Cybersécurité

Sensibilisation aux bonnes pratiques informatiques

L'importance de la sensibilisation

<u>QUIZ :</u> Dans quelle proportion le facteur humain est-il impliqué dans les cyberincident ?

- **10 %**
- **30 %**
- **60 %**
- **90 %**

L'importance de la sensibilisation

<u>QUIZ :</u> Dans quelle proportion le facteur humain est-il impliqué dans les cyberincident ?

- **10 %**
- **30 %**
- **60 %**
- **90 %**

*(Étude IBM) : par **négligeance**, **ignorance** ou **malveillance**.*

Cela peut etre suite à un clic sur un lien, l'activation d'un executable, l'envoie de données à un tiers, etc.

Sommaire

01 - L'importance de la donnée

L'importance de la donnée

Nous produisons de plus en plus de "Data" :

- multiplication des appareils *(personnels, professionnels, objets connectés, etc.)*
- multiplication des applications générant de la "Data"
- généralisation de la dématérialisation
- numérisation des anciennes données

L'enjeu majeur de la cybersécurité

Nous consommons de plus en plus de "Data" :

L'enjeu majeur de la cybersécurité

La donnée : le pétrole du 21ème siècle!

Liste des entreprises par capitalisation boursière :

1996	2021
General Electric	Apple
Royal Dutch Shell (essence et gaz)	Microsoft
Coca-Cola	Alphabet
Nippon Telegraph et Telecom	Amazon
Exxon Mobil (essence et gaz)	Tesla
	Meta

02 - La multiplication des risques

La multiplication des risques

Retour sur la menace cyber pour la période 2019 - 2021

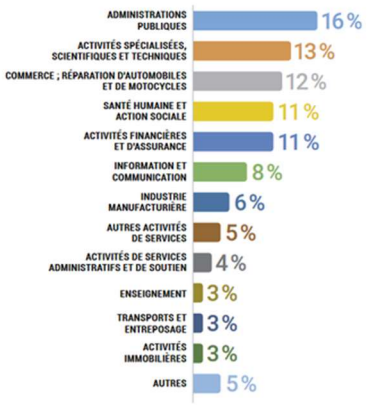
Carte relative aux cyberattaques sur les organismes publics :

https://umap.openstreetmap.fr/fr/map/cyberattaques-sur-les-organismes-publics-2019-2021_635160#7/47.610/1.813

La multiplication des risques

LES NOTIFICATIONS DE VIOLATION DE DONNÉES PERSONNELLES

Les secteurs d'activité les plus concernés :



La multiplication des risques

Lors d'une attaque cyber, le Système d'information (SI) est visé.

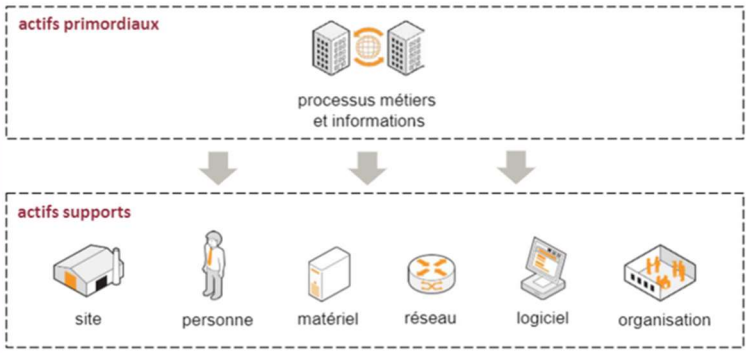
Qu'est ce qu'un Système d'Information ?

Ensemble des **ressources** destinées à **collecter**, **classifier**, **stocker**, **gérer**, **diffuser les informations** au sein d'une organisation.

Doit permettre et faciliter la mission de l'organisation.

La multiplication des risques

Qu'est ce qu'un Système d'Information (SI)?



Contient un ensemble d'**actifs primordiaux** (processus métiers et informations) et d'**actifs supports** (site, matériels, réseau, logiciels, personnes, etc.)

La multiplication des risques

Hétérogénéité des Systèmes d'Information (structure et logiciel)

VS

La multiplication des risques

Hétérogénéité des systèmes de protection

VS

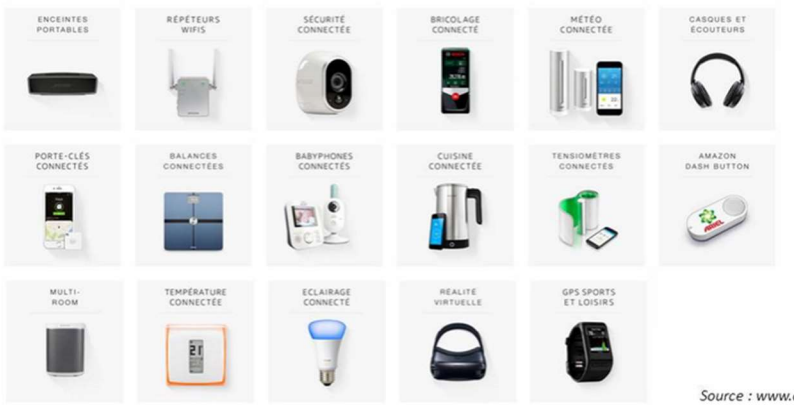
La multiplication des risques

Hétérogénéité des comportements des utilisateurs

VS

La multiplication des risques

Apparition de nouveaux "objets connectés"



Source : www.amazon.fr

La multiplication des risques

Exemples de risques cyber pouvant impacter une collectivité territoriale :

Prise de controle des comptes de messagerie

Défiguration de site Internet

Piratage d'objets/automates connectés

Prise en otage des données

Vol de données sensibles, à caractère personnel

Utilisation des ressources serveurs de la collectivité

.....

03 - Quelques exemples locaux

Quelques exemples locaux

La mairie de Bayonne victime d'une cyber-attaque "très puissante"

Lecture 1 min.

Accueil • Pyrénées-Atlantiques • Anglet

Béarn : l'hôpital d'Oloron Sainte-Marie victime d'une cyberattaque, le parquet de Paris saisi

Lecture 1 min.

Accueil • Pyrénées-Atlantiques • Oloron-Sainte-Marie

Le centre hospitalier de Dax visé par une cyberattaque de grande ampleur

Lecture 1 min.

Accueil • Landes • Dax

Béarn : une cyberattaque russe a ciblé le service d'assainissement d'Oloron

Lecture 2 min.

Accueil • Pyrénées-Atlantiques • Oloron-Sainte-Marie

04 - Notions de cybermalveillance

Notions de cybermalveillance

Quel type d'attaque ?

"Cryptovirus"ou "Ransomware"

Botnet

Spyware

Ver

Virus

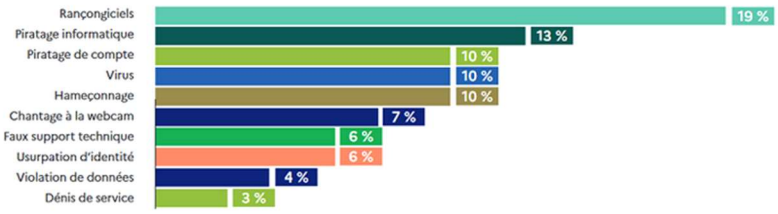
"Cheval de Troie" ou "Trojan"

"Deni de service" ou "DoS"

Phishing

Notions de cybermalveillance

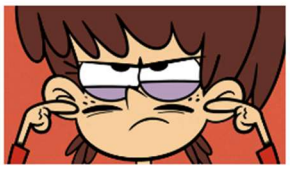
Les principales cyber menaces pour les collectivités et administrations

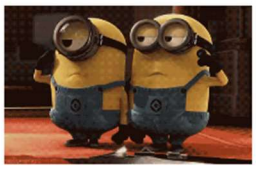


source : Cybermalveillance.gouv.fr

Notions de cybermalveillance

Quel type d'attaquant et pour quelle motivation ?





Notions de cybermalveillance

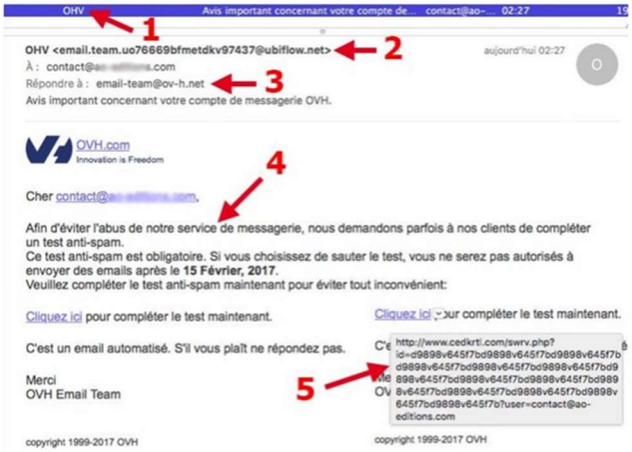
Faux support technique

Notions de cybermalveillance

Comment repérer une arnaque par courrier électronique ?

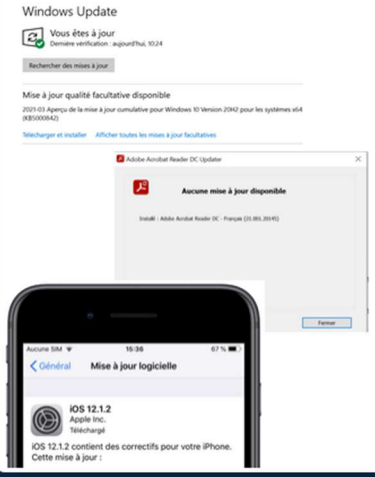
- Le courrier vous est-il **réellement destiné**?
- Le message évoque une **facture**, un **dossier**, un **thème** qui ne vous parle pas?
- Connaissez vous l'**expéditeur**?
- Le courrier nous demande t'il de réagir **dans les plus brefs délais**?
- Le niveau de **langage** du courriel est il **correct**?
- Quelle est la **destination du lien** présent dans le courriel?
- Le lien de la barre d'adresse est-il en « HTTP**S** » avec un **cadenas** présent (sur un site)?

Notions de cybermalveillance



05 - Differents types de sécurisation

Sécurisation : logicielle



- Être **vigilant avec les sites** sur lesquels ont réalise des téléchargement (programmes, applications, etc.)
- Vérifier que les **mises à jour logicielles** et **système** se réalisent régulièrement (les virus exploitent les failles connues)
- Tous les **logiciels** peuvent présenter des failles et doivent **être mis à jour** : Shockwave, Javascript, Acrobat reader, etc.

Sécurisation : logicielle

<u>Utiliser et mettre à jour des Antivirus et Antimalware :</u>

- Ils nécessitent des mises à jour régulières du moteur et de la base virale (téléchargement automatique)

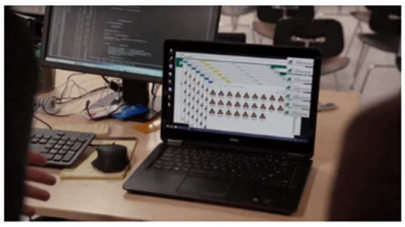
- Des scans doivent régulièrement être lancés

- Vérifier les options (actives ou pas)

- Analyser les supports amovibles

- Analyser les mails

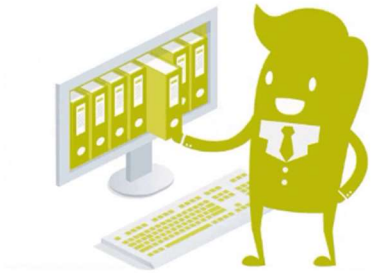
Sécurisation : logicielle



Symptômes de présence de codes malveillants

- Ralentissement
- Ouvertures régulières de fenêtres pop-up et de publicités
- Modification de la configuration de votre navigateur Web
- Surconsommation des ressources
- Désactivation de l'antivirus / antimalware
- Echec des mises à jour antivirus / système

Sécurisation : utilisateur



- N'attribuer que les **accès et droits nécessaires** aux utilisateurs (pas de compte administrateur par défaut, droit en écriture ou lecture, etc.)

- Créer des **comptes nominatifs**, éviter les comptes génériques

- Diffuser la **charte d'utilisation des SI**

- Rendre **inactif les comptes obsolètes**

Sécurisation : utilisateur

Temps requis pour déchiffrer un mot de passe

Traduction libre des données recueillies par Hive Systems via howsecureismypassword.net (2020)

NOMBRE DE CARACTÈRES	CHIFFRES SEULEMENT	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES	SYMBOLES, CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	1 seconde	5 secondes
7	Instantanément	Instantanément	25 secondes	1 minute	6 minutes
8	Instantanément	5 secondes	22 minutes	1 heure	8 heures
9	Instantanément	2 minutes	19 heures	3 jours	3 semaines
10	Instantanément	58 minutes	1 mois	7 mois	5 ans
11	2 secondes	1 jour	5 ans	41 ans	400 ans
12	25 secondes	3 semaines	300 ans	2000 ans	34k ans
13	4 minutes	1 an	16k années	100k ans	2M ans
14	41 minutes	51 ans	800k années	9M ans	200M ans
15	6 heures	1k ans	43M ans	600M ans	15G ans
16	2 jours	34k ans	2G ans	37G ans	1T ans
17	4 semaines	800k ans	100G ans	2T ans	93T ans
18	9 mois	23M ans	2T ans	100T ans	$7(10^{45})$ ans

Formation *Éduquer à la cybersécurité* cadre21

Mettre en place une **politique de mot de passe rigoureuse** :

- Ne pas choisir le même mot de passe pour différents comptes (utiliser un coffre fort numérique ex : Keepass)
- Changer régulièrement de mot de passe
- Ne pas communiquer ou noter son mot de passe

KeePass

Sécurisation : utilisateur

Sensibiliser les utilisateurs :

- Se tenir informé de l'**actualité** sur la sécurité

- Faire **attention** aux **pièces jointes**

- **Désactiver l'exécution des liens hypertextes** et l'activation des images dans les mails

Sécurisation : physique

- Protéger **physiquement les locaux** (accès par badges, clé, alarmes, etc.)

- Ne pas avoir des **prises réseaux** accessibles au **public,** de WI-FI commun

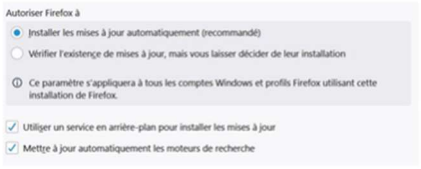
- Se protéger contre les **incidents « environnementaux »** (incendie, inondation, panne électriques, etc.)

06 - Bonnes pratiques

Bonnes pratiques

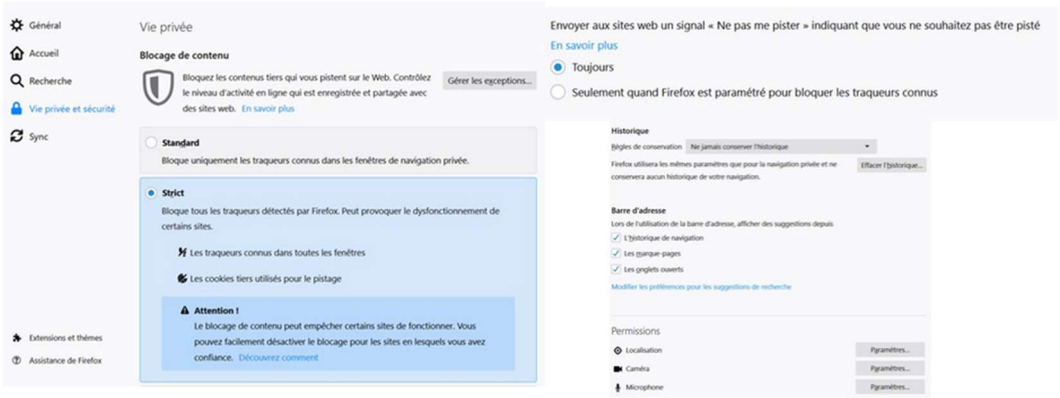
Navigation sur Internet

Naviguer avec un navigateur à jour (vérification dans « à propos » et dans les options)



Bonnes pratiques

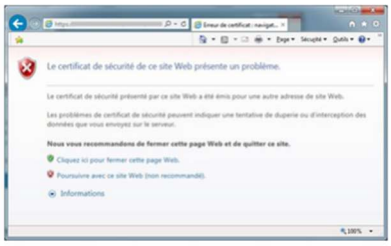
Paramétrer les options de navigation



Bonnes pratiques

Vérifier que vous naviguez en « https » (cadenas)

Ne forcez pas les « erreurs de certificat de sécurité »



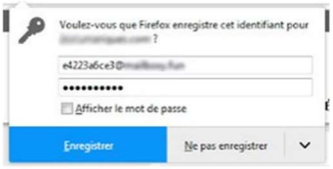
Bonnes pratiques

Mettre à jour l'ensemble de vos logiciels et applications

- Activer les mises à jour automatiques

Bonnes pratiques

Ne pas enregistrer ses mots de passe



Bonnes pratiques

Utiliser un gestionnaire de mot de passe (coffre-fort)

Changer le mot de passe au moindre soupçon

N'utilisez pas vos mots de passe sur un ordinateur partagé, public

Bonnes pratiques

Verrouiller ses sessions Windows

Veille

En cas de fonctionnement sur batterie, mettre le PC en veille après

15 minutes

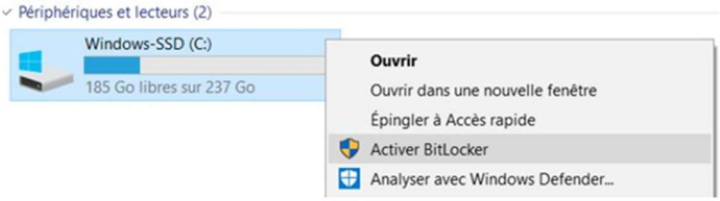
En cas de branchement sur le secteur, mettre le PC en veille après

30 minutes

Lock Computer (WIN-L)

Bonnes pratiques

Chiffrer les disques et supports amovibles



VeraCrypt

Bonnes pratiques

Différenciez les usages « travail » et « domicile »

- Utiliser des **mots de passe différents** pour les services **personnels** et **professionnels**
- **Ne pas mélanger** les **messageries** pro et perso
- **Distinguer** les **services de stockage** (cloud) pro et perso
- **Eviter** les réseaux **Wi-Fi publics** ou inconnus
- Méfiez vous des **supports USB** provenant d'autres utilisateurs

Bonnes pratiques

Mettre à jour et sécuriser vos outils personnels (dans le cadre du BYOD)

- Mettre en place les **codes d'accès**
- **Chiffrer les données** de l'appareil
- Appliquer les **mises à jour** de sécurité
- Ne pas laisser votre appareil **sans surveillance**
- Contrôler les **autorisations** de vos applications
- Faire des **sauvegardes**

Bonnes pratiques

Gérez vos sauvegardes

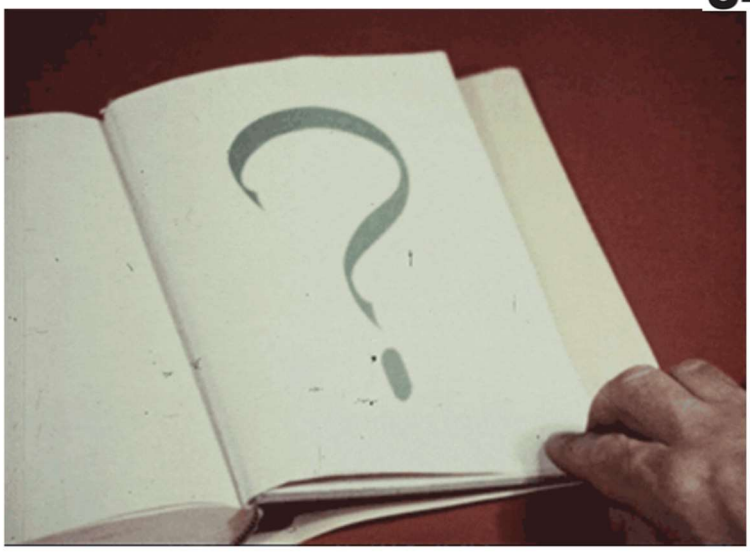
- Réalisez des sauvegardes quotidiennes (planifiées)
- Externalisez vos sauvegardes
- Testez vos sauvegardes
- Protégez vos sauvegardes

Bonnes pratiques

Utilisation des imprimantes

- Ne pas **oublier** les **originaux** dans les imprimantes
- Utiliser les fonctions d'**impression « décalées »**
- Vérifier le **paramétrage** des imprimantes (accès Internet)
- Utiliser des **destructeurs de documents** pour supprimer les papiers « sensibles »

06 - Questions diverses



Un accompagnement proposé par La Fibre64, l'APGL64 et l'ADM64