**November 2015**

# High Profile and International Events Cyber Security Advice

## Introduction

1. Targeting of high profile and international events by state-sponsored or other foreign adversaries, cyber criminals and issue motivated groups is a real and persistent threat. The information contained on government systems, whether classified or unclassified, is of strategic interest to cyber adversaries. Information gathered through cyber espionage can be used to gain an economic, diplomatic or political advantage.
2. There are many examples of entities being targeted due to their involvement in high profile events. In November 2012, Association of Southeast Asian Nations (ASEAN)-themed malicious emails were sent targeting Australian government agencies in an attempt to compromise their networks and obtain sensitive information. These emails appeared to come from entities associated with ASEAN events.
3. In July-August 2013, Asia-Pacific Economic Cooperation and G20-themed malicious emails were sent to multiple Australian government agencies from webmail accounts misrepresenting persons and organisations having an association to these events.
4. Australian government staff involved with the 2014 G20 Brisbane summit received spear-phishing emails that appeared to repurpose legitimate Australian Government emails. The emails contained G20-themed attachments and organisational details that the staff were expecting and appeared to come from organisations they had been dealing with.
5. It is important to be aware of malicious activities. There are some simple steps that all users can take to reduce the risk of cyber espionage.

## Socially engineered emails – Think before you click

6. Socially engineered email is the most common technique used to gain access to government information and networks. It is common for targeted emails to be sent to a broad range of Australian government departments before, during and after the event.
7. The aim of malicious cyber actors is to gain access to non-public information any way possible. These adversaries look for a weak link to try and break into a network. It is important to remember that you may be targeted even if you are not directly involved with the event.

**What are socially engineered emails?**

Socially engineered emails attempt to deceive the recipient into clicking on a link or attachment which can install malicious software onto their computer. Once installed, malicious software can facilitate the theft of official or sensitive government information. Socially engineered emails may appear to be work related, or target a specific interest to your work or personal life. They can also appear to come from someone you know.

8. If you suspect you have received a socially engineered email you should ask yourself some questions before opening the email:
    a. Is the email from a trusted source?
    b. Is the manner in which the email is written consistent with what you expect from the sender?
    c. Is the sender encouraging you to download a file, open an attachment or visit a website for further information?
9. Here are a few tips to defeat the socially engineered email threat:
    a. If you have any doubt about the legitimacy of an email you can check the authenticity with the sender by contacting them through alternative means (e.g. phone call or SMS).
    b. Never click on a link in an email. First, hover your cursor over the suspicious link to display the actual link – ensure that actual link matches the written link displayed in the email. If necessary, you should type or copy and paste the link into your internet browser.
    c. Be aware of unusual file types, for example .jar and .exe, and do not open them if they are not what you were expecting.
10. Signs that you may have inadvertently opened a malicious document include:
    a. An attachment that contains no content, flickers when opened or crashes the application;
    b. Opening a web link that directs you to a website with limited or unexpected content; or
    c. Dialogue boxes that close before you have had a chance to read them.
11. To help ensure the legitimacy of your email communications, if available, take the option to digitally sign your emails when communicating externally as part of your official duties. If you suspect that you've been the target of a socially engineered email, do not delete or forward the email. Rather, contact your ICT security team immediately and provide them with the details they request.

## Using webmail for government business – Do you need to be mobile?

12. Web-based email (webmail) is email accessed using a web browser, such as Gmail, Hotmail or Yahoo Mail. You should avoid using webmail for when communicating official or sensitive government information. This is because webmail will bypass the security controls which your ICT security team has put in place. They will have no visibility of, or ability to protect, the information that is shared through such email accounts.
13. If you need to be mobile in support of your official duties at the high profile or international events, please discuss possible secure access solutions with your ICT security team.

## Removable media and mobile devices – If it's not yours don't use it!

14. Removable media (e.g. USB flash drives, CD/DVD disks) and mobile devices (eg. smartphones and tablets) can be inadvertently or intentionally contaminated with malicious software.

15. **Gifting.** It is common to receive small gifts, such as removable media in the form of a USB device from stakeholders when attending events, including those also attending these events. People with a malicious intent may use these opportunities to gift electronic devices that are preloaded with malicious software. When these devices are used or connected to an Australian government network or personal device, malicious software may install and run, which can allow the theft of official or sensitive data.

16. Gifted electronic devices should not be used, and should be handed in to ICT security staff as soon as possible. Your ICT security team has the ability to scan removable media to make certain there is no hidden malicious software.

17. Some tips to reducing the risk associated with removable media and mobile devices include:

    a. Do not accept complimentary or promotional removable devices.

    b. Do not offer or allow another unauthorised person to insert any removable media or mobile electronic device into a computer that connects to important information or any government network.

    c. Where possible only insert your removable media or mobile devices on trusted computers. In some cases, by inserting these devices into an unknown computer there is a chance a virus exists on that computer which could be transferred to your removable media, or vice versa.

    d. When charging mobile devices you should only use a trusted computer to connect to the device charger.

    e. Maintain physical control over your mobile devices (whether they are your own or agency-issued), not only to minimise the risk of theft or loss, but also to protect the confidentiality of information stored on the device.

## Connecting to public networks – What are you communicating?

18. Savvy cyber intruders have been known to exploit hotel or conference facility networks to gain access to mobile devices. Avoid communicating any official or sensitive information on devices that are not connected to a secure network. Where possible try to avoid using hotel internet kiosks and internet cafes to send or receive important data. Do not connect to open Wi-Fi networks for business purposes. Only wireless communications that are needed and can be secured should be enabled.

19. Avoid or limit the use of wireless networks. Where possible, Australian government staff are encouraged to use a Virtual Private Network to connect to their organisations' secure network.

## Internet presence including social media – Who can see your information?

20. Users of social media need to be aware that they will be an attractive target to adversaries through their online presence. Users posting information about their involvement in high profile or international events unknowingly provide people with information that can be used to elicit government information from them or to tailor social engineering campaigns to compromise an agency network. Users should assume everything posted on social networking websites is permanent. Be aware that online professional profiles, such as being listed on the Australian Government Directory, can present a similar risk.

21. To prevent being a target to of a socially engineered campaign users should;

    a. Carefully consider the type and amount of information posted;

    b. Restrict the amount of personal information posted;

    c. Consider limiting access to posted personal data to 'friends only'.

## Travelling overseas with an electronic device

22. At high profile and international events overseas, consider that the compromise of your device could have an impact on your department, its information and reputation. In most countries, you have no expectation of privacy in Internet cafes, hotels, offices or public places. In most cases, this advice is most relevant for corporate devices. For personal devices, consider the general advice provided above or consult Australian Signals Directorate (ASD)'s advice available on our website.

23. Prior to departure, consult your ICT security. They can confirm that your device's configuration is correct and that all updates, patches, encryption and antivirus software have been installed and base-line the device prior to departure and again on return to look for any signs of compromise.

24. Remove all non-essential data from the device. In particular, reconsider the need to take sensitive or classified information overseas, for example Sensitive: Cabinet.

25. Disable Bluetooth and wireless capabilities and the ability to 'auto-join' a network. This will prevent your device from inadvertently connecting to untrusted networks.

26. Ensure strong passphrases are used, based on requirements outlined in the *Australian Government Information Security Manual* (ISM). However, agencies should consult available ASD device-specific guidance, as passphrase policies may differ from the generic advice in the ISM. A passphrase should never be written down and stored with the device.

27. Maintain physical control over devices, not only to minimise the risk of theft or loss, but also to protect the confidentiality of information stored on the device. It is advisable to keep your device in your possession at all times and not trust hotels, hotel room safes or other services to provide physical protection of equipment. Never check your device in as luggage; devices should be taken onto the plane as hand luggage.

28. Do not connect to open Wi-Fi networks for business purposes. Only wireless communications that are needed and can be secured should be enabled. Instead, connect back to your agency Virtual Private Network to use the Internet.

29. When you return, advise your ICT security staff if the device was taken out of your possession for any reason, particularly if you have travelled to a high risk country. Also advise them if you left your device in your hotel room for an extended period of time. ICT security staff should be able to check the device for any malicious software or evidence of compromise.

## Further Information

30. This document draws from the advice contained in ASD's Protect publication range available at www.asd.gov.au, in particular:

31. *Detecting socially engineered emails*
www.asd.gov.au/publications/protect/socially_engineered_email.htm

32. *Implications of using webmail for government business*
www.asd.gov.au/publications/protect/webmail-government-business.htm

33. *Security tips for the use of social media websites*
www.asd.gov.au/publications/protect/security_tips_for_using_social_media_websites.htm

34. *Travelling overseas with an electronic device*
www.asd.gov.au/publications/protect/electronic_devices_os_travel.htm

35. *Technical Advice: Travelling overseas with an agency-issued electronic device*
www.asd.gov.au/publications/protect/electronic_devices_os_travel_tech_advice.htm

## Contact Details

36. If you have any questions regarding the security of your information or devices you should contact your ICT security team in the first instance.

37. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

38. Australian businesses or other private sector organisations seeking further information should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.