The Biggest Cybersecurity Breaches of the Last Decade

- Why do you think cybersecurity has become such a high priority for many companies?
- What are some common mistakes that people make with personal cybersecurity?
- Do you know of any important hacks? What were they, and what effect did they have?
- Have you ever seen any movies about hackers? How are they depicted?

1. Read about four of the biggest cybersecurity breaches in the last decade and match the article with the headline. Two of the headlines are not used.

Wordpress Apologizes for Recent Security Breaches

Spyware Companies Hacked: A lesson in Irony

Timing of Devastating Attacks "no coincidence" Government Officials say

North Korea fights back against Hackers!

Bad English Saves Millions!

Outrage Grows: How the Elite have been Cheating all along

a) *Timing of Devastating Attacks "no coincidence" Government Officials say*

In December of 2015, a piece of malware attacked the Ukrainian power grid, causing massive blackouts across Ukraine. One year later a similar attack happened, this time causing even more blackouts. The Malware is called "Industroyer" and was created by a hacking group called Sandworm. The group are thought to be connected to the Russian government, and the attacks were co-ordinated with Russia's invasion of Crimea.

b) *Bad English Saves Millions!*

In 2016 hackers attempted to steal $81 billion from various banks around the world by sending fraudulent money transfer requests. The Reserve Bank of New York blocked the requests due to suspicious spelling mistakes on the transfer request, but the Bank of Bangladesh lost almost $100 million. The hack resulted in massive security updates to SWIFT, the international money transfer system, and resulted in SWIFT banning North Korea, who are thought to be behind the attack, from their system.

c) *Outrage Grows: How the Elite have been Cheating all along*

"The Panama Papers" are documents that revealed how thousands of the world's richest people use tax havens to avoid paying taxes. In 2016 the documents were leaked from Panamanian law firm Mossack Fonseca. The firm's outdated WordPress website was easily breached by hackers. Daphne Caruana Galizia, the first journalist to report on the leaks, was killed by a car bomb a year after she went public with the papers.

d) *Spyware Companies Hacked: A lesson in Irony*

In 2014 a hacktivist called "Phineas Fisher" started hacking into several software companies. Phineas leaked the source-code and many internal documents from multiple companies, exposing the companies for developing shady hacking tools and surveillance programs.

2. Look at the predictions and discuss with a partner whether or not you agree with the predictions. Match the underlined phrases to their definition below.

- I think passwords will almost certainly become obsolete, and most online clearance checks will be done by fingerprint or facial scans.
- It's only a matter of time before someone hacks a military drone.
- It's unlikely that the average person will get hacked or have their data stolen.
- Eventually it will be possible to hack into a person's thoughts!
- I doubt that my country's government actively tries to hack other countries or organisations

a) It will happen, but we don't know when *It's only a matter of time*

b) I don't think it will happen *doubt*

c) It will very, very probably happen *almost certainly*

d) It probably won't happen *It's unlikely*

e) It will happen, but after a long time *Eventually*

3. Now make some predictions of your own about technology using the phrases above.

4. You are going to watch a video about a dangerous computer virus. The vocabulary in the box is contained in the video. Complete the sentences with the words in the box.

forged	dormant	centrifuge
lurking	capabilities	exploit
clearance	evidence	watchdog

a) The man was seen *lurking* around the house a few hours before the robbery.

b) I'm afraid you don't have the *clearance* to access that information.

c) Uranium can be enriched (made more powerful) by spinning it in a special *centrifuge.*

d) Some fashion brands *exploit* people in poor countries, setting up sweat shops for cheap labour.

e) There is no *evidence* that the virus came from North Korea.

f) The documents were clearly *forged,* they didn't even have the correct stamp on them.

g) This virus can lie *dormant* for years until somebody decides to activate it.

h) The SEC is the major financial *watchdog* in America. It's their job to make sure companies follow the law.

i) The old video conferencing software didn't have screen sharing *capabilities,* so we had to get a new one.

5. Watch the video "Stuxnet: The Virus that almost started WW3"[1] and answer the questions.

a) Was Stuxnet the most sophisticated/complex virus in the world when it was created? *Yes*

b) What is the difference between the clearance the Stuxnet virus has and the clearances most other viruses have? *Stuxnet had real clearances, not forged ones.*

c) What could Stuxnet do to nuclear power reactors? *It could shut down nuclear powerplants*

d) What is a zero day, and why are some hackers willing to pay so much for them? *System gaps or weaknesses that the creators are unaware of*

e) Why do some people believe Israel was behind Stuxnet? *Because the virus code has references to the Hebrew bible*

[1] https://www.youtube.com/watch?v=7g0pi4J8auQ&ab_channel=RealHumanStories