

**RICHTER**

**pour** **ISACA**  
Institut canadien d'assurance de la qualité de l'information  
Section de Québec

**Date/heure :**

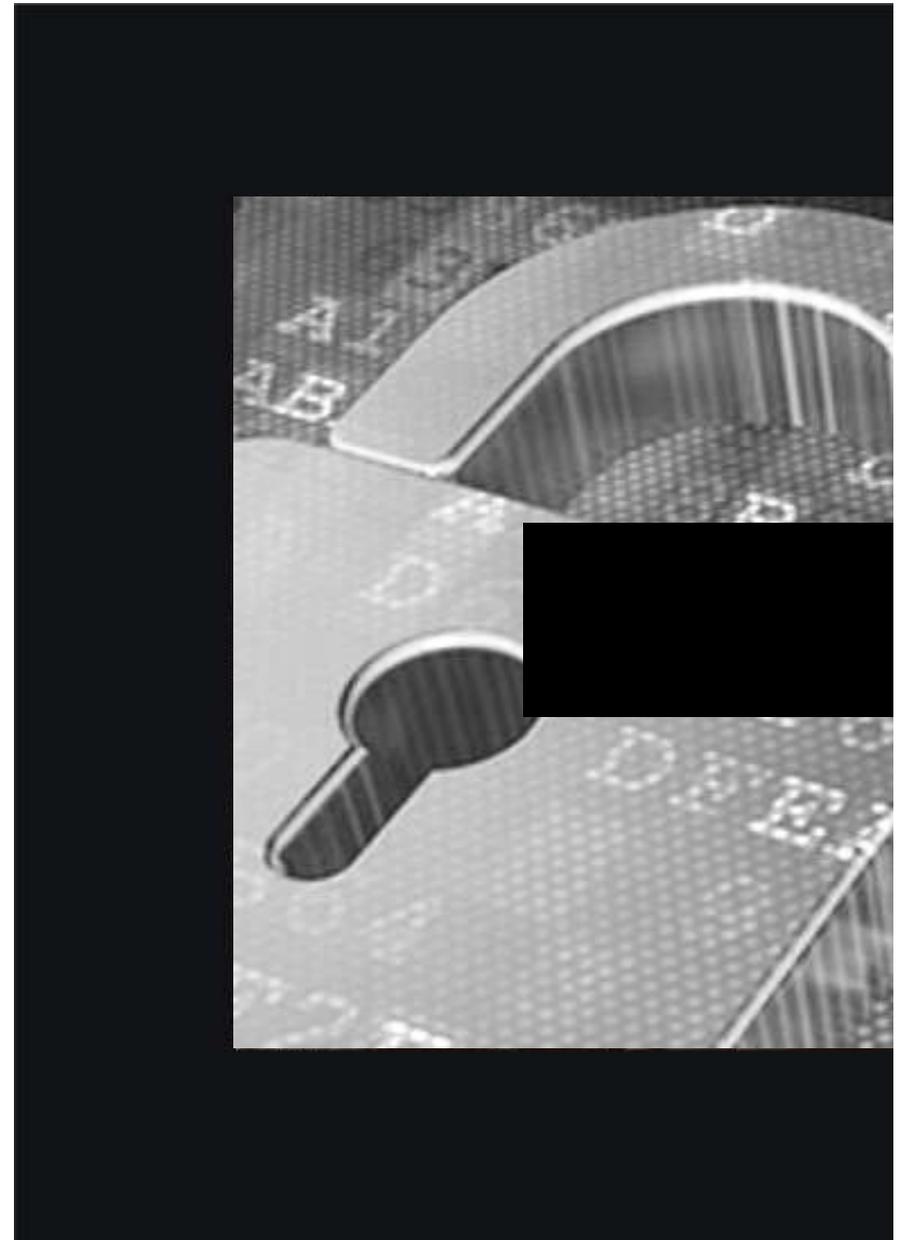
mer. le 1er juin 2017  
15:00 – 16:00

**Lieu :**

Grand Salon – Pavillon  
Desjardins - Université Laval -  
Québec

# Les secrets du Digital Persona, nos données, un vrai terrain de « jeux »...

par **Bertrand Milot**, CISM, CRISC, CRMP, PCSM, CJCISO, ISO.27001 LA  
Premier Directeur Service-Conseil Risques & Cybersécurité



# Biographie



- M. Bertrand Milot est Premier directeur, Services-conseils en risque, performance et technologie. M. Milot compte près de **20 ans d'expérience en TI dont 13 spécialisés en cyber-sécurité** ainsi qu'en gouvernance de la sécurité de l'information, des risques et de l'architecture d'entreprise. Il a également mené plusieurs cyber-enquêtes et a géré des crises importantes liées à des incidents de cyber-sécurité, notamment dans le cas d'attaques par rançongiciel (ransomware).
- M. Milot mène des analyses de risques complètes qui prennent autant en compte la sécurité physique de l'information que sa sécurité logique, ainsi que les vulnérabilités au niveau des personnes, des processus et des technologies. Il s'appuie sur ses connaissances approfondies pour comprendre et transformer les organisations en organisations cyber-résilientes, capables de résister aux menaces émergentes. Au cours des années, M. Milot s'est spécialisé dans les domaines bancaires et financiers au travers de multiples mandats d'analyse de cyber-maturité et d'audits (**Banque Laurentienne, Desjardins, Crédit Mutuel, TMX – Bourse de Montréal, Euroclear Bank & Euroclear SA/NV**), le domaine des Fintechs (Kotio SA, Croesus Finansoft), de la consultation (**KPMG, Richter**) et de l'aéronautique (**Bombardier**). Il a enseigné à l'Université d'Évry, à l'École Polytechnique de Montréal et est l'auteur de plusieurs articles et conférences liées à l'évasion de données du Digital Persona par les IoT, aux enjeux de contrôle et gouvernance des services info-nuagiques, sur la cyber-intimidation en milieu corporatif et sur les défis de la protection des données personnelles et corporatives. M. Milot sera la ressource principale pour ce mandat.



**Bertrand Milot**  
**CISM, CRISC, CRMP, PCSM,**  
**C|CISO, ISO.27001 LA**

Premier directeur, Services-conseils en risques, performance et technologie  
Senior Manager, Risk, Performance and Technology Advisory Services

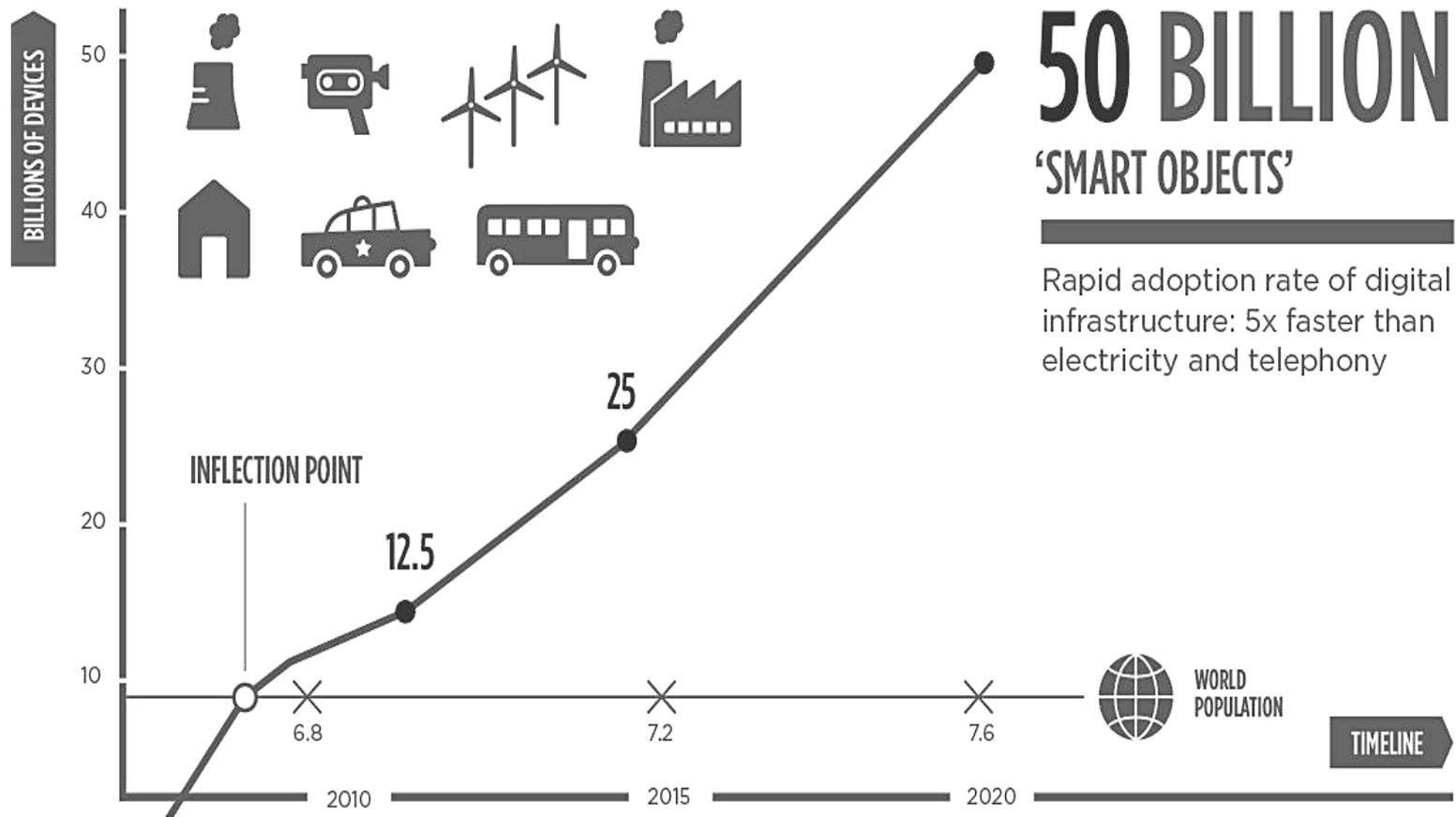
**T. +1 (514) 934-3551**  
**C. +1 (514) 806-4864**

**BMilot@Richter.ca**

# Combien d'IP publiques par personne ?



## Combien d'appareils connectés par personne ?





**La réalité de  
notre empreinte  
numérique...**

# Bande Annonce du film « Sex Tape » 2014

Jay et Annie s'aiment, mais dix ans de mariage et deux enfants ont un peu érodé leur passion. Pour ranimer la flamme, ils décident de filmer leurs ébats lors d'une séance épique. L'idée semble bonne... jusqu'à ce qu'ils s'aperçoivent que la vidéo a été envoyée par erreur à tout leur entourage familial et professionnel via le « cloud » ! Pris de panique, ils sont prêts à tout pour faire disparaître le film à scandale chez chacun des destinataires. Ils jouent leur réputation, leur carrière, leur mariage et leur santé mentale...

[https://www.youtube.com/watch?v=x92e4C\\_TDIk](https://www.youtube.com/watch?v=x92e4C_TDIk)



# De quoi parlons-nous ?



*BEAUCOUP DE DONNÉES...*



Quel est le point commun ?

**C'est GRATUIT!!!**

**...ou presque.**

*Selon Benjamin SONNTAG, co-fondateur de La Quadrature du Net,  
il faut être vigilant :*

**« Si le service est gratuit, c'est  
que le produit, c'est vous ».**

**“Le produit, c'est nous...” Ça paraît évident mais pourquoi ?**



**Le savoir / l'actif informationnel :**

**“L'or numérique est la matière première  
inusable et sans-limites”**

### **Idriss J. Aberkane : la Corée du Sud et l'économie de la connaissance**

Gangnam, le quartier high-tech, commercial et branché de Séoul, où siège notamment Samsung, est le visage du "miracle sur la rivière Han".

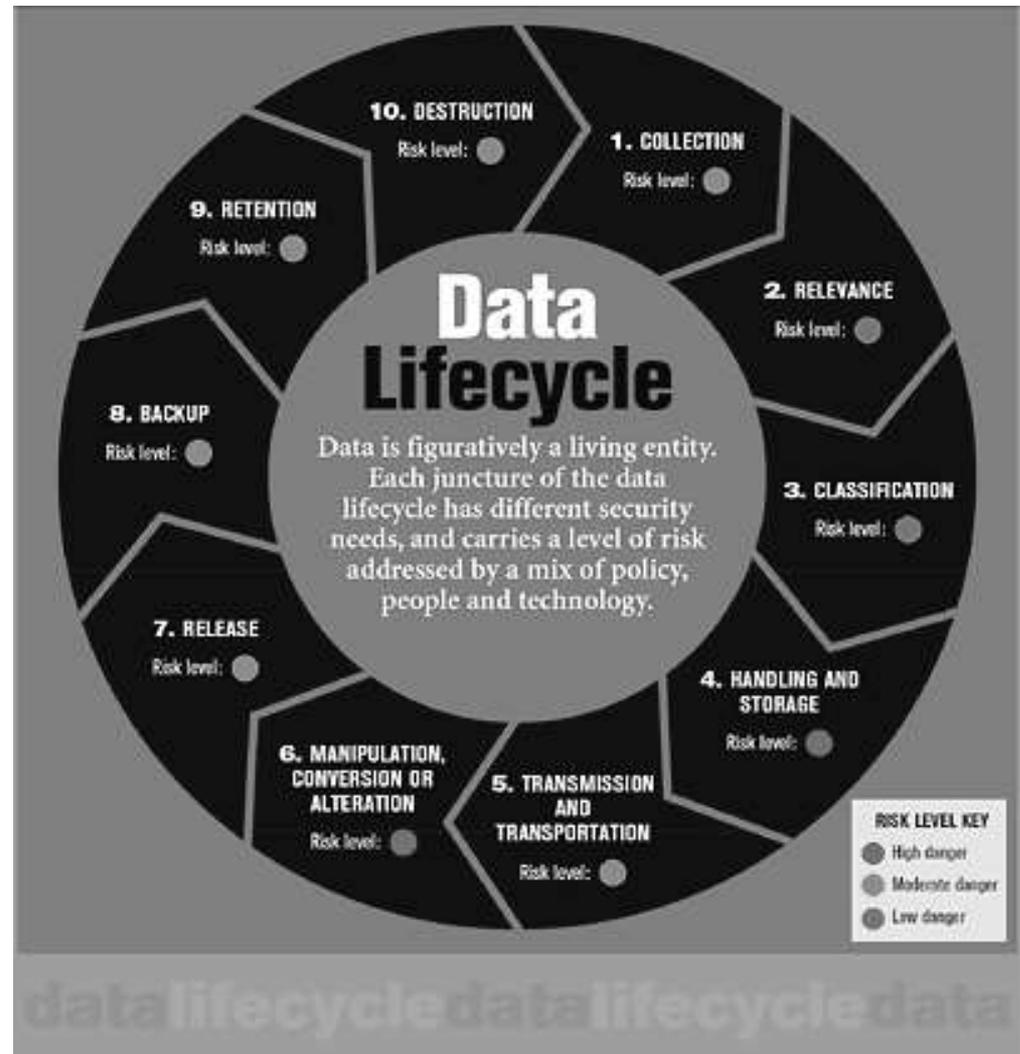
**PAR IDRISS J. ABERKANE (EN CORÉE DU SUD)**

Modifié le 08/08/2014 à 14:23 - Publié le 08/08/2014 à 12:30 | [LePoint.fr](http://LePoint.fr)



Peut-on  
sécuriser la  
donnée elle-  
même ?

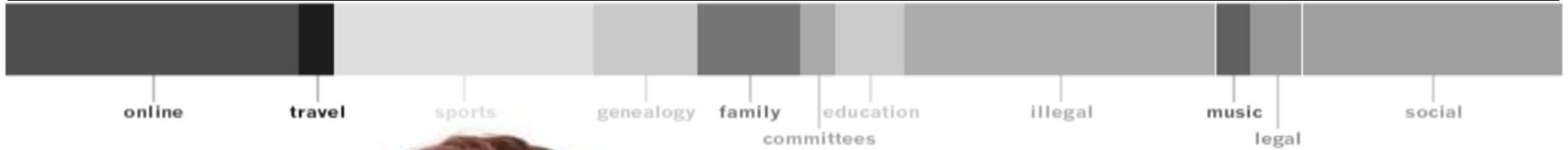
*Réponse :*  
**NON**





**Qu'est-ce que le  
Digital Persona ?**

# La cible : le Digital Persona, l'ADN numérique...



## La fausse question du « Pourquoi moi ? »...



**L'information se vole en se dupliquant, il y a de l'information  
derrière chaque porte...**



## Les questions de base...



**L'actif informationnel est l'actif le plus critique en qualité et en quantité, alors posons-nous des questions :**

- Est-ce que mon iPhone m'appartient ? ...et iCloud ?
- Est-ce que mes données sont protégées dans le nuage ?
- Est-ce que mon compte est supprimé quand je le ferme ?
- Dans le nuage, où sont mes données ?



**Les règles du  
Digital Persona que  
l'on ne lit pas et les  
menaces que l'on  
ignore...**

# Votre iPhone ne vous appartient sûrement pas...



- “Your use of Apple software or **hardware products is based on the software license** and other terms and conditions in effect for the product at the time of purchase.”

<https://www.apple.com/legal/sla/>

- “The software **are licensed, not sold**, to you by Apple Inc. ("Apple") **for use only** under the terms of this License.”

<https://ssl.apple.com/legal/sla/docs/iOS81.pdf>

# Mon smartphone ne va pas bien...



## Apple: une faille de sécurité affecte l'iPhone, l'iPad, l'iPod et le Mac

AFPQC | Par Agence France-Presse  
Publication: 24/02/2014 14:16 EST | Me s



Le système d'exploitation **iOS d'Apple** est aux prises depuis le début de l'année avec une **faille de sécurité** qui n'a toujours pas été réparée.

C'est l'**application Mail** de la Pomme, installée sur iPhone et iPad, qui est touchée par la brèche.

Les utilisateurs doivent se méfier d'une fenêtre leur demandant d'entrer leurs informations pour se connecter à leur compte iCloud ou Facebook, par exemple, à l'ouverture d'un courriel suspect.

Dans l'éventualité au compte en que

Un **hacker québécois**, Alexandre Hélie, 21 ans, a récemment obtenu un emploi chez Apple après avoir découvert trois failles dans le système d'exploitation de l'entreprise. De quoi faire rêver les jeunes qui ne vivent que pour l'informatique..

Étudiant doué au cégep et à l'université, surtout en mathématiques et en physique, Alexandre Hélie se destinait à une carrière en informatique. Plutôt que de terminer ses études universitaires, il est devenu un **hacker autodidacte** : pirate informatique vertueux, il a appris à contourner des protections logicielles. Lorsqu'il découvre la faille, il la signale au légitime propriétaire.

Et des failles, Alexandre Hélie en a découvert trois chez Apple. «J'ai écrit un rapport, je l'ai envoyé à Apple, et deux heures plus tard ils m'ont appelé, en panique, me disant : "Ne publie pas ça !", a-t-il confié en exclusivité à TVA Nouvelles.

«À ce moment-là, je m'attendais à une récompense », en argent. «Parce que la majorité des grosses compagnies donnent de grosses sommes pour de telles trouvailles.»

Le groupe informatique Apple a découvert une faille jugée importante et qui peut affecter tous ses types et la tablette iPad comme les ordinateurs Mac.

Apple a sorti vendredi soir une mise à jour de sécurité de son système d'exploitation mobile iOS, pour met sécurité. La mise à jour (iOS 7.0.6) est téléchargeable sur les iPhone 4 et suivants, l'iPad 2 et les modèles plus récents, ainsi que le baladeur iPod touch.

<http://www.tvaouvelles.ca/2016/01/29/un-hacker-quebecois-embauche-par-apple>

## UNE FAILLE DE SÉCURITÉ EXPOSE PLUS DE 939 MILLIONS DE SMARTPHONES ANDROID !

PAR TRAVIMAXX | 16 JANVIER 2015 | INFORMATIQUE & SMARTPHONE, SÉCURITÉ

Selon Tod Beardsly, un analyste en sécurité informatique, la plupart des smartphones Android sont aujourd'hui exposés à une très grave faille de sécurité, qui pourrait ne jamais être corrigée.



## Ce code en accès libre pourrait transformer une appli iOS en malware

QUÉBEC, 16 JANV. 2015



Le système d'explo  
il exposerait  
est un outil qu  
tes sur le Pla  
de de ne pas  
rtphone. Bien  
votre smartp  
linee utilise et  
que les versio  
4.4 ou Andri  
vous dispose  
5.0, vous cou  
oogle n'empê  
rtphone de l  
terminaux, j

Une librairie open source permet aux développeurs de diffuser des mises à jour d'applications mobiles en court-circuitant le processus de vérification d'Apple. Une bonne idée, mais une pratique plutôt risquée.

La meilleure manière de renforcer la sécurité de son smartphone, c'est de le mettre à jour. Si Android 4.4 est en effet la solution au problème, la mise à jour n'est disponible que pour un nombre très restreint de terminaux Android. Reste bien sûr, l'ultime solution : l'achat d'un nouveau smartphone. Mais vu le prix de ceux-ci, nul doute que beaucoup d'utilisateurs préféreront courir le risque de garder leur ancien smartphone..

Source : Geeko

## Les CGU de l'un de ces géants du web...



« Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à ou à travers de nos Services, **vous accordez à \_\_\_\_\_** (et à toute personne travaillant avec \_\_\_\_\_) **une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées [...], de communication, de publication, de représentation publique, d'affichage public ou de distribution publique desdits contenus. [...]**

*Cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos Services [...]. »*

**...et on enfonce le clou !**



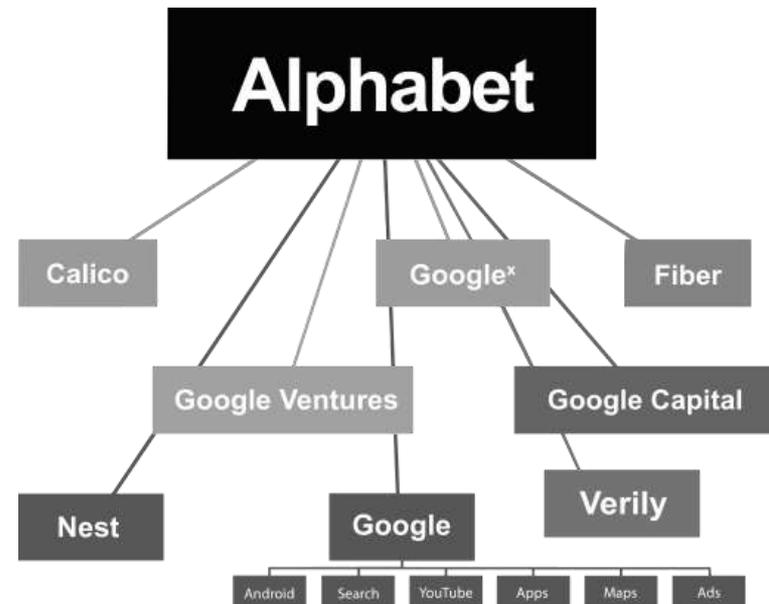
**« Assurez-vous que vous disposez de tous les droits vous permettant de nous accorder cette licence concernant les contenus que vous soumettez à nos Services. [...] »**

**« [...] en outre dégager de toute responsabilité \_\_\_\_\_, ses sociétés affiliées, ses agents et ses salariés et les garantir contre toute réclamation, poursuite ou action en justice résultant de ou liée à son utilisation des Services ou faisant suite à une violation des présentes Conditions d'Utilisation, y compris toute responsabilité et charge financière résultant de réclamations, de pertes ou de dommages constatés, de poursuites engagées et de jugements prononcés, et des frais de justice et d'avocat afférents. »**

## Google nous dit...



« **Nous transmettons des données personnelles à nos filiales ou autres sociétés ou personnes de confiance qui les traitent pour notre compte, selon nos instructions, conformément aux présentes Règles de confidentialité et dans le respect de toute autre mesure appropriée de sécurité et de confidentialité.** »



# Qui est GOOGLE™ ...?



## Et quand on supprime ses données du « Cloud » !?



« **63%** des fournisseurs cloud **conservent leurs données indéfiniment** et n'ont aucune disposition en matière de rétention des données [...]. »

« ...même lorsque vous supprimez des données utilisées par nos services, **nous ne supprimons pas immédiatement les copies résiduelles se trouvant sur nos serveurs actifs ni celles stockées dans nos systèmes de sauvegarde.** »

# Que sait-on de ces mêmes géants du web ?



On September 9, 2014  
**5 MILLION**  
Gmail Logins Were Leaked.

**Over 1 Billion Accounts May Have Been HACKED!**

CWN  
@CyberRisk\_Devs

#BREAKING Bell Internet Hacked, 40,000 Customer Credentials leaked by @NullCrew\_FTS cyberwarnews.info/2014/02/01/bel ... #news #hacks #Leaks #infosec



Bell Internet Hacked, 40,000 Customer Credentials leaked by @NullCrew... Today the official NullCrew has returned to the hack scene with a leak of data from Bell Internet (<http://www.bell.ca>) after about 12months away. [cyberwarnews.info](#)

40 TWEETS  
27 LIKES  
3:40 AM - 7 Feb 2014

167 Million  
**LinkedIn**  
Hacked accounts on SALE!

TC News Startup Mobile Gadgets Trending All Facebook Tech Snap

**Snapchat Employee Data Leaks Out Following Phishing Attack**

Posted Feb 25, 2014 by [Jim Russell](#) | Sponsored



MOTHERBOARD

**Hackers Stole Account Details for Over 60 Million Dropbox Users**



QUARTZ

**Tinder's privacy breach lasted much longer than the company claimed**

By Zachary M. Seward July 31, 2013



**273 million passwords stolen from Google, Yahoo, Microsoft in major security breach**

By Konstantin Hart, [Konstantin Hart](#)

108,291



...et Facebook ?



More Obama cronyism for Healthcare.gov and National Economic Council  
 Facebook "key logs" users even if the "status" is not posted

DECEMBER 18, 2013 BY MIKE 1 COMMENT

1 0 Rate This

More indications of how messed up our relationship with social media companies has reports that Facebook "key logs" users (records users' keystrokes) even when the status Facebook is watching everything keystroke and mouse movement you make when you

Facebook has said that it is within its terms of service to see what users are typing even if the status or comment is never posted on the social network.

The Menlo Park, Calif., company confirmed that it can track users' unpublished posts. Facebook researchers disclosed that they had tracked the activity of about 5 million Facebook users in the U.S. and England.

The researchers' study looked at how often these users censored themselves by not publishing comments on Facebook. If users typed more than five characters, the content was considered to be self-censored if it was not published within 10 minutes of being typed.

Later in the article

Facebook said it was no longer tracking any users when it comes to unpublished posts. It also has no plans to track the unpublished words and letters that users type.

But Facebook said the study was conducted in accordance to the terms of service that every user agrees to when they sign up for the social network.

So where in Facebook's terms of service is this justified? The company said this is covered in its



### Facebook piste tous les visiteurs sans distinction

Ariane Bakry, 1 avril 2015, 14:44



Facebook 6 Twitter 13 Google+ 2 LinkedIn 0 Donnez votre avis

Le réseau social suit à la trace tous ses visiteurs, y compris ceux qui n'ont pas de compte Facebook ou qui ont choisi de ne pas être suivis. D'après un nouveau rapport à charge de chercheurs européens.

La tension monte d'un cran entre le réseau social américain et Bruxelles. Après qu'un avocat de la Commission européenne a recommandé aux internautes soucieux de confidentialité de fermer leur compte Facebook, des chercheurs européens affirment que le réseau social piste tous les visiteurs du site Facebook.com, y compris ceux qui n'ont pas ouvert de compte sur la plateforme. Des chercheurs de l'université catholique de Louvain (KU Leuven) et de l'université libre néerlandophone de Bruxelles (VUB) ont contribué au rapport commandé par l'autorité belge en charge de la protection de la vie privée (CPVP). Une nouvelle ébauche du rapport a été rendue publique le 31 mars 2015.

### Here's Proof That Facebook Knows You Better Than Your Friends

Miss Park, Substack.com, Jan 12, 2015

Your operating system knows you so well, says science

Nobody knows as better than our family and friends, right? Who else could predict how you'll react to good and bad news, or whether to pick the pie or ice cream for dessert?



### Facebook accusé d'analyser les messages privés

La semaine 101 01 2015 à 16:21 - 100 x jour à 00 01 2014 à 10:47

Facebook 6 Twitter 13 Google+ 2 LinkedIn 0 Donnez votre avis



Facebook est de nouveau inquiété par la justice pour le respect de la vie privée. Lors d'un procès, deux utilisateurs américains du réseau social ont lancé une action collective contre l'entreprise devant les tribunaux. Ils accusent en effet Facebook d'intercepter les messages privés commentés des liens, sans le consentement des utilisateurs.

Facebook a tiré les messages des plaignants et analysé les liens envoyés notamment pour de l'analyse de données et le profilage des utilisateurs, a-t-il affirmé dans la plainte, contre reproches l'entreprise des utilisateurs américains affectés par cette pratique. Pour les plaignants, le réseau social exploitait de toute discrétion les messages privés pour obtenir des informations plus personnelles que celles mises en ligne publiquement.

# Conséquences en 2015...



20 minutes

Actualité Entertainment Economie Sport Locales T'as vu ? Vidéos H

MONDE POLITIQUE SOCIÉTÉ SANTÉ

## Facebook: La Commission européenne conseille de fermer son compte

5 CONTRIBUTIONS RÉAGISSEZ À CET ARTICLE

PARTAGER 568 TWITTER 94 +1 9

IMPRIMER ENVOYER



Illustration sur le réseau social Facebook. - M.Libert / 20 Minutes

**20 Minutes avec agence**

Publié le 31.03.2015 à 16:15  
Mis à jour le 31.03.2015 à 16:15

MOTS-CLÉS  
facebook

«Vous devriez songer à fermer votre [compte Facebook](#), si vous en avez un». C'est ce qu'a recommandé, la semaine dernière, Bernhard Schima, avocat de la Commission européenne pour qui la «législation actuelle ne peut pas garantir une protection adéquate des données des citoyens européens».

Le conseil a été prodigué, la semaine dernière, par Me Bernhard Schima, lors d'un procès portant sur la confidentialité des données des Européens exportées vers des services en ligne américains.

### A LIRE AUSSI

23/05/14 | WEB  
Facebook protège enfin la vie privée des nouveaux abonnés

18/04/14 | WEB  
Facebook lance un service pour localiser ses amis (mais en respectant la...)

17/04/14 | INTERVIEW  
E-reputation: «Partager sa vie privée sur le Web n'est pas néfaste»



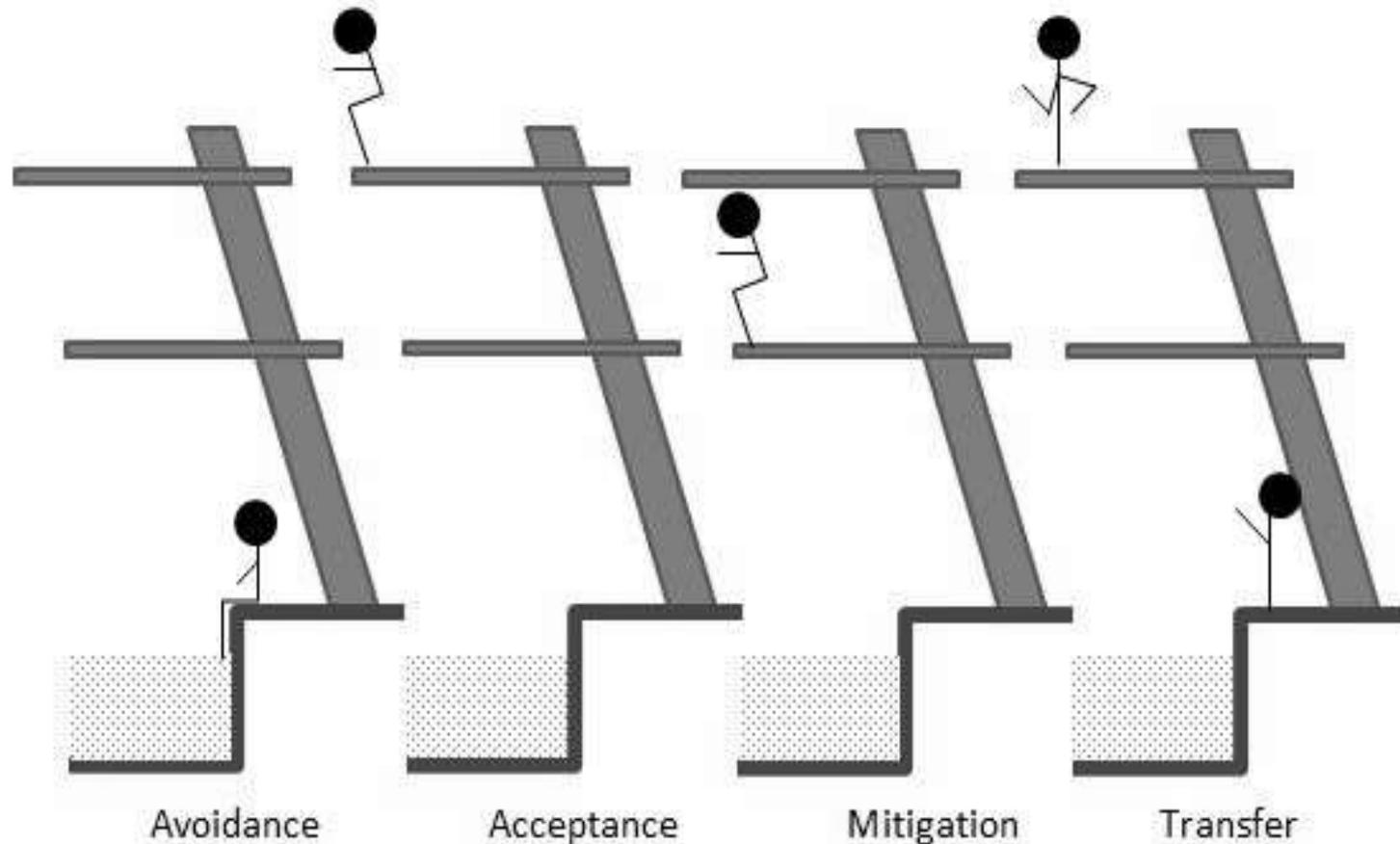
## Campagne Dave

Afin d'inciter le public à faire preuve de vigilance et de prudence dans la communication d'informations personnelles via internet, Safeinternetbanking.be a lancé une campagne ludique. Au centre de cette campagne, on retrouve Dave, un voyant aux pouvoirs « paranormaux ». Des passants croisant Dave par hasard avaient la possibilité de s'arrêter auprès de lui afin d'obtenir un conseil gratuit et personnalisé. Une opération qui a récolté un franc succès. Or, derrière Dave, se cachaient quelques hackers qui soufflaient à l'oreille du voyant toute les informations laissées par son client sur des sites internet publics. Comment s'appelaient ses enfants, combien avait coûté sa maison, combien d'argent il avait sur son compte en banque, combien d'argent il avait consacré à l'achat de vêtements le mois précédent, et quel était son numéro de compte, etc.

[https://www.youtube.com/watch?v=spopho\\_wJOU](https://www.youtube.com/watch?v=spopho_wJOU)



# Comment traiter un risque ? ...et CE risque en particulier ?



*Strategies for dealing with risk*

*R. Jaffa*

# Attention... conférence interactive !

- Le sondage est anonyme !
- Hautement sécurisé !
- Les résultats sont en temps réel.
- Le principe est simple...

Who directed the Oscar-winning  
2008 film Slumdog Millionaire?

- A. Danny Boy
- B. Danny Boyle
- C. Danny Baker
- D. Susan Boyle
- E. Frankie Boyle
- F. Danny DeVito



# Notre système interactif de sondage



Connectez-vous sur...

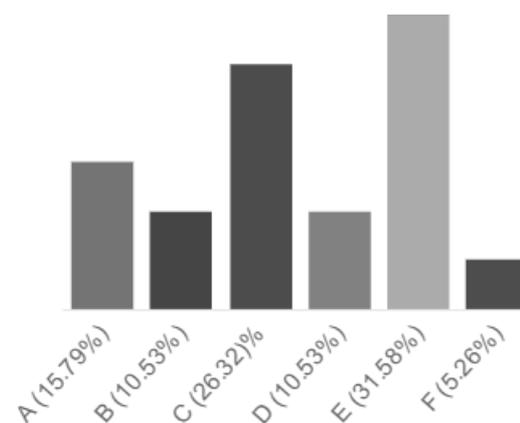
<http://www.101vote.com/>



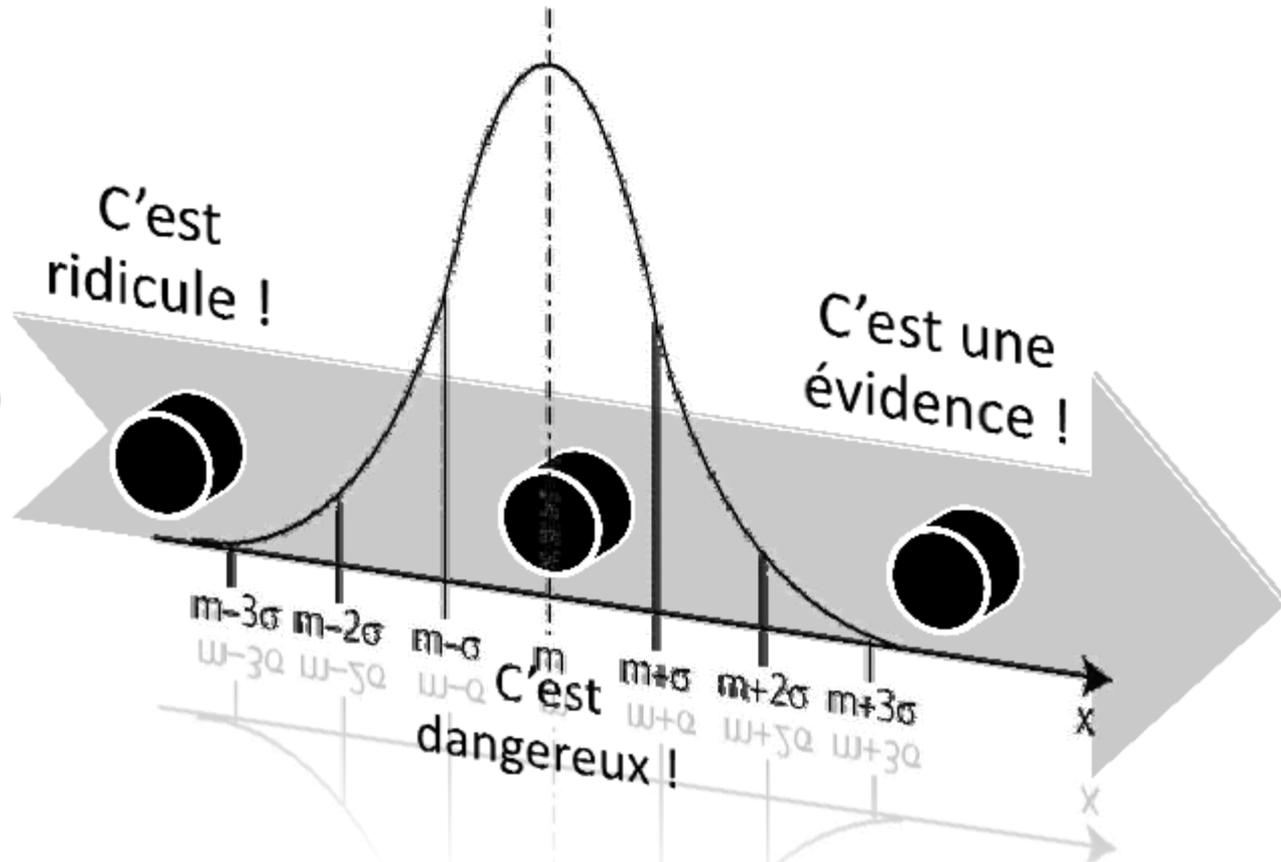
## Question : Quelle est votre réponse personnelle face à ce risque ?



- A. Oui, j'ai totalement accepté ce risque, sinon je ne vis plus !
- B. Oui, je l'accepte, mais ça me gratte un peu quand même.
- C. Oui, je suis conscient et j'accepte, mais à contrecœur...
- D. Non, je ne l'accepte pas, mais je ne peux pas faire autrement...
- E. Non, je ne l'accepte pas et je mets doucement des solutions alternatives.
- F. Non, je ne l'accepte pas du tout, j'ai des solutions pour y remédier !



# Le risque, c'est une question de gestion du changement...



# Tellement de brèches que des services se créent...



;-) Home Pwned sites FAQs Twitter A troyhunt.com project

## ';-)have i been pwned?

Check if you have an account that has been compromised in a data breach

enter your email address **pwned?**

This is a screenshot of the 'Have I Been Pwned?' website. The header is dark blue with a logo on the left and navigation links: Home, Pwned sites, FAQs, Twitter, and A troyhunt.com project. The main content area is a lighter blue with a large white rounded rectangle containing the text "';-)have i been pwned?". Below this is a sub-headline: "Check if you have an account that has been compromised in a data breach". At the bottom, there is a white input field with the placeholder text "enter your email address" and a dark blue button labeled "pwned?".

**BreachAlarm** Home Business Sources Blog Help Log in or Sign up

## Password hacking compromised more than 150 million accounts this past year.

Find out if a password hack has exposed your password online.

We scan the Internet for stolen password data posted by hackers, and let you know if we spot your email address in a security breach.

Watch the video!

my email address **Check Now** OR Get notified of hacks that affect my password: Email Watchdog FREE and paid plans

This is a screenshot of the BreachAlarm website. The header is white with the BreachAlarm logo and navigation links: Home, Business, Sources, Blog, Help, Log in, or, Sign up. The main content area has an orange background. It features a large headline: "Password hacking compromised more than 150 million accounts this past year." followed by a sub-headline: "Find out if a password hack has exposed your password online." and a paragraph: "We scan the Internet for stolen password data posted by hackers, and let you know if we spot your email address in a security breach." To the right of the text is a video player with a play button and a "TOP SECRET" stamp. Below the text is a white input field with the placeholder text "my email address", a green "Check Now" button, and an "OR" button. To the right of the "OR" button is another paragraph: "Get notified of hacks that affect my password: Email Watchdog FREE and paid plans".



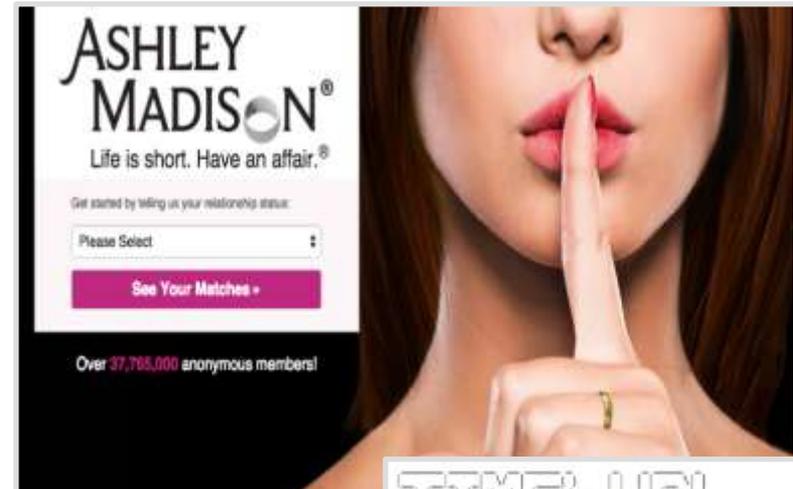
**Des brèches et  
des risques plus...  
...dérangeants...**

# Les autres brèches, un peu plus dérangeantes...



## Ashley Madison, petit rappel des faits...

- Service en ligne d'adultère
- Le slogan :  
« *Life is short. Have an affair* »
- Ouvert depuis 2001
- 124 millions de visites par mois
- Ultimatum en Juillet 2015
- 35 millions de comptes utilisateurs divulgués





# Ashley Madison dans les chiffres, c'est...

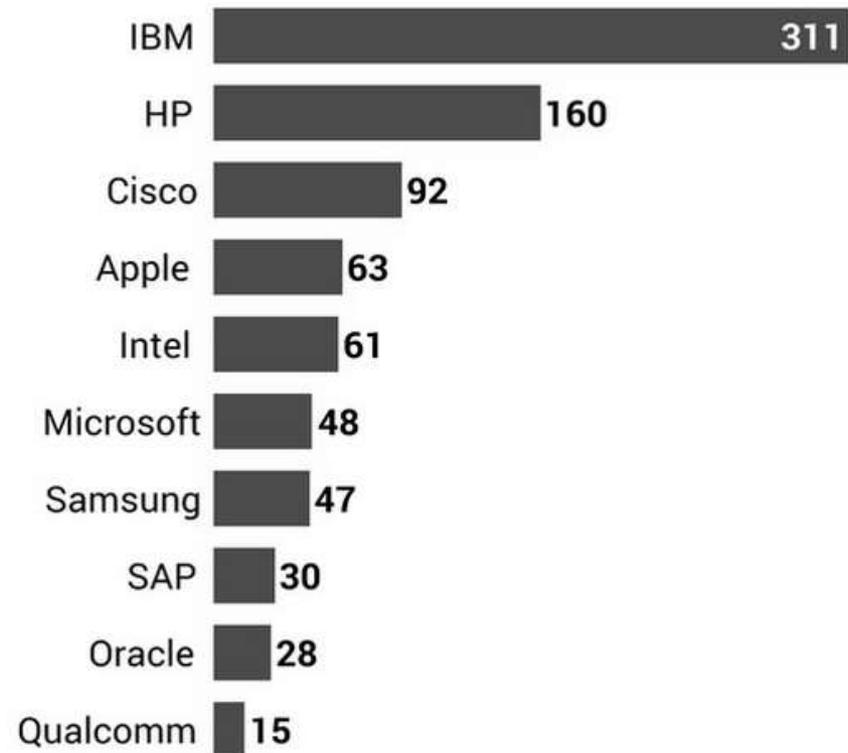


- Extorsions de masse et criminalité à étages

## Adresses professionnelles utilisées :

- 553 adresses de fonctionnaires fédéraux (courriels terminant en **.gc.ca**)
- 315 adresses terminant par **.qc.ca**
- 132 adresses d'universités au Québec
- 24 adresses se terminant par **@cbc.ca** et 5 par **@radio-canada.ca**

Number Of Valid Ashley Madison Accounts Among The Largest Tech Companies



## Et il y a eu pire fin 2016...

### Hack exposes 412 million accounts on Adult FriendFinder, making it one of largest data breaches ever

 ANDREA PETERSON, WASHINGTON POST | November 15, 2016 10:09 AM ET  
More from Washington Post



- *“The site was **previously hacked in May 2015**, when 3.5 million user records were exposed.”*
- *“I’m afraid so. Of the 412 million accounts exposed on the breached sites, in **5,650 cases**, **.gov email** addresses have been used to register accounts. The same goes for **78,301 .mil email** addresses.”*

# Plus généralement, même les adeptes de vidéos “Olé-Olé”...

## Attaque de YouPorn : des milliers d'identifiants dans la nature

Protégez-vous, ici comme ailleurs 142



Par Vincent Hermann  
le jeudi 23 février 2012 à 17:55

Si vous êtes un utilisateur du site célèbre site porno YouPorn, sachez que vos identifiants sont peut-être partis faire une balade dans la nature. Une brèche dans la sécurité de l'un des services du site a permis une fuite d'information bien que cette dernière ait potentiellement été très exagérée jusqu'à présent.



### 1 million YouPorn users exposed; data breach required no security penetration

February 22, 2012, 2:35 PM — Some stories make you want to wash your hands afterward. With others it's simpler to just wear vinyl gloves while you type.

## Brazzers porn site data breach: Details of 800,000 users leaked by hackers

YOUNA SOURCEBOOK | Thursday 4 September 2016 10:16:55



2 min

## xHamster breach pops 380,000 porn account login details on the internet

By NSA — 5 months ago in BREACH

## Porn-surfing corporate bosses infect networks, then keep data breaches a secret

57% of U.S. enterprise malware investigations involve data breaches that are never disclosed, with many executives surfing to infected porn sites.



**SECURITY**

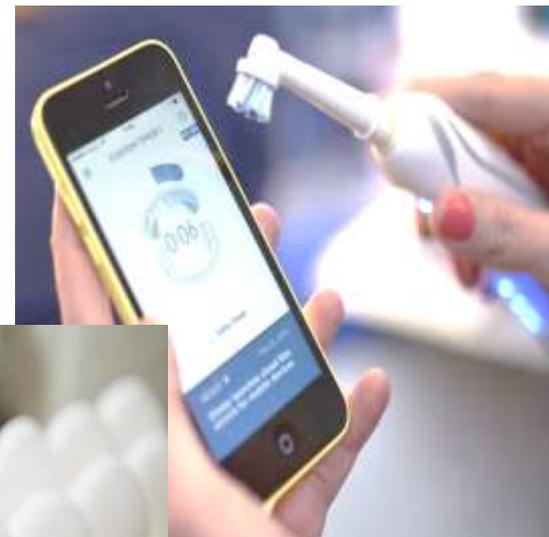
### Porn Viewing Habits Could Be the Next Big Leak: Here's What To Do

By [@InfoSecNews](#) / November 27, 2015 / 6 minutes

A large, light gray, stylized letter 'E' graphic that serves as a background for the main text. It has a thick, blocky appearance with rounded corners.

# Quid des “IoT” ?

# L'avenir ? Le risque lié aux « IoT » dans tout ça !



## Risques ?

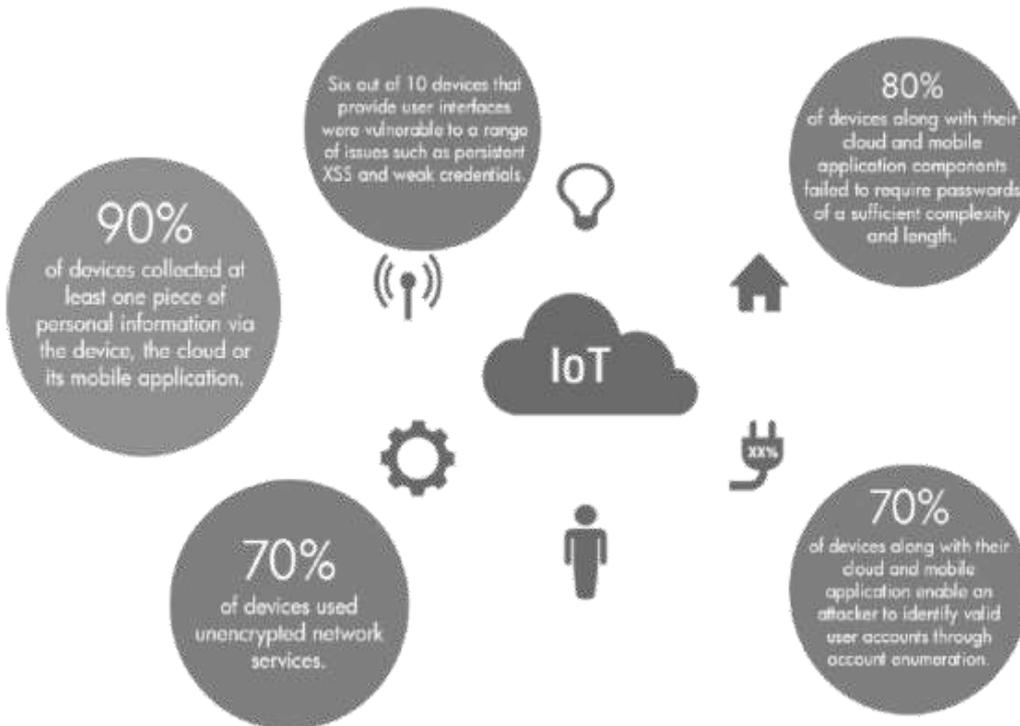
Oui, j'ai moi-même succombé et accepté le risque... ☹️



# Des vulnérabilités ?



## HACKING fitbit in 10 Seconds



Forbes / Tech

10 Seconds to Buy Now

BY CLAUDIO BIANCHI AND DANIEL WERNER

### Yes, You Can Hack A Pacemaker (And Other Medical Devices Too)

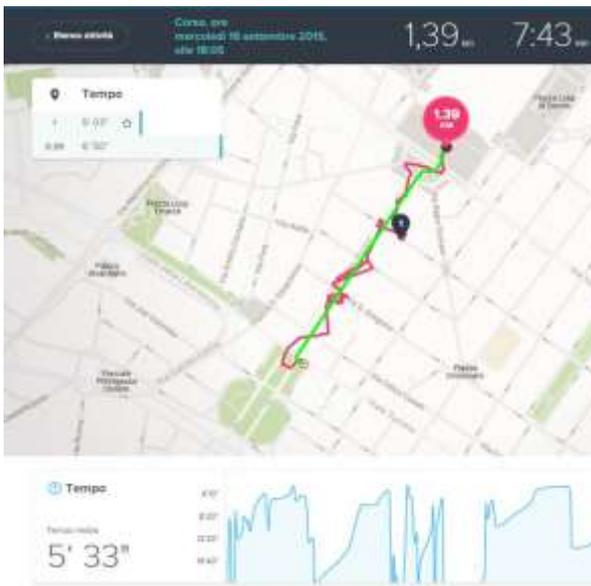
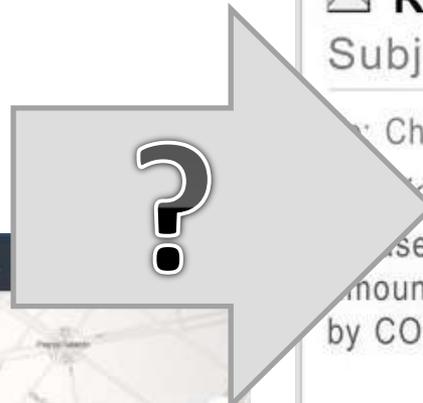
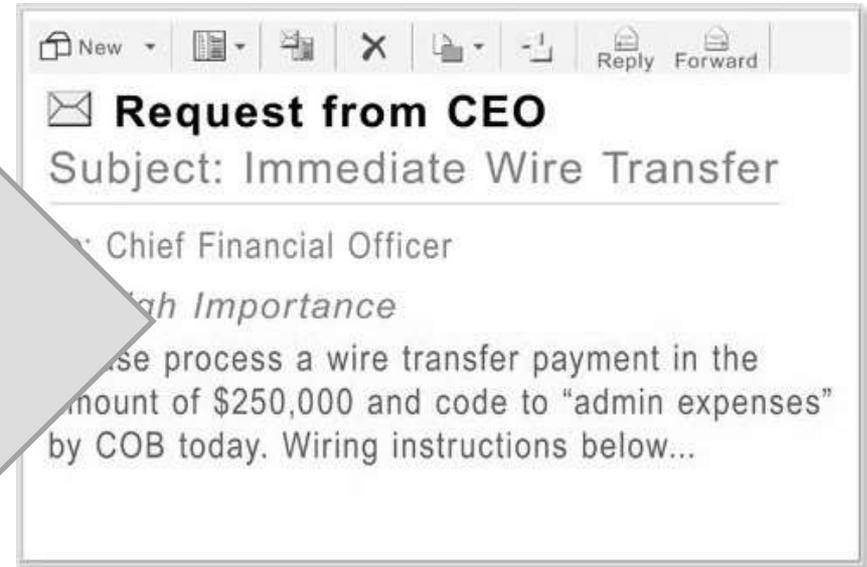


On Sunday's episode of the Emmy award-winning show *Howland*, the Vice President of the United States is assassinated by a group of terrorists that have hacked into the pacemaker controlling his heart. In an elaborate plot, they obtain the device's unique identification number. They then are able to remotely take control and administer large electrical shocks, bringing on a fatal heart attack.

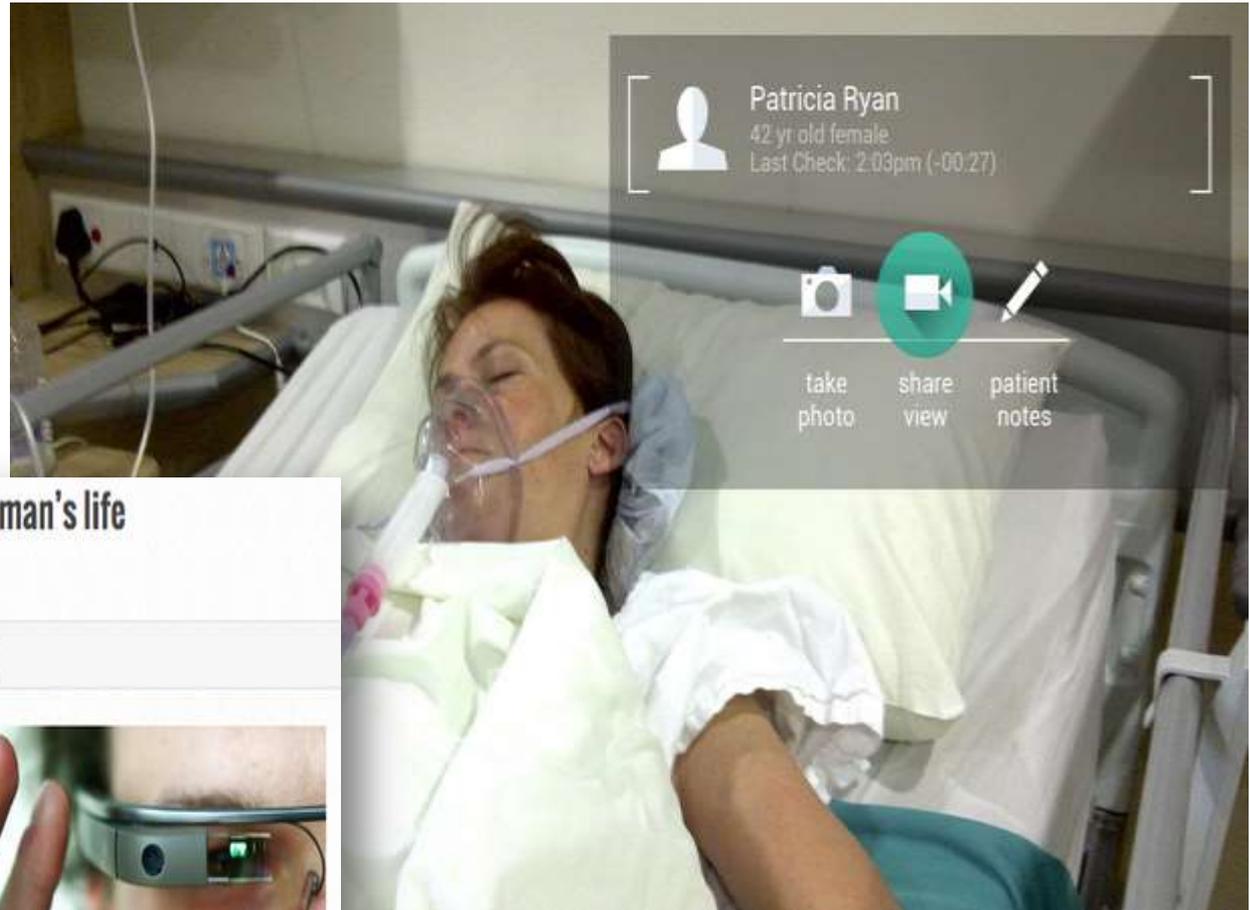
Viewers were shocked - many questioned if something like this was possible in real life. In short: yes (although the part about the attacker being halfway across the world is questionable). For years, researchers have been exposing numerous vulnerabilities in internet-connected implanted medical devices.



# Risques pour une organisation ?



# Déjà en pilote pour le domaine médical...



## How Google Glass helped a doctor save a man's life

By *Joel Joseph* on April 9, 2014

[Tweet](#) 4 [g+](#) +2 [Pin it](#) [f Like](#) 0

Over the past one year, Google Glass has been experimented in a number of fields like healthcare, sports, medical industry etc. But even before the device is commercially available, a doctor at the Beth Israel Deaconess Medical Center claims that the device helped him to save one of his patients. This is actually great news for the device, which has been getting plenty of negative reviews lately with respect to its privacy protection.



## Question : qui détient des « IoT »

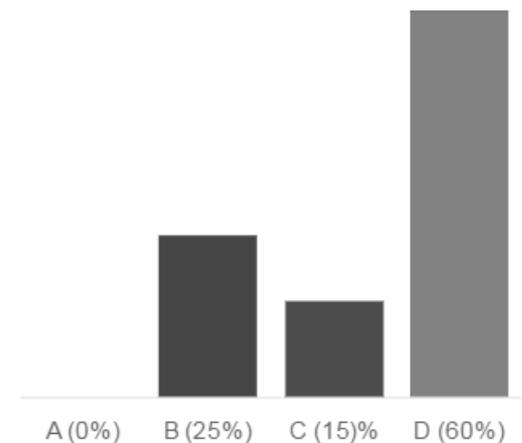


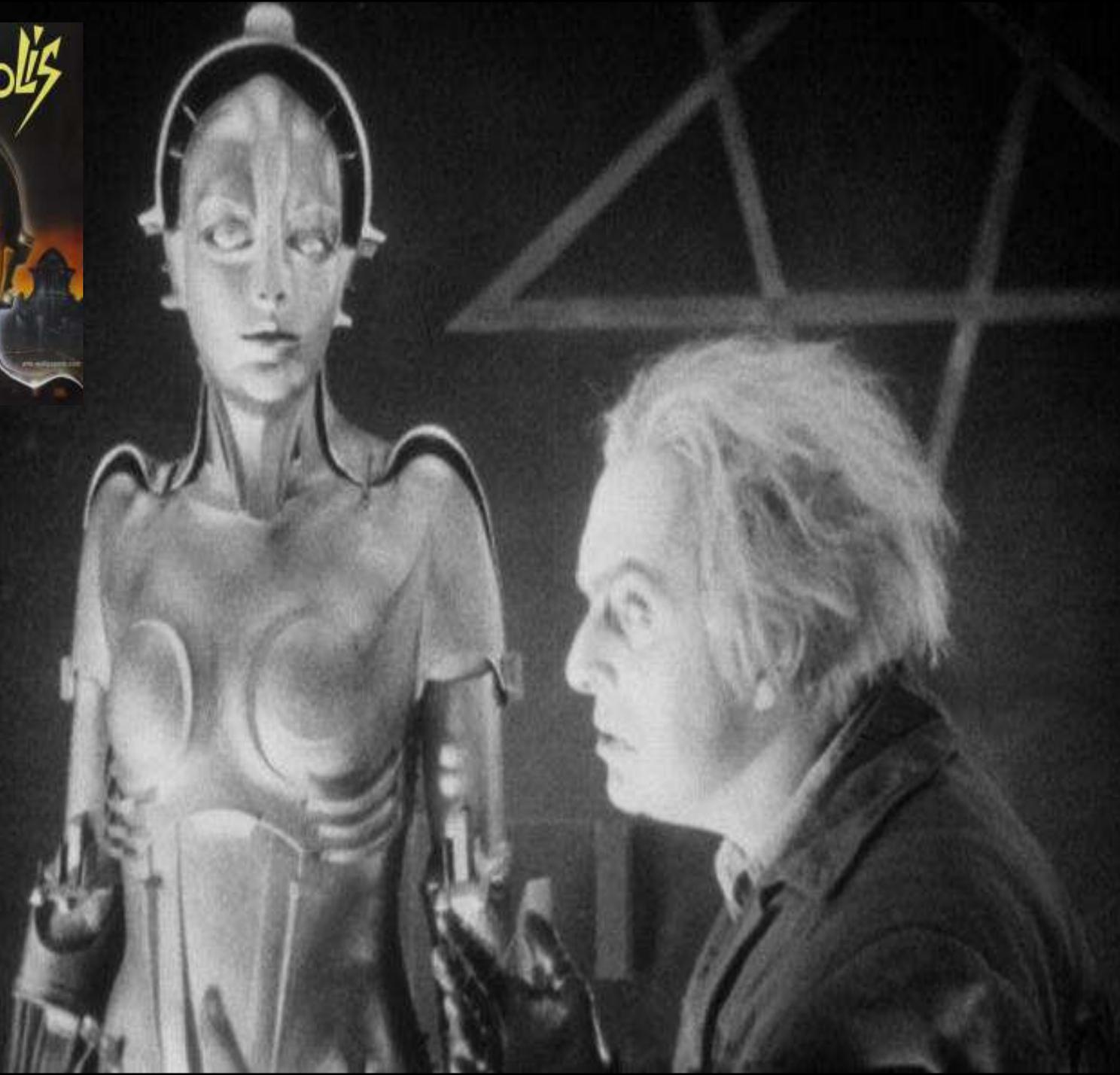
A – J'en ai personnellement et ils pourraient être détournés pour impacter indirectement l'organisation ou les organisations pour lesquelles je travaille.

B – J'en ai mais les données sont triviales, j'opère une protection spécifique et/ou je connais très bien leurs écosystèmes de données.

C – J'en ai mais ils sont sur un réseau clos non connecté à Internet.

D – Je n'en ai pas.





## Question : l'androïde intime

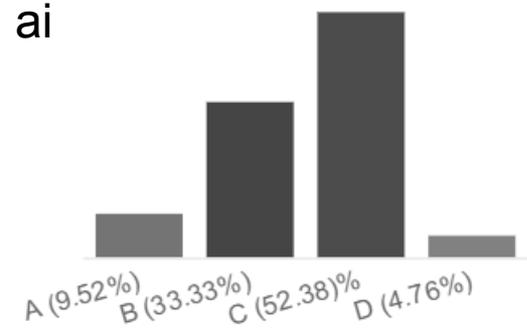


A – Ça n'existe pas encore et ne sera pas sur le marché avant 5 ans !

B – Ça n'existe pas sur le marché, mais un prototype existe peut-être...

C – Ça existe sûrement et ça sera vendu dans 1 an ou 2...

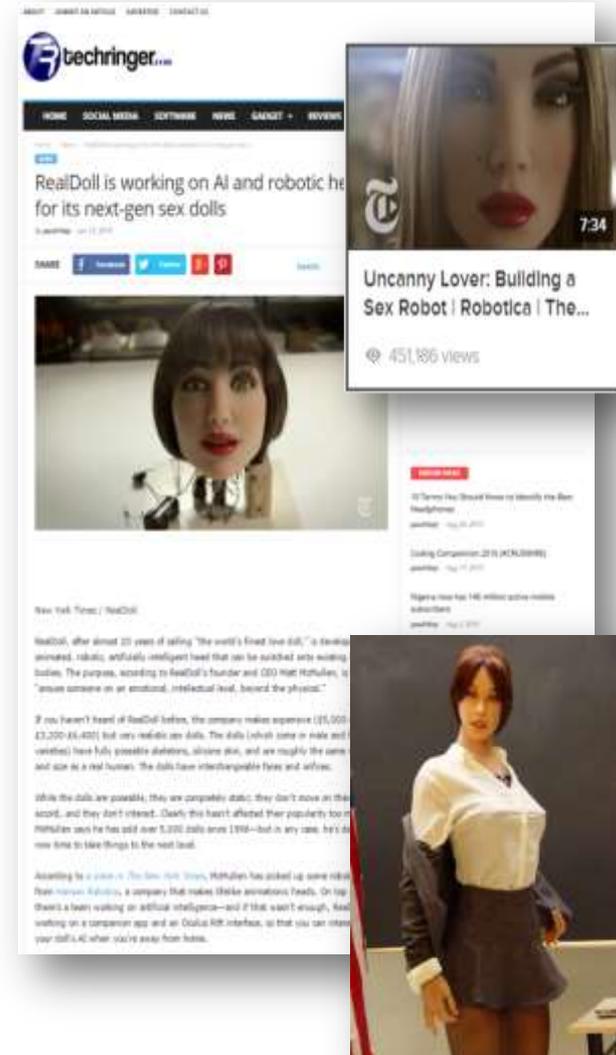
D – Ça existe, c'est cool, je vais en acheter un ou j'en ai déjà un !



# La « RealDoll » de Abyss Creations

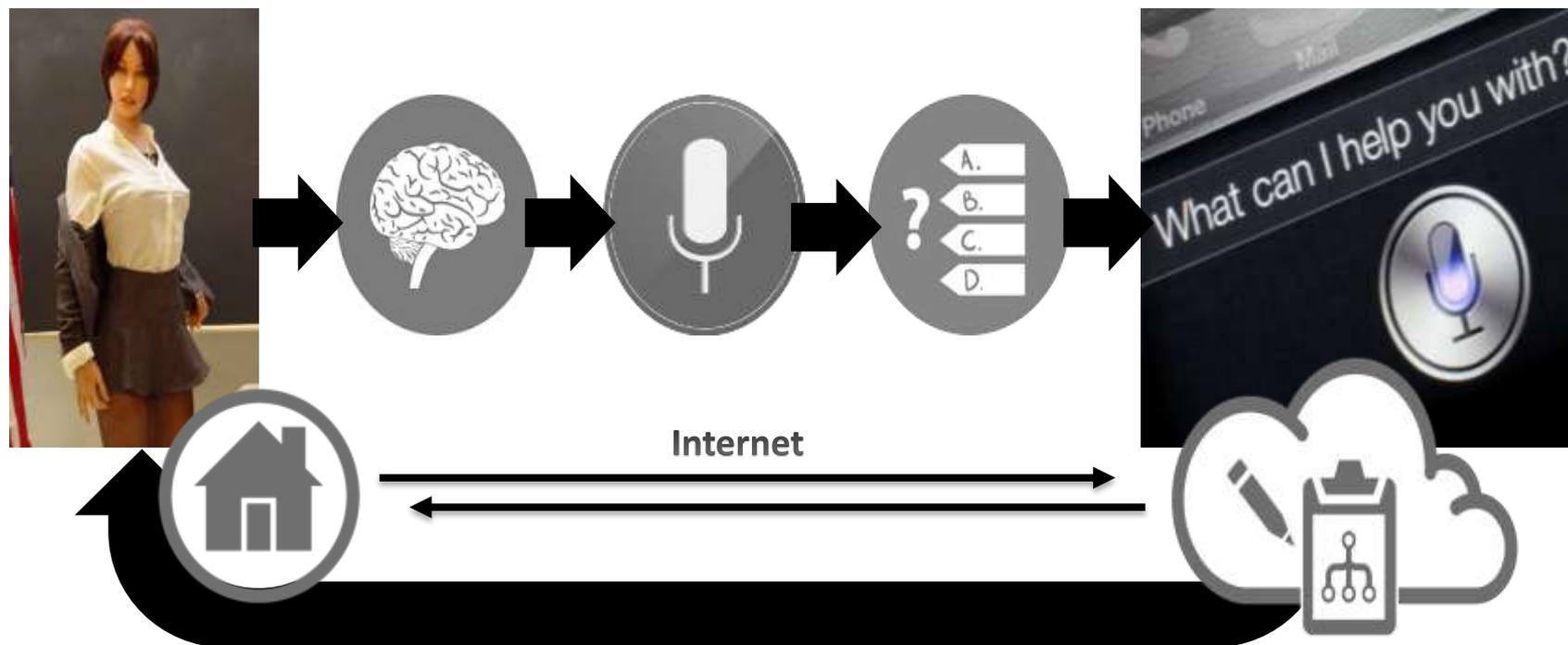


- **1996** : Abyss Creations annonce la 1ère “Real Doll”
- Howard Stern l’a essayé et a adoré
- Depuis 2010, **plusieurs dizaines de milliers** sont en circulation à travers la planète et d’autres marques concurrentes sont apparues.
- 19 ans plus tard, **Abyss Creations annonce l’IA** et la motorisation
- RealDoll CEO Matt Mullen : **“We’re looking at 2017 for having a working model completed.”**



# Donc, un robot intime, de l'intelligence artificielle... Et alors ?

- « The devil hides in the details ! »





**Qui peut bien  
vouloir tout ça...?  
Et de quelle  
façon...?**



# Les impacts et les chiffres

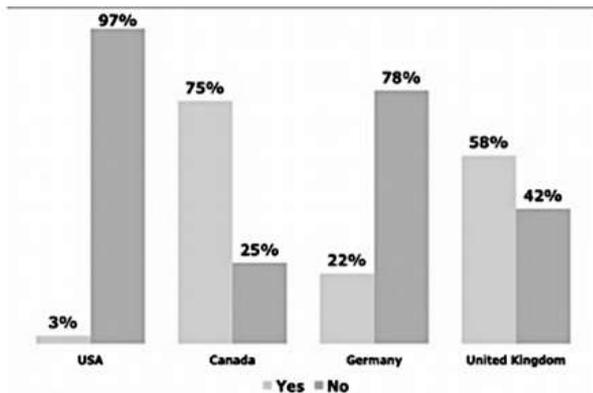


L'extorsion par ransomware arrive en tête des menaces déclarées  
L'assureur AIG indique que le phénomène représente 16 % des sinistres que lui ont déclaré ses clients. Mais il arrive tout juste devant les atteintes ...  
lemagit.fr

## Nearly 40% of Ransomware Victims Pay Attackers

Ransomware is targeting more consumers, and many of them are paying hundreds to attackers.

Source: <http://www.techradar.com/news/cybersecurity/2014/08/20/2014-08-20-ransomware-victims-are-paying-hundreds-to-attackers>



# CRYPTOWALL RANSOMWARE

## Hacking Group Generated \$325 Million in Revenue.

### Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LE1PgVh6S9VEXWV2dZ7y1SRd7e9B1bWtQ**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

### What we did?

We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world (Encryption - Wikipedia). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever

### Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

<https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c76ffa5>

### Why we do that?

We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. **I personally have lost both my parents and my little sister in 2015**. The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. (Syria War in Wikipedia)

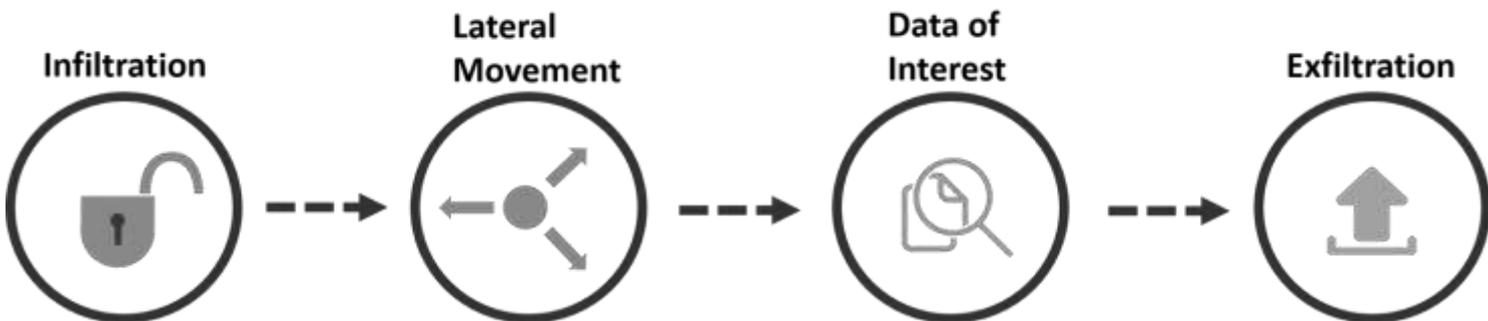
Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people. We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.



# ANGLER EXPLOIT KIT

*1st Attack:*  
**Password Stealer**

*2nd Attack:*  
**Ransomware**



# La revente dans le Darknet ?



**FRESH VISA CC/CVV FROM USA (excellent quality)**

If you pay! You get the material in the format:  
 Inumber|exp|cvv2|holder|country\_code|state\_code|city|zip|address|email|phone Excellent quality! Material produced by me. (oneSeller/UsaCC) Welcome , pleasant shopping! Thank you!

Sold by **oneSeller/UsaCC** - 3608 sold since Jun 8, 2015 **Vendor Level 5** **Trust Level 4**  
 41 items available for auto-shipment

| Product class | Features      | Origin country | Features  |
|---------------|---------------|----------------|-----------|
| Quantity left | Digital goods | Worldwide      | Worldwide |
| Ends in       | Unlimited     | Ships to       | Worldwide |
|               | Never         | Payment        | Escrow    |

Default - 1 days - USD +0.00 / item

Purchase price: USD 7.00

Qty: 1 **Buy Now** **Queue**

0.0219 BTC

**Blue Cross Blue Shield**

Member Name  
**FIRST M LASTNAME JR**

Member ID  
**DZW920000000**

Member 004336  
 9101003777

Member 004336  
 9101003777

**Blue Dental Blue Vision** Rx

**Healthcare Database (397,000 Patients) from Atlanta, Georgia, United States**

Rating for this product based on number of finalized sales

Seller: **thedarkoverlord** (0) 0% Positive feedback  
 Visit store: [thedarkoverlord doesn't have a store](#)

Finalize Early: **No, FE is not required.** Shipping Type: **Normal**

Quantity: 0 **In stock / 0 sold**

Postage Option:

Price: **0 634.73**  
**BTC 634.7292**

**Buy it Now**  
**Add to favorites**

**HANSA**

**V.I.P. Healthcare - Full info medical records (DOB, SSN, PHOTO, Insurance, Drugs, Lab results)**

**USD 0.99**  
 0.00009

**Only 2 left!**

Vendor: **[Redacted]** **Level 1/3**

Class: **Digital**

Delivery: **Instant Delivery**

**Buy Now**

1 Question Report

Also profiles:

- V.I.P. Healthcare - Full info medical records (DOB, SSN, PHOTO, Insurance, Drugs, Lab result) - **USD 0.99** 0.00009

**Listing Details**

V.I.P. Healthcare medical records  
 Full info:  
 DOB, SSN, PHOTO  
 Insurance info with card photo.  
 Med info.  
 Prescribed Drugs info.  
 Never used.

**2376 x INDIA (IDENTITY DOCS) + (PROOF OF ADDRESS) / ALMOST FREE !**

2376 x HIGH IDENTITY DOCS + (PROOF OF ADDRESS) / ALMOST FREE / MY OWN PRIVATE COLLECTION Together 2376 scans ITS A SET OF ALL DOCUMENTS (IDENTITY DOCS + (PROOF OF ADDRESS) POSSIBLE TAX ONLY ALL TOGETHER FOR \$299 Scans are delivered immediately after you click buy now (auto-del) !! (README)

Sold by **Doc1** - 0 sold since Feb 25, 2019 **Vendor Level 5** **Trust Level 5**  
 230 items available for auto-shipment

| Product class | Features      | Origin country | Features  |
|---------------|---------------|----------------|-----------|
| Quantity left | Digital goods | Worldwide      | Worldwide |
| Ends in       | Unlimited     | Ships to       | Worldwide |
|               | Never         | Payment        | Escrow    |

Default - 1 days - USD +0.00 / item

Purchase price: USD 299.00

Qty: 1 **Buy Now** **Buy Now** **Queue**

0.000000 0.000000

**Product Description**

2376 x HIGH IDENTITY DOCS + (PROOF OF ADDRESS) / ALMOST FREE !  
 MY OWN PRIVATE COLLECTION  
 Together 2376 scans ITS A SET OF ALL DOCUMENTS (IDENTITY DOCS + (PROOF OF ADDRESS)  
 POSSIBLE TAX ONLY ALL TOGETHER FOR \$299  
 Scans are delivered immediately after you click buy now (auto-del)

# Autres exemples ?



## 5x UNITED KINGDOM PASSPORT SCAN - ONLY \$2 EACH!! TEMPORARY PRICE / 90% + VALIDITY

These are great quality scans of documents. You will receive: 5x UNITED KINGDOM - PASSPORT SCAN - ONLY \$3 EACH!! TEMPORARY PRICE / 90% + VALIDITY Scans are delivered immediately after you click buy now (autoship)  
----- READ THE BOTTOM TEXT BEFORE BUYING

Sold by **Zoy3** - 895 sold since Feb 26, 2016 **Vendor Level 5** **Trust Level 5**  
600 items available for auto-dispatch

|               | Features      | Origin country |
|---------------|---------------|----------------|
| Product class | Digital goods |                |
| Quantity left | Unlimited     | Ships to       |
| Ends in       | Never         | Payment        |

SEE MY STORE FOR MORE - 1 days - USD +0.00 / item

Purchase price: USD 10.00

Qty: 1 **Buy Now** **Buy Now** **Queue**

0.000 BTC / 0.0158 USD

Description **Bids** Feedback Refund Policy

### Product Description

These are great quality scans of documents.

You will receive:

5x UNITED KINGDOM - PASSPORT SCAN - ONLY \$3 EACH!! TEMPORARY PRICE / 90% + VALIDITY

Scans are delivered immediately after you click buy now (autoship)

----- READ THE BOTTOM TEXT BEFORE BUYING

These can be used for a variety of things, these are REAL victims, not fake Photoshopped scans. These are REAL people and their REAL documents. Most vendors on here sell fictitious/Photoshopped in but don't provide the opportunity's these can provide. You will effectively have a real persons identity

These are x5 scans so you will receive a download link for 5 scans, so 5 victims.

The price will go up shortly as we need to gain interest for this product.

Things you could possibly use these for:

- Set up PayPal/Banking accounts
- Pay day loans
- Buying Real estate
- Making deposit
- Fake Cheques
- Blackmail
- Fullz



## 750+ CS US FULLZ + DL SCAN (original) + CR + BG + docs

PA only in stock right now. Need more info? Check this out: <http://www.escrow.com/escrow/escrow/listing.php?id=215835> You will get SSN, DOB, Background report, Credit report, DL, Original Scan. Every fullz has Driver License HQ Scan. It's ORIGINAL scan! Every fullz has a lot of scans of medical docs. You can choose between less than 750 credit score and more than 750 credit score fullz. ...

Sold by **...** - 478 sold since Jun 29, 2016 **Vendor Level 6** **Trust Level 4**

|               | Features      | Origin country | Features  |
|---------------|---------------|----------------|-----------|
| Product class | Digital goods |                | Worldwide |
| Quantity left | Unlimited     | Ships to       | Worldwide |
| Ends in       | Never         | Payment        | Escrow    |

Credit Score < 750 - 1 days - USD +10.00 / item

Purchase price: USD 10.00

Qty: 1 **Buy Now** **Queue**

| Browse Categories  |       |
|--|-------|
| <input type="checkbox"/> Fraud                                   | 5517  |
| <input type="checkbox"/> Accounts & Bank Drops                   | 2687  |
| <input type="checkbox"/> CVV & Cards                             | 991   |
| <input type="checkbox"/> Dumps                                   | 242   |
| <input type="checkbox"/> Other                                   | 784   |
| <input checked="" type="checkbox"/> Personal Information & Scans | 613   |
| <input type="checkbox"/> Drugs & Chemicals                       | 11416 |
| <input type="checkbox"/> Guides & Tutorials                      | 2219  |
| <input type="checkbox"/> Counterfeit Items                       | 711   |
| <input type="checkbox"/> Digital Products                        | 1841  |
| <input type="checkbox"/> Jewels & Gold                           | 278   |
| <input type="checkbox"/> Weapons                                 | 284   |
| <input type="checkbox"/> Carded Items                            | 395   |
| <input type="checkbox"/> Services                                | 1296  |
| <input type="checkbox"/> Other Listings                          | 425   |
| <input type="checkbox"/> Software & Malware                      | 238   |
| <input type="checkbox"/> Security & Hosting                      | 104   |

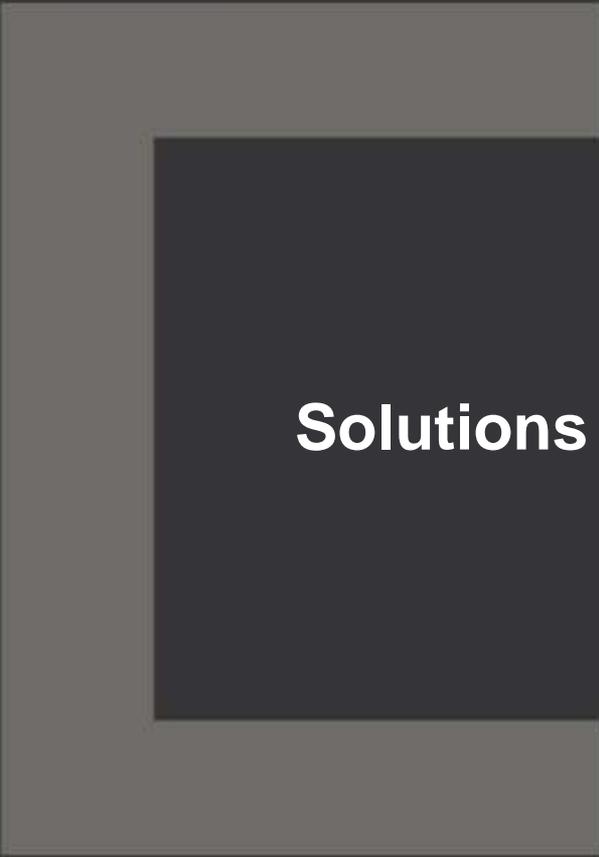
### Search Results [Save Search]

|  |  |                                       |
|--|--|---------------------------------------|
|  | <b>[PE 100%] + USA PROFILES SSN/DOB/DL/BANK + FREE COICVV+</b><br>Item # 2451 - Personal Information & Scans - wakawaka (1443) | Buy price<br>USD 1.50<br>(0.004 BTC)  |
|  | Views: 15400 / Bids: Fixed price<br>Quantity left: Unlimited (503 automatic items)   |                                       |
|  | <b>EVOscans custom made scan</b><br>Item # 1092 - Personal Information & Scans - Battalion (348)                               | Buy price<br>USD 34.23<br>(0.104 BTC) |
|  | Views: 6635 / Bids: Fixed price<br>Quantity left: 2  |                                       |
|  | <b>+USA CC WITH KNOWN BALANCES + - (\$50-\$40,000 \$)</b><br>Item # 6477 - Personal Information & Scans - SPARTANZ (663)       | Buy price<br>USD 0.00<br>(0.000 BTC)  |
|  | Views: 4858 / Bids: Fixed price<br>Quantity left: Unlimited  |                                       |
|  | <b>Personal Information +</b><br>Item # 241 - Personal Information & Scans - BookMistok (257)                                  | Buy price<br>USD 1.00<br>(0.004 BTC)  |
|  | Views: 4823 / Bids: Fixed price<br>Quantity left: Unlimited  |                                       |

## Les cyber-criminels ont compris...



- **L'intérêt financier de toutes nos données.**
  - Exemple : Les e-Mules, les « ransomwares », la re-vente...
- **La facilité d'influence, de corruption et d'intimidation de l'humain.**
  - Exemple : Ashley Madison et son black mailing. Et la nouvelle tendance : passe le « ransomware » à ton voisin...!
- **L'expansion de la sur-connectivité (et du bruit qui va avec).**
  - Exemple : La majorité (estimation à plus de 80%) des téléphones et tablettes Android sont très vulnérables sans une protection installée volontairement par l'utilisateur.



**Solutions ?**

# Les nouvelles dimensions à concevoir...



- Les assurances du « Digital Persona » contre la perte, le vol et l'usurpation d'informations et d'identités...
  - Exemples : on ne respecte pas les bonnes pratiques de navigation et de protection, la prime augmente...
- La régulation de protection des données doit reconnaître et prendre en charge la donnée personnelle corrélée capable d'identifier une personne. La donnée personnelle corrélée bien que créée par un acteur tiers doit appartenir ultimement à la personne qu'elle identifie.
  - Exemples : Le régulateur devrait légiférer en ce sens : aucun contrat ou texte d'accord d'utilisation ne devrait permettre de transgression de la loi.
- Le fichier du « Digital Persona » avec déclaration des données corrélées pour chaque individu. Les fournisseurs qui requièrent et corrélient trop d'informations personnelles et les individus qui en laissent trop aller.
  - Exemples : on vend / donne / publie ses informations à tout va, la prime d'assurance augmente...

## Les nouvelles solutions à considérer...



- Le blockchaining social : blockchain et réseaux sociaux
- L'ISP par chiffrement quantique : tiers de confiance de transfert de données
- Le ZKIP : l'exemple du sondage de cette présentation

# Bien comprendre les écosystèmes et leur chevauchement...



## Intégrer la cyber-crise aux processus organisationnels

- Mettre à jour les exercices de BIA
- Mettre à jour le plan de gestion de crise
- Mettre à jour le plan de BC / DR
- Mettre à jour le processus de gestion des incidents TI

## Choisir et disposer les bons acteurs autour de la table

## Simuler, simuler et simuler encore



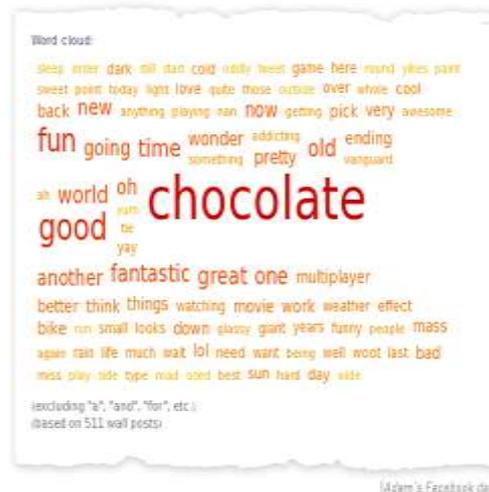
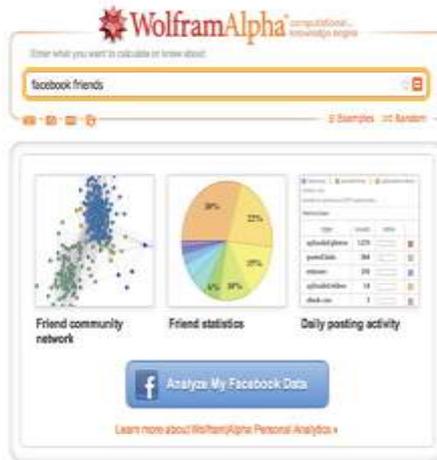


**Quelques outils à  
emporter...**

# Le test à faire...



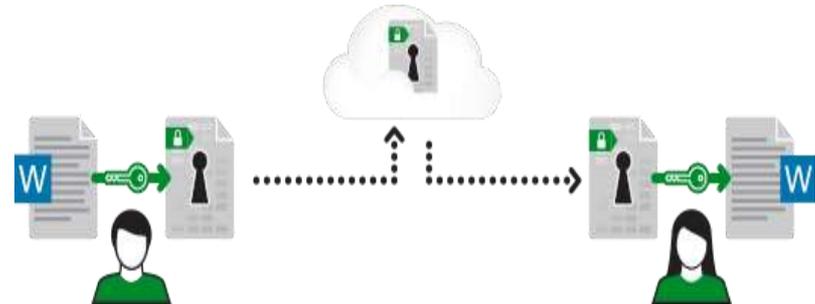
- À la base un projet de Stephen Wolfram de corrélation intelligente de données ouvertes par modèles d'indexation massive et « deep learning »...



# Chiffrer l'infonuagique...

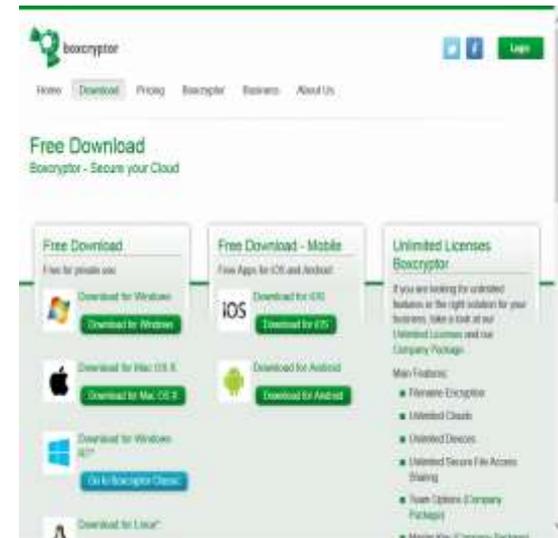


- BoxCryptor



*....ou totalement gratuite et opensource ?*

- VeraCrypt + Cloud (Google Drive, DropBox...etc.)
- 7zip + Cloud (Google Drive, DropBox...etc.)

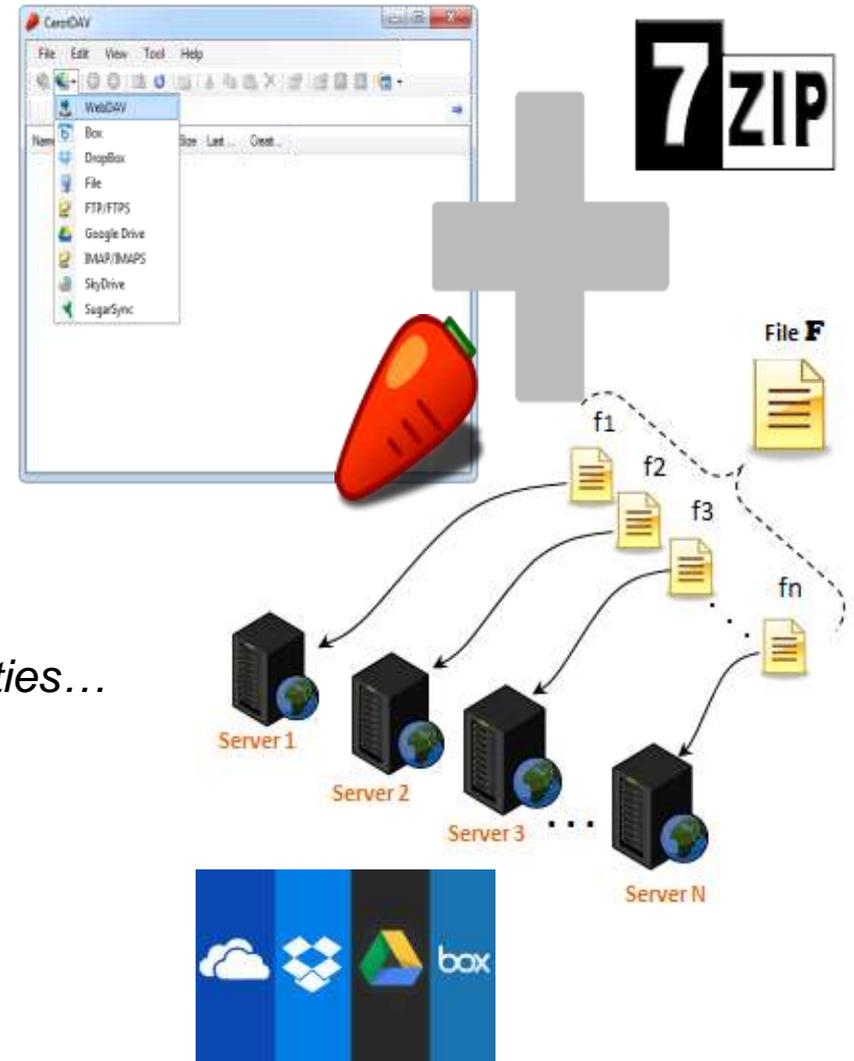


# Diviser pour mieux contrôler....



1. Diviser le fichier en plusieurs morceaux
2. Chiffrer chaque morceau
3. Envoyer chaque morceau chiffré sur un stockage différent

• *Note : l'étape 1 et 2 peuvent être interverties...*



# Vérifier sa “e-Réputation” ...



- <https://www.nothing-to-hide.fr/>
- « **51 %** des recruteurs scrutent désormais leurs profils via (les) réseaux sociaux », d'après Olivia de Faÿ, directrice du recrutement chez Mazars.

Nothing to Hide  
BY MAZARS

LANCEZ LE SCAN →

Découvrir Mazars

Êtes-vous certain de bien maîtriser votre e-réputation ?

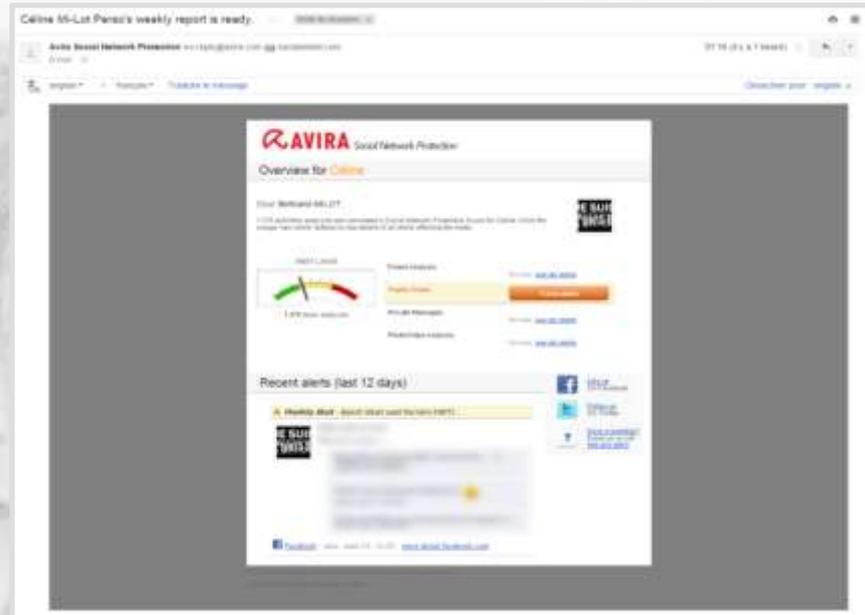
Lancez le scan pour voir ce que votre futur employeur peut découvrir sur vous !

LANCEZ LE SCAN →

Votre e-reputation en 3 étapes

Je l'ai testé pour vous...

- Laisseriez-vous votre enfant seul sur une place publique...



# Gardez vos données physiquement proches ! E

128 Gb = -50\$

USB Raptor <sup>Beta</sup>  
Lock and unlock your computer using USB flash drives as keys



EZ-TFA

SanDisk Ultra Fit 128GB USB 3.0 Flash Drive (SDCZ43-128G-GAM46) [Newest Version] by SanDisk

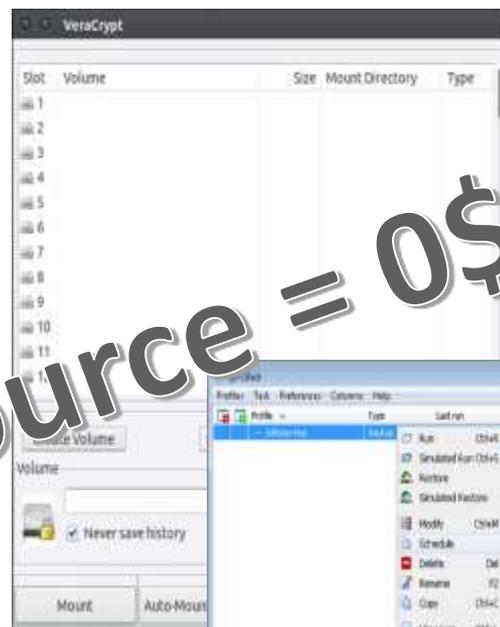
★★★★☆ 293 customer reviews | 3 answered questions

List Price: ~~CDN\$ 53.00~~  
Price: **CDN\$ 49.99** Prime  
You Save: **CDN\$ 3.01 (6%)**

**In Stock.**  
Want it Friday, June 27? Order it in the next **2 hours and 37 minutes** and choose **One-Day Shipping** at checkout. Ships from and sold by Amazon.ca. Gift-wrap available.



Opensource = 0\$



# MERCI

**Richter S.E.N.C.R.L.  
1981, McGill College  
Montréal QC H3A 0G6**

**181, Bay St., bureau 3320  
Bay Wellington Tower  
Toronto ON M5J 2T3**

**[www.richter.ca](http://www.richter.ca)**

**Visitez-nous sur :**

**Facebook  
LinkedIn  
Twitter**

**RICHTER**  
ÉVOLUTION PAR EXCELLENCE

