary.

- **Accounts** – Consider separating your accounts. For example, you may wish to use one account for personal correspondence and social networking (using your personal credentials to sign up, such as your personal email address) and a separate business/work account (using your business credentials to sign up, and providing business contacts details rather than your own personal ones).

- **Security settings** – Review the privacy/security settings on social media and other accounts and to ensure your information can only be accessed by those who you wish to view it (N.B. website administrators will be able to view all your information). Many sites such as Facebook allow you to vary your privacy settings so that trusted contacts can see more information, and others can see less. It is also sometimes possible to restrict who can see past postings.

- **Contacts lists** – Review your list of contacts on social networking sites. Do you want all of these contacts to be able to access your information? Consider removing anyone who you don't remember connecting with or have no need or desire to remain in contact with. Consider carefully whether to accept requests to connect with people who you don't recognise.

- **Phishing** – Beware of unsolicited messages from people you don't recognise, particularly those with files attached or hyperlinks included in the message body. This could be an attempt to send malicious software to your computer which can be used to steal data, record your key strokes (potentially to steal passwords), or take control of your computer. Phishing emails can come from trusted contacts if their computer has been compromised, so always be careful when reading emails with attachments or hyperlinks, particularly if these look odd. One way to spot phishing emails which come from trusted contacts is to check if they've been sent to everyone in their contacts list. Emails such as this may not contain any text, just a hyperlink.

- **Passwords** – Make sure passwords are long and strong (containing a mixture of letters, numbers, and symbols). Avoid using the same passwords for multiple accounts so that if someone, such as a criminal computer hacker, were to gain access to one account, they would not easily be able to gain access to other accounts such as online banking or email accounts.

Step 3 – Keeping your online profile under review

It is important to keep your online accounts under review as the privacy configurations on the websites you use may change over time and this can affect how much of your data is available to the public. You may also find that a change of job role or change of circumstances means that you want more or less information about yourself to appear online.

After reviewing your settings and making any changes, try searching for yourself again on **Google** or **pipl.com** to see how you now appear online.

Further information

- Comprehensive security advice about online social networking can be downloaded from the Centre for the Protection of National Infrastructure (CPNI) website – see cpni.gov.uk/advice/personnel-security1/online-social-networking.

- Another useful website is **www.getsafeonline.org** – a collaboration between Government and the private sector which provides advice on online security and safety.