**Module I: Cookies**

In the context of the Internet, cookies refer to small pieces of data stored on a user's computer or device by websites they visit. The main purpose of cookies is to remember specific information about the user and their interactions with a website, allowing for a more personalized and efficient browsing experience.

Cookies serve several important functions:

* **Session management:** Cookies are commonly used to manage user sessions. They help websites remember user login status, so users don't have to log in repeatedly as they navigate
* **Personalization**: Cookies enable websites to remember a user's preferences, such as language settings, theme choices, and other customizable options, making posterior visits more adjusted to the user's preferences
* **Tracking and analytics:** Websites use cookies to track user behavior, such as the pages they visit, the links they click, and the time spent on each page. This data is valuable for website owners to analyze and improve their site's performance and user experience.
* ‎‎‎‎‎‎‎‎‎‎‎‎‎**Advertising:** Cookies are often used by advertisers and ad networks to track user activity across multiple websites, helping them deliver targeted advertisements based on a user's interests and browsing history.

It's essential to note that while most cookies are harmless and facilitate a smoother online experience, there are concerns about privacy and security. Some cookies can track users across different websites, potentially revealing sensitive information. As a result, privacy regulations and browser settings often allow users to control or block cookies to protect their online privacy.

For the most part, accepting cookies on a website will not result in any catastrophic event. However, something to take into consideration and be wary of is when a website asks if you want your device to remember what your login credentials are for that website. While this would make logging into a website more convenient, it could potentially create a problem if you are reusing passwords or tend to create extremely easy passwords, as hackers could easily find that information in a data breach and your personal information could put you at risk.

If you are disclosing private information on a website, and they ask if you want to accept the cookies policy, it is best to pass and decline. Because this personal information can be used to access accounts, so you should keep that information away from the data-mining websites.

Link to minigame: [*https://forms.office.com/r/ehdvc59ZAh*](https://forms.office.com/r/ehdvc59ZAh)

**Module II: Passwords**

Passwords are a fundamental security mechanism for protecting sensitive information and preventing unauthorized access. However, weak or easily guessable passwords can be vulnerable to attacks. It's essential to use strong passwords that are unique for each online account and follow good password practices, such as avoiding common words, including a mix of uppercase and lowercase letters, numbers, and special characters.

To enhance security further, many websites and services have adopted additional authentication measures, such as two-factor authentication (2FA) or multi-factor authentication (MFA). These methods require users to provide not only their password but also a second form of identification, such as a one-time code sent to their mobile device or a fingerprint scan, making it more challenging for unauthorized individuals to access an account even if they have obtained the password.

A secure password is crucial for protecting online accounts. To ensure security, make sure to follow these practices when creating and managing your passwords:

* **Length:** Aim for a minimum of 12 characters.
* **Complexity:** Use a mix of uppercase and lowercase letters, numbers, and special symbols.
* **Unique passwords:** Use a different password for each account. Avoid common words, phrases, and easily obtainable information, as well as keyboard patterns or sequential characters.
* **Regular updates:** Change passwords regularly, especially for critical accounts.
* **Extra security:** Enable two-factor authentication (2FA) or multi-factor authentication (MFA).

Link to minigame: [*https://forms.office.com/r/Z5gqK1XX3K*](https://forms.office.com/r/Z5gqK1XX3K)