Australian Government

Department of Defence

Intelligence & Security

Key Messages

Facilitator's Edition

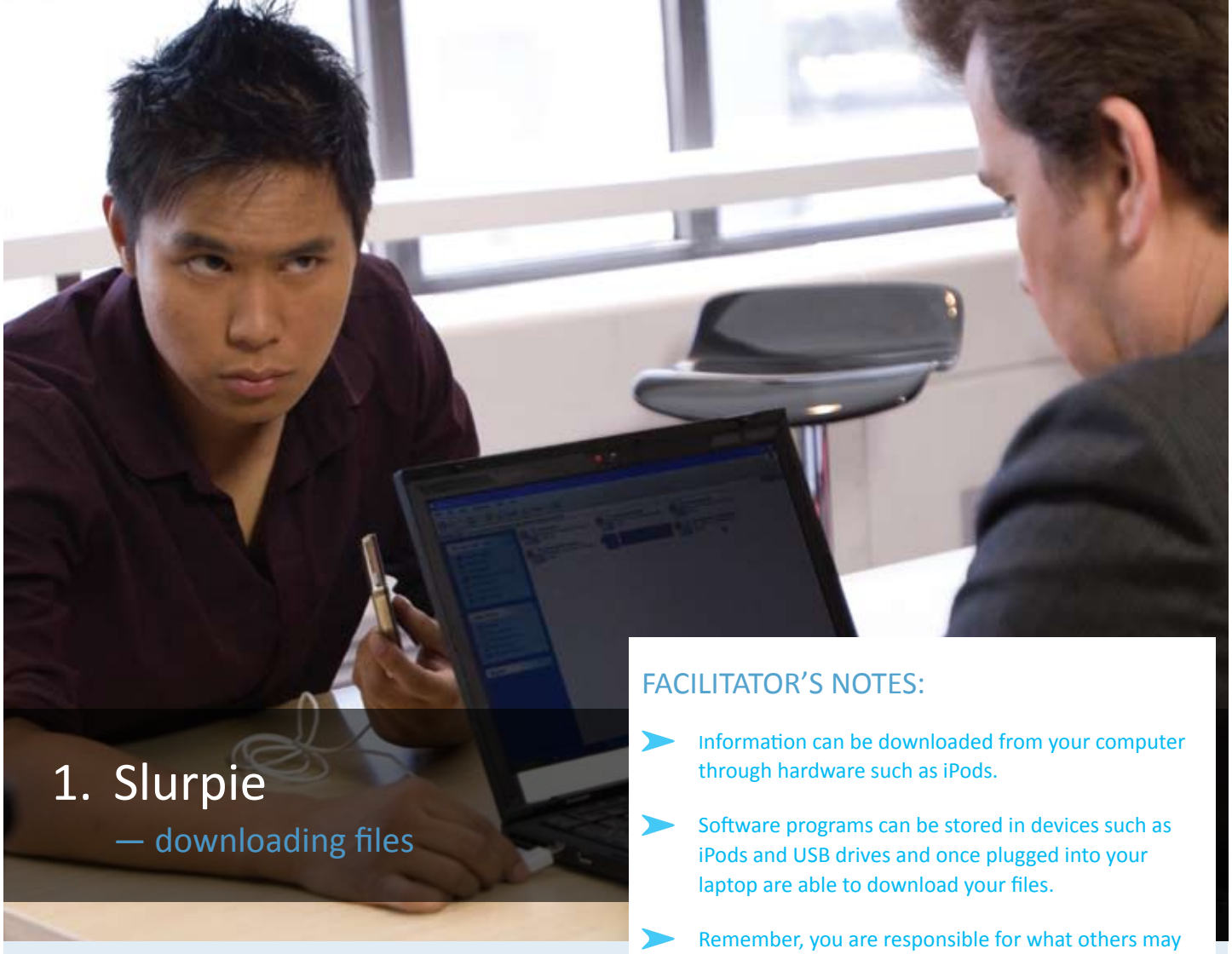
DEFENCE SIGNALS DIRECTORATE

2009

KEY MESSAGES

- Information security is important, regardless of where you are.
- You are vital to ensuring the security of your information.
- Understanding your organisation's information security policy is essential.
- Threats are real and so are the consequences.
- If in doubt talk to your IT staff.

- The CyberSense DVD will allow you as the facilitator to promote information security in your organisation.
- You can use this DVD to help your staff understand the importantance of information security policy in your organisation.
- By facilitating this DVD you will be able to answer questions that arise from the content and engage in discussion on information security with your staff.



1. Slurpie
— downloading files

KEY MESSAGE:

- Be aware of the dangers of allowing other people to access your work computer.

MITIGATION:

- Never allow unauthorised access to your computer.

FACILITATOR'S NOTES:

- Information can be downloaded from your computer through hardware such as iPods.
- Software programs can be stored in devices such as iPods and USB drives and once plugged into your laptop are able to download your files.
- Remember, you are responsible for what others may do to your computer if you give them access to it

2. Wireless interference
— the security of wireless connections

KEY MESSAGE:

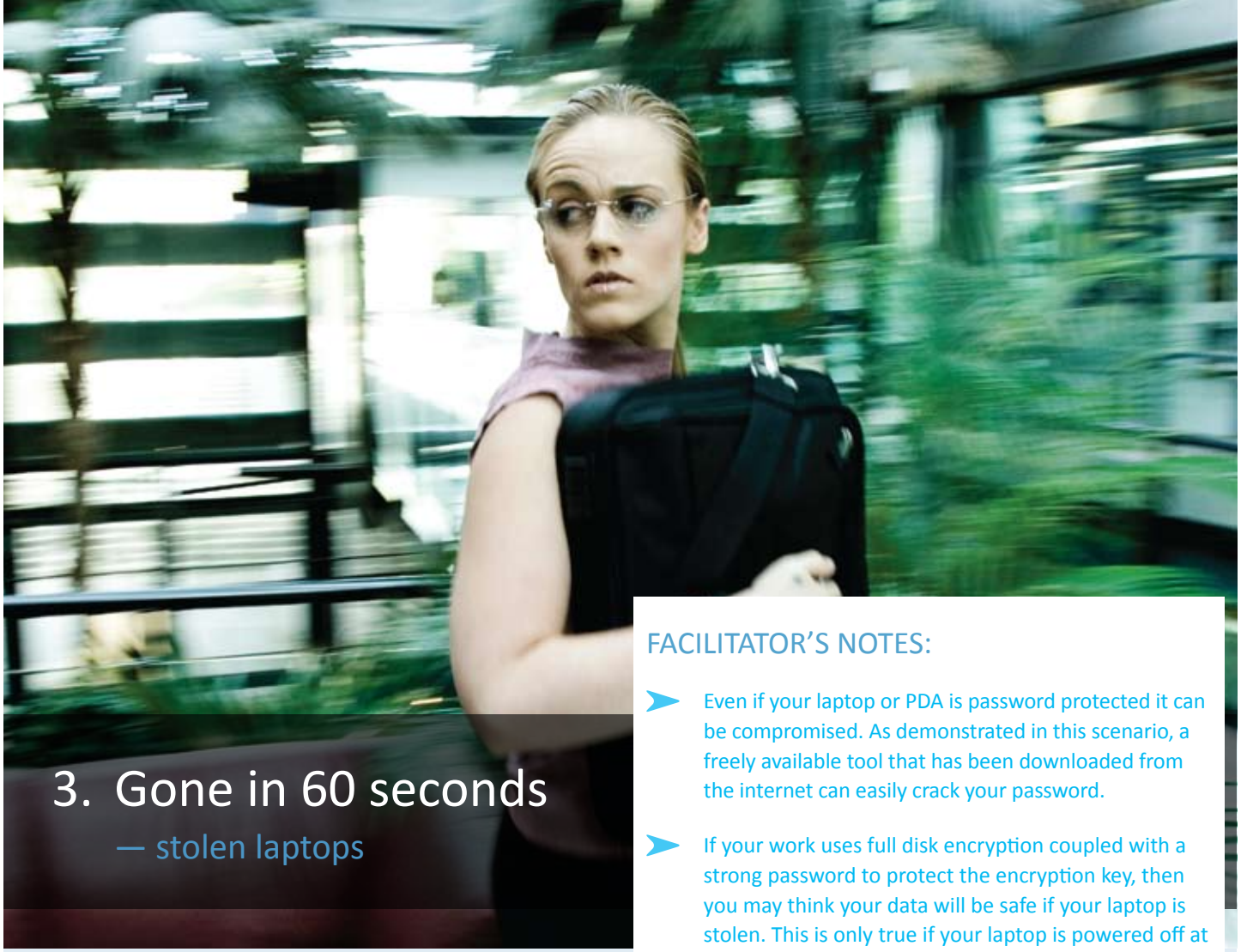
- Be aware of the dangers of accessing work communications using public wireless connections.
- Be cautious of discussing personal or sensitive information in a public place.

MITIGATION:

- Do not use public wireless networks for communications on sensitive or classified topics.
- If you need to discuss classified information use a DSD approved phone and follow IT security policy.

FACILITATOR'S NOTES

- Wireless communications are vulnerable to interception.
- There is software available for some mobile phones that, if installed, has the capability to turn on the microphone for the purposes of eavesdropping on conversations in the vicinity.
- Connecting your work computer to a public wireless network is not safe practice. You are vulnerable to a range of attacks, including:
  - An attacker eavesdropping on your connection (i.e. the wireless network uses weak encryption)
  - An attacker redirecting your communications to a fake wireless server to take control of your connection (this is called wireless access point spoofing)
  - Your computer being further compromised by an eavesdropper or access point spoofer.
- It is important to know that using public infrastructure can lead to your computer being compromised. If your computer is compromised, it doesn't matter how secure your connection to your work server is. For example, your work may use a Virtual Private Network (VPN) connection to allow staff to conduct business over the internet. If you computer is compromised, an attacker can access the VPN as well.



3. Gone in 60 seconds
— stolen laptops

KEY MESSAGE:

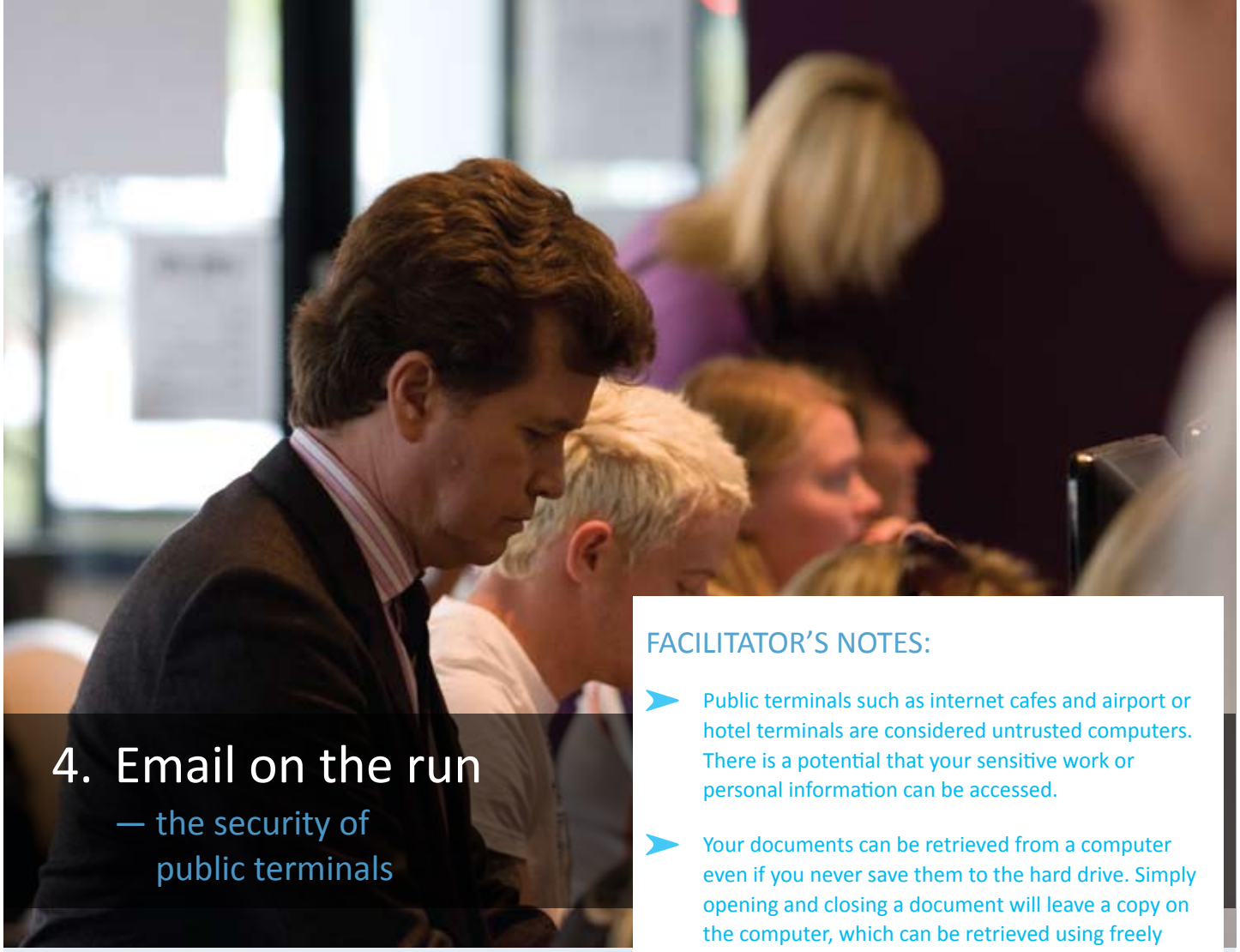
- Physical security is important - look after your equipment.
- Weak passwords will not protect your data if your computer is stolen.

MITIGATION:

- Never leave your laptop or PDA unattended.

FACILITATOR'S NOTES:

- Even if your laptop or PDA is password protected it can be compromised. As demonstrated in this scenario, a freely available tool that has been downloaded from the internet can easily crack your password.
- If your work uses full disk encryption coupled with a strong password to protect the encryption key, then you may think your data will be safe if your laptop is stolen. This is only true if your laptop is powered off at the time it is stolen.



4. Email on the run
— the security of public terminals

KEY MESSAGE:

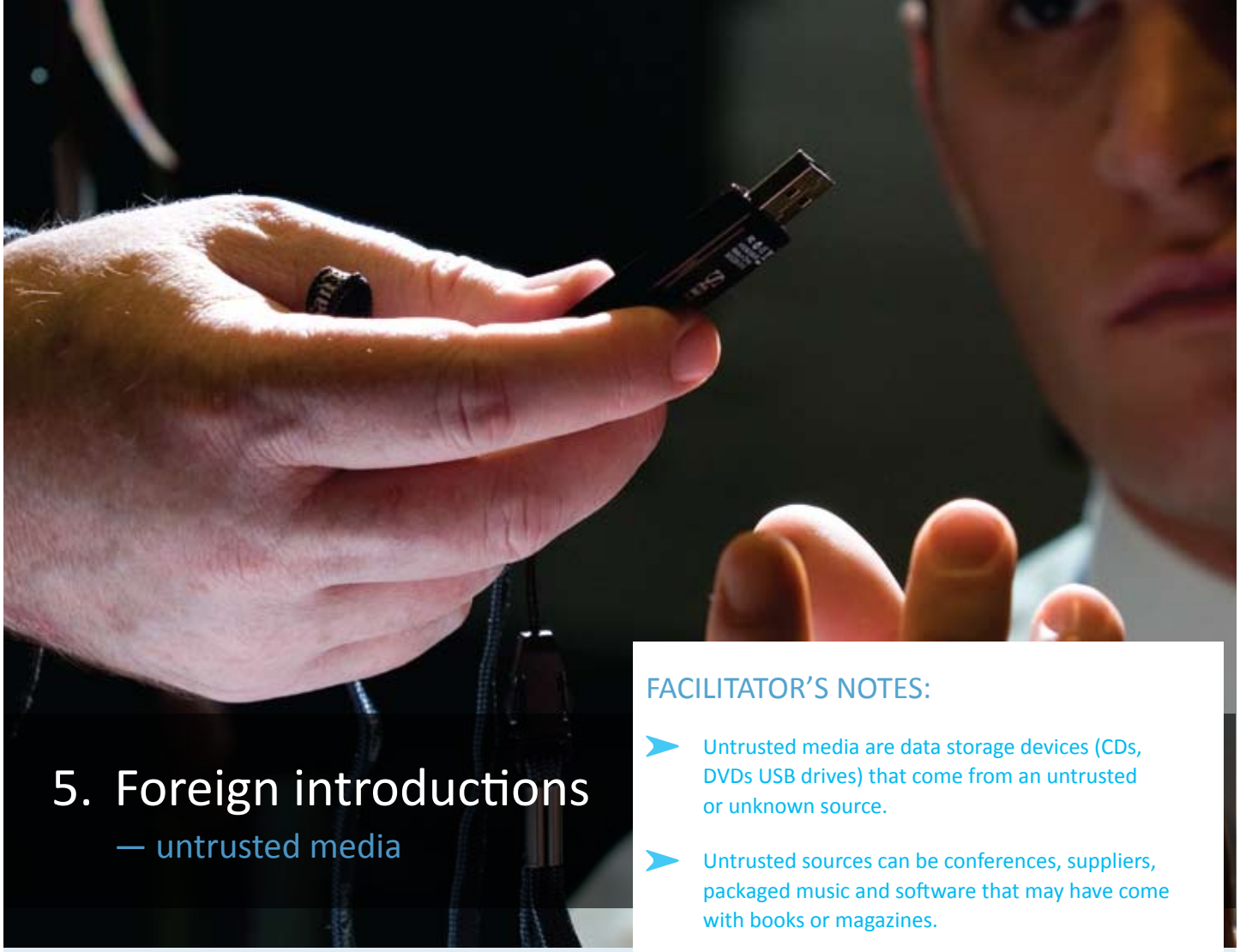
- Public terminals are not secure.
- You have no control over what is running on a public computer, or who can access it.

MITIGATION:

- Do not use public internet terminals to conduct sensitive work business.

FACILITATOR'S NOTES:

- Public terminals such as internet cafes and airport or hotel terminals are considered untrusted computers. There is a potential that your sensitive work or personal information can be accessed.
- Your documents can be retrieved from a computer even if you never save them to the hard drive. Simply opening and closing a document will leave a copy on the computer, which can be retrieved using freely available software.
- Key loggers bypass encrypted communications used by internet banking websites and secure web servers (HTTPS) because they intercept keystrokes between the keyboard and the web browser, which are not encrypted.
- A key logger can be installed on a computer which is then used to capture sensitive data. A key logger records keystrokes as they are typed into the computer. A key logger can also store copies of files and web pages that are downloaded.



5. Foreign introductions
— untrusted media

KEY MESSAGE:

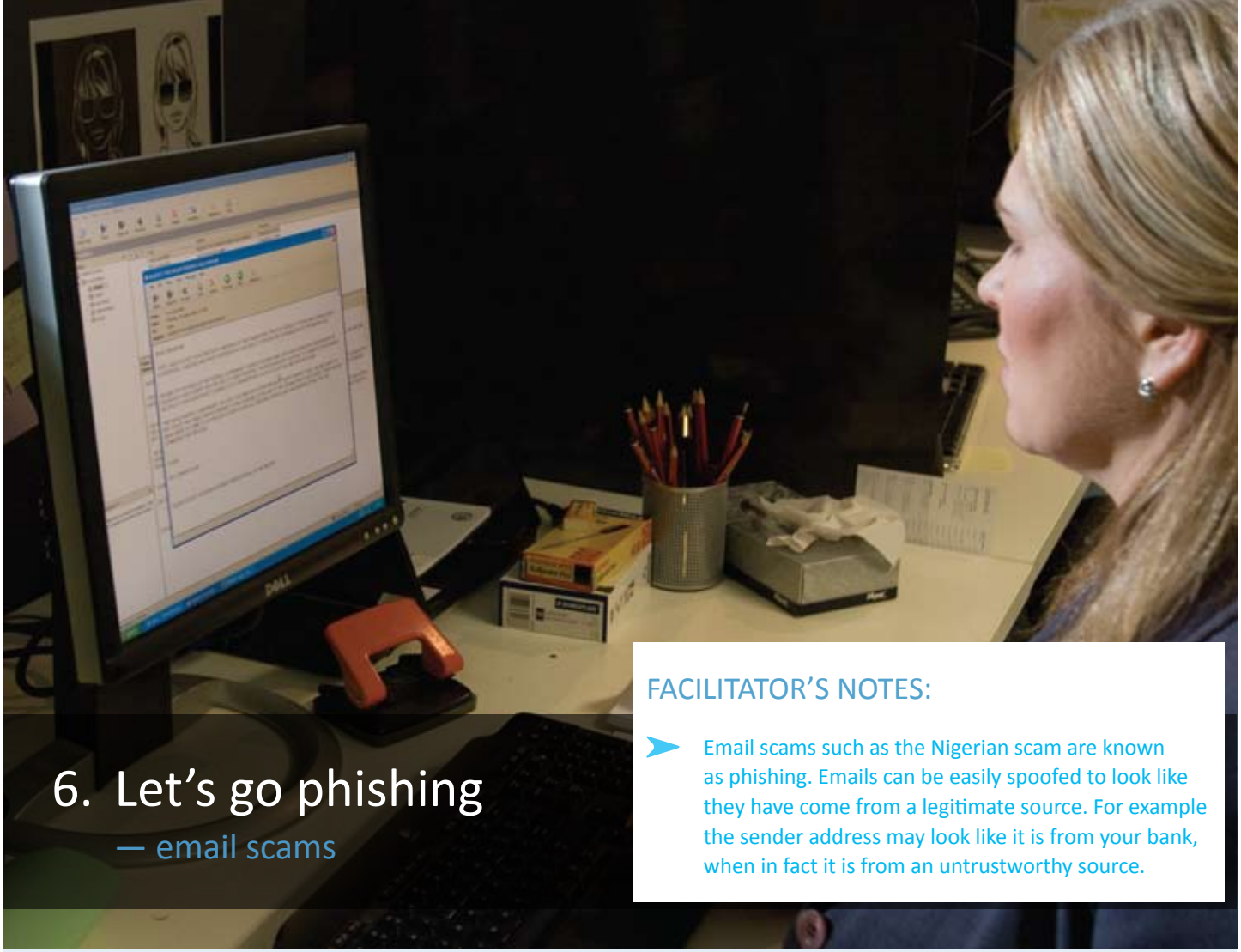
- Data storage devices such as USB drives can infect your computer with a virus or trojan.

MITIGATION:

- Never insert foreign media into a departmental computer without having it checked by IT staff.

FACILITATOR'S NOTES:

- Untrusted media are data storage devices (CDs, DVDs USB drives) that come from an untrusted or unknown source.
- Untrusted sources can be conferences, suppliers, packaged music and software that may have come with books or magazines.
- Untrusted media can have programs such as viruses or trojans on it that will run when the media is put into any computer.
- The virus or trojan can be included with the rest of the content on the media. The malicious software can be made to run when the media is in any computer by putting an auto run file on the media.
- Sometimes a virus can be unintentionally placed on removable media. A USB from a trusted source may still have a virus on it that the organisation or individual was unaware of.



6. Let's go phishing
— email scams

FACILITATOR'S NOTES:

- Email scams such as the Nigerian scam are known as phishing. Emails can be easily spoofed to look like they have come from a legitimate source. For example the sender address may look like it is from your bank, when in fact it is from an untrustworthy source.

KEY MESSAGE:

- Use caution when opening emails, especially from an unexpected or unknown source.

MITIGATION:

- Never follow links from unsolicited emails.
- Always type in the website address manually from your own records.

7. Watching your every move

— the importance of IT security

KEY MESSAGE:

- Never allow unauthorised access to your computer.
- Do not discuss sensitive or classified matters over a public communications network. Wireless networks are inappropriate for sensitive or classified work communications.
- Never leave your laptop or PDA unattended.
- Only log in to your departmental network from approved computers.
- Only use media issued by your department or another trusted authority, and only after it has been checked by your IT security team.
- Never follow links from unsolicited emails. Always type in the website address manually from your own records.

FACILITATOR'S NOTES

- This module shows that some attacks are almost impossible for a user to mitigate against. Users must at some stage open e-mail attachments and other content from unknown sources in the course of their day to day job.
- This module is meant to generate discussion about the kinds of policies or technical controls that your agency's IT security staff have implemented.
- Some of these policies or technical controls may be unpopular, but they are there for a good reason: to prevent agency computers and networks from being compromised.
- The key message is that understanding the need for IT security policies and controls leads to better adherence by staff, because some attacks can only be mitigated by system-wide, technical security

Australian Government

Department of Defence

Intelligence & Security