FACT SHEET – RISKS OF SOCIAL MEDIA

What is Social Media

Social Media includes web-based and mobile technologies used to create online communities to share information, ideas, personal messages and other related content. It allows users to communicate mostly on a personal level and at times for business purposes. Social media includes platform such as Twitter, Facebook, MySpace, YouTube.

Risks of Social Media

There are several risks associated to the use of social media. These include:

- **Malware:** Social media sites are prime targets for malware distribution. The possibility of malicious users trying to post malware (such as virus, worms, spyware and more) in contents posted (including videos, music files) on such sites are always high.

- **Click-Jacking**: Click-Jacking occurs when hyperlinks beneath legitimate clickable content are concealed and which, when clicked, causes the user to unknowingly perform actions, such as downloading malware, or sending his/her ID to a site. Numerous click-jacking scams have employed "Like" and "Share" buttons on social media sites.

- **Hacking:** All social networking sites are subject to flaws and bugs. Some social networking sites make use of third party applications (e.g. widgets in facebook). There is always a risk that a hacker or malware seeks potential holes to exploit within the application.

- **Phishing:** There are a number of hackers on social networks who may try to steal or use personal information. There are also websites that are set up to appear to look like ones favorite social networks in order to steal the user's password and use it to destroy his/her profile or send out spam messages and viruses. Users may also be redirected from legitimate websites to fraudulent ones for the purpose of extracting confidential data.

- **Spamming:** If Government emails are used on social networking sites, there is a 98 % chance the email address will be subject to receiving spam and be a target for phishing attacks, causing issues on the Government's network.

- **Disclosure of Inappropriate and Sensitive Information:** Forums, chat rooms, blogs may lead to disclosure of sensitive information if one is not careful on how to operate it. If no authorization mechanism is present on what can be posted and who can post information, this may lead to disclosure of information.

- **Fraud, Identity or Information Theft:** It is very common for social engineers to use social networks to acquire initial information about a person or to obtain private organisation information for the purpose of fraud, identity or information theft, and other crimes. Without constant efforts to preserve the identity of the displayed content, blogs, channels, groups and profiles might be spoofed or hacked.

- **Risks to intellectual property:** Distribution of copyrighted media content within a social network is difficult to oversee. Legal frameworks for management of intellectual property within social network environments are still developing, and the internal rules for each social network vary in the level of protection provided to content uploaded to the social network.

- **Ownership of Information:** Contents posted on sites such as Facebook, Twitter will lie under the jurisdiction of its corresponding country. People should be vigilant on the sensitivity and category of information that are posted on such sites.

- **Social Engineering:** Such attacks refer to extracting information from employees/users, through conversation/chat rooms, without giving them the feeling that they are being interrogated. Users interacting on sites should be aware and informed of such social engineering attacks.

- **Productivity Loss:** Social networkers are the weakest link and their actions can create problems. If every employee in a 50-employee organisation spends 30 minutes on social networking every day of a working week that would total a cumulative productivity loss of 6,500 hours in one year, which may indirectly entail cost to the organisation resulting in a loss of productivity.

- **Doxing:** Once information is posted to a social networking site, it is no longer private. The risk of doxing, where a person's or the organization's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles are publicly released is eminent.

Young surfers and children in particular have become ardent fans of social media over the recent years. It hence becomes important for parents to understand the risks that their children face by interacting on social media sites. In addition to the above mentioned risks, children face the following dangers through the use of social media:

- Cyber bullying
- Online grooming
- Invasion of privacy
- Exposure to inappropriate content
- Internet addiction

Preventive Guidelines

- Adhere to Government policies and procedures such as the Internet Usage Policy, IT Security End User Guidelines.
- Keep sensitive (such as Government's information, work details, date of birth, address) and personal information private.
- Install the latest patches on your computer's operating system.
- Always run an up-to-date internet browser.
- Make sure your screen name does not reveal too much about you.
- Do not maintain relationships with strangers online.
- Always make sure you are at the right site when you enter your credentials.
- Be careful about what you do, how you behave, and what you say in a public or social forum.

Additional measures to be taken are as follows:

- Have an updated antimalware solution. *Refer to Fact Sheets on Computer Virus and Spyware.*
- Use strong passwords. *Refer to Fact Sheet on Effective Password Management.*
- Beware of unsolicited invitations from spammers. *Refer to Fact Sheets on Spam, Phishing.*
- Practice safe internet surfing. *Refer to Fact Sheets on Safe Internet Surfing and Communicating on the Net.*

Over the years, various fact sheets on the above topics were issued by the IT Security Unit. Detailed guidelines which help to counter risks of social media are contained in each fact sheet.

These previously circulated fact sheets, also available on the Classified Section of the Government Portal (publicsector.gov.mu), include:

- Computer Virus issued in November 2004
- Spam issued in November 2004
- Phishing issued in March 2005
- Spyware issued in July 2005
- Safe Internet Surfing issued in May 2006
- Communicating on the Net issued in November 2006
- Effective Password Management issued in November 2009