Opération Cactus

Ce document est individuel et n'a pas vocation a être noté.

Au sujet de la cybersécurité :

Ce que je Sais	Ce que j'ai enVie d'apprendre	Ce que j'ai Appris

Question 1 : qu'est-ce que la cybersécurité ?

Question 2 : comment est-ce que les cybercriminels peuvent m'atteindre ? Comment puis-je être piraté(e) ?

Question 3 : quels sont les enjeux de la cybersécurité ? En quoi est-ce que ce sujet peut tous nous concerner ?

Enjeux individuels	Enjeux collectifs

Question 4 : qu'est-ce qu'un infostealer ?

Question 5 : quels peuvent être les moyens simples à mettre en oeuvre pour se protéger ?

Individuellement	Collectivement

Question 6 : que risque-t-on si on usurpe le compte de quelqu'un, et commet des actes répréhensibles au nom de quelqu'un d'autre ?

Ce document récapitule les notions clés vues en classe.

Opération Cactus

Définition : la cybersécurité

La cybersécurité désigne l'ensemble des activités visant à protéger les données et les systèmes d'information contre les menaces issues du cyberespace.
La cybersécurité, c'est :
-Mettre en place toutes les initiatives pour que nos appareils et espaces numériques restent le plus protégés possible,
-Partager ces pratiques sûres autour de moi.

Protéger les systèmes d'information et les données, c'est garantir leur confidentialité, intégrité, disponibilité.

Confidentialité : une information, une donnée n'est accessible que par des personnes autorisées.
Intégrité : physique (les données sont exactes et non modifiées sur leur lieu de stockage ou de récupération, elles sont complètes, non altérées) et logique (les données sont exactes tout au long de leur utilisation, quel que soit le lieu de stockage et d'usage).
Disponibilité : on peut accéder aux données à tout moment (soit à distance, soit localement)

Les enjeux

Enjeux individuels	Enjeux collectifs
-Usurpation d'identité -Perte d'accès à mes comptes en ligne -Vol, perte, diffusion de données -Escroquerie financière	-Mise en danger des données de tous les utilisateurs du système -Perte de l'ensemble ou partie des données

Les infostealers

Un stealer est un virus informatique qui vole des informations comme tes mots de passe, tes comptes en ligne, jusqu'à de l'argent en cryptomonnaie, et même certaines données enregistrées dans ton navigateur (comme tes sessions ouvertes sur des sites web).
Les hackers utilisent ensuite ces informations pour pirater des comptes ou arnaquer des gens.
Comment ça se propage ?

Les stealers sont des logiciels malveillants qui peuvent être vendus ou distribués gratuitement sur Internet. Les détenteurs les diffusent souvent via :
✓ Des messages piégés (phishing/hammeçonage) qui poussent les gens à cliquer sur un lien dangereux.
✓ Des liens sur des plateformes de vidéos sur YouTube, Discord, etc., avec des liens vers des logiciels soi-disant utiles (triches pour jeux vidéo, mods, logiciels gratuits…).
✓ Parfois des instructions demandent de désactiver l'antivirus, pour permettre de télécharger et installer le programme (et donc d'éviter d'être détecter…).

Moyens à mettre en œuvre pour se protéger

1 Ne pas télécharger, ni utiliser de logiciels, d'applications et de vidéos piratés ou d'origine douteuse qui peuvent souvent contenir un virus.

2 Ne jamais désactiver votre antivirus à la demande d'un logiciel.

3 Face à un message suspect (inattendu, alarmiste, aguicheur...), ne pas ouvrir les pièces jointes ou cliquer sur les liens.

4 Mettre régulièrement à jour vos appareils, logiciels et applications.

5 Utiliser des mots de passe forts qui ne disent rien sur vous et différents pour chaque accès afin d'éviter des piratages en escalade.

6 Deux sécurités valent mieux qu'une : activer la double authentification lorsque cela vous est proposé.

7 Ne pas stocker vos mots de passe de manière non sécurisée : post-it, fichiers textes, messages brouillons, notes sur votre smartphone...

8 Utiliser un gestionnaire de mots de passe ou un trousseau d'accès sécurisés, stockés de préférence en local, pour conserver vos mots de passe en sécurité. Vous n'aurez ainsi à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes.

9 Ne jamais sauvegarder vos mots de passe dans le navigateur d'un ordinateur partagé.

10 Se déconnecter systématiquement de votre compte après utilisation, pour éviter que quelqu'un puisse y accéder après vous.

Que faire en cas d'attaque ?

Si tu es victime ou pense être victime d'un acte malveillant en ligne :
virus, hameçonnage, arnaque bancaire...
Tu peux cliquer sur l'outil de diagnostic et d'assistance en ligne :

17 CYBER
Mon assistance en ligne

https://17cyber.gouv.fr/

Les risques légaux

Le piratage informatique est une infraction grave pouvant entraîner une peine jusqu'à 10 ans d'emprisonnement.

En cas d'usurpation d'identité, il convient de déposer plainte immédiatement.

Tu n'es pas responsable des actes commis. Cependant, une enquête sera nécessaire pour prouver l'usurpation.