MEC	**PART 2 HACKERS**	6:40 – 10:55	**SMARTPHONE PRIVACY** Activity time: approximately 20 minutes	**Teacher's Guide**

Part 2 explores the world of hacking (checking out the pros in a convention in Las Vegas as they demonstrate what is possible). Asha, the programme presenter, speaks with different professionals about ways one's personal data could be accessed.

PREVIDEO	Students read intro. Then go through vocabulary with them, eliciting and clarifying where you can.

a flaw to up the ante to lock sb out (of st) a throwaway email to drain st

Q1	**New window**	*What does 'to spoof somebody' mean in this context of hacking?*

Ask the students if they know what it might mean. Then show them by opening a new window to find

http://www.thefreedictionary.com/spoof (You can search for it using the key words: free dictionary)

Students read & look at the appropriate definition. (With the exception of very high levels and in the interests of saving time, it isn't recommended to go over the other definitions.)

3. Computers To assume or emulate the identity of another (user or device) in order to gain access to a system.

Q2	**6:40 – 6:55**	*This convention is made up of many 'white hat hackers'. Who are they?*

Play the section about Defcom, the largest hacker convention in the world and elicit answers.

They hack for the greater good to expose flaws in the industry.

Q3	**7:15 – 7:39**	*What can the "Briefcase of Doom" do and how is it done?*

Play section and elicit answers. ***It can clone your credit cards just by placing the briefcase near your bag.***

Q4	**7:40 – 9:47** (7:56 – 9:20)	GAP-FILL: Chris and Michelle are human hackers. They can hack somebody by simply using information that was shared online and from that, take on the identity of the victim to gain access to more information by pretending to be that person. They use Asha, the presenter, as an example. *Fill in the gaps as they do their work:*

Play section and elicit answers.

1. They ***spoof*** Asha's number so it looks like she's calling from her phone.
2. They get her phone balance and what she owes on a recording from typing in her ***phone number***.
3. They get Asha's ***account number*** by pretending to be her while speaking to the company's representative on the phone.
4. They next get her ***banking*** details.
5. They add ***a new name (her fiance's name)*** to the account.
6. Then they do a ***password reset*** on that same bank account so Asha no longer can access her own bank account.

Q5	**7:40 – 9:47** (9:32 – 9:38)	*What information is dangerous to put online?*

Play section and elicit answers. ***date of birth, home address, email address***

Q6	**9:50 – 10:55** (10:37 – 10:42)	Asha was sent a link to her cellphone, which she clicked onto, & this provided the man to get photos of her. Besides the photos, he mentioned he can easily access three other things. *What were they?*

Play section and elicit answers. ***1- her calendar*** ***2- instant messages*** ***3- even her banking details***