Australian Government

Department of Defence

Intelligence & Security

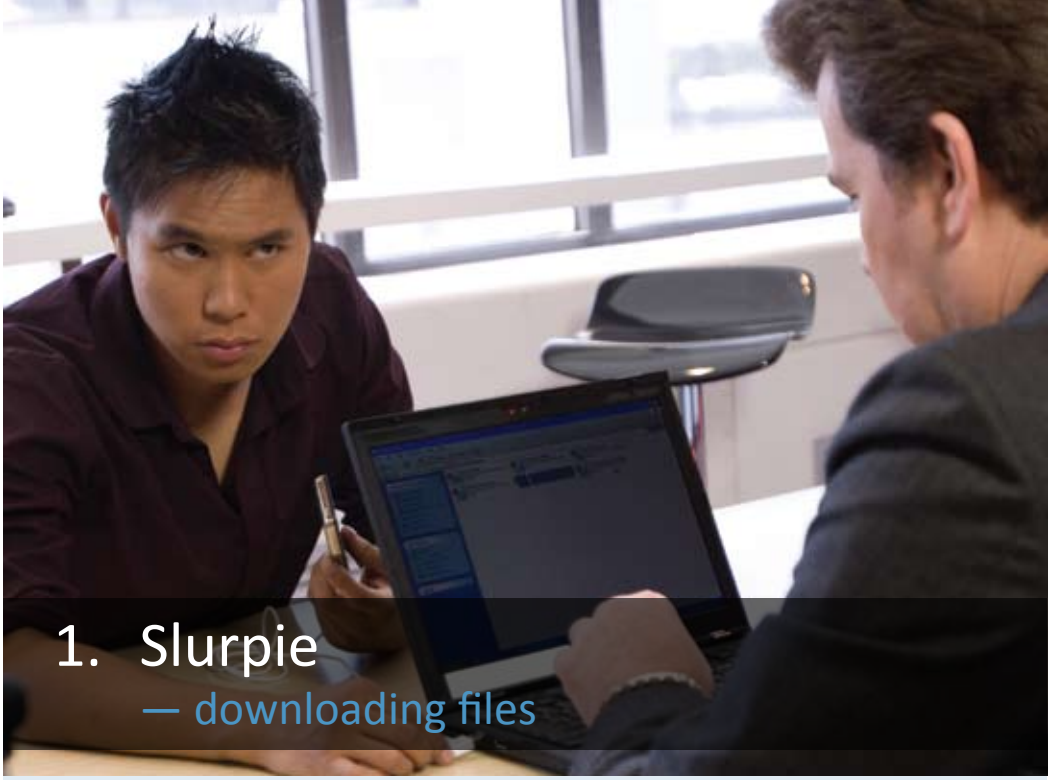
Key Messages

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.



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.

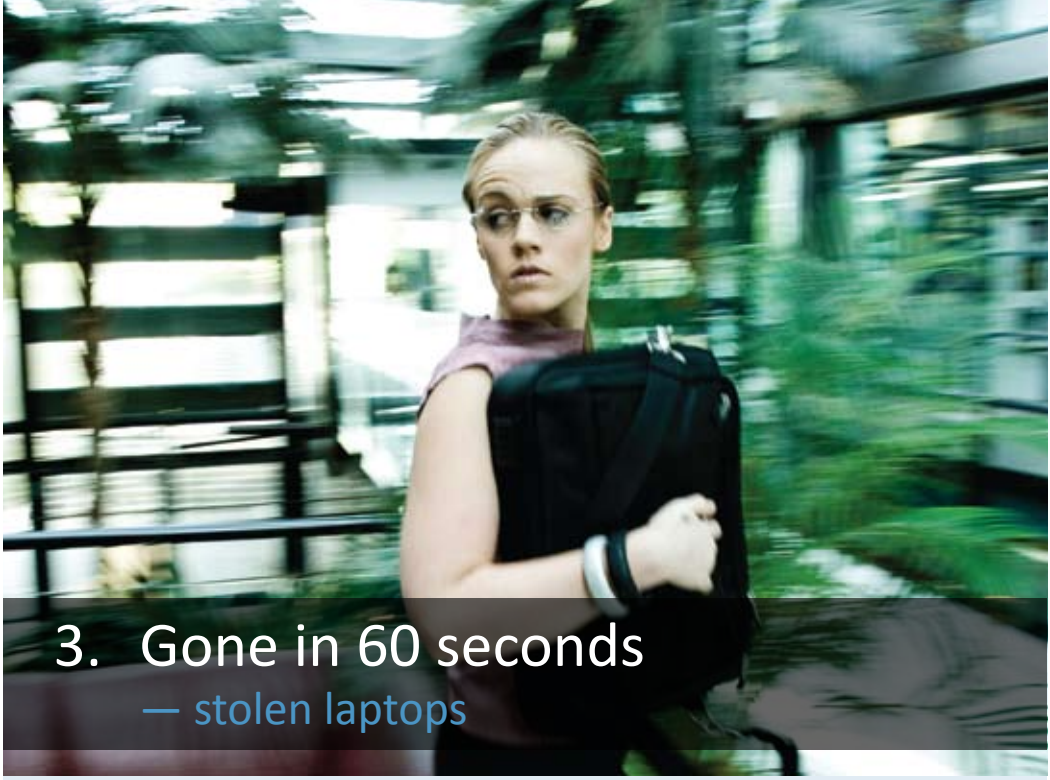
2. Wireless interference
— the security of wireless connections

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.



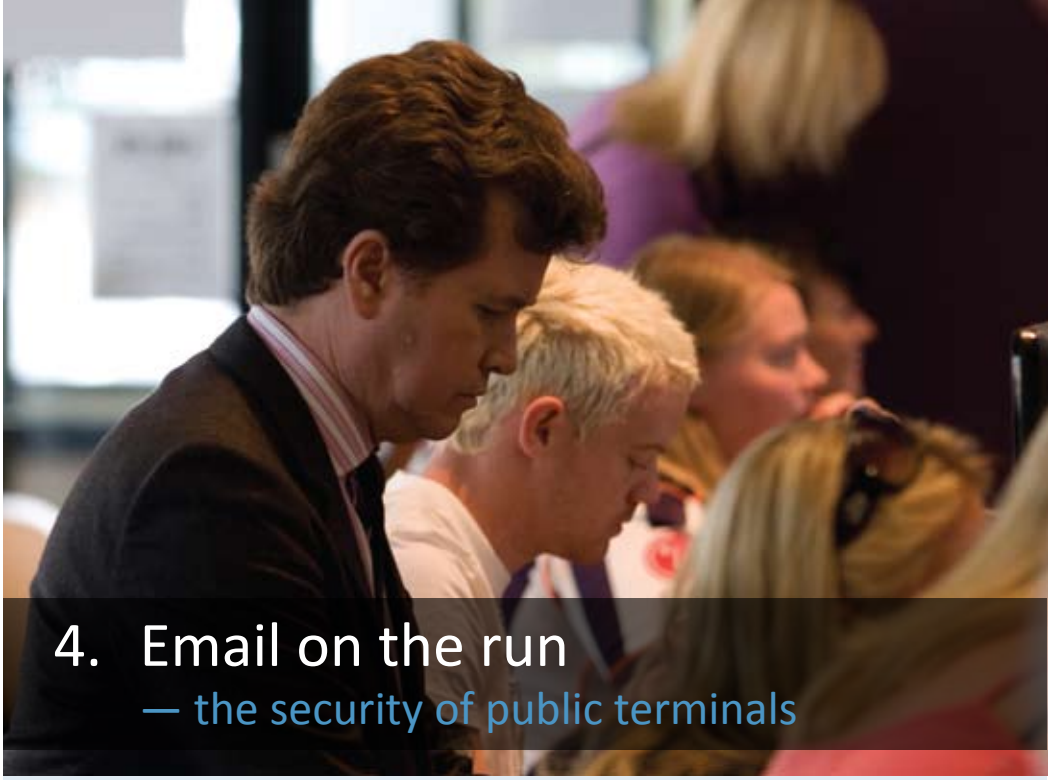
3. Gone in 60 seconds
— stolen laptops

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.



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.

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.

6. Let's go phishing
— email scams

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. Public 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.

Australian Government

Department of Defence

Intelligence & Security