Australian Government
Australian Cyber Security Centre

ASD
AUSTRALIAN SIGNALS DIRECTORATE

PROTECT

FEBRUARY 2017

# Detecting socially engineered emails

1. Socially engineered emails present a significant threat to information security. This document offers tips for identifying malicious emails and avoiding compromise of your network and information. This document is intended for all users.

## What are socially engineered emails?

2. Sending socially engineered emails is the most common technique used in malicious cyber intrusions targeting Australian Government agencies. Socially engineered emails attempt to deceive the recipient into downloading malicious software by clicking on a link or attachment. They may appear to be work related, or target a specific interest. They can also appear to come from someone you know. Inadvertently accessing these malicious files can have serious consequences, including the theft of Australian Government information.

## Who do they target?

3. Senior officials and their staff, system administrators, users with access to sensitive information, users with remote access and users whose role involves responding to unsolicited emails are at a higher risk of being targeted. Such users should be especially vigilant and employ strategies to mitigate the risk.

## How can socially engineered emails be identified?

4. While socially engineered emails can be highly sophisticated, there are ways to differentiate them from legitimate emails. Consider the following questions when you next read your emails:

    a. **Do you *really* know who is sending you the email?**

        i. Do you recognise the sender and their email address?

        ii. Is the tone consistent with what you would expect from the sender?

        iii. Is the sender asking you to open an attachment or access a website?

    b. **Are you expecting an email from them?** Socially engineered emails can be crafted to appear to come from a relevant and trustworthy source, including from within your organisation. Many use content relating to current events in order to deceptively gain your trust.

c. **Is the content of the email relevant to your work?** Malicious cyber actors may use fraudulent emails which relate to your area of interest.

d. **Does the email ask you to access a website or open an attachment?** This technique is commonly used to run malicious code on a victim’s computer, which could compromise agency data. You should always type the web address into your browser instead of clicking a link, and avoid clicking on any link that has been shortened, as you have no way of verifying the actual address. Exercise judgment and be cautious when opening attachments or accessing websites.

e. **Is the web address relevant to the content of the email?** Always place your mouse over the link and check that the web address is consistent with the link. For example, an email purportedly from a financial institution that contains a link to a pharmaceutical website may be malicious, as the two are unrelated enterprises. Clicking the link could redirect you to a malicious website.

f. **Is the email from a personal email address?** If it seems unusual to receive an email from a work colleague or superior from a personal email address, the email could be malicious. Call the sender to verify the legitimacy of the email before opening any attachments or clicking on any links.

g. **Is the email suspiciously written?** Incorrect spelling and capitalisation, abnormal tone and language, or the absence of a specific addressee can indicate that an email is not legitimate.

h. **Have you received the same email twice?** This could be a sign that malicious cyber actors are seeking to increase the likelihood that you will open their email and action their request.

## How should you handle malicious communication?

5. If you suspect that you’ve been the target of a socially engineered email attack, do not delete or forward the email and contact your IT security team immediately.

## Further information

6. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.asd.gov.au/infosec/ism/index.htm

7. ASD’s *Strategies to Mitigate Cyber Security Incidents* complements the advice in the ISM. The complete list of mitigation strategies can be found at:

   http://www.asd.gov.au/infosec/mitigationstrategies

## Contact details

8. Australian government customers with questions regarding this advice should contact the ASD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au.

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