"Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds."

John Perry Barlow (1947 – 2018), American political activist and privacy campaigner

1. Data Protection Discussion

1. What is data protection and why is it so important in the modern day?
– Data protection involves safeguarding sensitive information from unauthorized access, use, or disclosure. It's crucial in the modern age due to the vast amount of personal and sensitive data stored digitally, making individuals vulnerable to identity theft, financial fraud, and privacy breaches.

2. What are the different types of personal information that exist?
– Personal information encompasses a wide range of data, including but not limited to: names, addresses, phone numbers, email addresses, social security numbers, financial information, medical records, biometric data, and online identifiers like IP addresses.

3. Are we sharing too much information publicly these days?
– There is a growing concern that individuals are sharing too much personal information publicly, especially on social media platforms, which can lead to privacy violations, identity theft, and exploitation by malicious actors.

4. How dangerous do you think it is to put personal information on social networking sites like Facebook?
- Sharing personal information on social networking sites like Facebook can be extremely dangerous as it increases the risk of identity theft, cyberstalking, harassment, and unauthorized access to sensitive data. Additionally, the information shared on these platforms can be used for targeted advertising or manipulation.

5. What information have you seen shared on social networking sites that you wouldn't feel comfortable sharing yourself?
- Examples of personal information shared on social networking sites that one might not feel comfortable sharing include: home addresses, phone numbers, financial details, personal relationships, travel plans, and intimate photos or videos.

6. Are you sure all of your personal information is secure? How do you keep your personal information safe?
- Ensuring the security of personal information requires implementing robust security measures such as using strong, unique passwords, enabling two-factor authentication, regularly updating privacy settings, being cautious about sharing sensitive information online, and using encryption tools for data protection.

7. Are you always careful about what documents you throw away?
- It's essential to be mindful of what documents are discarded, as they may contain sensitive information that could be exploited by identity thieves or fraudsters. Shredding documents containing personal data before disposal can mitigate the risk of unauthorized access.

8. What personal information do you regularly give to companies or other organizations? How can you be sure they will keep that information safe?
- Companies and organizations regularly collect personal information from individuals for various purposes such as account registration, online purchases, and marketing activities. To ensure the safety of personal information shared with these entities, individuals should review privacy policies, opt-out of unnecessary data collection, and choose reputable organizations with strong data protection measures in place. Additionally, staying informed about data breaches and exercising caution when sharing personal information online can help mitigate risks.

- **data protection** (noun) – *a legal requirement to protect personal information stored on a computer system.*
- **biometric data** (noun) – *information that relates to a person's physical or biological characteristics.*
- **to hack** (verb), **hacker** (noun) – *to gain unauthorised access into a computer system; a person who hacks.*
- **to encrypt** (verb), **encryption** (noun) – *to convert electronic data or communications into code that cannot be read by another person unless they have the encryption key.*
- **VPN (virtual private network)** (noun) – *an encrypted internet connection that keeps sensitive communications secure and prevents activity on the internet from being traced.*
- **data breach** (noun) – *the unauthorised release of information stolen from a computer system.*

Using the vocabulary words above, complete the following sentences (remember to use the correct form of the word, e.g. verb conjugation or plural noun):

1. Every business needs to pay attention to data protection laws if they don't want to face hefty compensation claims.
2. Hackers released thousands of documents from Mossack Fonseca's computer system that showed the offshore bank accounts held by the world's elite.
3. If you have any files you don't want hackers to read, it's vital that you encrypt them.
4. In 2017, Equifax suffered a data breach which led to the social security numbers of 145 million Americans being made public.
5. One advantage of using a VPN is that you can set your IP address to another country and access the Netflix library of that country.
6. The new passport will contain biometric data including fingerprints and a retina scan to help prevent illegal migration.

Data Protection vocabulary comprehension questions

1. What do you know about the data protection laws in your country?

- In Spain, data protection laws are primarily governed by the Organic Law on Data Protection and guarantee of digital rights (LOPDGDD) and the General Data Protection Regulation (GDPR) of the European Union. These laws establish the principles and requirements for the safe and legal handling of personal data in the country, ensuring the privacy and rights of Spanish citizens.

2. What kind of biometric data is stored about you?

- In Spain, stored biometric data may include fingerprints, facial features, voice structures, and even genetic information in some cases, depending on the applications or services used.

3. What are some common reasons why people hack computers?

- Common reasons why people hack computers may include stealing personal or financial information, industrial espionage, system sabotage, data hijacking for extortion (ransomware), theft of intellectual property, or simply for challenge or notoriety within the hacker community.

4. Is all the data on your computer encrypted? If not, do you think it should be?

- Not all data on my computer is encrypted, but I believe it should be to ensure greater security and

privacy. Encryption helps protect the confidentiality of information, especially in case of loss or theft of the device.

5. Do you ever use a VPN? If so, why? If not, do you think you should?

- Yes, I sometimes use a VPN to protect my online privacy and security, especially when accessing public networks or wishing to avoid surveillance by Internet service providers and third parties. I believe it is important to use a VPN to maintain online privacy and protect against potential cyber threats.

6. Can you think of any major data breaches? What kind of information was released?

- A notable example of a data breach in Spain was the security breach at Santander Bank, where personal and financial data of thousands of customers were leaked. The leaked information included names, account numbers, addresses, and other sensitive information that could be used for identity theft or financial fraud.