En vous appuyant uniquement sur les documents suivants, vous rédigerez une note de synthèse répondant à la question suivante :

To what extent can new information technologies be a threat to privacy?

Votre note de synthèse comportera entre 400 et 500 mots.

Liste des documents :

1. ‘Wi-Fi security flaw for smartphones puts your credit cards at risk’, The Guardian
2. ‘The Information Equation’, The Economist
3. ‘iPhone keeps record of everywhere you go’, The Guardian
4. ‘Privacy is more of a concern for app users 45 and older’, Nielsen
5. Privacy awareness week poster, Chris Slane
Wi-Fi security flaw for smartphones puts your credit cards at risk

guardian.co.uk, Monday 25 April 2011 21.00 BST

Millions of smartphone users who use Wi-Fi wireless internet "hotspot" connections in public are vulnerable to fraud and identity theft, a Guardian investigation has established.

In tests conducted with volunteers – to avoid breaching telecommunications and computer misuse laws – security experts were able to gather usernames, passwords and messages from phones using Wi-Fi in public places.

In the case of the best-selling Apple iPhone 4 and other smartphone handsets, the information could be harvested without the users' knowledge and even when they were not actively surfing the web if the phone was turned on.

BT, the UK's biggest provider of such hotspots with five million of its "Openzone" connections in the UK in train stations, hotels and airports, admitted that it has known of the weakness for "years" and that it is working on a permanent fix.

Using a £49 piece of communications equipment and software freely available for download from the internet, the investigation established that crooks could set up bogus Wi-Fi "gateways" to which the latest generation of mobile phones would automatically connect. Once a connection is established, all the information passing through the gateway can be either be read directly or decrypted using software that will run on a laptop.

In another test, a fake Wi-Fi hotspot invited people to "pay" for internet access with their credit card – but required them to click a box to accept terms and conditions which clearly stated "you agree we can do anything we like with your credit card details and personal logins". A number of people entered their details.

Not only could the information be used to steal identities, hijack email accounts and commit fraud but also to gather information about individuals and company employees. With the information gained in our investigation, fraudsters could have bought goods online or sent multiple e-gift vouchers worth as much as £1,000 each to pre-set email addresses. It is believed that such vouchers are already being traded by crooks over the internet.

(...) Stuart Hyde, the Association of Chief Police Officers' lead on e-crime prevention, said: "We became aware of the potential for criminals to use Wi-Fi in this way last year and have become increasingly concerned. All they need is to set themselves up in a public place with a laptop and a mobile router called 'BTOpenzone' or 'Free Wifi' and unsuspecting members of the public come along and connect to them.

"Once that happens, there is software out there that enables them to gather usernames and passwords for each site a user signs in to while surfing the net. And once criminals have access to your email accounts, Facebook account, Amazon history and so on, the potential for fraud and identity theft is very serious indeed."
WITHIN minutes of Japan's earthquake on March 11th, the Bank of Japan's crisis-management team was up and running. Companies like Nissan and Sony immediately assessed the impact on their supply chains. A 43-person German search-and-rescue team were airborne within hours. (…)

At the same time, Google Japan turned its attention from search to rescue too. Engineers set up online services that have been developed for disaster situations. It represents a new form of data-driven humanitarian assistance. Where the heroism and hard work of relief workers in Japan is well understood, the role that information played in overcoming the disaster is not.

One service is "Person Finder". It allows anyone to enter names into an online registry to report the missing, search for people or confirm someone is safe—with interfaces in eight languages. Survivors themselves can report their whereabouts. (…)

Google also used its map service to show the areas and times of planned power cuts due to the energy shortfall in the region. Google even obtained traffic data from Honda's and Pioneer's GPS navigation systems to identify the most efficient driving routes in the region. Of course information is never neutral—so Google executives had to decide whether exposing it might encourage individuals to travel to the affected areas to help (usually unwise unless one is associated with aid groups) or potentially spark a panic to flee from the Fukushima nuclear reactor.(…)

Nothing about Google Japan's response was novel per se—the services had been rolled out in other crises. But the scale of the usage set it apart from other disasters, explains Robin Moroney of Google. Unlike in Haiti's earthquake or the Southeast Asian tsunami in 2004, almost all Japanese have sophisticated cellphones and access to fast wireless and broadband networks. The result is that the Japan quake, tsunami and nuclear crisis marks the most wired data-driven disaster-relief initiative so far.

Like America's 9/11, Japan's 3/11 saw the wireless voice network fail under congestion, while e-mails and text messages passed through easily. Mobiles sometimes worked when blackouts kept everyone in the dark. Communications and information were as much a lifeline as electricity and water. (…) However technology's usefulness is not uniform. "For us old folk confused by the scarcity of information, the radio has been our most reliable source of news," wrote "Grandfather Hibiki" from Sendai in "#Quakebook", a compilation of writings organised via twitter whose proceeds are donated to charity. "Very few people of my generation use the internet," he reminded readers.

(…) What is certain is that the role of information during crises will only grow. (…) At some point, the public will have to ask itself whether maintaining such systems is the proper role of government, business or civil-society groups.
Document 3.

iPhone keeps record of everywhere you go

Charles Arthur, guardian.co.uk, Wednesday 20 April 2011 14.06 BST

Privacy fears raised as researchers reveal file on iPhone that stores location coordinates and timestamps of owner's movements

Security researchers have discovered that Apple's iPhone keeps track of where you go – and saves every detail of it to a secret file on the device which is then copied to the owner's computer when the two are synchronised.

The file contains the latitude and longitude of the phone's recorded coordinates along with a timestamp, meaning that anyone who stole the phone or the computer could discover details about the owner's movements using a simple program.

For some phones, there could be almost a year's worth of data stored, as the recording of data seems to have started with Apple's iOS 4 update to the phone's operating system, released in June 2010.

"Apple has made it possible for almost anybody – a jealous spouse, a private detective – with access to your phone or computer to get detailed information about where you've been," said Pete Warden, one of the researchers.

Only the iPhone records the user's location in this way, say Warden and Alasdair Allan, the data scientists who discovered the file and are presenting their findings at the Where 2.0 conference in San Francisco on Wednesday. "Alasdair has looked for similar tracking code in [Google's] Android phones and couldn't find any," said Warden. "We haven't come across any instances of other phone manufacturers doing this."

Simon Davies, director of the pressure group Privacy International, said: "This is a worrying discovery. Location is one of the most sensitive elements in anyone's life – just think where people go in the evening. The existence of that data creates a real threat to privacy. The absence of notice to users or any control option can only stem from an ignorance about privacy at the design stage."

Although mobile networks already record phones' locations, it is only available to the police and other recognised organisations following a court order under the Regulation of Investigatory Power Act. Standard phones do not record location data.

MPs in 2009 criticised the search engine giant Google for its "Latitude" system, which allowed people to enable their mobile to give out details of their location to trusted contacts. At the time MPs said that Latitude "could substantially endanger user privacy", but Google pointed out that users had to specifically choose to make their data available. The iPhone system, by contrast, appears to record the data whether or not the user agrees.
Document 4.

Privacy is more of a concern for app users’ 45 and older

Extent to which using location-based services/check-in apps is privacy concern

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Concerned</th>
<th>Indifferent</th>
<th>Not Concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>13-17 years</td>
<td>55%</td>
<td>38%</td>
<td>7%</td>
</tr>
<tr>
<td>18-24 years</td>
<td>52%</td>
<td>38%</td>
<td>10%</td>
</tr>
<tr>
<td>25-34 years</td>
<td>50%</td>
<td>34%</td>
<td>13%</td>
</tr>
<tr>
<td>35-44 years</td>
<td>56%</td>
<td>61%</td>
<td>10%</td>
</tr>
<tr>
<td>45-54 years</td>
<td>63%</td>
<td>56%</td>
<td>10%</td>
</tr>
<tr>
<td>55+ years</td>
<td>63%</td>
<td>56%</td>
<td>8%</td>
</tr>
</tbody>
</table>

Source: The Nielsen Company (April 2011)

*App Users = application users

Document 5.

* Le petit chaperon rouge = Little Red Riding Hood