Institut National
Universitaire
Champollion

L3 Maths Info
Anglais

Security and Privacy issues in IT

Agnès Mouysset

Cybercrime

What is it?

Brainstorming: In pairs, brainstorm as many forms of cybercrime as you can.

Can you give recent examples of cybercrime cases?

Have you or has anyone you know ever been a victim of cybercrime? What happened?

What / Who are the main targets of cybercriminals?

Watch the video about corporate security breaches

- *Fill in the table below with information from the video about several cyberattacks.*

When did the attack happen?	• *Christmas Day* •	*September 2014*
What company was attacked?	*Sony*	.....
What happened?	• .... • *important corporate data were released to the public*	....
Who were the attackers?		*not mentioned*

- *How do hackers manage to break into these company's systems, according to Hugh Thompson?*

They target specific employees, like systems administrators and use ..... to find out what their favorite ..... or sports team is and then craft an email that looks so painfully normal you really think it's from a friend or a ..... . The recipient is then ..... into clicking on a link and downloading a .....

- *What do firms like Blue Coat and Cyphort do?*

.....

- *Hackers are always isolated individuals. Right or Wrong?*

.....

- *A lot of shopping is now done online. Right or Wrong?*

.....

- *Who does PayPal work with and why?*

.....

- *What should customers do to protect themselves from hackers?*

.....

- *What should businesses do to protect themselves from hackers?*

.....

.....-the main risk factor in information security

What do you think is the missing part of this headline?

computer viruses	industrial espionage	human error	Internet fraud	terrorism

Listen to a report to check your answer.

Listen again and note down what these percentages refer to:

60%: .....

47%: .....

Reading: Cyberattack affects thousands (Wannacry)

Guess the answers to the questions below and then check your answers by reading the text.

1. How many computers were affected since the attack started?

a. 100,000 b. 200,000 c. 500,000

2. How much do the hackers want to unlock users' files?

a. $300 b. $500 c. $1000

3. What will happen within 3 days if users don't pay the ransom?

a. all their files will be deleted *c. the ransom will double*

b. a virus will completely destroy their computer

4. On Monday, how much money had the Hackers made from the attack?

a. $38,000 b. $66,000 c. $94,000

Cyber-attack should be a wake-up call, says Microsoft ***The Independent*** May 15th, 2017

1. The cyber-attack that has affected 150 countries around the world since Friday should be "a wake-up call" for governments, Microsoft says.
2. It blamed governments for storing data on software that was open to attack, which was then accessed by hackers. Microsoft said the latest virus took advantage of a weakness in Microsoft Windows that was noticed by US investigators. Information about this was stolen from the NSA (National Security Agency).
3. Many companies and organisations worldwide became victims of the WannaCry attack, including Britain's NHS (National Health Service), US courier service FedEx and French car maker Renault.
4. Russia was one of the countries that was badly affected, its Central Bank and government office computers were attacked by the virus.
5. In China, state media said more than 29,000 organisations across the country were affected, most of which were academic.
6. The virus takes control of users' files and demands $300 to get back access to data. To prevent new infections, many companies had experts working on the problem over the weekend.
7. More than 200,000 computers were affected since the attack began. By Monday, the virus was not spreading as fast, but people were still reporting cases.
8. On Monday morning, researchers found that only about $38,000 had been paid into the accounts linked to the attacks.
9. The virus threatens to delete files within seven days if the ransom is not paid, and also warns that the ransom amount will double after three days.
10. In a statement on Sunday, Microsoft president and chief legal officer Brad Smith criticised the way governments store information about security weaknesses in computer systems.
11 The company also said that many organisations had failed to keep their systems up-to-date, which allowed the virus to spread. Microsoft said they had released a Windows security update in March, but many users hadn't run it. He added that if customers didn't update their systems, there was no way for them to protect themselves against attacks.
12. Updating a personal computer can be very simple, but for an organisation like Britain's NHS, which was badly affected, it is expensive, complex and takes a lot of time.
13. The attack has also spread faster and more easily than previous ones. Once the virus infects one computer within a network, it can spread to all the computers in that network "within seconds," said Israel Levy, the CEO of the internet security firm Bufferzone.
14. For example, if one of your colleagues opens an infected PDF that is attached to an email, soon everyone in that office could be under attack.
15. Levy also said that six months ago, this problem didn't happen as this type of virus could only attack one machine at a time.
16. With help from a young security technician, the attack was stopped for a short time, but a new version of the virus soon started to infect computers again.
17. 22 year-old Marcus Hutchins, or `MalwareTech', was called an "accidental hero" after he helped to slow down the progress of the virus. He bought a web address to track it, which stopped it by chance. The web security expert's boss gave him an extra week off work because of the unexpected events. Sources: BBC News, CNN, The Telegraph

Put true (T)or false (F) next to each statement. Say why the false statements are false.

1. A fault in a Microsoft programme was the reason that hackers could attack computers with a virus.

2. Microsoft said that it was their fault that hackers could access files on government systems.

3. China has reported only a few cases of the virus.

4. Many Windows users had run security updates.

5. The virus could only attack one computer at a time.

6. A young tech expert managed to stop the progress of the virus for a short time when he was trying to find out where it came from.

Find a word or phrase in the article which means ...

1. a warning to take action to change something (noun, P.1): .....
2. made use of (something) that will give you some benefits (phrase, P.2): .....
3. people whose job it is to find out the facts about something (noun - plural, P.2): .....
4. relating to education in universities and colleges (adj., P.5): .....
5. containing the latest information (adj., P.11): .....
6. happening before something else (adj., P.13): .....
7. movement forward (noun - uncountable, P.17): .....

Discuss any of the questions below in pairs or small groups.

1. Who do you think is more to blame for this cyber-attack? Microsoft, governments or us? Why?

2. Do you think that all hackers want is money when they spread a virus? Why/why not?

3. What do you think that we can do to protect ourselves from future cyber-attacks?

Video: Protect your computer from malware

How do you protect your devices (computer, ...) from viruses, etc..?

Watch the video:

1. *Malware is short for ..... .*
2. *Malware is .....*
3. *Who uses malware? What do they use it for? How do they do it?*

   .....

   .....

   .....

4. *What should you do to protect yourself?*

   .....

   .....

   .....

   .....

   .....

   .....

   .....

5. *What shouldn't you do?*

   .....

   .....

   .....

   .....

   .....

   .....

6. *What are the signs that may warn you that your computer has been infected?*

   .....

   .....

   .....

   .....

   .....

Vocabulary

1. *Complete this product description of an Internet security program. The mixed-up letters of the missing words are in brackets.*

EFG

EFG [inta-riuvs] ..... software is the only program you need for complete protection from online threats.

EFG scans all incoming and outgoing email attachments, helping to protect your PC against [rivessu] ....., [romsw] ....., [Torsjan] ..... and other types of [lawmare] ..... . A [lawlrife] .....shields your system from attack by [reschak] ....., while the program can also detect if a website's [igidlat ercteacfiti] ..... is out-of-date or suspicious, allowing you to carry out financial transactions online with total security.

In addition to all of the above, the EFG Professional Edition also comes with email [crynetipon] ..... and the EFG [rawsyep] ..... scanner, helping you to keep your system free of unwanted advertising and [socoiek] ..... .

EFG Basic is available to download as [warfeeer] ..... by clicking here. Alternatively, you can purchase the EFG Professional Edition for only £29.95. Click here to visit our [rescue witebes] ..... or pay using PayPal by clicking here.

2. *Complete the sentences with an appropriate phrasal verb.*

break into	*shut down*	*find out*
hack into	*throw away*	*track down*
keep ahead	*log on // log off, log out*	*hand over*

- Hackers try to ..... passwords so they can penetrate a system.
- Don't ..... your password to anyone who asks for it.
- The police .....the hacker by talking to his friends and acquaintances.
- Some hackers ..... systems to get commercially valuable information.
- When you ..... to a network, you have to provide an ID.
- Never ..... your credit card receipts where someone can find them.
- It's a constant race to ..... of the hackers.
- Hackers ..... (closed) Hotmail for five hours.
- After you've transferred the money from your account, do remember to ..... from the bank's website.

Simple Past

Complete these extracts from wikis about cybercrime with the past simple form of the verbs in brackets. Then decide what kind of cybercrime each wiki is describing. Choose a word from the box.

cyberstalking	*phishing*	*spreading of malicious software*
piracy	*theft of intellectual property*	

1. In July 2001, the online file-sharing network Napster (shut)..... its website following legal action from several major record labels. .....
2. In late 2006, a computer worm (take) .....control of hundreds of pages on MySpace and (change) .....links to direct surfers to websites designed to steal their login details. .....
3. The first well-known worm (be) .....the Internet Worm of 1988, which (infect) ..... SunOS and VAX BSD systems. .....
4. A 2007 study (find)..... that 28% of female internet users had experienced online harassment. In 84% of cases, the incidents (happen) .....in a chat room. .....
5. In 2008, author J K Rowling (say)..... that a company trying to publish an online Harry Potter encyclopedia had 'stolen her words'. .....

Passives

- To form the passive we use to be and the past participle.

*They **collect** metadata at the NSA. (*Active – present simple)

*Metadata **are collected** at the NSA.* (Passive - present simple)

- To change the tense of a passive sentence, we change the tense of *to be.*

*New surveillance cameras **are being installed** in the city centre.*

*280 m music tracks **were pirated** in the UK between November 2012 and January 2013.*

*A US government website **has been hacked** twice over the weekend.*

*People who download films illegally **will be prosecuted**.*

- We often use a passive sentence when we don't want to say who performs the action because it is of little interest or difficult to know.

*Software piracy **is** sometimes **carried out** on a corporate level.*

When it is necessary to identify who performs the action, we use *by*.

*This innovative software **was designed by** BRS Labs.*

- Passive sentences can be used to report what is commonly believed to be true, using verbs such as *believe, report, estimate,say* and *think*.

*Losses due to software piracy **are estimated** at billions of dollars.*

*Cybercrime **is thought to be** a major threat to our security.*

*Edward Snowden **is believed** to have acted alone.*

- In passive structures, verb+preposition groups stay together.

*I don't like **being spied upon**.*

*My phone conversations **have been listened to**.*

- With verbs with 2 objects like *give* or *send*, a passive structure is very common.

*They have given **us** some very good advice on how to protect ourselves against phishing.*

*→**We have been given** some very good advice on how to protect ourselves against phishing.*

*They told **us** not to open suspicious attachments.*

*→**We were told** not to open suspicious attachments.*

- We often make passive with *get,* especially to suggest that things happen by accident, unexpectedly or outside our control.

*My computer **got hacked into** last week.*

Exercises: Active or Passive?

A) Put the verbs in brackets into the correct form.

1. Most bank robberies ..... (*carry out / simple present)* with a computer, not with a gun.
2. Security worries ..... *(bother / simple past)* our parents' generation as much as they bother us.
3. More sophisticated technology ..... *(use/ future with 'will')* to defeat company espionage.
4. Fifty years from now we ..... *(use / future continuous)* completely secure computer systems.
5. Make certain computer files ..... *(back up / simple present)* every night.
6. Security concerns ..... *(use / present perfect)* by politicians to justify reducing civil liberties.
7. Recently government ..... (introduce / present perfect continuous) more serious security measures.

B) *Put the verbs in brackets into the correct tense and form.*

1. The criminal who ..... (steal) personal details of thousands of Internet users ..... (catch /finally) yesterday.

2. Yesterday, Paul ..... (download) a malicious programme and his computer ..... (infect) with a virus.
3. ..... (somebody / ever / hack) into your computer?
4. What ..... (do) at the moment to stop cybercriminals from stealing money?

C) Fill in the blanks in these extracts from a Guardian article by Christian Payne with the passive form of the verbs in brackets in the right tense.

The principle of privacy is worth fighting for *Tuesday 18 March 2014*

From encryption of our day-to-day communications to well-scrutinised opensource hardware and software, securing our communications needs to become a mainstream behaviour

I once heard of a TV journalist who kept the names and addresses of his Syrian sources in a little black book.

He ..... (*to detain, simple past*) by the secret police in Damascus, which was scary for him but worse for his contacts.

The journalist ..... (*to free, simple past*), shaken but unharmed. The activists fared less well. Despite frantic efforts to warn each other and flee, some ..... (to catch, simple past) and ..... (*to hear from + not, present perfect*) since.

That all happened before the Snowden revelations. It's a reminder that even if you're unfazed by GCHQ and the NSA reading your less-than-riveting emails or tapping your boring phone conversations, issues of data security are often deadly serious.

It's often said that nothing online is private and as the Snowden files have shown, this may well be true. Nonetheless, we have a duty to not simply resign ourselves to that sorry state of affairs. Our responsibility is to do whatever we reasonably can to keep private and sensitive information exactly that - private.

Let's start with email. Email ..... (*never / to design, simple past)* to be private and anonymous. When it ..... (*to develop, simple past*) 40 years ago the main focus was to share research data from one computer to another.

Email headers and routing protocols show you who's sending and who's receiving. That's just how it works.

I'm no expert in all of this and neither is 99% of the population. But many are now fed up with governments snooping and archiving, companies scraping data in order to profile its users so it can serve more effective adverts.

I'm inherently and, I'm sure, rightly, suspicious of any app or platform that says it's secure.

Even if an app..... (*to declare, simple present)* safe by those qualified to do so, and the encryption algorithms have at least a few years' head start, what if someone has inserted malware on to the hardware to log your keystrokes, or intercept your voice and camera data before it even hits the app?

Consider encryption an act of protest and dissent, one that doesn't even require you to stand at a barricade or .....*(teargas, simple present with get).* On a larger scale, if we care about the principle of privacy in our own societies, we have to make strong encryption normal practice, for everything.

The principle of privacy, if we want privacy, needs ..... *(to fight for) at* every level. It has become a terrible cliche to talk about George Orwell's nightmare vision of 1984, but read the book again and ..... (*to remind, imperative)* of the horror it depicts. If governments can peek through your webcam, so can the criminals. If governments can read your email, so can the criminals. Sometimes they're the same thing.

Phishing Scams

Situation

You are an expert on online security. You have been invited to speak to the employees of the city council about protecting themselves. Recently, there has been great concern about people falling victim to online fraud. Senior management have decided that all the employees should receive some training on how to identify and respond to possible online scams. You have been asked to give a short presentation on the practice of phishing.

1. Use the website below to learn about phishing and record the information you find.

http://www.onguardonline.gov/articles/0003-phishing

- *How to protect yourself from phishing scams*

Type of phishing scam	Recommended action

- *Example of a phishing scam:*

2. Give your presentation.

Good ..... . It's a pleasure to be here with you today. My name is ..... and I'm going to be talking about .....

My presentation is divided into 3 parts.

First of all, I'm going to explain .....

Secondly I'm going to tell you .....

And finally, I'm going to give you an example of ..... to help you .....

Right, let's go straight to the 1st part: .....

Ok, I'd now like to turn to .....

Finally, let's look at .....

Ok, that brings me to the end of my presentation.

If you have any questions, I'll be happy to take them now.

Reading: Emails

1. *Read the emails and put them in the correct order.*

a) ....

Hi Tom

Just realized that it can't be a problem with the server becauses everyone else's machines seem to be working normally. But I still can't get into the system. Do you think it might have something to do with the Trojan that hit me last week?

Raj Fernando

b) .....

Raj

Sorry it's taken so long to get back to you. I think we've ironed out the problem now. You and the others with the same problem are all hooked up to the International Customer Database (ICB) and the problems seem to be coming from there. We've blocked the ICB (and we may need an hour or two to fix that), but you should be able to access your email now.

Tom Wilton Systems Manager

c) .....

TO ALL DEPARTMENTS
As you know, we are installing the new central server this weekend and this means the system will be completely shut down from 4 pm on Friday until some time on Saturday afternoon. Everything should be up and running by the time everyone returns to work after the weekend, but there may be a few glitches that we'll need to sort out. Please bear with us and let me know if there are any problems.
Tom Wilton Systems Manager

d) .....

Raj

Would you mind switching to your laptop for the rest of the morning? I think we may have some kind of intrusion. It's worrying, anyhow. I'll come down to your office as soon as I can, OK?

Tom Wilton Systems Manager

e) ....

Good morning Tom,

I can't log on at all this morning! I assume that the system must still be down, and that you had some unforeseen problems over the weekend. No hassle! Just checking.

Raj Fernando

f) .....

Hi Tom

I've managed to log on but there's a message on the screen that says'The system has detected that a third-party application has removed ICB3.2, possibly without your consent. This may cause programs not to run as expected.' Any ideas what that means?

Raj Fernando Assistant Marketing Director

g) .....

Dear Raj

OK, I'll see if I can find out what's going on. It could take an hour or two, OK? We seem to have two or three terminals in the building with the same problem.Tom Wilton Systems Manager

2. *Find the words and phrases 1-6 in the emails and give a synonym.*

1. hooked up to: .....
2. ironed out: .....
3. up and running: .....
4. glitches: .....
5. bear: .....
6. no hassle: .....

3. *Choose the correct modal verb to complete the dialogue.*

I was thinking of getting this antivirus program. Do you think it *might / must* be a good idea to pay for the upgrade?

Yes, probably. The free download *can't / could* be as good as the premium, and you need something reliable.

But if it's more or less the same, I *can't / could* spend all this money for nothing.

It *may not / must* be a lot better. Otherwise no one would buy it.

But it *might / might not* provide things I don't need. Like the parental controls, for example.

You know what? I think I *may / must* ask the people in the IT department for their advice.

Reading: Philip Pullman: illegal downloading is moral squalor

1. Complete the sentences using these key words from the text.

copyright theft countless outrageous piracy dazzling monetise

a) ..... is the crime of stealing.

b) If something is ....., it is extremely impressive.

c) ..... is the legal right to have control over the work of a writer, artist, musician etc.

d) If something is ....., it is extremely shocking or unreasonable.

e) ..... is the crime of making and selling illegal copies of computer programs, books, DVDs or Cds.

f) ..... means 'a very great number of'.

g) If you ..... an activity, you earn money from it.

2. Read the article

Philip Pullman: illegal downloading is moral squalor

Bestselling author says web piracy is akin to 'reaching into someone's pocket and taking their wallet' Mark Brown, guardian.com 15 September 2013

1. Illegal downloading is a kind of "moral squalor" and theft as much as reaching in to someone's pocket and stealing their wallet is theft, the author Philip Pullman will say this week. In an article for Index on Censorship, Pullman, who is president of the Society of Authors, makes a robust defence of copyright laws. He is withering about internet users who think it is OK to download music or books without paying for them.

2. "The technical brilliance is so dazzling that people can't see the moral squalor of what they're doing," he writes. "It is outrageous that anyone can steal an artist's work and get away with it. It is theft, as surely as reaching into someone's pocket and taking their wallet is theft."
3. His article comes after music industry leaders met David Cameron in Downing Street last Thursday where the issue of web piracy was discussed.
4. Pullman, writer of the *His Dark Materials* trilogy, says authors and musicians work in poverty and obscurity for years to bring their work to the level "that gives delight to their audiences, and as soon as they achieve that, the possibility of making a living from it is taken away from them". He concludes: "The principle is simple, and unaltered by technology, science or magic: if we want to enjoy the work that someone does, we should pay for it."
5. Pullman is writing in the next issue of the campaign group's magazine in a dialogue with Cathy Casserly, chief executive of Creative Commons, which offers open content licences "that lets creators take copyright into their own hands". Casserly argues that there is much wrong with copyright, which was created "in an analogue age". She writes: "By default, copyright closes the door on countless ways that people can share, build upon, and remix each other's work, possibilities that were unimaginable when those laws were established."
6. She says artists need to think creatively about how they distribute and monetise their work, quoting the science fiction writer Cory Doctorow who said: "My problem is not piracy, it's obscurity."
7. *Index on Censorship* agrees. The magazine's editor, Rachael Jolley, said: "Existing copyright laws don't work in the digital age, and risk criminalising consumers. We need new models for how artists, writers and musicians earn a living from their work."
8. The debate is a lively one and the scale of illegal downloading vast. Data collected by Ofcom suggests that between November 2012 and January 2013 in the UK, 280m music tracks were digitally pirated along with 52m TV shows, 29m films, 18m ebooks and 7m software or games files.
9. Ofcom has said 18% of internet users aged over 12 admit to having recently pirated content, and 9% say they fear getting caught. Pullman writes in his article: "The ease and swiftness with which music can be acquired in the form of MP3 downloads is still astonishing to those of us who have been building up our iTunes list for some time."
10. One thing to emerge from the Downing Street meeting was Cameron's appointment of the Tory MP Mike Weatherley to be his adviser on the subject. A spokesman for the BPI, the record industry trade body, said: "Mike Weatherley is a strong champion of copyright and the artists and creative producers it's there to protect. We hope his influence and the prime minister's endorsement of copyright will be brought to bear on the approach of the UK's intellectual property office."

squalor ['skwɒlə] = misère noire, conditions sordides (*to live in squalor*)

3. Choose the <u>best</u> answer.

1) What does Philip Pullman think of people who download music or books without paying for them?

a) He compares them to pickpockets.

b) He calls them pirates.

c) He calls them criminals.

2) What, according to Cathy Casserly , is wrong with copyright laws?

a) They do not prevent piracy.

b) They were created in an analogue age.

c) They prevent people from sharing, building upon and remixing each other's work.

3) What, according to Pulmann, is "a simple principle"?

a) That people should pay for enjoying someone else's work.

b) That the possibility of making a living from your work should be taken away from you.

c) That it is too easy and swift to download music.

4) What, according to the editor of *Index on Censorship,* is the potential problem of existing copyright laws?

a) They are not creative enough when it comes to distributing artists' work.

b) They might criminalize consumers.

c) They do not enable artists, writers and musicians to earn a living from their work.

4. Find the word

1. a three-word phrasal verb meaning *manage to do something bad without being punished for it (*§ 2): .....
2. a verb meaning *state that someone is guilty of a crime when they thought they were acting legally* (§ 7): .....
3. a noun meaning *an occasion when someone gives official or public support to a person or thing* (§ 10): .....

5. Discussion

Should people be criminalized for downloading music, films, books and so on from the internet free of charge? Why? Why not?

6. Role playing: *In groups of 4, talk about the issue of digital music distribution (what some may label 'piracy' while others call it 'file-sharing'!).*

Jake A successful musician He has made money from selling music and this money has been hard earned.	**Rob** A struggling musician who is trying to break into the music business
Megan An executive who works for a large record label	**Luis** A young music fan

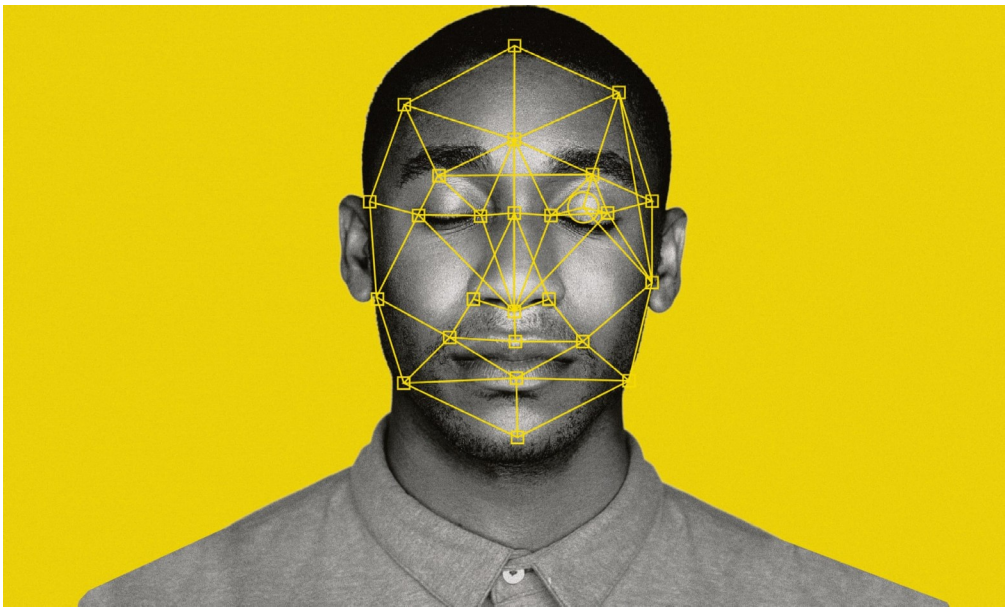
Surveillance

Facial Recognition

In groups, brainstorm how you would answer the following questions:

- *Where is the technology used and what for? (some ideas: Facebook / Airports / Shopping centres / Football stadiums / Mobile Phones)*

- *How does it work?*



- *How accurate is it?*

- *Your opinion*

Minority Report : Science Fiction and Reality

Watch the 1st scene (beginning to 13.30)

- **Beginning →1:50: the murder scene**

Who? What? Why?

.....

.....

- **1:50 → 13:30**

  - **at the Department of Precrime**

Year? .....

Explain Jon Anderton's job (he's the character played by Tom Cruise)

.....

.....

What is 'precrime'?

.....

.....

*How do the precrime officers **know** that someone is going to commit murder? Who tells them?*

.....

.....

Who's Danny Witwer?

.....

What is Jon trying to do?

.....

.....

Why is Jon's job particularly difficult today?

.....

.....

- **Howard Marx's arrest:**

What kind of gadgets / devices are used by the precrime department?

.....

.....

.....

Complete Jon's sentence:

'You're under arrest for.....
..... at 08.00 hours and 4 minutes.'

What does Howard Marx say?
'I ..... anything'.

What do you think about this sentence?
.....

- **14:11→15:23: the commercial about precrime**

What is the country going to vote about?
.....

Would YOU vote 'yes'? Why or why not?
.....

.....

.....

- **Watch the scene at the shopping mall (Scene 16 -1:25:00→1:25:30)**

Describe what happens in the store. Think about iris recognition and personalised ads.

.....

.....

How true today is Minority Report's world?

During pre-production, Spielberg consulted numerous scientists in an attempt to present a more plausible future world than that seen in other science fiction films

Spielberg described his ideas for the film's technology to before the movie's release:
'I wanted all the toys to come true someday.I want there to be a transportation system that doesn't emit toxins into the atmosphere. And the newspaper that updates itself... The Internet is watching us now. If they want to. They can see what sites you visit. In the future, television will be watching us, and customizing itself to what it knows about us. The thrilling thing is, that will make us feel we're part of the medium. The scary thing is, we'll lose our right to privacy. An ad will appear in the air around us, talking directly to us. '

What kind of technologies used in the film have become reality? Are about to become reality?

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

CNN video: BRS Labs, Houston

What is the aim of the new software designed by BRS Labs in Houston?

How does it work?

Any differences with the Minority Report movie?

What are privacy advocates worried about?

What do the people at BRS Labs claim when these objections are raised?

Are we all spied upon?

Reading: The End of Forgetting Jeffrey Rosen

We've known for years that the Web allows for unprecedented voyeurism, exhibitionism and inadvertent indiscretion, but we are only beginning to understand the costs of an age in which so much of what we say, and of what others say about us, goes into our permanent - and public - digital files. The fact that the Internet never seems to forget is threatening, at an almost existential level, our ability to control our identities; to preserve the option of reinventing ourselves and starting anew; to overcome our checkered pasts...

1. What new Age have we recently entered according to Jeffrey Rosen?

2. Do you think '*The End of Forgetting*' is a good title for this text? Why?

3. The purpose of the article is:
   - to make people aware of the dangers of personal exposure on the web.
   - to criticize the government for not taking action against indiscreet websites.
   - to encourage people not to use the internet.

1. Four years ago, Stacy Snyder, then a 25-year-old teacher in training at Conestoga Valley High School in Lancaster, Pa., posted a photo on her MySpace page that showed her at a party wearing a pirate hat and drinking from a plastic cup, with the caption "Drunken Pirate." After discovering the page, her supervisor at the high school told her the photo was "unprofessional," and the dean of Millersville University School of Education, where Snyder was enrolled, said she was promoting drinking in virtual view of her under-age students. As a result, days before Snyder's scheduled graduation, the university denied her a teaching degree. Snyder sued, arguing that the university had violated her First Amendment rights by penalizing her for her (perfectly legal) after-hours behavior. But in 2008, a federal district judge rejected the claim, saying that because Snyder was a public employee whose photo didn't relate to matters of public concern, her "Drunken Pirate" post was not protected speech.

1) *What did Stacy Snyder post on MySpace?*

2) *What does the term 'First Amendment' refer to?*

3) *Match the following words or abbreviations with their equivalent:*

Pa. = Patagonia / postal address / Pennsylvania
Caption = descriptive phrase / pirate's cap / alcohol
Dean = former student / head / secretary
To sue = To go to court / to perspire / to complain loudly

4) *Did Stacy win her trial against Millersville University? Why?*

2. When historians of the future look back on the perils of the early digital age, Stacy Snyder may well be an icon. The problem she faced is only one example of a challenge that, in big and small ways, is confronting millions of people around the globe: how best to live our lives in a world where the Internet records everything and forgets nothing - where every online photo, status update, Twitter post and blog entry by and about us can be stored forever. With Web sites like LOL Facebook Moments, which collects and shares embarrassing personal revelations from Facebook users, ill-advised photos and online chatter are coming back to haunt people months or years after the fact. Examples are proliferating daily: there was the 16-year-old British girl who was fired from her office job for complaining on Facebook, "I'm so totally bored!!"; there was the 66-year-old Canadian psychotherapist who tried to enter the United States but was turned away at the border and barred permanently from visiting the country - after a border guard's Internet search found that the therapist had written an article in a philosophy journal describing his experiments 30 years ago with L.S.D.

1) *True or false : justify your answer*

a) The case of Stacy Snyder will soon be forgotten.

b) Some websites collect and highlight embarrassing information on people

c) A British girl was fired because she told her boss she was bored.

d) A Canadian Citizen was rejected at the US border because of an internet search.

2) *Many firms now use the web to get background information on their future employees. What sort of information can recruiters find on the internet? What tools do they use? What are the consequences of these practices?*

3. We've known for years that the Web allows for unprecedented voyeurism, exhibitionism and inadvertent indiscretion, but we are only beginning to understand the costs of an age in which so much of what we say, and of what others say about us, goes into our permanent - and public - digital files. The fact that the Internet never seems to forget is threatening, at an almost existential level, our ability to control our identities; to preserve the option of reinventing ourselves and starting anew; to overcome our checkered pasts.

4. In a recent book, *Delete: The Virtue of Forgetting in the Digital Age*, the cyberscholar Viktor Mayer-Schönberger cites Stacy Snyder's case as a reminder of the importance of "societal forgetting." By "erasing external memories," he says in the book, "our society accepts that human beings evolve over time, that we have the capacity to learn from past experiences and adjust our behavior." In traditional societies, where missteps are observed but not necessarily recorded, the limits of human memory ensure that people's sins are eventually forgotten. By contrast, Mayer-Schönberger notes, a society in which everything is recorded will "forever tether us to all our past actions, making it impossible, in practice, to escape them." He concludes that "without some form of forgetting, forgiving becomes a difficult undertaking."

5. It's often said that we live in a permissive era, one with infinite second chances. But the truth is that for a great many people, the permanent memory bank of the Web increasingly means there are no second chances - no opportunities to escape a scarlet letter in your digital past. Now the worst thing you've done is often the first thing everyone knows about you.

1) What is the difference between voyeurism and inadvertent indiscretion?

2) In what way does the internet threaten our ability to control our identities?

3) Viktor Mayer-Schönberger mentions 'societal forgetting' to describe the traditional way people forget about past mistakes. What expression does Jeffrey Rosen use when referring to an internet that never forgets?

4) In the last paragraph of the text, can you explain the expression 'a scarlet letter in your digital past'? Search the internet if you don't know what a 'scarlet letter' refers to.

Debating:

A: The right to be forgotten (officially recognised in French law in 2010) should be a universal human right.

B: Some countries may use it to curb free speech.

Video: Edward Snowden

What do you know about Edward Snowden?

Watch the video and explain why Edward Snowden is considered by some as a traitor and by others as a hero.

What do <u>you</u> think?

Debating:

- *Should whistleblowers be protected?*
- *Individual privacy matters more than national security*

The truth about Mass Surveillance and the State, with your host

Brenda the Civil Disobedience Penguin

"The US Government has built a system that has as its goal the complete elimination of electronic privacy worldwide."

This is incredible!

I've just read Glenn Greenwald's new book on Snowden. I read it all the way through, it even has pictures.

Imagine the sum total of everyone's communications on the internet.

Billions of phone calls and emails every day - exabytes of metadata, all of our hopes and dreams and sadness captured by the NSA in huge server farms.

The infinite and unfathomable sadness of all of that data.

It seems privacy is for people who have something to hide.

Well I have things to hide. Not illegal things, not even very interesting things, but they're my things. And it's nobody else's business.

SECRET PENGUIN BUSINESS

If you are always being watched, you are not free. Eventually you will internalise the surveillance and act accordingly. Don't just take this penguin's word for it - it's actual really truly science.

NSA

FYI more people in the U.S.A are killed by lightning than by terrorism.

www.firstdogonthemoon.com

You can use a VPN or Tor or whatever but most folk couldn't be bothered. Those things are a pain the butt.

Now connect your PGP Proxywoozle to the FAPnet servobot

And whatever you do don't insult Anonymous because those people are... they're... lovely people. Lovely, lovely people.

Whether it is done openly or in secret, mass surveillance is inherently repressive, regardless of whether or not the state misuses the data, which of course they do that is their job.

You are all suckers. They own you!

Things we have learnt as a result of reading "No place to hide" by Glenn Greenwald

- Edward Snowden is a proper hero
- The NSA knows you read this cartoon.
- No seriously they actually know.
- How about the fourth amendment of the U.S. Constitution you people are funny
- Yes I know Steve Bell drew penguins in The Guardian first, it's an homage
- Alright it's not an homage but he doesn't have a penguin monopoly does he?
- I can be a drawer of penguins if I want
- FYI I would play Penguin Monopoly.

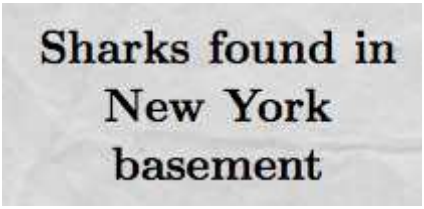
3 HOTELS ON ROSS ISLAND!

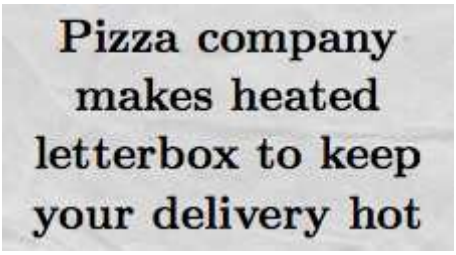
first dog on the moon

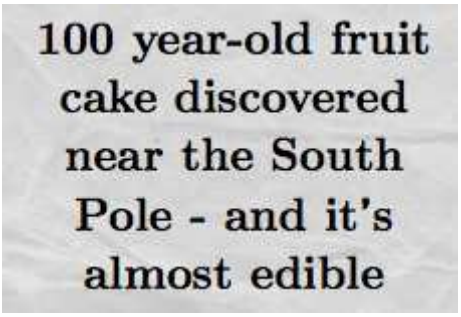
Real or fake news?

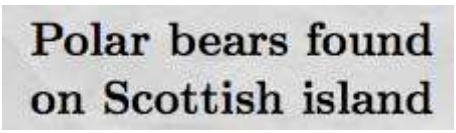
What is fake news?

Work in small groups. Decide if these stories are real or fake news









Discuss:

1. Do you think that most people are able to spot if news is fake or real? Why/why not?

2. Do you think that experts are right to be worried about the power of fake news? Why/why not?

3. How do you think that we can deal with the problem on the internet?

Are we trading privacy for convenience?

Do you shop online or order and buy over the phone? Have you always had a good experience?

Do you ever look at the targeted ads that appear on the websites you are logged on to? What do you think of them?

Video: Pizza Palace

What is the customer doing?

How does the customer sound when he answers 'Yes' to 'Is this Mr Kelly?'

What does the pizzeria employee mean when she says 'We just got wired into the system, sir'?

What does she know about James Kelly?

Did James finally order what he first wanted to order? How does he sound?

What do you think of 'Hmmm...Up to you, sir.'?

Give your opinion on the video.

Speaking: If it's free, it means <u>you</u> are the product.

The IoT (Internet of Things)

What is the Internet of Things?

Role play: the Internet of things

Past Paper:The government just admitted it will use smart home devices for spying

Trevor Timm The Guardian 9 February 2016

1. If you want evidence that US intelligence agencies aren't losing surveillance abilities because of the rising use of encryption by tech companies, look no further than the testimony on Tuesday by the director of national intelligence, James Clapper. As the Guardian reported, Clapper made clear that the internet of things – the many devices like thermostats, cameras and other appliances that are increasingly connected to the internet – is providing ample opportunity for intelligence agencies to spy on targets, and possibly the masses. And it's a danger that many consumers who buy these products may be wholly unaware of. "In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials," Clapper told a Senate panel as part of his annual "assessment of threats" against the US.

2. Clapper is actually saying something very similar to a major study done at Harvard's Berkman Center released last week. It concluded that the FBI's recent claim that they are "going dark" – losing the ability to spy on suspects because of encryption – is largely overblown, mainly because federal agencies have so many more avenues for spying. This echoes comments by many surveillance experts, who have made clear that, rather than "going dark", we are actually in the "golden age of surveillance".

3. Privacy advocates have known about the potential for government to exploit the internet of things for years. Law enforcement agencies have taken notice too, increasingly serving court orders on companies for data they keep that citizens might not even know they are transmitting. Police have already been asking Google-owned company Dropcam for footage from cameras inside people's homes meant to keep an eye on their kids. Fitbit data has already been used in court against defendants multiple times. But the potential for these privacy violations has only recently started reaching millions of homes: Samsung sparked controversy last year after announcing a television that would listen to everything said in the room it's in and in the fine print literally warned people not to talk about sensitive information in front of it.

4. While Samsung took a bunch of heat, a wide array of devices now act as all-seeing or all-listening devices, including other television models, Xbox Kinect, Amazon Echo and GM's OnStar program that tracks car owners' driving patterns. Even a new Barbie has the ability to spy on you – it listens to Barbie owners to respond but also sends what it hears back to the mothership at Mattel.

5. Then there are the rampant security issues with the internet of things that allow hackers – whether they are criminal, government or something in between – to access loads of data without any court order, like the creeps who were eavesdropping on baby monitors of new parents. Just a few weeks ago, a security researcher found that Google's Nest thermostats were leaking users' zipcodes over the internet. There's even an entire search engine for the internet of things called Shodan that allows users to easily search for unsecured webcams that are broadcasting from inside people's houses without their knowledge.

6. While people voluntarily use all these devices, the chances are close to zero that they fully understand that a lot of their data is being sent back to various companies to be stored on servers that can either be accessed by governments or hackers.

7. While Clapper's comments are generating new publicity for this privacy worry, the government has known about the potential to exploit these devices for a long time. The then CIA director David Petraeus made clear that intelligence agencies would use the internet of things to spy on people back in 2012, saying: 'Items of interest will be located, identified, monitored and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters – all connected to the next-generation internet using abundant, low-cost, and high-power computing.' As Wired put it, Petraeus was expressing excitement the CIA would soon be able to spy on you through your dishwasher.

8. Author and persistent Silicon Valley critic Evgeny Morozov summed up the entire problem with the internet of things and "smart" technology in a tweet last week: While internet-connected devices are not going away – it's a certainty they will only get more prevalent – it's important that companies make them as secure as the end-to-end encryption the FBI director loves to complain about, and that we press the government to enact strict new rules to prevent our privacy from being invaded thanks to the weakest link among televisions or dolls or thermostats that line billions of homes around the world.

Read <u>The government just admitted it will use smart home devices for spying</u>

1. **Choose the best answer. (2 marks)**

- The Internet of Things is

□ the Internet infrastructure linking our computers, tablets and smartphones

□ a network where objects such as dishwashers are connected to the Internet

□ a future network of virtual objects

- What may increasingly expose our private lives to potential snoopers and hackers?

□ our smartphones, tablets and computers

□ our home cameras, fitness trackers, thermostats,

□ our shopping habits

2. **Right or Wrong? Justify your answer by quoting from the article. (16 marks)**

a) Only people suspected of being criminals will have their devices spied upon by US intelligence agencies. **R W**

.....

.....

b) When people buy Internet-connected devices, they know the data produced by these devices is not secure. **R W**

.....

.....

c) The FBI has recently complained about being prevented from accessing encrypted messages. **R W**

.....

.....

d) According to many experts, it has never been easier to spy on private individuals. **R W**

.....

.....

e) US police and courts are not allowed to use data provided by connected devices. **R W**

.....

.....

f) Samsung was widely criticised when they announced an all-listening television. **R W**

.....

.....

g) The data collected by smart home devices is securely protected from hacking. **R W**

.....

.....

h) We do not know yet if smart home devices will become popular with consumers. **R W**

.....

.....

3. Find words in the article that can be used to complete the following sentences. (2 marks)

- **Paragraphs 2 and 3:**

1. If something is ....., it is exaggerated, made to seem greater than it really is.
2. People who publicly support something are its ..... .

- **Paragraphs 4 and 5:**

3. If you are secretly listening to other people's conversations, you are ..... on them.

- **Paragraphs 6, 7 and 8:**

4. If something is ....., it is put firmly and deeply into something else.

Write 180 words (+ or – 10%) on ONE of the following topics: (20 marks)

1. Apple's CEO Tim Cook has recently refused to let the FBI gain access to the locked iPhone of a main suspect in the San Bernardino's mass shooting. Do you agree?

2. Are you looking forward to living in a smart home filled with Internet-connected devices?

3. Are you worried about how much you've left online (embarrassing photos, unwise comments, past mistakes, things you posted and then regretted...) or do you think this is the price to pay for the convenience of the Internet? How do you protect your online privacy?

Vocabulary

Translate the words and expressions below and write a sentence for each one.

to be available at the click of a mouse
to be aware of

to back up data
a bait
to betray sensitive data
biometric security devices
to bombard a website
a cybersecurity **breach**
to breach a system
to breach privacy
to break into a system
to bring down / to take down a website
to bypass security measures

to cash in (on people's fear of losing their computer files)
censorship
Do the benefits of the digital age **come at a cost to** our privacy?
to be compromised
to comply with rules / regulations
convenient
to crash a website
cyberwarfare

to damage data
to deceive / **to fool / to cheat** somebody

to encroach on (our privacy)
to encrypt data = chiffrer des données

to be fooled by a scam
foolproof
to forge
fraud

genuine
to get into a system
to give up privacy **for the sake of** convenience
to guarantee privacy

a hack (= a break-in)
to hack into a system
to hijack a computer

to be **immune to** (cyberattacks)
to impersonate a business
to infect a computer
to interfere with
to invade somebody's privacy

to keep ... secret

to launch a malicious programme

malicious
to mine data

Do the benefits of convenience **outweigh** those of privacy?

to pretend (to...)c
to propagate a virus

ransomware
to replicate itself
to reveal personally **sensitive** information
to respect people's **right to** privacy

a scam
a scammer
to scramble data
to secure a website
to snoop on / **to spy on**
a spoof site
to spread a virus
to spread to other computers
to stalk someone
to steal data
to sue somebody

to show **tailored** adverts
to tap someone's phone
to tap into a system
to be **tech-savvy**
a threat to privacy **/ to threaten** people's privacy
to be **under threat**
to track down somebody
to track people's web use
to trick people **into** giv**ing** sensitive information / **into** reveal**ing** personal information

to be wary of ...
to weigh the benefits of ..... **against** the risks

Language practice

1. *Find the appropriate prefixes or suffixes to form the following words.*

charger	to load	to ..... *télécharger (vers un serveur) / téléverser*
		to ..... *télécharger (depuis Internet)*
pouvoir	to be able	to ..... *mettre un site hors d'état*
numérique	digital	to ..... *numériser*

2. *Form 4 compound nouns with the following elements and translate.*

digital, divide, engine, identity, provider, search, service, theft

.....	.....
.....	.....
.....	.....
.....	.....

3. *Translate. (Mind the 'faux amis'!)*

- You will be charged if you listen to music on this website.
  .....
- A cracker is someone who manages to steal information on someone else's computer.
  .....
- You need to register on the site before you can post a message.
  .....

4. *Translate into French.*

- Digital natives are supposed to prefer watching videos on YouTube to reading books.
  .....
- I was able to retrieve my parents' confidential data in a few clicks.
  .....
- Their website went down last week and has been off-line since then.
  .....
- Should the authorities crack down on illegal downloading?
  .....

5. *Translate into English.*

- Tu risques d'avoir une amende si tu télécharges illégalement des films ou des clips.
  .....

Glossary (technical terms)

algorithm: a set of precise rules or instructions for solving a problem.

anti-virus (program or software): a computer program or set of programs used to detect, identify and remove viruses from a computer system.

applications (program or software): a computer program designed to be used for a particular purpose, e.g. a word processor, spreadsheet or database program.

authentication: a process that checks the identity of a user or an object.

to back up: to store a copy of data on a storage device to keep it safe.

biometric device: a security device that measures some aspect of a living being, e.g. a fingerprint reader or an eye scanner.

chatroom: a virtual space on a website where online discussions organized around specific interests are held in real time by users typing messages.

to crack: to break into a computer system in order to steal information or cause damage.

cyberspace: the combination of all the data on all the computer networks throughout the world accessed using the Internet.

database (program): a type of applications program used for storing information so that it can be easily searched and sorted.

data mining: the process of analysing a large amount of stored data to find new useful information.

to decipher: to change coded information into normal text.

to decrypt: to recover the original text from an encrypted message.

to debug: to correct an error from a programme, remove a bug.

defacing: a computer crime that involves changing the information shown on another person's website without permission.

denial of service attack: a type of computer crime that involves swamping a server with large numbers of requests.

digital certificate: an electronic message used to show a transaction is trustworthy. It contains information about the company processing the transaction including their public key and is electronically 'signed' by a trusted digital-certificate issuer.

to eavesdrop (on a conversation, a phone call...): to secretly listen to someone's conversation

email attachment: a file that is attached to an email message.

to encrypt: to transform data into coded form to make it secure.

encryption: the transformation of data into coded form to make it secure.

firewall: a combination of hardware and software used to control the data going into and out of a network. It is used to prevent unauthorised access to the network by hackers.

freeware: computer programs that are available to anyone who wants to use them at no cost to the user.

global positioning system (GPS): a system that determines the user's location by comparing radio signals from several satellites.

hacker: a skilled programmer who attempts to gain unauthorised access to a network system.

hijacking: a computer crime that involves redirecting anyone trying to visit a certain website elsewhere.

host: a program that carries a virus. / a computer that provides a service on a network.

Internet service provider (ISP): an organisation that provides Internet connections for a fee.

iris recognition: the process of identifying a user by scanning their eyes.

keystroke: the process of pressing and releasing a key on a keyboard.

mail bombing: a computer crime that involves inundating an email address with thousands of messages slowing or even crashing the server.

metadata: data about data in a document.

Open Source: part of a system of software development where anyone is free to take a copy of the source code and extend, develop or fix bugs in it.

to patch: to make a small repair, to correct a programme by inserting a fix.

piggy-backing: a computer crime that involves using an other person's identification code or using that person's files before he or she has logged off.

PIN (Personal Identification Number): a unique number used by electronic systems to indicate who a person is.

PlayStation: a games console developed by the Sony Corporation.

public key cryptography: a method of coding messages using public and private keys to prevent others from reading them.

raw data: data that has not been processed.

salami shaving: a computer crime that involves manipulating programs or data so that small amounts of money are deducted from a large number of transactions or accounts and accumulated elsewhere.

smart card: a plastic card containing a processor and memory chip. It can be used to store large amounts of confidential data.

software piracy: a computer crime that involves unauthorised copying of a program for sale or distributing to other users.

spoofing: a computer crime that involves tricking a user into revealing confidential information such as an access code or a credit card number.

streaming: a process of downoading and storing the next part of a computer signal while the first part is being used.

trapdoor: a technique used in a computer crime that involves leaving within a completed program an illicit program that allows unauthorised and unknown entry.

Trojan: a technique used in a computer crime that involves adding concealed instructions to a computer program so that it will still work but will also perform prohibited duties. It appears to do something useful but actually does something destructive in the background.

to troubleshoot: to find and fix faults in a system.

to unencrypt: to remove the encryption from a file.

user-authentication system: a system that identifies users.

Oral exam

You will play the role of a student exchanging ideas with another student about one of the following topics. Do some research into the topic at home but don't bring any written sentences / dialogue to your oral exam, only a few key words / ideas.

1.
Role A: You have decided to shut your Facebook account because you agree with Leif Harmsen, who says: 'It's not "your" Facebook profile, it's Facebook's profile about you.' You never shop online and think both big corporations and governments are increasingly tracking people online.

Role B: You are an Internet addict, you love the convenience of social networking sites and online shopping and think only criminals have something to fear from 'Internet surveillance'.

2.
Role A: A few years ago, the high court of justice of the United Kingdom ordered 6 broadband providers to block access to 3 music and movie file-sharing websites. You agree with this decision, which seems to be the only way to fight online piracy and protect artists.

Role B: You don't agree and think people should be allowed to download movies and music tracks for free.