Hygiène Numérique et Protection des Données Personnelles

Évitons le pire

Bertrand Thierry

Jeudi 4 mars 2021

Mes Données, Mes Droits, Mes Devoirs

Je suis ce que sont mes données

Identité Numérique

L'Identité Numérique = Notre lien à la technologie

4 Principaux types d'identifiants

Type	Info
Déclarés	*Nom, Prénom, ...*
Observés	*Heure de connection/déconnection, ...*
Inférés (Déduites)	*Horaire de travail, ...*
Cachés	*MAC, IP, ...*

Données Personnelles ?

*Toute **information** se rapportant à une personne physique **identifiée ou identifiable**, **directement ou non**, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité.*

Pour la CNIL : Tous ces Identifiants = Données à Caractère Personnel

. Source(s) : Service-public.fr

9 Droits

1. Droit d'information : *Comment sont utilisées mes données ?*
2. Droit d'opposition *à ce qu'on organisme utilise mes données*
3. Droit d'accès *aux données qu'un organisme détient sur moi*
4. Droit de rectification *sur les informations inexactes*
5. Droit au déréfencement (à l'oubli) : *Ne plus associer mon nom-prénom à un contenu visible dans un moteur de recherche*
6. Droit d'effacement *de données me concernant*
7. Droit à la portabilité *pour les réutiliser ailleurs*
8. Demander une intervention humaine *si décision auto.*
9. Geler l'utilisation de vos données *e.g. vérification longue*

À qui demander ?

1. Au responsable de traitement
2. Refus ou absence de réponse ? Plainte à la CNIL

. Source(s) : La CNIL

Devoirs

Responsable de Traitement (≃ service web)

> *Le responsable du traitement des données doit mettre en œuvre les mesures de sécurité des locaux et des systèmes d'information pour empêcher que les fichiers soient déformés, endommagés ou que des tiers non autorisés y aient accès. Il doit prendre toutes les mesures nécessaires au respect de la protection des données personnelles dès la conception du produit ou du service.*

Exemple de sanction

SERGIC : sanction de 400 000€ pour atteinte à la sécurité des données et non-respect des durées de conservation

06 juin 2019

La formation restreinte de la CNIL a prononcé une sanction de 400 000 euros à l'encontre de la société SERGIC pour avoir insuffisamment protégé les données des utilisateurs de son site web et mis en œuvre des modalités de conservation des données inappropriées.

. Source(s) : Service-Publique.fr, CNIL

Limites

Effet Streisand : exemple de la DCRI (2013)

1. DCRI (ex DGSI) demande à **supprimer un article Wikipédia** (*Station hertzienne militaire de Pierre-sur-Haute*)
2. Fait **pression sur un contributeur** bénévole disposant des droits d'administrateur (*et président de wikimédia France*)
3. Conséquence : l'article devient **le plus consulté** (*et a été traduit dans d'autres langues*)

Internet n'oublie rien

1. Archive.org : Archive de très nombreux sites web avec historique
2. Politwoops : Tweet supprimé ?

Comment nos Données sont Volées ?

Tour d'horizon des cyber-attaques les plus courantes

Ce que n’est pas une cyber-attaque

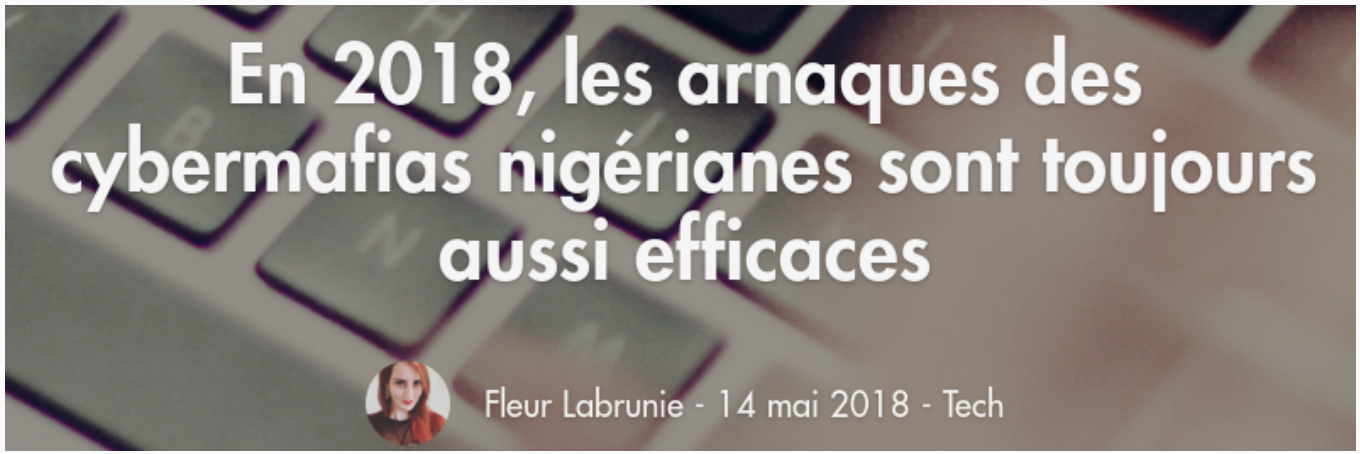
NCIS : 2 idiots, 1 keyboard and a sandwich

https://www.youtube.com/watch?v=u8qgehH3kEQ

Ingénierie Sociale

Pourquoi s'embêter puisqu'on peut demander ?

Type de Phishing
Scam 419



- 5M de "Yahoo Boys"
- 4 morts recensés

. Source(s) : Numérama, 14/05/2018

- Avez-vous déjà reçu ce genre d'email ?

Ingénierie Sociale

Pourquoi s'embêter puisqu'on peut demander ?

Type de Phishing
Scam 419 Business Email Compromised

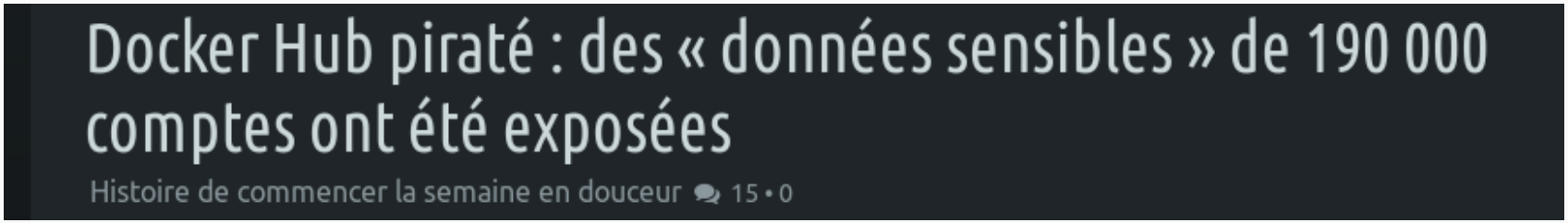
(sur la périodre 2013 - 2017)

. Source(s) : FBI, 04/05/2017

Attaquer le service

Un mot de passe c'est bien. Tous les mots de passe, c'est mieux

Nom	#Données	Année
Dockerhub	190 000	2019



. Source(s) : NextInpact, 29/04/2019

Attaquer le service

Un mot de passe c'est bien. Tous les mots de passe, c'est mieux

Nom	#Données	Année
Dockerhub	190 000	2019
L'Express	700 000	2018

Info ZDNet : Près de 700.000 données lecteurs de l'Express dans la nature

Sécurité : *Depuis des semaines, des pirates peuvent accéder sans problème à cette colossale base de données de 60 Go contenant noms, prénoms, adresse mail et profession. Nous avons enquêté.*

. Source(s) : ZDNet, 01/03/2018

Attaquer le service

Un mot de passe c'est bien. Tous les mots de passe, c'est mieux

Nom	#Données	Année
Dockerhub	190 000	2019
L'Express	700 000	2018
Uber	57 Millions	2017

et Uber a payé 100 000$ pour tenter d'étouffer l'affaire

. Source(s) : Numerama, 22/11/2017

Attaquer le service

Un mot de passe c'est bien. Tous les mots de passe, c'est mieux

Nom	#Données	Année
Dockerhub	190 000	2019
L'Express	700 000	2018
Uber	57 Millions	2017
Facebook	87 Millions	2014

. Source(s) : NextInpact, 05/04/2018

Attaquer le service

Un mot de passe c'est bien. Tous les mots de passe, c'est mieux

Nom	#Données	Année
Dockerhub	190 000	2019
L'Express	700 000	2018
Uber	57 Millions	2017
Facebook	87 Millions	2014
Marriott	500 Millions	2018

Hôtels Starwood (Marriott) : fuite de données, y compris bancaires, pour 500 millions de clients

. Source(s) : NextInpact, 03/12/2018

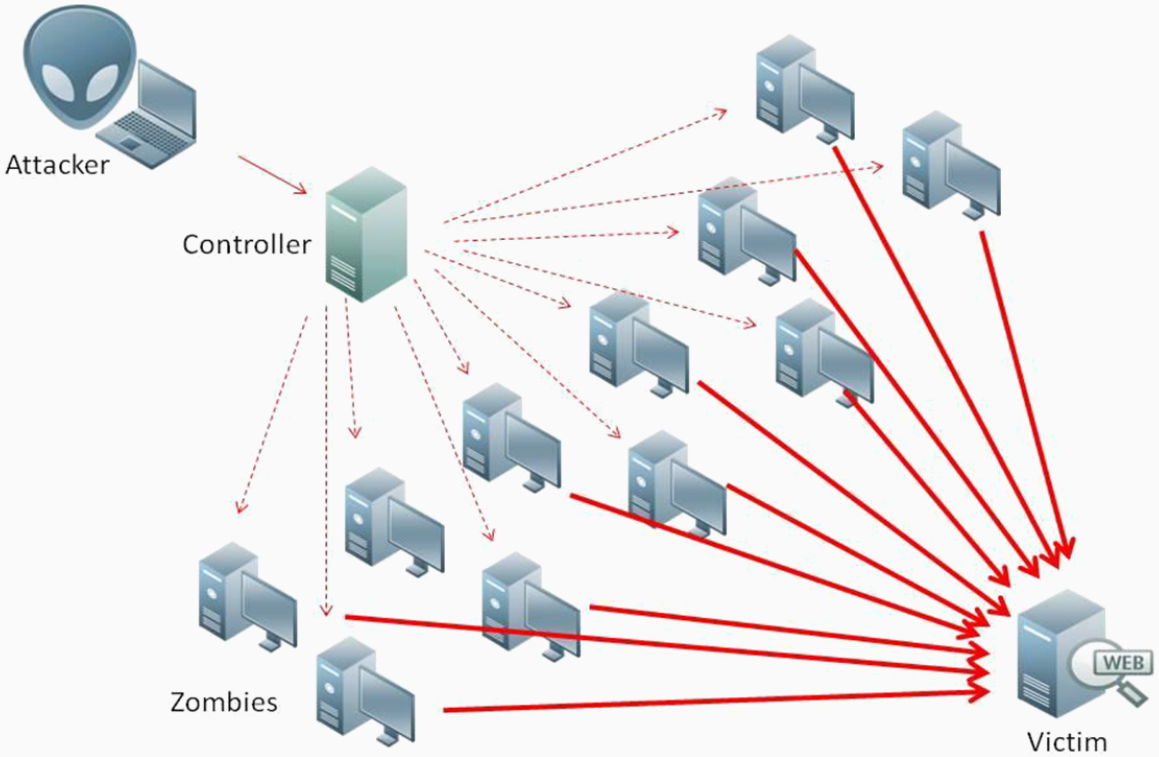
Attaquer le service

Un mot de passe c'est bien. Tous les mots de passe, c'est mieux

Nom	#Données	Année
Dockerhub	190 000	2019
L'Express	700 000	2018
Uber	57 Millions	2017
Facebook	87 Millions	2014
Marriott	500 Millions	2018
Yahoo !	3 Milliards	2013 (admis en 2017)

. Source(s) : NextInpact, 04/10/2017

(D)DoS : (Distributed) Deny of Service



Conséquence Service ou infrastructure inutilisable

Exemple Attaque Massive contre l'Estonie en 2007 (du 26 avril au 18 mai)

. Source(s) : image Wikipedia, NextInpact

Ransomware (Ransongiciel)

Cyber-Braqueur : Chiffrement + Demande de ranson

Nom	Victime (ex.)	Perte / Dégât
Phobos	Sarrebourg	Paralysie


BFMTV ▸ Tech

La ville de Sarrebourg en Moselle victime d'une cyberattaque

14/06/2019 à 11h57

. Source(s) : BFM, 14/06/2019

Ransomware (Ransongiciel)

Cyber-Braqueur : Chiffrement + Demande de ranson

Nom	Victime (ex.)	Perte / Dégât
Phobos	Sarrebourg	Paralysie
RobinHood	Baltimore	18M$ (1 mois)

THE BUTCHER'S BILL —

Baltimore's bill for ransomware: Over $18 million, so far

Mayor says Baltimore is "open for business," but city has lost millions from slowed payments.

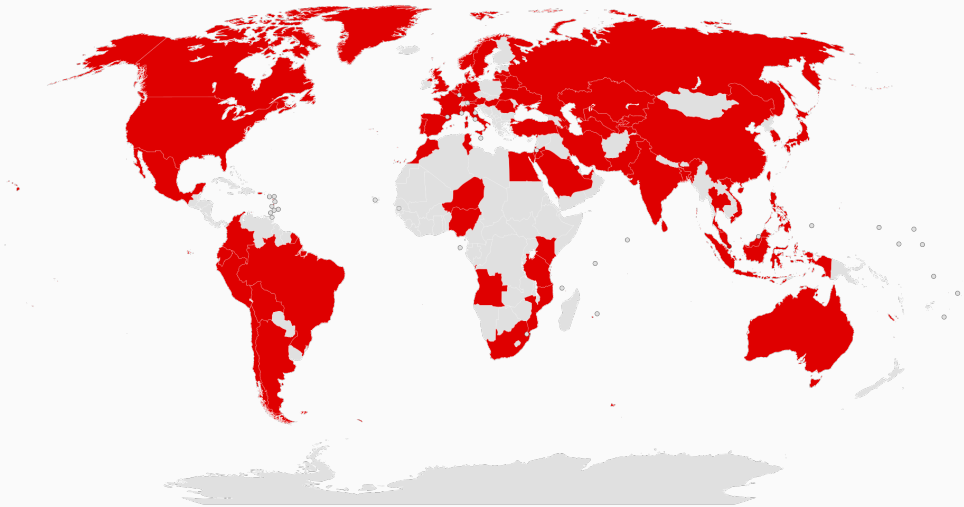
SEAN GALLAGHER - 6/5/2019, 6:25 PM

. Source(s) : Ars Technica, 06/05/2019

Ransomware (Ransongiciel)

Cyber-Braqueur : Chiffrement + Demande de ranson

Nom	Victime (ex.)	Perte / Dégât
Phobos	Sarrebourg	Paralysie
RobinHood	Baltimore	18M$ (1 mois)
Wannacry	300k ordi 150 Pays	Beaucoup



. Source(s) : Wikipédia

Ransomware (Ransongiciel)

Cyber-Braqueur : Chiffrement + Demande de ranson

Nom	Victime (ex.)	Perte / Dégât
Phobos	Sarrebourg	Paralysie
RobinHood	Baltimore	18M$ (1 mois)
Wannacry	300k ordi 150 Pays	Beaucoup
NotPetya	Maersk	>200M$

. Source(s) : https://www.youtube.com/watch?v=VaqIYlYmDbA

Ransomware (Ransongiciel)

Cyber-Braqueur : Chiffrement + Demande de ranson

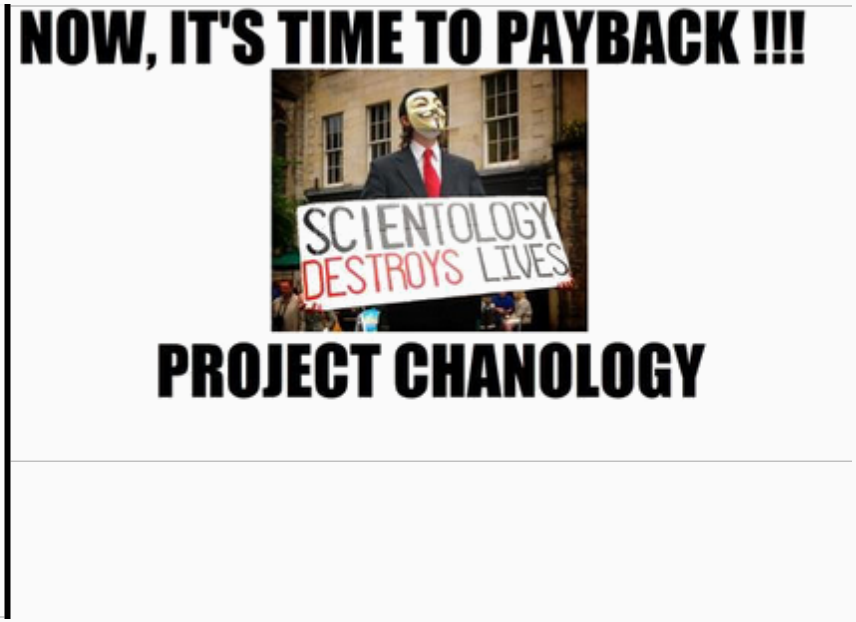
Nom	Victime (ex.)	Perte / Dégât
Phobos	Sarrebourg	Paralysie
RobinHood	Baltimore	18M$ (1 mois)
Wannacry	300k ordi 150 Pays	Beaucoup
NotPetya	Maersk	>200M$

Et vous ? Avez vous déjà été victime d'un ransomgiciel ?

. Source(s) :

Qui sont les Pirates ?

Groupe *Anonymous, Shadow Brokers, Egregor,...*



. Source(s) : Numérama, 24/08/2015

Qui sont les Pirates ?

Groupe *Anonymous, Shadow Brokers, Egregor,...*

Un Individu *Script Kiddy, ...*

Allemagne : une cyberattaque massive fait trembler le pays

Les données personnelles de centaines de personnalités, dont Angela Merkel, ont été mises en ligne durant le mois de décembre. Seul parti épargné : l'AfD.

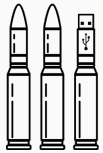
Le(s) coupable(s) ? Un jeune homme de 20 ans

. Source(s) : L'Express, 08/01/2019

Qui sont les Pirates ?

Groupe *Anonymous, Shadow Brokers, Egregor,...*

Un Individu *Script Kiddy, ...*



Un État *Stuxnet, SolarWinds...*

. Source(s) : Numérama, 07/12/2018, icones : hacker : icon8, cyberwar : Skye Selbiger

Pourquoi Moi ? Quelles sont les Nuisances possibles ?

Je ne suis pas une personnalité publique, qui cela intéresserait d'avoir mes données personnelles ?

Quelqu'un qui veut commettre un délis (et se cacher derrière vous)

Que peut faire un méchant avec mes données personnelles ?

Usurpation d'identité :

- Demande de crédit (et ne pas le rembourser)
- Nuire à votre réputation ou à celle de votre employeur
- ...

Que vaut mon identité numérique sur le marché noir ?

- Identifiant/Mdp : quelques dollars
- Données de santé : 50$
- Passeport US : 70$

Conclusion

Les Cyberattaques

1. **Quotidiennes et Massives** (3000 à 18000 / jour)
2. **Tous les services** sont attaquées, souvent avec succès
3. Quantité de données = *O*(**Millions**)

Corollaire : Mes Données ...

1. ...**ont été attaquées** (directement ou indirectement)...
2. ...sont probablement **déjà fuitées**...
3. ...et/ou le **seront bientôt** (Have I been pwned ?)

Risques

1. **Usurpation d'identité** : *Crédit, Atteinte à la réputation, ...*
2. **Pertes de données** : *Ransomware, ...*
3. Dévoiler des **informations privées sensibles** : *santé, politique,...*

Hygiène Numérique

Quelques bonnes pratiques pour espérer éviter le pire

Mots de Passe

https://www.youtube.com/watch?v=aHaBH4LqGsI

Mots de Passe : les plus utilisés en 2020

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213
11. ↑ (12)	1234567	165,909	Less than a second	2,516,606

. Source(s) : NordPass.com

Mots de Passe : Gestionnaire

1 Service = 1 Mot de Passe

- 1 seul mot de passe (maître) **compliqué**
- **Génère** et **stocke** les nouveaux mdp **aléatoires**
- **Facilite la vie !** : remplissage automatique, ...
- Optionnel : **Synchronisation** (Smartphone, ...)

Nom	Avantages	Inconvénients
KeePass2	Sécurisé, Local, Open Source	No Synchro, Complex.
★ Bitwarden	Open Source, Tarif	?
Dashlane	User-Friendly, Alertes	Tarif
LastPass	Tarif, Alertes	Très utilisé (attaqué ?), US

. Source(s) : Comparatif des gestionnaires (NextInpact), NextInpact (23/02/2021 - Bitwarden), Privacy Tools

Mots de Passe

> *Votre mot de passe doit être traité de la même manière qu'une brosse à dents : vous ne le partagez pas et vous le changez régulièrement !*

Choisir un bon Mot de Passe Maître

- Au moins 12 caractères (plutôt 16)
- Majuscule, Minucule, Chiffre, Symbol

Exemples d'Algorithmes

- Première lettre de chaque mot d'une phrase
- Le LJLL est situé à Paris dans le 5ème arondissement ! (`LLJLLesàPdl5èa!`)
- Formule mathématique : `sin^2(x)+cos^2(x)=1`

. Source(s) : Article NextInpact, Recommandations de la CNIL, Recommandations du CERN

Mots de Passe : l'avis d'un spécialiste

https://www.youtube.com/watch?v=yzGzB-yYKcc

Sauvegarde + Sauvegarde + Sauvegarde = ☺

Stratégie 3 2 1

- 3 sauvegardes sur 2 supports différents dont 1 « hors site »
- Limitation de pertes : crash, Vol, ransomware, incendie/cambriolage
- e.g : Ordi/NAS + Cloud + HDD externe ailleurs (coffre banque, famille) mis à jour à chaque visite ($\simeq$ 6 mois ?)

Cloud professionnel

- MyCore (CNRS) : 100Go, sauvegarde à J-1, J-6 et J-15
- PLM Box : 100Go

⚠ Synchronisation $\neq$ Sauvegarde !

- Ransomware ☹ $\Longrightarrow$ Cloud chiffré aussi 😭
- Suppression locale ☹ $\Longrightarrow$ Suppression dans le Cloud 😭

. Source(s) : Dossier NextInpact, Cachem.fr

Emails : la porte d'entrée

4 emails différents (au moins)

#	Utilisation	Caractéristiques
1	Banques, Sécu	Jamais divulguée
2	Professionnel, Famille	prénom.nom@truc.com
3	Shopping, Forum, ...	Pas de nom/prénom
4	Poubelle	bogossdu75@hotmail.fr

Augmenter la Sécurité

- Authentification à 2 Facteurs (SMS, QRCode, ...)
- Vérifier votre question secrète

PGP (chiffrement)[1]

Vous en servez vous ?

1. Ou alors utilisez Protonmail !

Chiffrement : protéger ses données

Attention : crypter n'a aucun sens

Clé Publique / Clé Privée

- La clé **publique** sert à **chiffrer** des données
- La clé **privée** sert à **déchiffrer** les données
- **Décrypter** : tenter de déchiffrer sans connaître la clé

La clé publique peut être vu comme une boite aux lettres et la clé privée comme la clé de la boite

Rendre les données illisibles par un tiers

- Perte / vol de l'ordinateur, clé usb, ...
- Perte de confiance dans le gourvernement (NSA, ...)
- Envoie de pièce jointe sensible (carte d'identité, ...)

Danger

- Perte des données (bug, oubli mot de passe, ...)

Chiffrement : protéger ses données

Disque Dur (local)

- En théorie nous devons chiffrer **tout le disque dur** ...
- ...Sinon, créez un dossier chiffré avec VeraCrypt

Cloud ?

- **Chiffrer** avant d'envoyer dans cloud "public" (dropbox, ...)

⚠ **Un mot de passe Windows/Linux/Mac n'est pas du chiffrement !**

Objets Connectés : Internet of Things/ Internet of Threads

IoT ?

- Enceinte « intelligente » : Google Home, Amazon Alexia
- Montre, ampoule, balance, cravate, ...connectées
- Caméra IP

Une sécurité qui laisse à désirer

- Virus Mirai : attaque DDoS par objets connectés, Infection en quelques minutes
- Insecam (faites y un tour !)
- Ceinture de Chasteté piratée [1]

Opinion radicale : Ne pas en acheter (sauf caméra ?)

Sauf si vous vous y connaissez très (très) bien.

1. NextInpact, 12/01/2021 : « Votre pénis est à moi »

Conclusion

To Do list

- Installer un gestionnaire de mots de passe
- Sauvegarder vos données
- Multiplier les Emails
- Chiffrer vos données sensibles du disque dur
- Mettre à Jour ses logiciels quotidiennement !!
- Renoncer aux gadgets connectés 😉

Références

Merci merci merci !

Pour réaliser ces slides

- MOOC : Protection de la vie privée dans le monde numérique
- MOOC : Défis et enjeux de la cybersécurité - session 1
- Média : NextInpact, Numérama, Wikipédia, ...

Pour vous aider

- NextInpact : journal spécialisé dans les nouvelles technologies
- Cachem.fr : spécialisé NAS : tuto, forum, ...
- PrivacyTools.io : Liste de logiciels/services *privacy by design*
- Framasoft : Association fournissant de nombreux services libres
- La Mère Zaclys : Association fournissant de nombreux services (cloud, ...)

Merci pour votre attention

Annexe

Limites

Alpha Bay = ?

- Plateforme dark market (drogue, arme, ...)
- Similaire à Silk Road (fermée par le FBI)

Une Erreur de Jeunesse

1. Inscription $\Longrightarrow$ e-mail de `Pimp_Alex_91@hotmail.com`
2. Forums de commentcamarche.com, il y a 10 ans :

   > *`Alpha02` : Hello ! Comment se débarasser d'un virus qui a vérolé une de mes photos ? Merci !* ***Alexandre Cazes***

3. Conclusion : DEA arrête Alexandre Cazes et ses ...
   - 12,5M$,
   - Lamborghini, Porsche, Mini Cooper, BMW
   - Cryptomonnais (6M$)
   - Propriétés en Thailande, Chypre et Barbades

. Source(s) : NextInpact