Ministry of Technology, Communication and Innovation

IT Security Unit

Protecting Information while on the Move

IT Security Awareness July 2017

Information on the move

Mobile technology has drastically changed the way business is conducted. Mobile devices have become instrumental in most organisations. Laptops, tablets, smartphones and a plethora of other mobile technologies have already become indispensable for many organisations.

Risks to information

Although mobile devices bring multiple benefits, they can expose valuable data to unauthorised persons if the proper precautions are not taken to ensure the safety of the devices, and the information they contain. It is important to consider the risks associated to their uses so that appropriate measures can be identified beforehand.

Protecting Information while on the move!

Organisations need to protect their information in an appropriate manner wherever stored.

Information should always be protected to maintain confidentiality, integrity and availability.

Be Smart,
Safe
&
Secure
on the Move

There are many things to consider when using mobile technology in an organisation. You will find below some good practices and tips on mobile technology usage.

DOs:

✓ Ensure that information stored on the mobile devices is backed up and that the backup is stored in a secure location.

✓ Use strong and complex passwords to control access to mobile devices.

✓ Keep up to date with new developments - Mobile technologies are growing rapidly and are more exposed to risks and malware threats.

✓ Make use of encryption features to mitigate risks associated with loss of information.

✓ Use appropriate physical security when storing devices containing Government data.

✓ Exercise caution when connecting mobile devices in cyber cafes, public areas or free Wi-Fi access zones.

DON'Ts:

✗ Never leave mobile devices in areas where they can be conspicuously seen or easily taken.

✗ Do not share or leave password information in places where unauthorised users can find it.

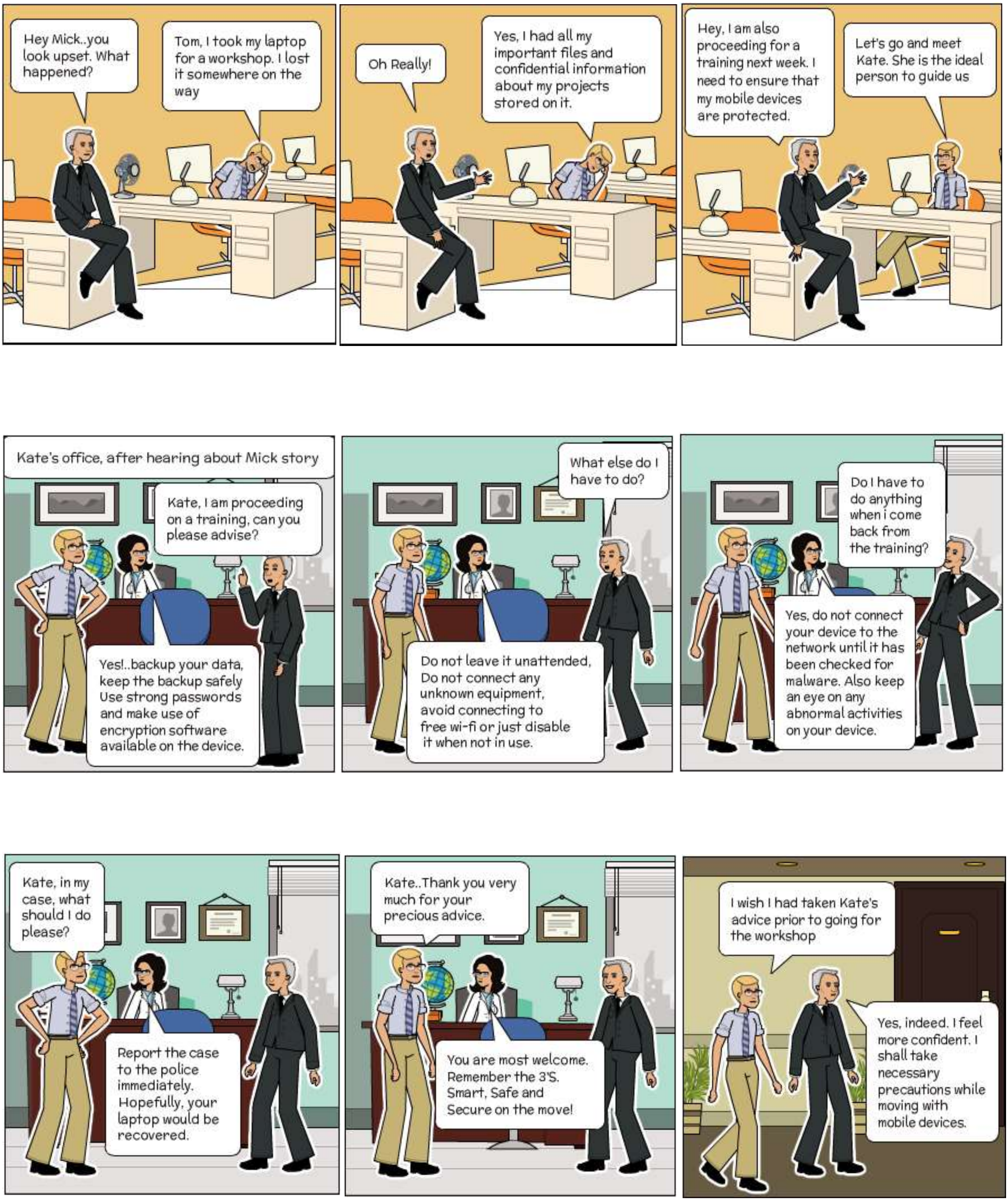
✗ Avoid connecting portable media (such as pen drive or memory card) to your mobile devices as they may contain malware.

✗ Do not enable Wi-Fi or Bluetooth when not in use.

REMEMBER:

- If any device is found to be compromised, request the IT department to take necessary remedial actions.
- Do not connect mobile devices to the organisation's network until they have been checked for malware.
- Report lost or stolen devices as soon as possible to the relevant authorities.

Be Smart, Safe and Secure on the Move


Hey Mick..you look upset. What happened?
Tom, I took my laptop for a workshop. I lost it somewhere on the way
Oh Really!
Yes, I had all my important files and confidential information about my projects stored on it.
Hey, I am also proceeding for a training next week. I need to ensure that my mobile devices are protected.
Let's go and meet Kate. She is the ideal person to guide us
Kate's office, after hearing about Mick story
Kate, I am proceeding on a training, can you please advise?
Yes!..backup your data, keep the backup safely Use strong passwords and make use of encryption software available on the device.
What else do I have to do?
Do not leave it unattended, Do not connect any unknown equipment, avoid connecting to free wi-fi or just disable it when not in use.
Do I have to do anything when i come back from the training?
Yes, do not connect your device to the network until it has been checked for malware. Also keep an eye on any abnormal activities on your device.
Kate, in my case, what should I do please?
Report the case to the police immediately. Hopefully, your laptop would be recovered.
Kate..Thank you very much for your precious advice.
You are most welcome. Remember the 3'S. Smart, Safe and Secure on the move!
I wish I had taken Kate's advice prior to going for the workshop
Yes, indeed. I feel more confident. I shall take necessary precautions while moving with mobile devices.