|  |  |  |  |
| --- | --- | --- | --- |
| Une image contenant texte, Police, conception  Description générée automatiquement | Cybersécurité | |  |
| Thème du programme :  Les objets et les systèmes techniques : leurs usages et leurs interactions à découvrir et analyser | |
| Compétence | | Connaissance | |
| - Identifier et appliquer les règles pour un usage raisonné des objets communicants et des environnements numériques (propriété intellectuelle, identité numérique, témoins de connexion, géolocalisation). | | Cybersécurité : protection des données personnelles, traces numériques (témoins de connexion, géolocalisation), identification, authentification, respect de la propriété intellectuelle  Cyberviolence : usurpation d'identité, usage détourné. | |

**La cyber-sécurité** consiste à protéger les données, les réseaux et les programmes contre les attaques numériques appelées cyber-attaques.

On laisse **des traces numériques** sur le net à chaque fois que l’on navigue avec nos recherches et nos adresses IP notamment. Ces informations sont aujourd’hui facilement " traçables" par les Hackers. Cela leur permet d’identifier un utilisateur pour ensuite lui voler ses données personnelles (mot de passe, code carte bancaire, ….)

Ces cyber-attaques permettent aux hackers d’accéder à des informations sensibles pour ensuite les utiliser, les modifier, les détruire et même les revendre.



**Il existe des moyens simples pour protéger ses données :**

- Mettre des mots de passe

- Crypter ses données

- Supprimer de manière régulière toutes traces numériques.

- Changer éventuellement régulièrement de mot de passe

**Les 4 techniques d’attaque les plus utilisées par les hackers sont :**

1 – l’attaque par force brute.

2 – l’attaque par ingénierie sociale.

3 – l’exploration du réseau informatique sur lequel un utilisateur est connecté.

4 – le vol des données sur un site où un utilisateur crée un compte.

Les entreprises accordent de plus en plus d’importance à la protection de leurs données. En plus de se protéger avec la propriété intellectuelle (ensemble des droits qui protègent les créations telles que les inventions, les innovations, etc..), les entreprises mettent tout en place pour analyser les failles de leur système, c'est-à-dire les faiblesses de leur [système informatique](https://fr.wikipedia.org/wiki/Syst%C3%A8me#Informatique,_robotique).

Ces faiblesses permettent à un hacker de porter atteinte à l'intégrité du système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Pour cela, les entreprises font appel à des hackers éthiques.



Hacker éthique : un vrai métier

Les hackers éthiques sont des "pirates informatiques bienveillants" qui testent et identifient les failles des systèmes et des réseaux informatiques des entreprises pour prévenir et neutraliser de potentielles attaques internes ou externes.

**La cyber-violence** est un acte agressif, intentionnel, perpétré par un individu ou un groupe aux moyens de courriels, SMS, réseaux sociaux, jeux en ligne, etc.



**La cyber-violence peut se décliner en plusieurs formes :**

- Parole malveillantes via les réseaux numériques : insultes, vidéos ou photos diffusées sans autorisation

- Intrusion dans les données personnelles : usurpation d’identité, vol de données, ….

Il est donc prépondérant de protéger ses données (soit par mots de passe ou cryptage) et d’analyser chaque mail ou sms reçus de manière à ne pas tomber dans les pièges tendus par des personnes malveillantes.