ACADÉMIE DE NORMANDIE	**DOCUMENT ENSEIGNANT** **COMMENT PROTÉGER SES DONNÉES PERSONNELLES ? INTRODUCTION**	Document de formation pour les enseignants

Compétences PIX Abordées :

CLG PROTECTION ET SÉCURITÉ ET CLG CYBERSÉCURITÉ CYCLE 4

Protection et sécurité		
4.1 Sécuriser l'environnement numérique		
Sécurité des équipements	Logiciels malveillants	Reconnaître les principales attaques liées à des logiciels malveillants et en distinguer les catégories
	Antivirus	Connaître le rôle d'un antivirus et les bases de son utilisation
4.2 Protéger les données personnelles et la vie privée		
Gérer ses données personnelles	Diffusion de données personnelles	Identifier les situations pouvant entraîner la diffusion publique de ses données personnelles
Traces numériques	Accès d'une application aux données	Maîtriser l'accès à ses données lors de l'installation d'une application

Situation déclenchante :

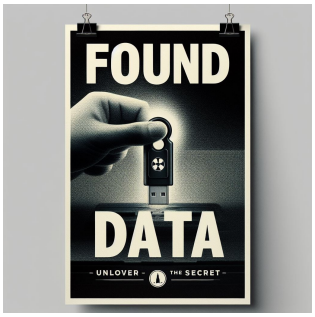
Regarder la vidéo : https://www.youtube.com/watch?v=xCLboWLVia0

Ou sans Publicité avec la digitale : https://ladigitale.dev/digiview/#/v/658ab33d2c6a9

Résume par une phrase la situation :

Une personne a oublié sa clef USB* dans le collège, un professeur s'en empare et rentre chez lui pour la lire.

TRAVAIL 1 : A la suite de cette vidéo – Quel aurait été votre comportement ? :



5 minutes de réflexion

- Donner la clef USB* au responsable informatique du collège ou du département

- Mettre une affiche sur la machine à café pour retrouver son propriétaire

- Laisser la clef USB sur la table

- La jeter à la poubelle si le propriétaire ne se manifeste pas

TRAVAIL 2 : A la suite de cette vidéo – Quels sont les risques de brancher cette clef USB sur votre poste informatique ? : DOCUMENTS RESSOURCES 1 ET 2 A LIRE SI BESOIN

10 minutes de réflexion par groupe

- Se faire infecter par un virus*

- Se faire infecter par un pirate informatique*

- Avoir un matériel informatique défaillant

- Avoir accès à des données personnelles* d'une autre personne

- Se faire pirater* ses comptes bancaires, des réseaux sociaux etc....

EN RÉSUMÉ :

Votre ordinateur pourrait être verrouillé par un logiciel de rançon* ou un enregistreur de frappe* pourrait enregistrer chacune de vos frappes... Permettant aux pirates de s'emparer de vos données d'accès à divers comptes, allant des médias sociaux aux institutions financières.

TRAVAIL 3 : Quelle décision prenez-vous ? 3 minutes de réflexion

- Nous décidons de remettre la clef USB* au responsable informatique du collège. Nous donnons la clef USB au professeur de Technologie.

Images générées par IA : https://www.bing.com/images/create

UTILISATION D'UNE CLÉ USB TROUVÉE, QUELS SONT LES RISQUES ?

Il vous est peut-être déjà arrivé de récupérer **une clé USB*** promotionnelle lors d'un salon professionnel, ou encore d'en trouver une dans la rue… Mais avez-vous déjà imaginé que ces périphériques pourraient être piégés et que le simple fait de les brancher pourrait avoir des conséquences sur la sécurité de votre ordinateur? Un quelconque périphérique USB en apparence inoffensif peut potentiellement se comporter **comme un virus* d'un niveau de dangerosité élevé.**

Que faire lorsque l'on trouve une clé USB* ?

La première chose à faire est de demander si elle appartient à quelqu'un. Si ce n'est pas le cas, il ne faut pas la laisser traîner sur un bureau, la jeter dans une poubelle ou encore l'insérer dans votre ordinateur puisque vous ne savez pas ce qu'elle peut contenir.

La meilleure solution est de la détruire afin qu'elle devienne inutilisable, et donc inoffensive pour vous mais aussi pour vos collègues.

Les risques liés à l'utilisation d'une clé USB* trouvée

Les risques sont nombreux puisqu'une simple **clé USB*** peut infecter votre ordinateur avec toute sorte de virus ou encore des **malwares**. En effet, une clé USB peut comporter toute sorte de menaces pour vous, votre système d'information et vos données personnelles, et cela peut causer d'importants dommages.

A savoir que des attaques ciblées sur votre entreprise peuvent aussi être exécutées depuis une clé USB. Vous pouvez être la proie d'un cybercriminel*, une fois la clé USB branchée, il est souvent trop tard et celle-ci a déjà infecté tout votre réseau*. Il peut aussi s'agir d'une entrée pour accéder à distance à votre ordinateur afin de récupérer vos identifiants et mots de passe, ou encore exfiltrer vos données.

Autre exemple, Une **« USB killer »**, pourra anéantir votre ordinateur en un simple branchement. Pour cela, elle délivre une tension très forte qui détruit l'électronique de l'appareil.

Comment se protéger face aux clés USB ?

Le plus simple serait de ne pas utiliser une clé lorsqu'on ne sait pas d'où elle vient. Cependant aujourd'hui il existe des produits de protection contre les menaces USB. On parle de **« station blanche »*** à l'entrée des entreprises sensibles et d'antivirus puissants.

4 conseils d'utilisation des clés USB en entreprise :

- Fournir des clés USB aux collaborateurs afin d'éviter toute menace extérieure

- Ne pas brancher une clé USB dont on ne connaît pas la provenance à un poste de travail

- Contrôler les clés USB qui n'ont pas été branchées dans un environnement sécurisé

- Brancher uniquement des clés préalablement vérifiées

Bien choisir sa clé USB, c'est aussi assurer la sécurité de votre entreprise et de votre vie privée.

Source : https://soteria-lab.com/blog/article/cle-usb-trouvee-risques/

Oh, regardez, quelqu'un a perdu sa clé USB !

S'il y a un conseil à donner lorsqu'on tombe sur une clé USB perdue, ce serait de la donner aux autorités ou de la déposer au bureau ou à la boîte des objets trouvés.

Cependant, comme les bons samaritains ne sont pas encore morts et que les gens sont des créatures naturellement curieuses, pour satisfaire leur curiosité, beaucoup d'entre eux brancheront une telle clé USB « trouvée » dans leur appareil pour en savoir plus. Les histoires ne sont pas seulement anecdotiques; **des recherches ont montré que les gens ont tendance à brancher des clés USB inconnues dans leurs ordinateurs.**

Malheureusement, les cybercriminels* utilisent souvent une clé USB « perdue » comme tactique d'ingénierie sociale, en espérant que leurs cibles feront exactement cela. Comme la personne qui branche la clé n'a aucune idée de son contenu, elle pourrait ouvrir la boîte de Pandore.

Cela pourrait entraîner l'apparition de diverses formes de logiciels malveillants dans l'appareil. Votre ordinateur pourrait être verrouillé par un logiciel de rançon* ou un enregistreur de frappe* pourrait enregistrer chacune de vos frappes... Permettant aux pirates de s'emparer de vos données d'accès à divers comptes, allant des médias sociaux aux institutions financières.

Si vous avez branché **un disque dur*** infecté sur votre ordinateur de bureau, la situation est bien pire : certains types de logiciels malveillants peuvent se propager à travers toute l'infrastructure d'une entreprise et l'infester. Si vous pensez que cela semble tiré par les cheveux, il vous suffit de vous souvenir du tristement célèbre logiciel malveillant Stuxnet, qui se serait propagé à l'aide de clés USB malveillantes. Et n'oublions pas le logiciel malveillant BadUSB, qui aurait pu permettre à des chapeaux noirs de prendre le contrôle complet d'une machine, d'espionner les utilisateurs, et même de voler des données.

Source : https://www.welivesecurity.com/fr/2020/09/21/cle-usb-inconnue/

Images générées par IA : https://www.bing.com/images/create

Les supports amovibles sont dangereux pour la sécurité informatique du collège : Disque dur, clef USB, disque dur, ou encore les smartphones

Prévention des virus, logiciels malveillants, ranconnage...

Il est important de protéger ses postes informatiques , ou son smartphone avec un antivirus :

Prévention des virus

Des solutions payantes ou gratuites sont disponibles

Analyser les supports externes chaque fois

Les enseignants disposent d'une solution gratuite ANTI-VIRUS afin de protéger leurs postes personnels ou smartphone :

Prévention des virus

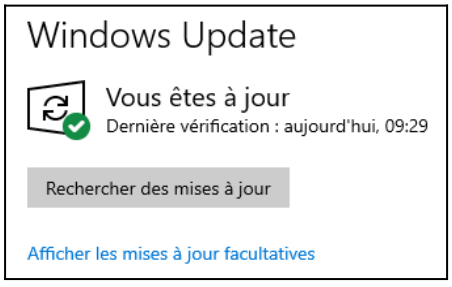
https://edu.trendmicro.fr/view/index.php

Lors de la charge de son smartphone sur une prise USB, il est important de le protéger par un capuchon USB – évitant les échanges de données :

Prévention des attaques de type "juice jacking"

Maintenir son système à jour :

Prévention des virus et des failles de sécurité



Séparer ses données personnelles et professionnelles :

Prévention des virus

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

Comment crypter les données de sa clef USB ou de son disque dur externe ?

Pour cela, vous devez télécharger un logiciel ou pas vous permettant de sécuriser votre clé USB.

Sur Windows ou mac : faites un clic droit sur le fichier ou dossier que vous souhaitez verrouiller.

Cliquez sur "Avancé" puis "chiffrer le contenu" ou sur "chiffrer"

4 façons les plus simples de crypter une clé USB :

1. BitLocker de Windows / 2. Rohos Mini Drive

3. Disk Cryptor / *4. USB Flash Security*

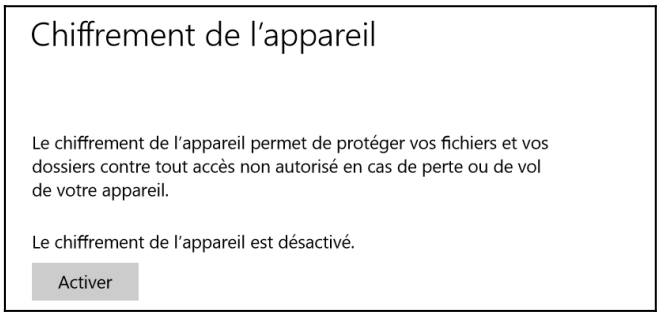
BitLocker est un logiciel développé par Microsoft dont le but est de chiffrer une partition.

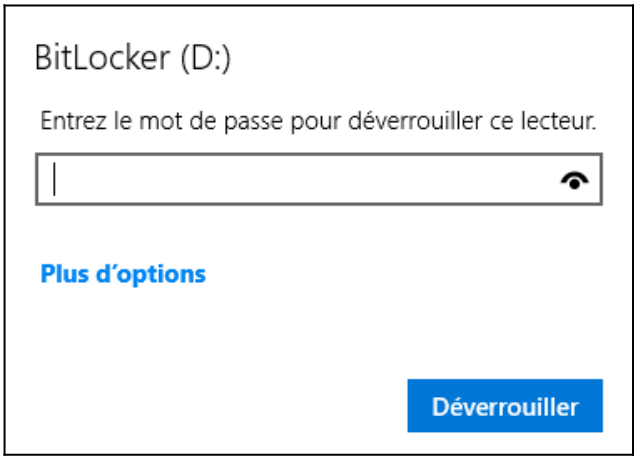
Une fois le disque chiffré, il est impossible de le lire sans la clé permettant le déchiffrement.

BitLocker n'est disponible que dans la version Pro de Windows 10.

Activez BitLocker :

Pour activer BitLocker, rendez-vous dans le menu Paramètres > Mise à jour et sécurité > Chiffrement de l'appareil, ou faites un clic droit sur la partition que vous souhaitez chiffrer et cliquez sur « Activer BitLocker ».





Images générées par IA : https://www.bing.com/images/create

CLEF USB : Une clé USB est un petit bloc facilement transportable et qui permet de stocker des données informatiques

VIRUS : Un virus informatique est une application malveillante ou un logiciel utilisé pour exercer une activité destructrice sur un appareil ou un réseau local

LOGICIEL DE RANÇON : Un rançongiciel ou ransomware est un logiciel malveillant ou virus qui bloque l'accès à l'ordinateur ou à ses fichiers et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

ENREGISTREUR DE FRAPPE : L'enregistrement de frappe consiste à surveiller toutes les frappes effectuées sur un clavier d'ordinateur, souvent sans la permission de l'utilisateur ou à son insu.

RESPONSABLE INFORMATIQUE : Le responsable informatique assure l'organisation, le suivi et la mise en œuvre de toute l'infrastructure système et informatique de l'entreprise.

MALWARES : Un malware ou maliciel est un logiciel malveillant capable de compromettre la sécurité d'un ordinateur ou des données qu'il contient.

CYBERCRIMINEL : Homme qui commet des actes à l'aide d'outils informatiques, notamment en piratant des données existantes sur Internet afin d'obtenir illégalement de l'argent ou un quelconque profit.

RÉSEAU : Un réseau informatique (en anglais : data communication network ou DCN) est un ensemble d'équipements reliés entre eux pour échanger des informations.

USB KILLER : USB Killer est un dispositif, ressemblant à une clé USB, qui détruit les composants physiques de n'importe quel appareil auquel il est connecté.

PIRATES INFORMATIQUES : Le piratage informatique est l'acte de compromettre les dispositifs et réseaux numériques en obtenant un accès non autorisé à un compte ou un système

DISQUE DUR : Le disque dur est l'un des principaux composants d'un ordinateur. Son rôle est de stocker des données informatiques.