Les Enjeux de la Vie privée sur Internet

Professeur Esma Aïmeur

Université de Montréal
Département d'informatique et de recherche opérationnelle
Montréal, Canada

Email : aimeur@iro.umontreal.ca
http://www.iro.umontreal.ca/~aimeur

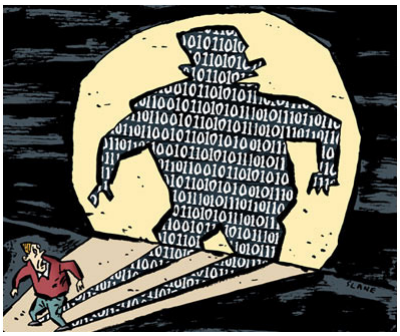
1

PLAN

- Introduction vie privée
- Domaines de collecte des données
- Techniques de collectes de données
  - Réseaux sociaux
  - Courtiers de données
  - Moteurs de recherche de personnes
  - Geolocalisation
  - Biométrie
- Vol identité et Reconstitution de profils
- Recommandations

2

Sur Internet, chaque personne laisse des traces numériques reliées à son identité.



3

Scandale PRISM: comment les Etats-Unis espionnent le web

L'Expansion.com avec AFP - publié le 07/06/2013 à 16:53

L'administration Obama a confirmé l'existence d'un programme permettant à la NSA d'accéder aux données issues de Google, Microsoft, Facebook à des fins de renseignement extérieur.

L'Agence nationale de sécurité américaine (NSA) et le FBI ont accès aux serveurs de neuf géants américains de l'internet, dont Microsoft, Yahoo, Google et Facebook, pour y surveiller les activités d'étrangers (mails, vidéos, audio...).

Skype, AOL, YouTube, Apple et PalTalk participeraient également au système

4

Définition vie privée

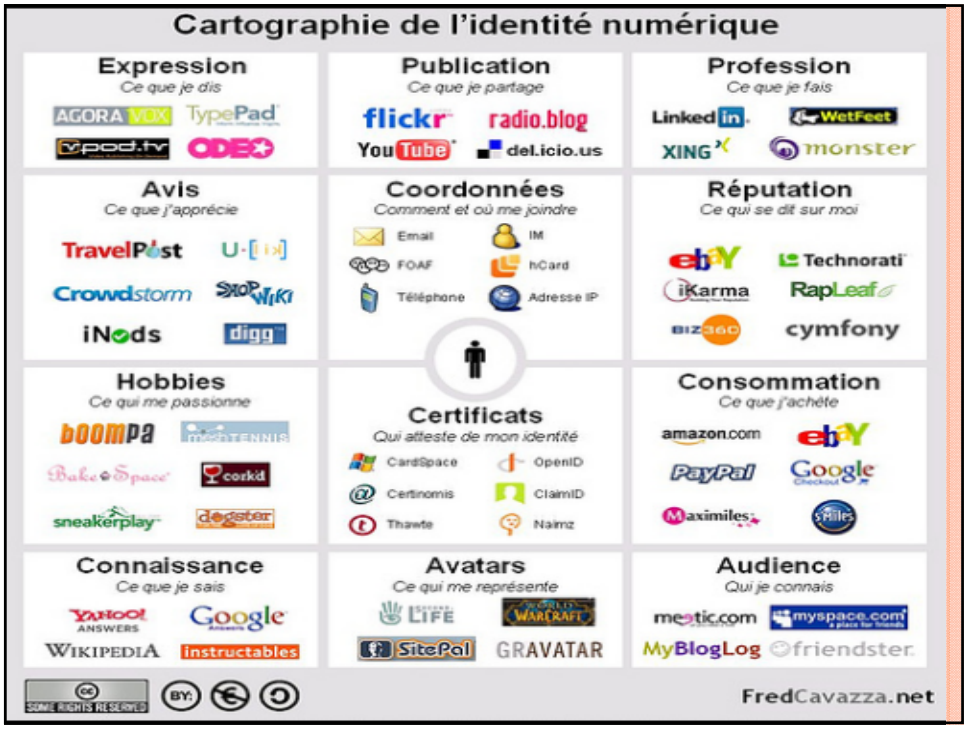
« Le droit d'une personne de contrôler l'accès à sa personne et aux renseignement qui la concerne. Le droit à la vie privée signifie que la personne décide des renseignements qui sont divulgués, à qui et à quelles fins. »

5

Atteinte à la vie privée

« Une atteinte à la vie privée suppose l'accès non autorisé à des renseignements personnels ou la collecte, l'utilisation ou la communication non autorisée de tels renseignements. Certains des cas d'atteinte à la vie privée surviennent lorsque des renseignements personnels sont volés, perdus ou communiqués par erreur (p. ex. transmis par courriel aux mauvaises personnes). Une atteinte à la vie privée peut également découler d'une erreur de procédure ou d'une défaillance opérationnelle.. »

6



« RIEN NE S'EFFACE SUR INTERNET»

8

Deux principes fondamentaux de protection de la vie privée

Minimisation des données:

- Seule l'information nécessaire pour compléter une application particulière devrait être collectée/utilisée (et pas plus).
- Application directe du critère de légitimité défini par la directive européenne sur la protection des données personnelles (*Directive 95/46/EC*).

Souveraineté des données:

- Les données liées à un individu lui appartiennent, il devrait pouvoir contrôler comment elles sont disséminées.

9

Autres principes fondamentaux

- Consentement explicite : avant de collecter les données personnelles d'un individu, il faut lui demander son autorisation et lui expliquer quelle utilisation sera faite de ses données.
- Transparence : le système ne doit pas être considéré comme une boîte noire dans laquelle l'individu doit avoir une confiance aveugle.
- Imputabilité : l'entité qui héberge les données personnelles doit les sécuriser au meilleur de ses moyens, et le cas échéant peut être tenue responsable (par exemple devant un juge) d'un bris de vie privée.
- Droit à l'oubli : sur demande de l'individu, ses traces doivent être effacées.

10

Les conditions de base de protection de la vie privée sur Internet

Anonymat : impossibilité pour d'autres utilisateurs de déterminer le véritable nom de l'utilisateur associé à un sujet.

Non-chaînabilité : impossibilité pour d'autres utilisateurs d'établir un lien entre différentes opérations faites par un même utilisateur.

Non-observabilité : impossibilité pour d'autres utilisateurs de déterminer si une opération est en cours.

11

http://www.ossir.org/resist/supports/cr/20070626/Deswarte-ProtectionViePrivee.pdf

11

Violation vie privée : Informations Recherchées

12

Informations d'identification (nom, prénom, âge, sexe, adresse, numéro de téléphone, ***nom de jeune fille de la mère***, numéro d'assurance sociale, numéro d'identification personnel, revenu, emploi, situation familiale, lieux de résidence, code utilisateur, pseudonyme)

Habitudes de consommation (magasins fréquentés, relevés de compte, actifs, obligations, etc.)

Habitudes de navigation (sites web visités, fréquences des visites, nom des forums, amis sur le net, etc.)

Habitudes de vie (loisirs, relations, moyens de déplacement, ***périodes de congés,*** etc.)

Données sensibles (carrière, employeur, dossier médical, casier judiciaire)

Données biologiques (groupe sanguin, code génétique, empreintes)

13

Sources d'information

Gouvernement : casier judiciaire, antécédents médicaux

Compagnies dont vous êtes clients : téléphone, Amazon

Compagnies dont vous n'êtes pas clients : sociétés mères, entreprises filiales

Entreprises en faillite

14

Services en Ligne

Search engines:
Bing, Google, Yahoo!, etc.

Personal data aggregators:
123people.com, Whozat.com, Pipl.com, Peekyou.com, PeopleSearch.net, etc.

Social network aggregator web sites:
Lifehacker.com, Spokeo.com, Spoke.com, etc.

15

PLAN

- Introduction vie privée
- **Domaines de collecte des données**
- Techniques de collectes de données
  - Réseaux sociaux
  - Courtiers de données
  - Moteurs de recherche de personnes
  - Geolocalisation
  - Biométrie
- Vol identité et Reconstitution de profils
- Recommandations

16

www.radio-canada.ca/regions/colombie-britannique/2013/02/09/002-nouvelle-carte-assurance-maladie-vie-privee-inquietudes.shtml

Vie privée : la nouvelle carte d'assurance maladie soulève des inquiétudes

Mise à jour le samedi 9 février 2013 à 20 h 56 HNE

La nouvelle carte du nom de BC Services Card sera bientôt distribuée à ceux qui renouvelleront leur permis de conduire. *Photo : Gouvernement de la C.-B.*

La commissaire à l'accès à l'information et à la vie privée de la Colombie-Britannique et des groupes de pression s'inquiètent de la sécurité de la nouvelle carte d'assurance-maladie.

COLOMBIE-BRITANNIQUE EN DIRECT

Art Phillips, maire Vancouver 1972-1976 mort hier, a développé les espaces verts et s'est opposé au projet d'autoroute en ville. #rccb

L'ancien maire de Vancouver Art Phillips est décédé vendredi des suites d'une infection. Il avait 82 ans. #rccb

Afficher le fil complet

Five nurses fired for Facebook postings

BY JENNIFER FINK, RN, BSN • JUNE 14, 2010

CAREER, CONTROVERSY, FACEBOOK, LIFE SOLUTIONS, NEWS AND OPINION, PATIENT CARE, TECHNOLOGY

Tweet 10 Like 958 Email +1 1

Image: JupiterImages | Getty Images + Scrubs Mag

Five California nurses were recently fired after allegedly discussing patients on Facebook.

The nurses, who worked at Tri-City Medical Center in Oceanside, lost their jobs after an internal investigation and three weeks of administrative leave. While no details of the incident have been revealed, Larry Anderson, CEO of Tri-City Medical Center, has said that no patient names, photos or identifying information were included in the posts.

This isn't the first time nurses have gotten into trouble for Facebook postings. In 2008, a photo of a topless British nurse — with patients in the background — appeared online, causing the hospital, Northampton General Hospital, to block acess to all social networking sites from work computers. In 2009, Wisconsin nurses were fired after two nurses took photos of a patient's X-ray and allegedly posted it to Facebook. While the Facebook page was quickly removed, one of the nurses in question admitted to discussing the incident on her Facebook page. Photos of nurses having a food fight at Stafford Hospital in the UK also surfaced in 2009, quickly creating an uproar because the incident took place after a heavily publicized report that linked patient deaths to staff shortages and poor nursing care.

While a number of hospitals have social media policies in place — and HIPAA strictly enforces patient privacy and confidentiality — incidents continue to occur. How do you think hospitals should handle questionable social media postings? Is it ever appropriate to upload work pictures or to


DATALOSS db
open security foundation
login | signup
sponsored by CREDANT
We Protect What Matters
About | Search | Submit New | Primary Sources | Laws | Reports | Stats | Analysis | Mail Lists | The Blotter | Fringe | Supporters
2010
2011
2012
Support DataLossDB
OSF needs your support! You can support OSF's DataLossDB in several ways, such as contributing news articles about data loss incidents or by updating older incidents as new information becomes available. Financial donations, which will support hosting, hardware upgrades, and advertising are also appreciated.
Sony had HOW many breaches?
2011-06-05 by Dissent
We thought keeping track of entities involved in the Epsilon breach was tough, but the recent spate of attacks on Sony networks has us working overtime trying to update the database. Thankfully, Jericho provided yeoman service and compiled a hyperlinked chronology of recent developments.
The Sony breaches have generated a lot of discussion. Some of it has centered on Sony's shocking failure to encrypt passwords and it being all-too-vulnerable to SQLi compromises (if those posting the data publicly are accurate as to how they compromised certain databases). Sony undoubtedly has a lot of explaining to do if it hopes to have future assertions of industry-standard security taken seriously.
To date, the two largest incidents affected over 100 million records. But were the PSN and Sony Online Entertainment (SOE) attacks two separate incidents or were they really one breach? Should DataLossDB.org have recorded one breach with over 100 million affected, or two incidents involving 77 million and 24.6 million, respectively? Or should we just treat the last 45 days' incidents as one #EPIC #FAIL and one big incident? In light of our mission to track unique breaches, the question is not trivial.
When news of the second incident broke, the first thought was to update the PSN entry and add another 24.6 million to that counter. But as more details emerged, it seemed clear that we should treat it as a separate incident. The attack had occurred on different days than the PSN attack, the data compromised were on different networks, it seems quite likely the different networks had different security measures involved (Sony later testified that databases with credit card data were treated with higher security), we did not know if the same individuals were involved in both attacks, and the company itself was reporting it as a second incident previously unknown to them and not as an update to the other breach. Our impression that
About OSF Data Loss
DataLossDB is a research project aimed at documenting known and reported data loss incidents world-wide. The effort is now a community one, and with the move to Open Security Foundation's DataLossDB.org, asks for contributions of new incidents and new data for existing incidents. For any questions about this site or the data contained within the site, please contact curators@datalossdb.org.
opensecurityfoundation events calendar
Latest Incidents
twitter / DataLossDB
RECORDS | DATE | ORGANIZATIONS
719 | 2012-02-22 | University of Florida
0 | 2012-02-20 | Mo Money Taxes
1,400,000 | 2012-02-20 | YouPorn
0 | 2012-02-18 | Go4Less
0 | 2012-02-16 | D.R. Horton Inc.
18,275 | 2012-02-16 | Central Connecticut State University
0 | 2012-02-15 | University of North Carolina at Charlotte
0 | 2012-02-14 | Solitude Mountain Resort
120 | 2012-02-14 | Capital Health, Hants Community Hospital
0 | 2012-02-13 | Microsoft Store India, Quasar Media
Search
Search
Largest Incidents
RECORDS | DATE | ORGANIZATIONS
130,000,000 | 2009-01-20 | Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
94,000,000 | 2007-01-17 | TJX Companies Inc.
90,000,000 | 1984-06-01 | TRW, Sears Roebuck
77,000,000 | 2011-04-26 | Sony Corporation


Transaction profile
Purchase history
Preference profile
Behavioral profile
20

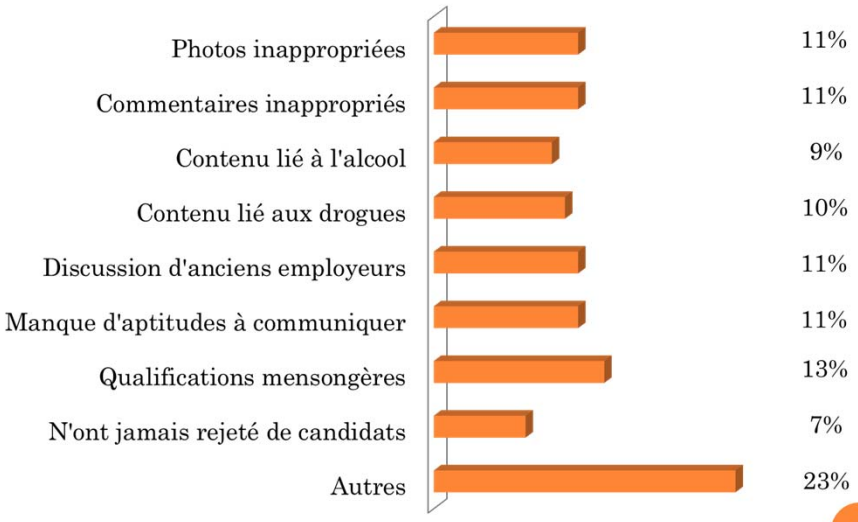
Negligeance des internautes

Pire ennemi: soi-même

- En divulguant trop d'informations sur soi (photos, histoire de notre vie, etc.).
- En faisant confiance facilement aux autres.
- En affichant des informations sensibles : la date de naissance, le numéro de téléphone, le lieu de travail, l'emplacement géographique, etc.
- En se comportant d'une façon émotionnelle:
  - La curiosité nous incite parfois à cliquer sur des liens malveillants.
  - La compassion peut nous pousser à envoyer de l'argent à un ami présumé qui prétend être victime de vol.
  - Etc.

22

RAISONS DE REJET DE CANDIDATS



Selon une étude par Reppler, plus de 300 employeurs interviewés

http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/

23

PLAN

- Introduction vie privée
- Domaines de collecte des données
- **Techniques de collectes de données**
  - Réseaux sociaux
  - Courtiers de données
  - Moteurs de recherche de personnes
  - Geolocalisation
  - Biométrie
- Vol identité et Reconstitution de profils
- Recommandations

24

Réseaux sociaux

25

Young people do not care

Filmed before being born, under constant surveillance by those who love them or are responsible for educating them, **they have already accepted the idea that privacy is an illusion.** They archive their own youth, as they see themselves as having an audience. **Wikipedia is their library and Skype is their phone.** As a result, **they endanger those around them and sometimes undermine their own future!**

26

Social media

- Misleading concept of community

  If users do not know how their profile data is shared protect it, this notion of a virtual "community" may lead share personal information they would have otherwise kept private.

- Secondary data collection by service suppliers

  their services, In order to personalize they gather a great deal of secondary information about their users (geographic location, habits, tastes or preferences, etc.)

- Registration Process

  SNS do not check the identity of the users and anyone can assume any name without control

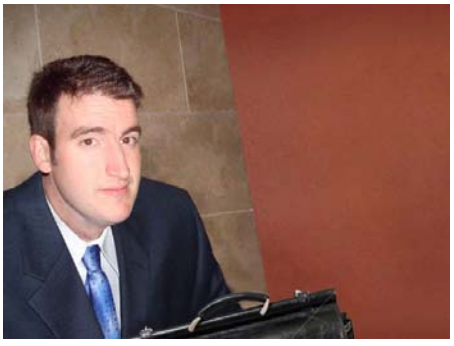
- Facial recognition

  Once a face is tagged in a picture, it becomes relatively straightforward to retrieve the name from other pictures

27

Une expérimentation de recrutement via les reseaux sociaux

(Alessandro Acquisti, 2014)



Social networking site

Types of Personal Information Posted on Facebook vs. All Social Networking Sites According to US Internet Users, January 2010 (% of respondents)

	Facebook	All so netw
First and last name	84%	80
Photos of myself	63%	57
E-mail address	51%	49
Birth date with year	42%	38
Birth date without year	30%	26
Photos of children	24%	21
Names of family, friends or associates	19%	16
Employer	17%	16
Children's names	16%	13
Home street address	7%	8%
Mobile phone number	7%	6%
Home phone number	4%	4%
Information indicating when home or away	3%	3%

Source: Consumer Reports National Research Center, "State of the Net 2010," May 4, 2010

115178 www.eMarkete

From Times Online

July 5, 2009

Wife blows MI6 chief's cover on Facebook

Nadia Gilani

The wife of the new head of MI6 has caused a major security breach and left his family exposed after publishing photographs and personal details on Facebook.

Sir John Sawers is due to take over as chief of the Secret Intelligence Service in November, putting him in charge of all of Britain's spying operations abroad.

But entries by his wife Shelley on the social networking site have exposed potentially compromising details about where they live and work, their friends' identities and where they spend their holidays. On the day her husband was appointed she congratulated him on the site using his codename "C".

Lady Sawers had put virtually no privacy protection on her account, making it visible to any of the site's 200m users around the world who choose to be in the open-access London social network on Facebook.

EXPLORE UK NEWS
- CRIME NEWS
- EDUCATION NEWS
- HEALTH NEWS
- SCOTLAND NEWS

TIMES RECOMMENDS
- Readers' land army plants a forest
- UK plans first nuclear fusion power plant
- MI5 may face new torture inquiry

BAFTAS 2010

And the award for Best Dressed goes to...

MY PROFILE | SHOP | JOBS | PROPERTY | CLASSIFIEDS

MOST READ | MOST COMMENTED | MOST CURIOUS

TODAY
- Robots and bees to beat the Taliban
- Obama's 'Chicago mafia'...
- Ashley Cole could be hit with fine of...
- Two more Britons caught up in Dubai Hamas hit

TODAY

TODAY
- Curiouser and Curiouser
- Has the political poster virtually had its...
- Sarkozy's depiction of pregnant,...
- Crisis? Blame the baby-boomers, not the...

FOCUS ZONE

Need to Know:
Industry sectors news at a glance. Interactive heatmap, video and podcast

- Need to Know
- Winter Sports
- Mapping Business
- Visit Las Vegas
- More reports

Business city guides
Overseas contacts and local business information

30

Surveillance sur Twitter

"Before I left to go on vacation, my boss asked that I keep my phone on me because he was working on a project and might need to ask me something. I said I'd be available but knew there was no way I'd answer. He called at least 10 times, and I never picked up.

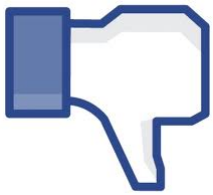
When I got back, he asked me why I hadn't answered, so I lied and said my phone had been stolen. He looked at me for a long time and then said, 'That's funny, because according to your Twitter account, you've been updating all week via your mobile device."

32

Cosmolitan 130, 2012

Surveillance sur Facebook

- *Social networks*
  - *"I'm a waitress. […] A few pals came in a month ago, and I gave them fries and didn't charge them.* ***One of them later posted on my wall that the 'free fries were banging'. I didn't even think about it, but my manager saw it and flipped****. I was let go immediately. Now I block everyone from seeing my profile unless they are a very close friend."*



33

Cosmolitan 130, 2012

De la difficulté à porter plainte dans le cyber

Jerome Saiz le 22 mars 2013 - 04:46, dans la rubrique Cyber Pouvoirs

4 commentaires, rejoignez la discussion ! et 33 mentions sur Twitter, merci à tous !

gendarmerie - juridique - lois - ntech - OCLCTIC - usurpation

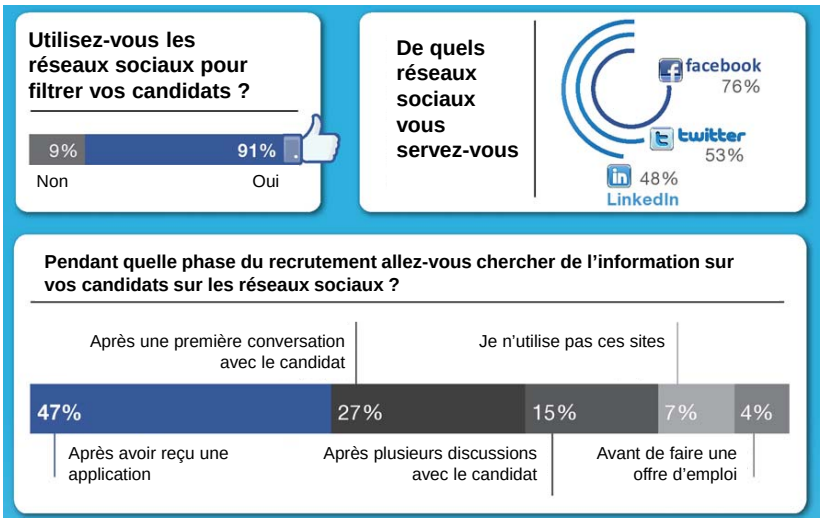
La mésaventure vécue le mois dernier par un adolescent de la région parisienne vient rappeler que malgré toute la bonne volonté du législateur en matière de répression dans le cyber, sur le terrain déposer plainte peut encore relever du parcours du combattant.

Le 27 février au soir, Théo apprend par des amis de classe qu'un faux profil Facebook à son nom vient d'être créé et que de nombreux camarades bernés sont désormais amis avec l'inconnu. Sur le profil, tout est exact : son nom, sa date de naissance, son groupe de musique préféré…

A un détail près : son homosexualité.

L'auteur du profil publie rapidement des images à caractère pornographique censées révéler la prétendue attirance de Théo pour les hommes, dans le but de nuire à sa réputation.

Sur le papier, il s'agit clairement d'une infraction pénale. La loi LOPPSI du 14 mars 2011



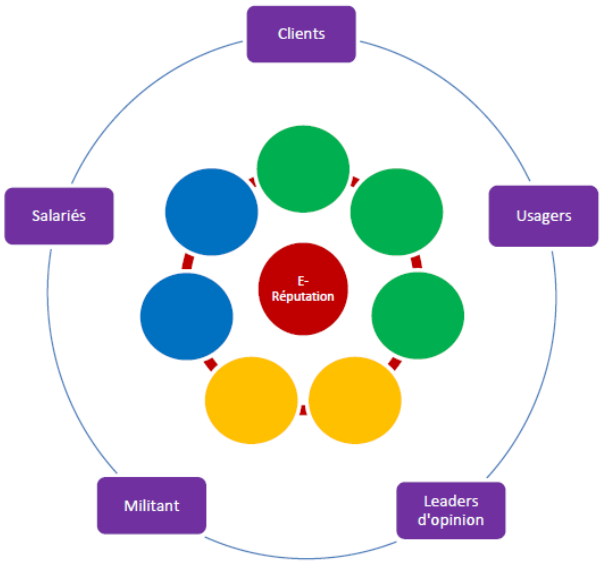
35

Selon une étude par Reppler, plus de 300 employeurs interviewés

http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/

CIGREF 2012

Les parties prenantes à la construction de l'e-réputation



36

Réputation d'une entreprise

Les atteintes informationnelles, comme la diffusion d'avis négatifs de consommateurs, le dénigrement, la rumeur et la diffusion de fausses informations

Les atteintes touchant à l'identité, comme le détournement de logo, l'usurpation ou le détournement de marques ou de produits

Etude sur les risques et opportunités liés à l'e réputation des entreprises
Les atteintes d'ordre technique, comme le phishing le piratage de site, le flog, splog, cybergriping ou bien cybersquatting

37

De nouveaux risques pour les entreprises

Des internautes mécontents, des concurrents malveillants, des collaborateurs manquant de discernement peuvent nuire à l'image d'une société.

Un acte isolé de salariés peut avoir de lourdes conséquences sur la réputation d'une entreprise.

Variation des ventes, rupture de contrats avec des partenaires, perte de la maîtrise de son image, augmentation des investissements en communication, détournement de l'image de marque, problème de recrutement, sont autant de conséquences que peut subir une entreprise dans la tourmente du net.

38

bigbrowser.blog.lemonde.fr/2013/01/03/sur-le-gril-quick-poursuit-en-justice-un-salarie-decrivant-son-travail-sur-tw

ost Visited Getting Started Authentification Galerie de composants ... Sites suggérés

3 janvier 2013

SUR LE GRIL – Quick poursuit en justice un salarié décrivant son travail sur Twitter

© AFP

Début novembre, un inconnu se présentant comme un salarié embauché en CDI dans un restaurant français de la chaîne de fast-food entreprenait de chroniquer ses journées de travail sur le compte Twitter @EquipierQuick. Les tweets alternaient détails anodins et critiques plus poussées.

Un technicien est gagné par le sommeil chez le client

- A telecom company's customer service reputation was tarnished by a *viral video* of a service technician caught sleeping in a customer's home.
- A word-of-mouth monitoring company identified the video and alerted key managers within moments of its posting.
- The company was able to instantly mobilize its crisis-response efforts and implement strategies for its corporate department, Web content managers, and marketing and operations teams.
- The damage would have been significantly worse had the company not used a reputation monitoring service

40

techno.lapresse.ca/nouvelles/internet/201101/08/01-4358240-les-fantomes-de-facebook.php

Visited Getting Started Authentification Galerie de composants ... Sites suggérés

maPRESSE DÉCOUVREZ MA PRESSE

ACTUALITÉS INTERNATIONAL AFFAIRES SPORTS AUTO ARTS CINÉM

Nouvelles Jeux vidéo

Applications Internet Mobilité Matériel informatique Logiciels Produits électroniques

Accueil > Techno > Nouvelles > Internet > Les fantômes de Facebook

Les fantômes de Facebook

Isabelle Hachey, La Presse
08 janvier 2011 | 07 h 56

Chaque jour, Facebook encourage ses utilisateurs à reprendre contact avec des amis qui ont passé l'arme à gauche. Déstabilisant, mais inévitable: une armée de fantômes hantent les réseaux sociaux. Et ses rangs ne peuvent que continuer à grossir. Des millions de gens mènent leur vie sur la Toile. Pourtant, rares sont ceux qui se sont demandé ce qu'il adviendra de leur identité virtuelle - et de leur patrimoine numérique - après l'ultime déconnexion.

Agrandir

Illustration: Philippe Tardif, La Presse

Pour en savoir plus
Facebook | Virginia Tech | Jean Charest | Pierre Côté | Internet | Réseautage social

AJOUTER À MA PRESSE

Taille du texte

Imprimer

Sébastien avait 234 amis Facebook. Comme des millions d'utilisateurs de ce populaire réseau social, il

Depressed woman loses benefits over Facebook photos

Last Updated: Saturday, November 21, 2009 | 12:11 AM ET CBC News

Facebook 71
Twitter 10
+1 3
Share 81
Email

A Quebec woman on long-term sick leave is fighting to have her benefits reinstated after her employer's insurance company cut them, she says, because of photos posted on Facebook.

Nathalie Blanchard, 29, has been on leave from her job at IBM in Bromont, Que., for the last year and a half after she was diagnosed with major depression.

Internal Links

- P.O.V.: Have you ever regretted posting something on a social networking website?

The Eastern Townships woman was receiving monthly sick-leave benefits from Manulife, her insurance company, but the payments dried up this fall.

When Blanchard called Manulife, the company said that "I'm available to work, because of Facebook," she told CBC News this week.

Nathalie Blanchard, shown here on a beach holiday during her sick leave. (Facebook)

She said her insurance agent described several pictures Blanchard posted on the popular social networking site, including ones showing her having a good time at a Chippendales bar show, at her birthday party and on a sun holiday — evidence that she is no longer depressed, Manulife said.

Blanchard said she notified Manulife that she was taking a trip, and she's shocked the company would investigate her in such a manner and interpret her photos that way.

Stay Connected with CBC News

Mobile Facebook Podcasts Twitter Alerts Newsl

Getting Started | Authentification | Galerie de composants ... | Sites suggérés

KrebsonSecurity
In-depth security news and investigation

21 Privacy 101: Skype Leaks Your Location

MAR 13

The events of the past week reminded me of a privacy topic I've been meaning to revisit: That voice-over-IP telephony service **Skype** constantly exposes your Internet address to the entire world, and that there are now numerous free and commercial tools that can be used to link Skype user account names to numeric Internet addresses.

The fact that Skype betrays its users' online location information is hardly news. For example, *The Wall Street Journal* and other news outlets warned last year about research showing that it was possible to coax Skype into revealing the IP addresses of individual Skype users. But I believe most Skype users still have no clue about this basic privacy weakness.

A Skype resolver service in action.

What's changed is that over the past year, a number of services have emerged to help snoops

www.skype.com/en/legal/privacy/?intsrc=client-_-windows-_-6.3-_-go-privacy#collectedInformation

1. WHAT INFORMATION DOES SKYPE COLLECT AND USE?

Skype may gather and use information about you, including (but not limited to) information in the following categories:

(a) Identification data (e.g. name, username, address, telephone number, mobile number, email address);

(b) Profile information (e.g. age, gender, country of residence, language preference and any information that you choose to make available to others as part of your Skype user profile as further described in Section 6);

(c) Electronic identification data (e.g. IP addresses, cookies);

(d) Banking and payment information (e.g. credit card information, account number);

(e) Call quality and survey results;

(f) Information about your usage of and interaction with Skype software, products, and websites (including computer, platform, device and connection information, client performance information, error reports, device capability, bandwidth, statistics on page views, and traffic to and from our websites, browser type and Skype WiFi enabled hotspot detection and usage statistics;

(g) Products or services ordered and delivered;

(h) The URL of videos that you have selected to appear in your mood message;

(i) Skype test calls made to ECHO123 (which are recorded and played back to the user and deleted thereafter);

(j) List of your contacts and related data (we will give you a choice as to whether you want Skype to use contact lists from other services to populate your Skype contacts);

(k) Your username and password for other email accounts where you have provided this to us and requested us to search for your friends on Skype (please note that Skype does not retain this information after completing the search or use it for any other purpose);

(m) Traffic data (data processed for the purpose of the conveyance of communications or the billing thereof, including, but not limited to, the duration of the call, the number calling and the number called); and

(n) Content of instant messaging communications, voicemails, and video messages (please see section 12);

(o) Location information, derived from your mobile carrier or from the mobile device that you use. In connection with the Qik products, you control when your location is shared with others. Your location is displayed and shared with other Qik users only in accordance with your privacy settings. You also may create location information by "geo-tagging" your submitted content with location information. Please manage your privacy settings for location information carefully;

(p) Mobile device information, such as manufacturer's name, device model number, operating system, carrier network;

(q) Location information and device identifiers, derived from your device, when you search for or connect to a Skype WiFi compatible hotspot. This information may be used to improve detection of eligibility to connect using Skype WiFi and for the purposes of offering, providing and marketing Skype WiFi to you;

(r) Access tokens for other accounts you associate with your Skype account (such as Microsoft account or Facebook), which are like an electronic key provided by the service that acts in place of a password for authentication.

JEREMY TOEMAN

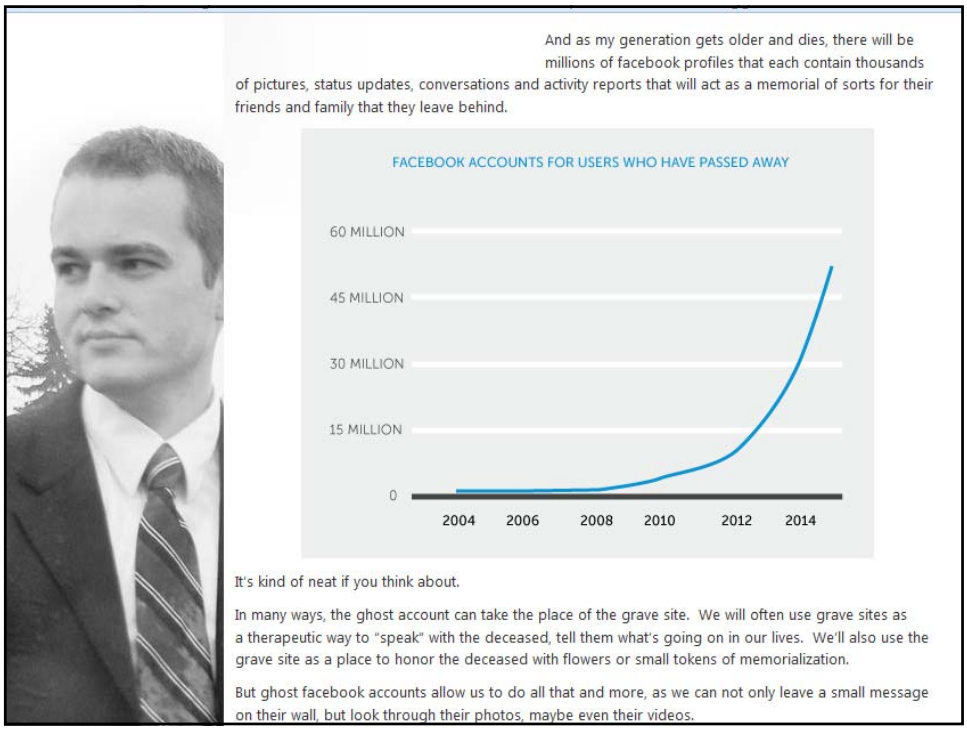
PRESIDENT OF DIJIT

- Legacy Locker (acquired by PasswordBox), safe, secure repository for your vital digital property that lets you grant access to online assets for friends and loved ones in the event of loss, death, or disability.

Un coffre-fort en ligne

Jeremy Toeman était à bord d'un avion secoué par les turbulences quand il a eu une révélation. « Je me suis demandé ce qui arriverait si je mourais. J'ai réalisé que personne n'avait accès à mes mots de passe. Tous mes avoirs numériques seraient bloqués à jamais dans le cyberespace », explique l'entrepreneur californien d'origine montréalaise. C'est ainsi qu'est né Legacy Locker, une sorte de coffre-fort virtuel qui entrepose les données confidentielles en ligne. Le jour venu, elles sont transmises par courriel aux légataires désignés. Des milliers de clients ont payé 300$ pour ce service. Sans être pressés d'être satisfaits...


www.calebwilde.com/2011/09/virtual-tombs-the-ghosts-of-facebook/
Most Visited Getting Started Authentification Galerie de composants ... Sites suggérés
CONFESSIONS OF A FUNERAL DIRECTOR
Working at the Crossroads of this World and the Next
Home
About
Good God Talk
Guest Posts / Advertising
Missional Living
The Book
Adoption
« Blurring the Lines Between Suicide and Murder: Thoughts on the death of Jamey Rodemeyer, Lady Gaga and Gay Bullying
Mourning and Social Media »
Virtual Tombs: The Ghosts of Facebook
Like 5 Tweet 5 +1 0 Share 8
I'm friends with about five dead people on facebook.
It's kinda odd, especially around their birthday when, inevitably, a couple people wish them "happy birthday" and you wonder, "Do ... they ... know why he/she isn't responding with a "thanks"?"
Most of my ghost friends died suddenly, leaving their password eternally forgotten and their facebook status in limbo.
ON FACEBOOK
Find us on Facebook
Confessions of a Funeral Director
Like
Confessions of a Funeral Director
Good Friday death reflections: Did Jesus die of a broken heart?
CONFESSIONS OF A FUNERAL DIRECTOR » Did Jesus Die of a Broken Heart?
www.calebwilde.com


And as my generation gets older and dies, there will be millions of facebook profiles that each contain thousands of pictures, status updates, conversations and activity reports that will act as a memorial of sorts for their friends and family that they leave behind.
FACEBOOK ACCOUNTS FOR USERS WHO HAVE PASSED AWAY
60 MILLION
45 MILLION
30 MILLION
15 MILLION
0
2004
2006
2008
2010
2012
2014
It's kind of neat if you think about.
In many ways, the ghost account can take the place of the grave site. We will often use grave sites as a therapeutic way to "speak" with the deceased, tell them what's going on in our lives. We'll also use the grave site as a place to honor the deceased with flowers or small tokens of memorialization.
But ghost facebook accounts allow us to do all that and more, as we can not only leave a small message on their wall, but look through their photos, maybe even their videos.

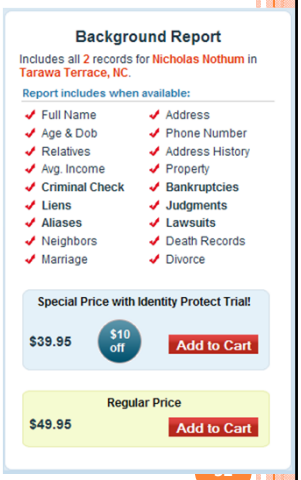
Courtiers de données

51

Courtiers de données (Data Broker)

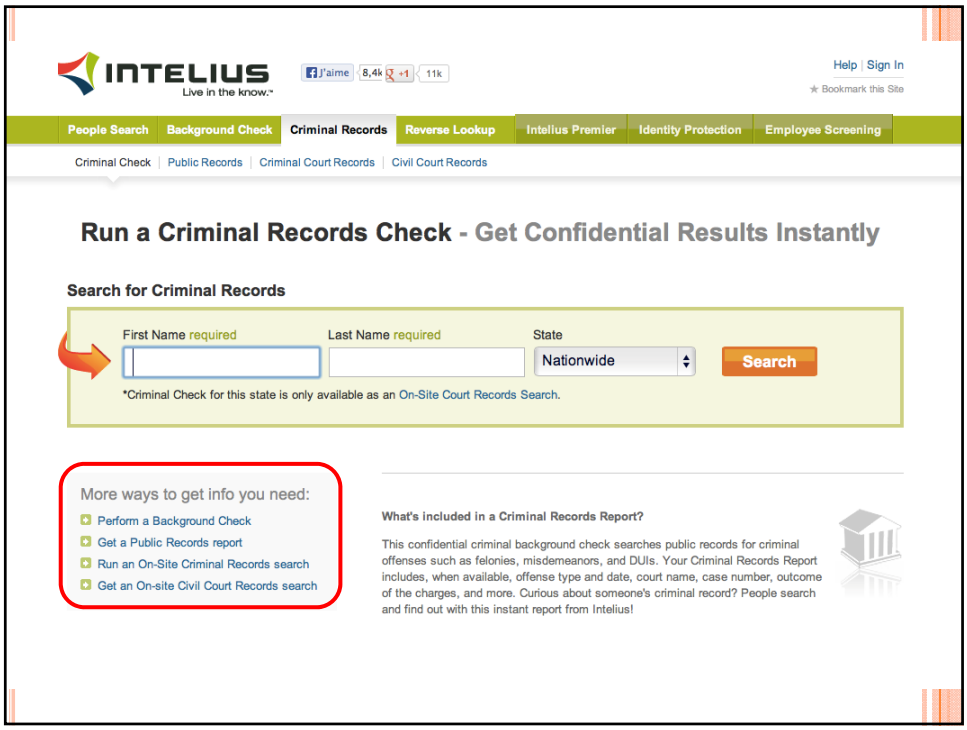
- Informations vendues sont non nominatives
  - permet de préserver la vie privée des internautes
- En cas de résiliation
  - informations supprimées de la base de données
- Exemple litigieux:
  - Intelius.com
  - Fondé en 2006
  - Slogan:

« se renseigner sur son entourage afin de savoir qui s'occupe de nos enfants »



INTELIUS
Live in the know.™


INTELIUS
Live in the know.
Help | Sign In
Bookmark this Site
People Search
Background Check
Criminal Records
Reverse Lookup
Intelius Premier
Identity Protection
Employee Screening
Criminal Check | Public Records | Criminal Court Records | Civil Court Records
Run a Criminal Records Check - Get Confidential Results Instantly
Search for Criminal Records
First Name required
Last Name required
State
Nationwide
Search
*Criminal Check for this state is only available as an On-Site Court Records Search.
More ways to get info you need:
Perform a Background Check
Get a Public Records report
Run an On-Site Criminal Records search
Get an On-site Civil Court Records search
What's included in a Criminal Records Report?
This confidential criminal background check searches public records for criminal offenses such as felonies, misdemeanors, and DUIs. Your Criminal Records Report includes, when available, offense type and date, court name, case number, outcome of the charges, and more. Curious about someone's criminal record? People search and find out with this instant report from Intelius!


INTELIUS
Live in the know.
Help | Sign In
Bookmark this Site
People Search
Background Check
Criminal Records
Reverse Lookup
Intelius Premier
Identity Protection
Employee Screening
Criminal Check | Public Records | Criminal Court Records | Civil Court Records
Run a Criminal Records Check - Get Confidential Results Instantly
Search for Criminal Records
First Name required
Last Name required
State
Nationwide
Search
*Criminal Check for this state is only available as an On-Site Court Records Search.
More ways to get info you need:
Perform a Background Check
Get a Public Records report
Run an On-Site Criminal Records search
Get an On-site Civil Court Records search
What's included in a Criminal Records Report?
This confidential criminal background check searches public records for criminal offenses such as felonies, misdemeanors, and DUIs. Your Criminal Records Report includes, when available, offense type and date, court name, case number, outcome of the charges, and more. Curious about someone's criminal record? People search and find out with this instant report from Intelius!

Other online data brokers

- *Abika.com, USSearch.com*
- Private information reselling
  - Name, address, birthdates, phone numbers
  - Marital status, name and age of children, family members
  - *Bankruptcy history, medical and criminal records*

55

Applications géo-sociales

- Foursquare
- Gowalla
- FacebookPlaces

56

Exemple de géolocalisation

« *Bonjour M. Tremblay, nous sommes heureux de voir que vous êtes à proximité, nous pensions justement à vous puisque vous n'êtes pas passé nous voir depuis près de 6 mois.*

Laissez-nous vous faire une offre imbattable sur les vos jeans préférés, nous en avons justement deux de votre taille en magasin.

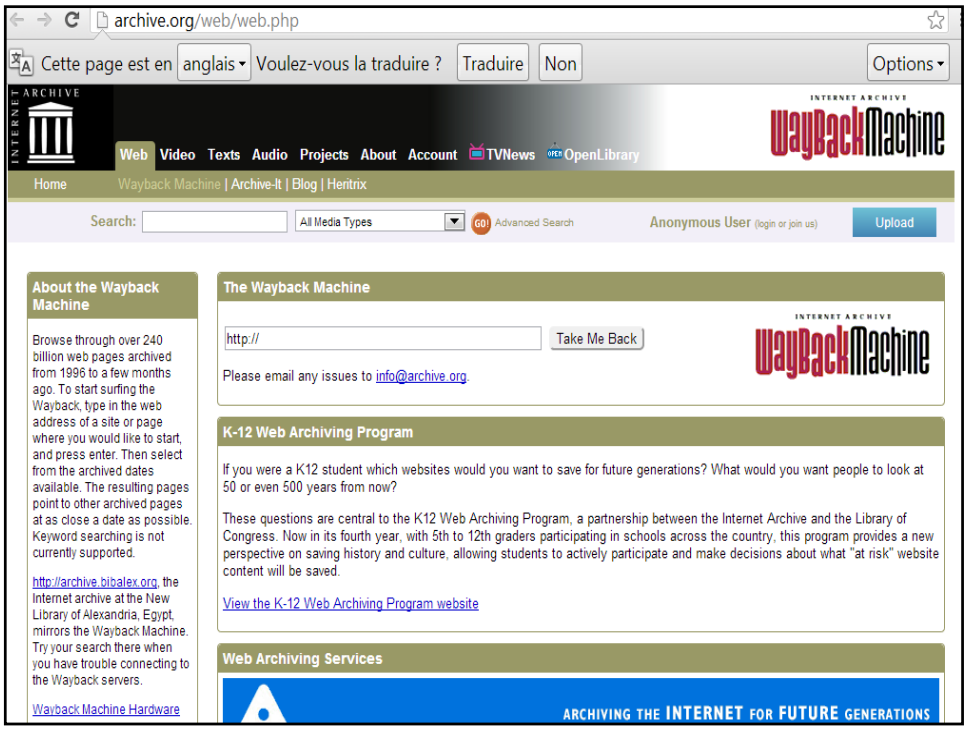
Comme vous n'êtes qu'à quelques minutes, nous vous faisons une offre de 20% de rabais valide pour les 20 prochaines minutes. Ne manquez pas ça, saisissez là! »

57

Non seulement on sait où vous êtes, mais on sait aussi où vous ne vous trouvez pas !

58


pleaserobme.com
Google
lost Visited
Getting Started
Authentification
Galerie de composants ...
Sites suggérés
PLEASE ROB ME
Raising awareness about over-sharing
Check out our guest blog post on the CDT website.
Like
Send
30,560 people like this.
Check your own Twitter timeline for checkins
Are you curious if people can see your checkins?
Enter your Twitter username and find out.
Your Twitter username
Share
More Info
Home
Why
Made Possible By
Foursquare
Twitter
@boyvanamstel


archive.org/web/web.php
Cette page est en anglais
Voulez-vous la traduire ?
Traduire
Non
Options
INTERNET ARCHIVE
Web
Video
Texts
Audio
Projects
About
Account
TVNews
OpenLibrary
WayBackMachine
Home
Wayback Machine | Archive-It | Blog | Heritrix
Search:
All Media Types
Advanced Search
Anonymous User (login or join us)
Upload
About the Wayback Machine
Browse through over 240 billion web pages archived from 1996 to a few months ago. To start surfing the Wayback, type in the web address of a site or page where you would like to start, and press enter. Then select from the archived dates available. The resulting pages point to other archived pages at as close a date as possible. Keyword searching is not currently supported.
http://archive.bibalex.org, the Internet archive at the New Library of Alexandria, Egypt, mirrors the Wayback Machine. Try your search there when you have trouble connecting to the Wayback servers.
Wayback Machine Hardware
The Wayback Machine
http://
Take Me Back
Please email any issues to info@archive.org.
K-12 Web Archiving Program
If you were a K12 student which websites would you want to save for future generations? What would you want people to look at 50 or even 500 years from now?
These questions are central to the K12 Web Archiving Program, a partnership between the Internet Archive and the Library of Congress. Now in its fourth year, with 5th to 12th graders participating in schools across the country, this program provides a new perspective on saving history and culture, allowing students to actively participate and make decisions about what "at risk" website content will be saved.
View the K-12 Web Archiving Program website
Web Archiving Services
ARCHIVING THE INTERNET FOR FUTURE GENERATIONS

Négligence des internautes

61

Moteurs recherche de personnes et aggrégateurs de données

62

CLASSE / MOTEUR	GRATUIT	PAYANT	MONDIAL	NATIONNAL
spock	✓		✓	
spokeo		✓	✓	
123people	✓		✓	
INTELIUS		✓		✓
PeopleSearch				✓
zoominfo		✓	✓	
PeekYou	✓			✓
peoplefinders	✓			✓
pipl	✓		✓	
wink People Search	✓		✓	
ziki		✓	✓	
yasni.com	✓		✓	
Yatedo	✓		✓	
ZABASEARCH		✓		✓
AnyWho	✓			✓

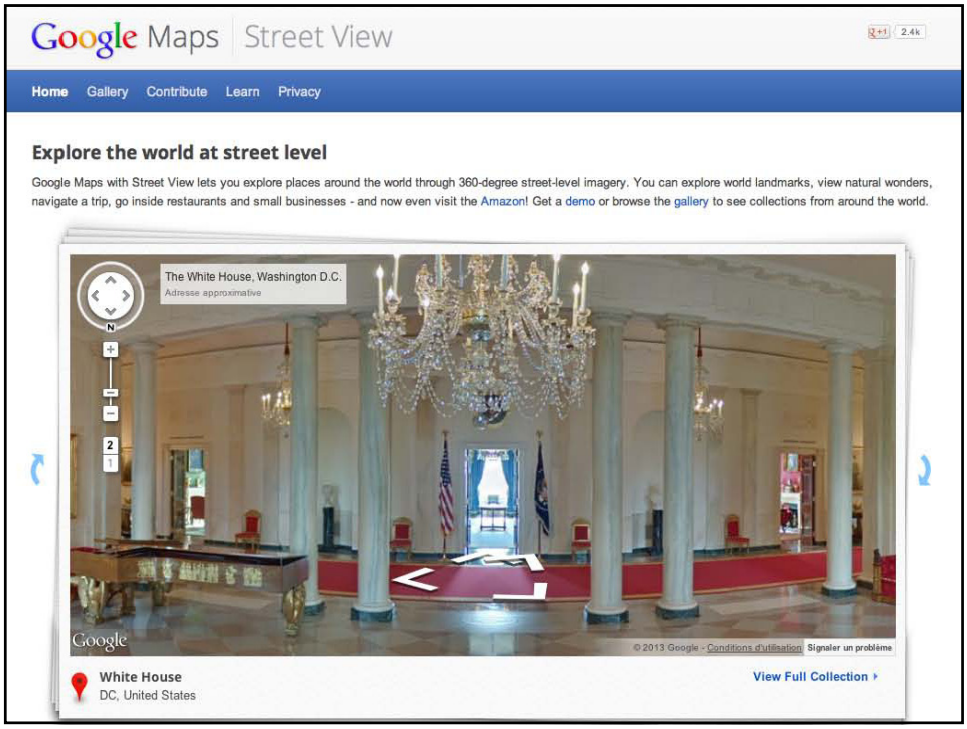
63

Google IS WATCHING YOU

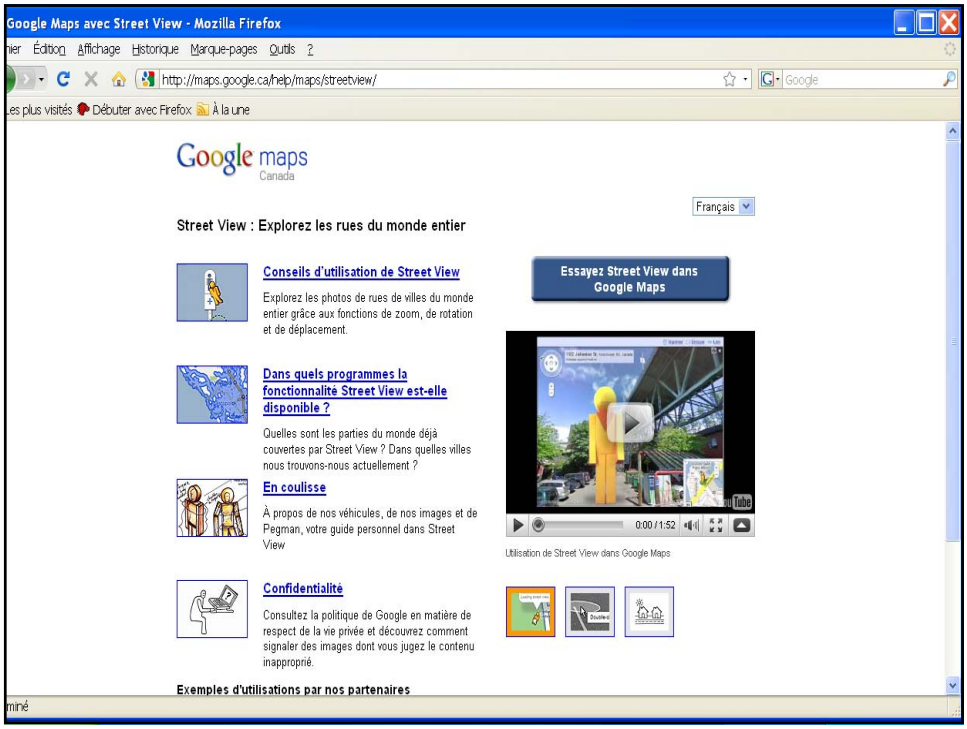
Alerts (topics and news stories in which one is interested)
Calendar (day to day personal and professional schedule)
Catalogs (items one wishes to purchase)
Code (computer programming skill set and the kind of problems on which one is working)
Earth (locations of interest)
Gmail (communications and responses to contacts)
Images (topics of interest)
Groups (groups to which one is affiliated)
Maps for mobile (one's location)
News (new stories of interest)
Orkut (family, friends, and colleagues)
Patent Search (patent idea and strategic plans)
Scholar (academic background and expertise)
SMS (contents of text messages and phone number)
Talk (contents of communication)
Translate (native language)
YouTube (topics of interest)
Google+ (your entire life)

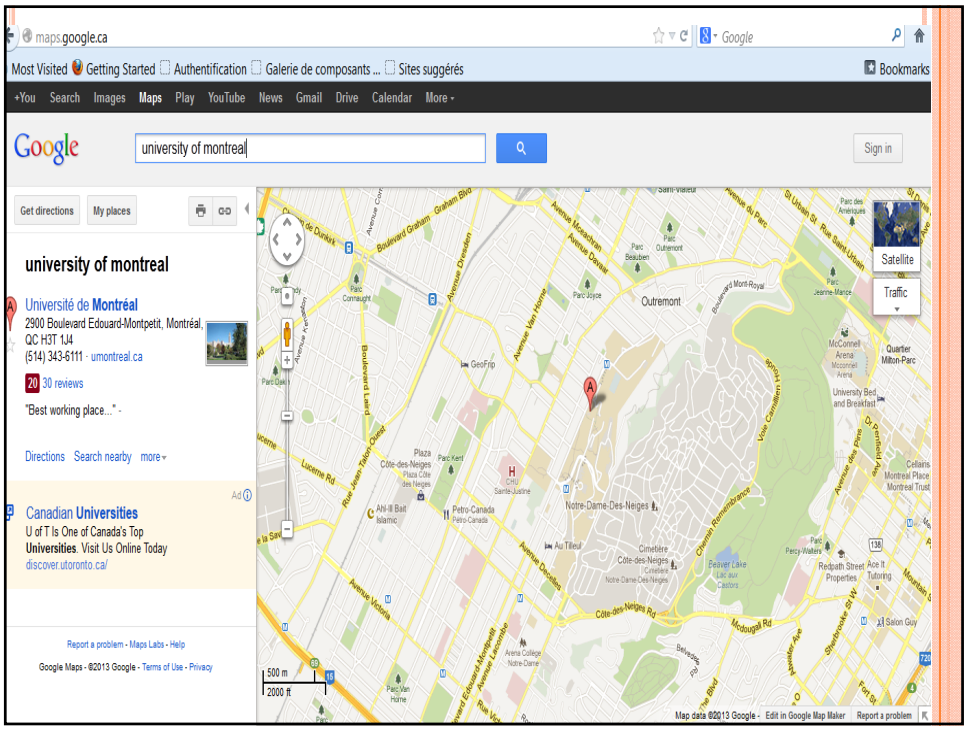
64

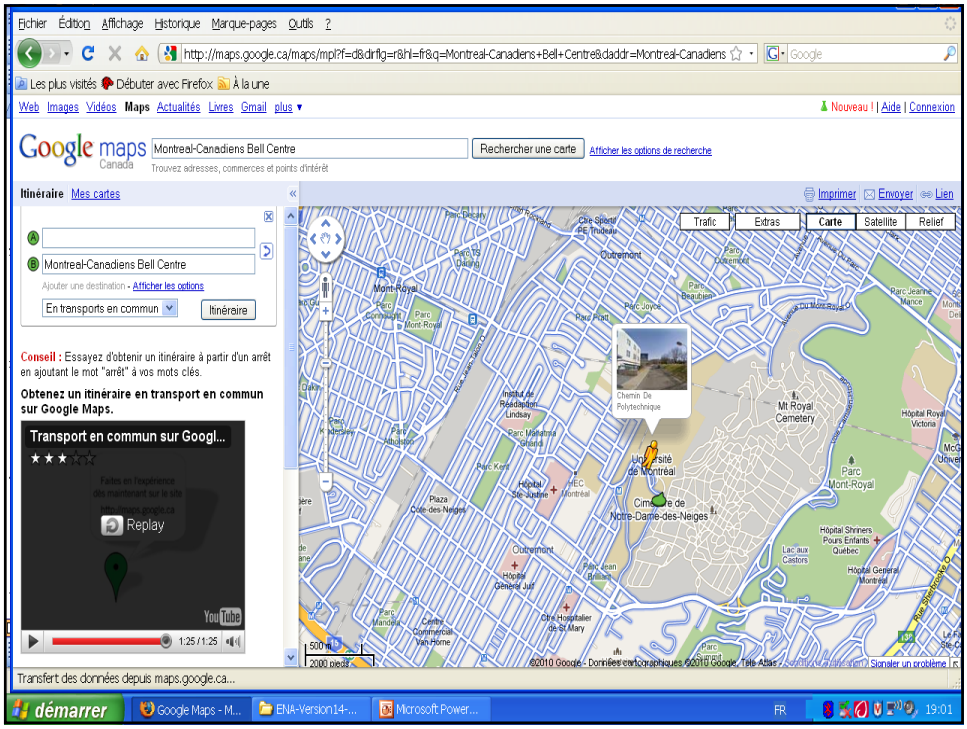
64

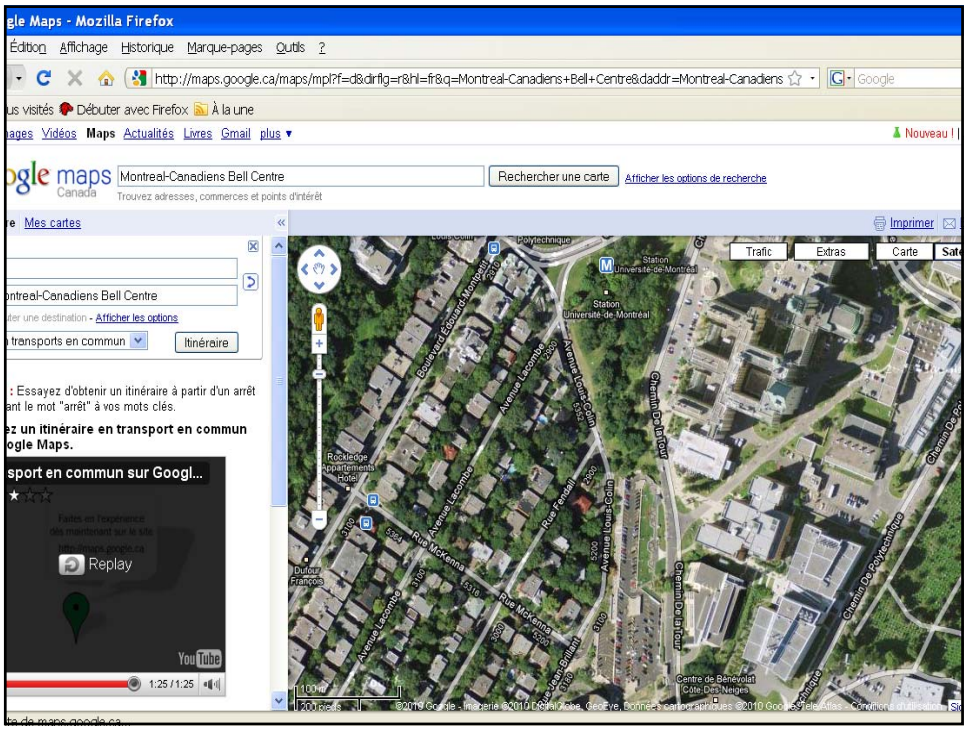

Google Maps Street View
Home Gallery Contribute Learn Privacy
Explore the world at street level
Google Maps with Street View lets you explore places around the world through 360-degree street-level imagery. You can explore world landmarks, view natural wonders, navigate a trip, go inside restaurants and small businesses - and now even visit the Amazon! Get a demo or browse the gallery to see collections from around the world.
The White House, Washington D.C.
Adresse approximative
Google
© 2013 Google - Conditions d'utilisation
Signaler un problème
White House
DC, United States
View Full Collection

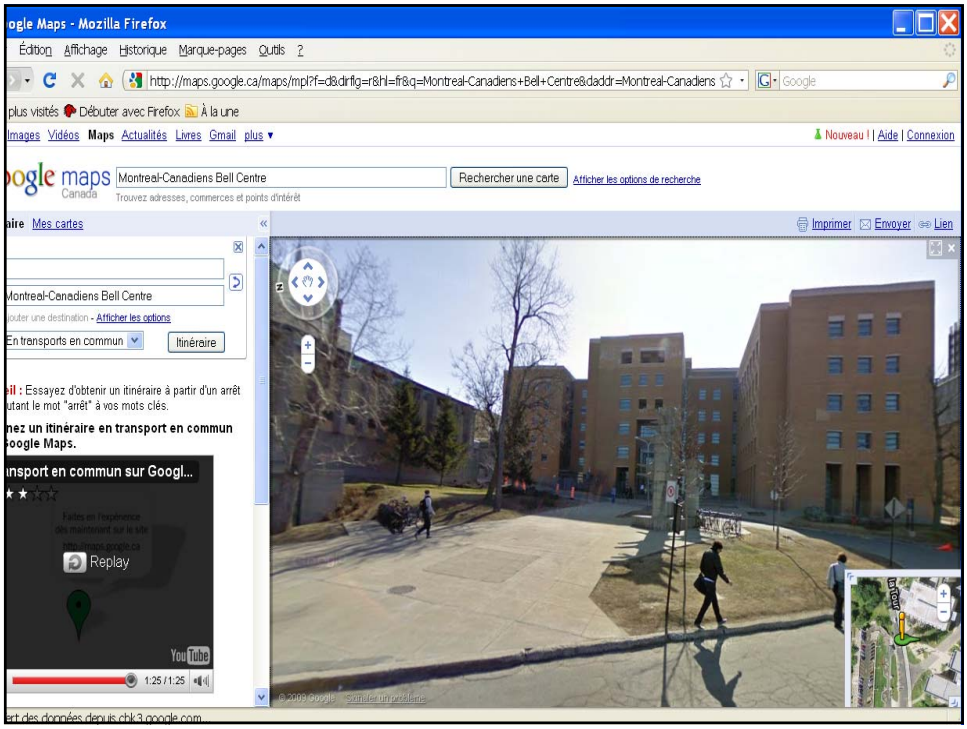
66


Google Maps avec Street View - Mozilla Firefox
http://maps.google.ca/help/maps/streetview/
Google maps
Canada
Français
Street View : Explorez les rues du monde entier
Conseils d'utilisation de Street View
Explorez les photos de rues de villes du monde entier grâce aux fonctions de zoom, de rotation et de déplacement.
Essayez Street View dans Google Maps
Dans quels programmes la fonctionnalité Street View est-elle disponible ?
Quelles sont les parties du monde déjà couvertes par Street View ? Dans quelles villes nous trouvons-nous actuellement ?
En coulisse
À propos de nos véhicules, de nos images et de Pegman, votre guide personnel dans Street View
Confidentialité
Consultez la politique de Google en matière de respect de la vie privée et découvrez comment signaler des images dont vous jugez le contenu inapproprié.
Exemples d'utilisations par nos partenaires
0:00 / 1:52
Utilisation de Street View dans Google Maps


maps.google.ca
Most Visited
Getting Started
Authentification
Galerie de composants ...
Sites suggérés
Bookmarks
+You
Search
Images
Maps
Play
YouTube
News
Gmail
Drive
Calendar
More
Google
university of montreal
Sign in
Get directions
My places
university of montreal
Université de Montréal
2900 Boulevard Edouard-Montpetit, Montréal, QC H3T 1J4
(514) 343-6111 · umontreal.ca
30 reviews
"Best working place..." -
Directions
Search nearby
more
Canadian Universities
U of T Is One of Canada's Top Universities. Visit Us Online Today
discover.utoronto.ca/
Report a problem - Maps Labs - Help
Google Maps - ©2013 Google - Terms of Use - Privacy
Satellite
Traffic
Outremont
Notre-Dame-Des-Neiges
Côte-des-Neiges Rd
Map data ©2013 Google - Edit in Google Map Maker
Report a problem


Fichier Édition Affichage Historique Marque-pages Outils ?
http://maps.google.ca/maps/mpl?f=d&dirflg=r&hl=fr&q=Montreal-Canadiens+Bell+Centre&daddr=Montreal-Canadiens
Google maps Canada
Montreal-Canadiens Bell Centre
Rechercher une carte
Afficher les options de recherche
Itinéraire Mes cartes
Montreal-Canadiens Bell Centre
En transports en commun
Itinéraire
Conseil : Essayez d'obtenir un itinéraire à partir d'un arrêt en ajoutant le mot "arrêt" à vos mots clés.
Obtenez un itinéraire en transport en commun sur Google Maps.
Transport en commun sur Googl...
Replay
Trafic Extras Carte Satellite Relief
Transfert des données depuis maps.google.ca...
démarrer
Google Maps - M...
ENA-Version14-...
Microsoft Power...
FR
19:01


gle Maps - Mozilla Firefox
Édition Affichage Historique Marque-pages Outils ?
http://maps.google.ca/maps/mpl?f=d&dirflg=r&hl=fr&q=Montreal-Canadiens+Bell+Centre&daddr=Montreal-Canadiens
Montreal-Canadiens Bell Centre
Rechercher une carte
Afficher les options de recherche
Mes cartes
Itinéraire
Replay
Trafic Extras Carte
Imprimer


ogle Maps - Mozilla Firefox
Édition Affichage Historique Marque-pages Outils ?
http://maps.google.ca/maps/mpl?f=d&dirflg=r&hl=fr&q=Montreal-Canadiens+Bell+Centre&daddr=Montreal-Canadiens
plus visités Débuter avec Firefox À la une
Images Vidéos Maps Actualités Livres Gmail plus
Nouveau ! | Aide | Connexion
oogle maps Canada
Montreal-Canadiens Bell Centre
Rechercher une carte
Afficher les options de recherche
Trouvez adresses, commerces et points d'intérêt
aire Mes cartes
Imprimer Envoyer Lien
Montreal-Canadiens Bell Centre
Afficher les options
En transports en commun
Itinéraire
il : Essayez d'obtenir un itinéraire à partir d'un arrêt
utant le mot "arrêt" à vos mots clés.
nez un itinéraire en transport en commun
Google Maps.
nsport en commun sur Googl...
Replay
YouTube
1:25 / 1:25
Entrer
© 2009 Google
rt des données depuis ch.k3.google.com


SB
P
© 2013 Google Image Date: October 2011
Report a problem
72

73

Google Admits To Accidentally Collecting Personal Data With Street View Cars

JASON KINCAID

Friday, May 14th, 2010 **0 Comments**

Talk about shooting yourself in the foot. Google has just admitted in an official blog **post** that its Street View cars have been "mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks" since 2006. In other words, as these cars have been driving around, they've been collecting unencrypted user data in addition to the SSID and MAC addresses they were supposed to be tracking.

It's not likely that Google grabbed enough data about many individuals for this to be a major privacy concern. After all, the cars were typically only in range of most of these Wifi networks for a few seconds. But this is certain to haunt Google nonetheless — the company has so much private data on so many people, that it's imperative that the public maintain its trust in the search giant and its "Don't be evil" mantra. Expect privacy advocates and the various governments that are putting Google under increasing scrutiny to refer back to this incident for quite a while, along with Google's recent Buzz **privacy debacle**.

Here's the explanation from Alan Eustace, Senior VP, Engineering & Research:

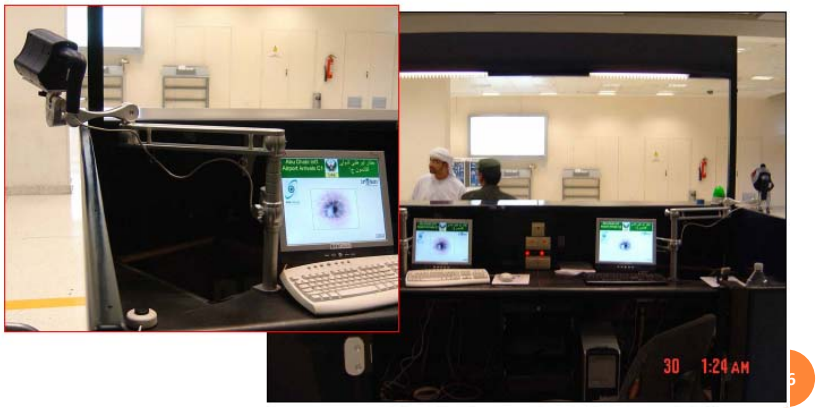
> *So how did this happen? Quite simply, it was a mistake. In 2006 an engineer working on an experimental WiFi project wrote a piece of code that sampled all categories of publicly broadcast WiFi data. A year later, when our mobile team started a project to collect basic WiFi network*

BIOMETRY

- Uses biological information
  - Fingerprints
  - Facial recognition
  - Retina recognition
- Usage
  - Monitor work hours
  - Control access to physical locations

75

Abu Dhabi Int'l Airport T1



Source: www.biometrics.org

76

94 La biométrie progres ×

94.citoyens.com/2012/la-biometrie-pousse-dans-les-cantines-du-val-de-marne,17-02-2012.html

Accueil | Cadre de vie | Economie | Loisirs | Politique | Grand Paris | Societe | Agenda | L'actu de votre ville ...

La biométrie progresse dans les cantines du Val de marne

Publié le 17 février 2012 par C.Dubois

L'authentification biométrique par contour de la main séduit de plus en plus de collèges et lycées du Val de Marne. Le principe : les élèves composent un code personnel à trois chiffres et posent leur main sur un appareil qui vérifie que c'est bien le contour de leur main qui est associé à ce chiffre.

S'il est difficile d'avoir les statistiques exhaustives des installations car les collectivités locales n'en disposent pas, un récent communiqué de la société Alise, l'un des prestataires de solution biométrique, fait état de 15 installations dans le département, rien que pour les établissements publics et avec ce fournisseur. Le dernier établissement inauguré dans le département, le collège Saint Exupéry de Fresnes, s'est du reste équipé d'office d'un accès biométrique à la cantine.

«Cela évite les pertes de cartes et c'est plus fiable car les absences sont directement pointées dans le système

A lire aussi

Cantines : Que Choisir distribue les bons et mauvais points dans le Val de Marne

Cantines: comment faire meilleur, moins cher, écolo?

Les élèves de sixième auront leur PC portable dès la rentrée 2012

L'internat d'excellence de Cachan en images

Chasse aux oeufs

Chasse aux oeufs de Pâques dans le 94

Résultats du bac

Articles les plus Populaires

Pâques: toutes les chasses aux oeufs du Val-de-Ma... : (voir les chasses aux oeufs 2013) De nombreuses co...

La première édition de la SoMad en images : Il ne faisait pas très chaud pour une fin de mois ...

Testé pour vous: la Foire du Trône : (voir aussi infos Foire du trône 2013) Manèges pou...

Le rassemblement citoyen tient son congrès fondat... : Nouveau mouvement politique initié par Corinne Lep...

Thierry Leleu devient préfet du Val de Marne : C'est un habitué de l'Est parisien qui vient d'être...

BBC NEWS EDUCATION & FAMILY

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environme

England | Northern Ireland | Scotland | Wales | UK Politics | Education

15 May 2012 Last updated at 13:02 GMT

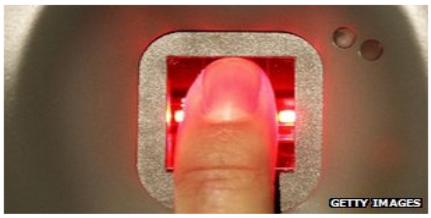
Share

Biometric data: Schools will need parents' approval

Schools in England will be banned from taking pupils' fingerprints and using face-recognition technology unless they get permission from parents.

New government guidance says written parental permission must be obtained to use students' biometric data.

Pupils themselves will also be allowed to refuse to participate.



It is believed that about a third of secondary schools in England use biometrics

Schools can use fingerprinting or face scanning for recording attendance, checking out library books, paying for lunch or accessing school buildings.

Last year the Association of School and College Leaders (ASCL) estimated that about 30% of secondaries in England were using biometric data.

Related Stories

Warning over pupil fingerprinting

PLAN

- Introduction vie privée
- Domaines de collecte des données
- Perte de données
- Techniques
- **Vol identité et Reconstitution de profils**
- Recommandations
- Axes de Recherche

79

Vol d'identité

80

LE VOL D'IDENTITÉ

«Votre écran d'ordinateur n'est pas un mur derrière lequel vous vous cachez, mais plutôt une fenêtre grande ouverte par laquelle deux milliards d'inconnus vous observent. »
Jean Chartier, Président de la Commission d'accès à l'information du Québec

(28 janvier 2011 la journée mondiale de la protection de la vie privée)

http://communiques.gouv.qc.ca/gouvqc/communiques/GPQF/Janvier2011/27/c5598.htm

81 81

Définition

Pas d'harmonisation de la définition

Selon l'Organisation de Coopération et de Développement Économique :

"Un vol d'identité se produit quand une tierce partie **acquiert, transfère, possède ou utilise** les informations personnelles d'une personne physique ou morale sans autorisation, avec **l'intention** de commettre, ou en lien avec une **fraude ou d'autres crimes**."

VOICI LE CAS D'UNE HISTOIRE RÉELLE

VOL D'IDENTITÉ EN 1 HEURE (USA) AVEC CONSENTEMENT DE LA PERSONNE

Professeur et ancien consultant dans une société de sécurité informatique a tenté une expérience originale.

Il a réussi à obtenir des informations confidentielles sur une personne et ainsi à s'introduire dans ses comptes bancaire.

HERBERT H. THOMPSON

La personne visée, s'appelle Kim, est très peu connue d'Herbert. Il sait juste comment elle s'appelle (nom et prénom).

- **Acte 1**: Basé sur ces informations, Herbert se lance dans une rapide recherche sur Google lui donne un blog et un C.V. de Kim.

Google

Le blog lui donne une foule d'informations personnelles comme son adresse Gmail.

Du C.V., il en retire une vielle adresse email fournit par l'établissement scolaire de Kim.

85

Acte 2: Il se connecte sur le site de la banque de Kim et fait une demande de récupération de mot de passe.
Le site indique qu'un email a été envoyé avec le nouveau mot de passe réinitialisé.

Du coup, sa prochaine cible devient le compte Gmail.

Gmail by Google

Acte 3: Il se connecte donc sur Gmail et fait une demande de récupération de mot de passe.
un email avec le mot de passe réinitialisé a été envoyé sur l'adresse scolaire de Kim.

86

Acte 4 : Nouvelle cible, le compte email de l'école.
Une nouvelle fois, il utilise la fonction mot de passe oublié.
On lui demande une adresse postale (trouvée sur le C.V.),
et une date de naissance.

Acte 5 : Herbert retourne sur le blog
où Kim raconte comment son
anniversaire s'est déroulé tel jour
Sur Facebook, ses amies lui souhaitent
joyeux anniversaire

Acte 6 : Il retourne sur le compte email scolaire de Kim,
fait plusieurs essais et tombe sur la bonne année de naissance.

Sur Gmail, il récupère le lien de réinitialisation du compte bancaire.

C'est fini! Il peut s'amuser avec l'argent de Kim.

87

TYPES DE VOL D'IDENTITÉ

88

Financier : transfert de fond du compte de la victime

Médical : traitement aux frais de l'assuré usurpé

Éducationnel : vol de crédit, falsification de notes etc.

Criminel : crime commis sous une autre identité

Synthétique : création ou combinaison de vraies identités

EXEMPLES ET STATISTIQUES

DONNÉES PERSONNELLES COLLECTÉES PAR LES ÉTABLISSEMENTS D'ENSEIGNEMENT

Données générales d'identification.

Données relatives au parcours scolaire de l'étudiant en dehors de l'établissement.

Données relatives au parcours académique de l'étudiant au sein de l'établissement.

- Enregistrées pour une durée illimitée.
- Une absence ou mauvaise protection.

⇒ Atteinte à la vie privée de l'étudiant ou de l'élève.

91 91

LES ÉLÈVES ET ÉTUDIANTS CIBLES DU VOL D'IDENTITÉ

30% des victimes du vol d'identité sont âgées entre 18 et 29.

21% des collégiens sont préoccupés par le vol d'identité.

89% des parents ont discuté des mesures de sécurité avec leurs enfants, mais ces derniers continuent à adopter des comportements à risque.

http://siblog.mcafee.com/identitytheft/college-students-at-risk-for-identity-theft/

92 92

ATTAQUES

«Nous en repoussons des milliers et des milliers tous les jours…Certaines attaques visent à prendre le contrôle des équipements de l'Université, … de mener contre un tiers une attaque dévastatrice ….»

Directeur de la sécurité informatique à Université de Montréal.

2009, Cyber attaques sur des collèges et universités au Québec

l'Université de Montréal a été la cible d'une cyber attaque:

Recherche de données confidentielles.

Interruption des systèmes pour une fin de semaine.

l'UQAM (L'Université du Québec À Montréal) a connu la même crise:

Le pirate s'est introduit dans d'autres universités au Québec, au Canada, aux États-Unis et en Europe.

Serveurs affectés, interruption des systèmes pendant 3 semaines.

http://www.nouvelles.umontreal.ca/campus/securite-informatique/20110117-luniversite-mieux-armee-pour-contrer-les-attaques-des-pirates-informatiques.html

93

93

Russian Hacker Selling 1.5 Million Facebook Accounts

Do you like this story?

Like 4,169 people like this.

A hacker who calls himself Kirllos has obtained and is now offering to sell 1.5 million Facebook IDs at astonishingly low prices — $25 per 1000 IDs for users with fewer than 10 friends and $45 per 1000 IDs for users with more than 10 friends — according to researchers at VeriSign's iDefense. Looking at the numbers, Kirllos has stolen the IDs of one out of every 300 Facebook users.

Information for sale includes login credentials; whether or not the e-mail addresses and passwords are legitimate is currently unknown. Typically, this information would be sold for between $1 and $20 per account, according to data from Symantec. Currently, around 700,000 accounts have been sold. The threads where the accounts are being sold have been removed, as far as we are able to tell.

The users whose e-mail addresses and passwords have been compromised risk having their identities stolen, but they could also become targets of more insidious scams. As always, we will keep you updated about any Facebook scams that come across our news desk.

Hacking Facebook isn't a new hobby for this person. Here's a screenshot of another offer the hacker previously made on a forum earlier this year; then, he was then selling 100,000 hacked accounts from users around the world:

94

Vol de photos sur Facebook:

http://www.rue89.com/2011/02/22/sur-facebook-une-inconnue-ma-vole-mes-photos-et-mon-identite-191649

Usurpation d'identité du frère pour commettre des crimes

http://www.leparisien.fr/faits-divers/il-usurpe-l-identite-de-son-frere-30-mois-de-prison-ferme-13-08-2010-1030598.php

Manque de vigilance d'un père, son fils achète un avion de combat

http://www.europe1.fr/International/A-7-ans-il-achete-un-avion-de-combat-409725/

95

FAUX PROFILS DE PERSONNES CÉLÈBRES

Miss Hawaii

http://www.staradvertiser.com/news/hawaiinews/20110120_Woman_pleads_guilty_to_theft.html

Omar Sy humoriste francais

http://www.gautrais.com/Usurpation-d-identite-sur-Facebook

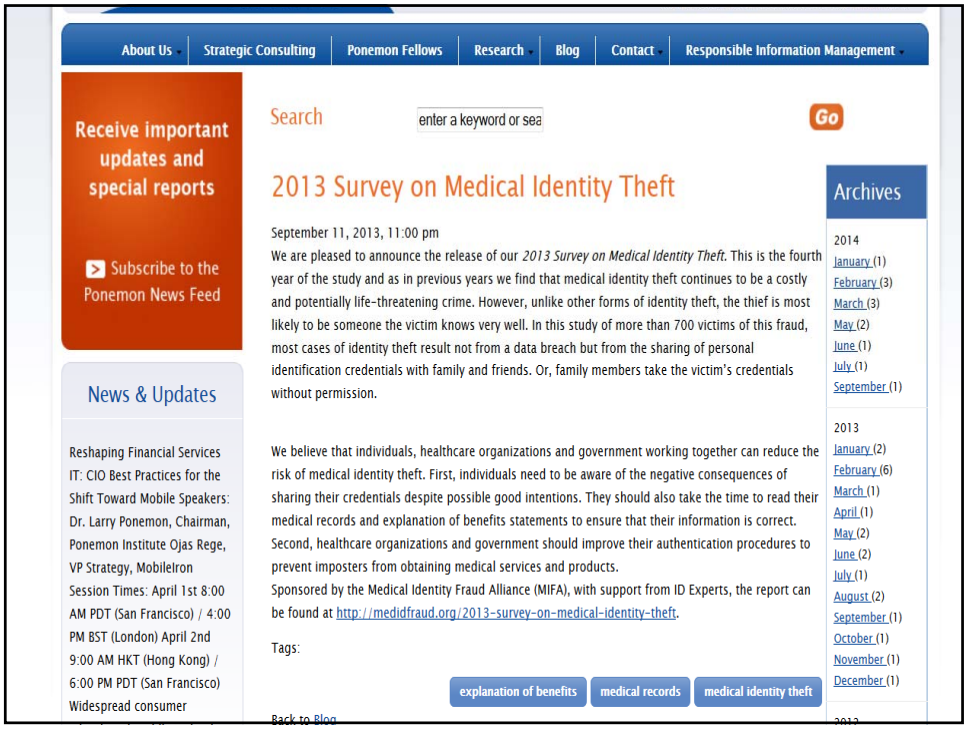
Christophe Rocancourt

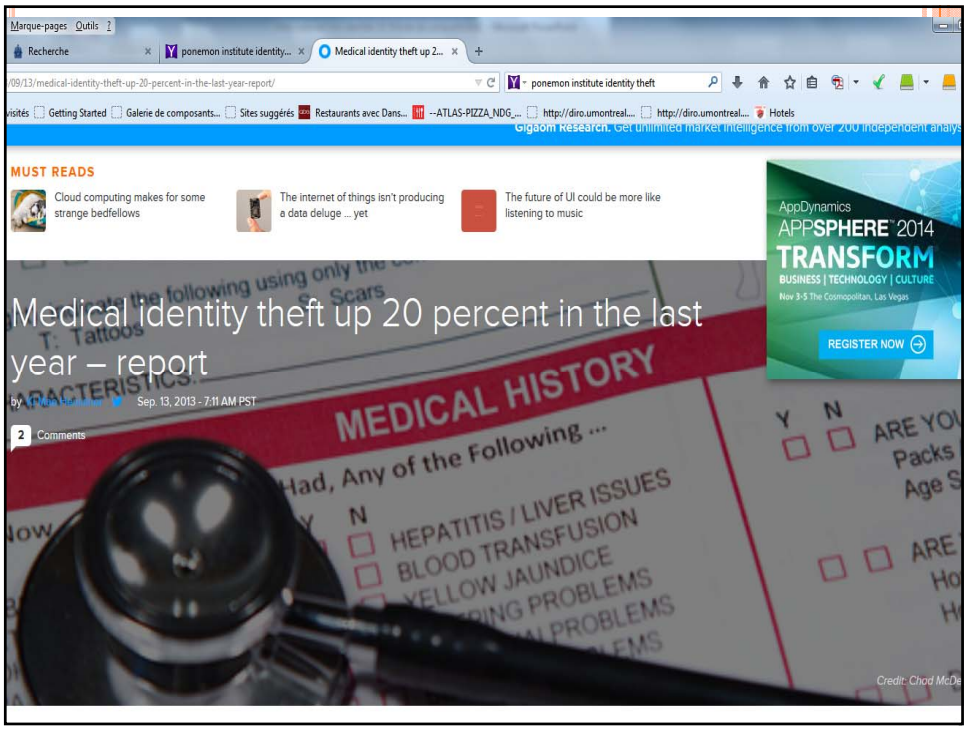
http://www.security-faqs.com/christopher-rocancourt-the-false-rockerfeller.html

Animateurs et vedettes québécoises

http://www.francoischarron.com/-/a3l4rgv3pm/menu/

96


About Us
Strategic Consulting
Ponemon Fellows
Research
Blog
Contact
Responsible Information Management
Receive important updates and special reports
Subscribe to the Ponemon News Feed
Search
enter a keyword or sea
Go
2013 Survey on Medical Identity Theft
September 11, 2013, 11:00 pm
We are pleased to announce the release of our 2013 Survey on Medical Identity Theft. This is the fourth year of the study and as in previous years we find that medical identity theft continues to be a costly and potentially life-threatening crime. However, unlike other forms of identity theft, the thief is most likely to be someone the victim knows very well. In this study of more than 700 victims of this fraud, most cases of identity theft result not from a data breach but from the sharing of personal identification credentials with family and friends. Or, family members take the victim's credentials without permission.
We believe that individuals, healthcare organizations and government working together can reduce the risk of medical identity theft. First, individuals need to be aware of the negative consequences of sharing their credentials despite possible good intentions. They should also take the time to read their medical records and explanation of benefits statements to ensure that their information is correct. Second, healthcare organizations and government should improve their authentication procedures to prevent imposters from obtaining medical services and products.
Sponsored by the Medical Identity Fraud Alliance (MIFA), with support from ID Experts, the report can be found at http://medidfraud.org/2013-survey-on-medical-identity-theft.
Tags:
explanation of benefits
medical records
medical identity theft
Back to Blog
Archives
2014
January (1)
February (3)
March (3)
May (2)
June (1)
July (1)
September (1)
2013
January (2)
February (6)
March (1)
April (1)
May (2)
June (2)
July (1)
August (2)
September (1)
October (1)
November (1)
December (1)
News & Updates
Reshaping Financial Services IT: CIO Best Practices for the Shift Toward Mobile Speakers: Dr. Larry Ponemon, Chairman, Ponemon Institute Ojas Rege, VP Strategy, MobileIron Session Times: April 1st 8:00 AM PDT (San Francisco) / 4:00 PM BST (London) April 2nd 9:00 AM HKT (Hong Kong) / 6:00 PM PDT (San Francisco) Widespread consumer

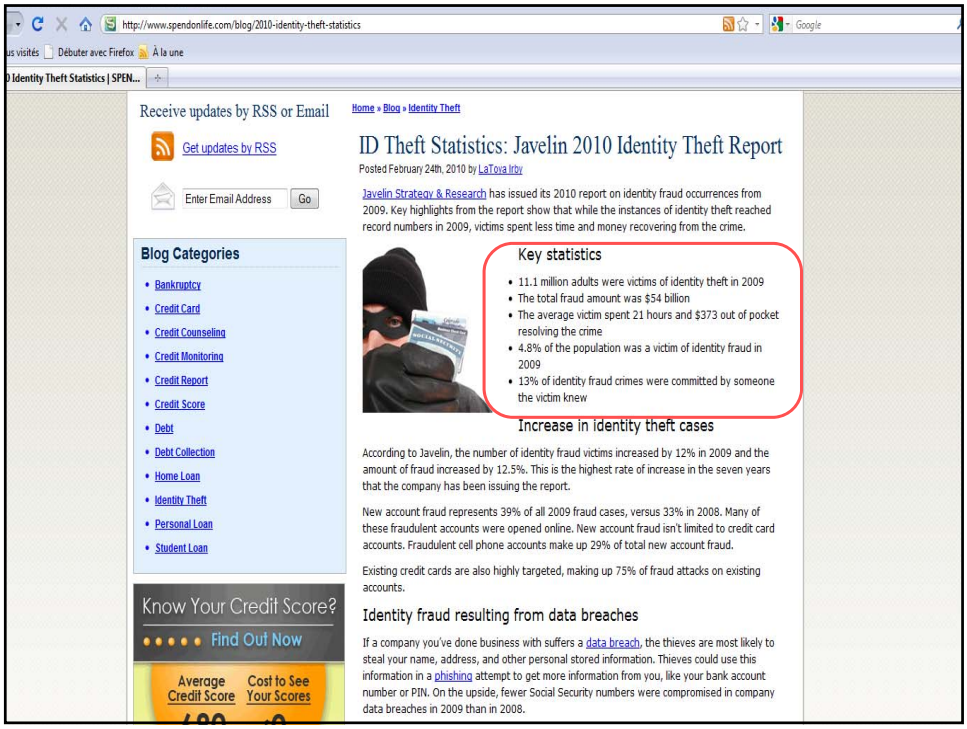

Marque-pages
Outils
Recherche
ponemon institute identity...
Medical identity theft up 2...
ponemon institute identity theft
Getting Started
Galerie de composants...
Sites suggérés
Restaurants avec Dans...
--ATLAS-PIZZA_NDG_...
http://diro.umontreal....
Hotels
MUST READS
Cloud computing makes for some strange bedfellows
The internet of things isn't producing a data deluge ... yet
The future of UI could be more like listening to music
AppDynamics
APPSPHERE 2014
TRANSFORM
BUSINESS | TECHNOLOGY | CULTURE
REGISTER NOW
Medical identity theft up 20 percent in the last year – report
Sep. 13, 2013 - 7:11 AM PST
2 Comments
MEDICAL HISTORY
HEPATITIS / LIVER ISSUES
BLOOD TRANSFUSION
YELLOW JAUNDICE

- You might want to start giving your health records and medical bills a closer look.
- According to a new survey from the Ponemon Institute, an independent group that focuses on privacy and data security, medical identity theft is on the rise: since 2012, the number of people affected by medical identity theft has increased nearly 20 percent. The survey, which was sponsored by the Medical Identity Fraud Alliance and ID Experts, found that a total of about 1.84 million people in the U.S. have been affected.

99

- For victims, the consequences are not only financial (last year, the groups estimate that medical identity theft led to more than $12 billion in out-of-pocket costs), they're also medical. Ponemon reports that those affected by medical identity theft are more prone to misdiagnosis and mistreatment or delayed treatment.
- The report also said that, in some cases, patients put themselves at risk because they share health information with family members (committing so-called "family fraud") so that loved ones can receive medical services or treatment.
- Ponemon and its partners also said that the spread of electronic health records has complicated medical identity theft — hackers can break into servers to steal information or access data through medical devices and mobile apps.

100



http://www.spendonlife.com/blog/2010-identity-theft-statistics

Receive updates by RSS or Email

Get updates by RSS

Enter Email Address Go

Blog Categories

- Bankruptcy
- Credit Card
- Credit Counseling
- Credit Monitoring
- Credit Report
- Credit Score
- Debt
- Debt Collection
- Home Loan
- Identity Theft
- Personal Loan
- Student Loan

Know Your Credit Score?

Find Out Now

Average Credit Score | Cost to See Your Scores

Home » Blog » Identity Theft

ID Theft Statistics: Javelin 2010 Identity Theft Report

Posted February 24th, 2010 by LaToya Irby

Javelin Strategy & Research has issued its 2010 report on identity fraud occurrences from 2009. Key highlights from the report show that while the instances of identity theft reached record numbers in 2009, victims spent less time and money recovering from the crime.

Key statistics

- 11.1 million adults were victims of identity theft in 2009
- The total fraud amount was $54 billion
- The average victim spent 21 hours and $373 out of pocket resolving the crime
- 4.8% of the population was a victim of identity fraud in 2009
- 13% of identity fraud crimes were committed by someone the victim knew

Increase in identity theft cases

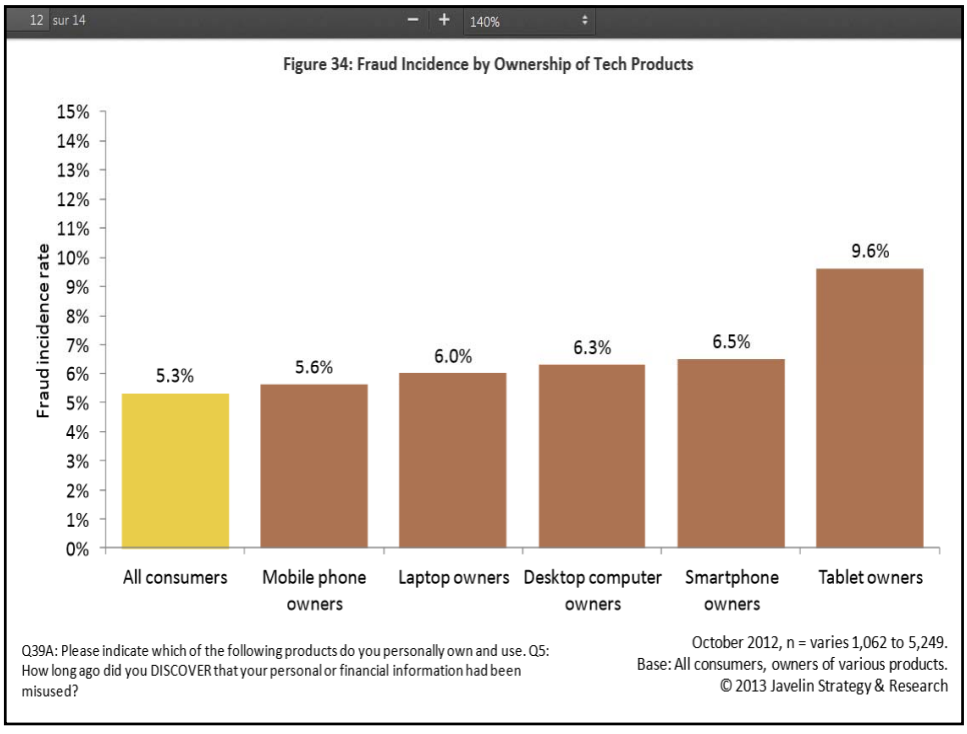
According to Javelin, the number of identity fraud victims increased by 12% in 2009 and the amount of fraud increased by 12.5%. This is the highest rate of increase in the seven years that the company has been issuing the report.

New account fraud represents 39% of all 2009 fraud cases, versus 33% in 2008. Many of these fraudulent accounts were opened online. New account fraud isn't limited to credit card accounts. Fraudulent cell phone accounts make up 29% of total new account fraud.

Existing credit cards are also highly targeted, making up 75% of fraud attacks on existing accounts.

Identity fraud resulting from data breaches

If a company you've done business with suffers a data breach, the thieves are most likely to steal your name, address, and other personal stored information. Thieves could use this information in a phishing attempt to get more information from you, like your bank account number or PIN. On the upside, fewer Social Security numbers were compromised in company data breaches in 2009 than in 2008.

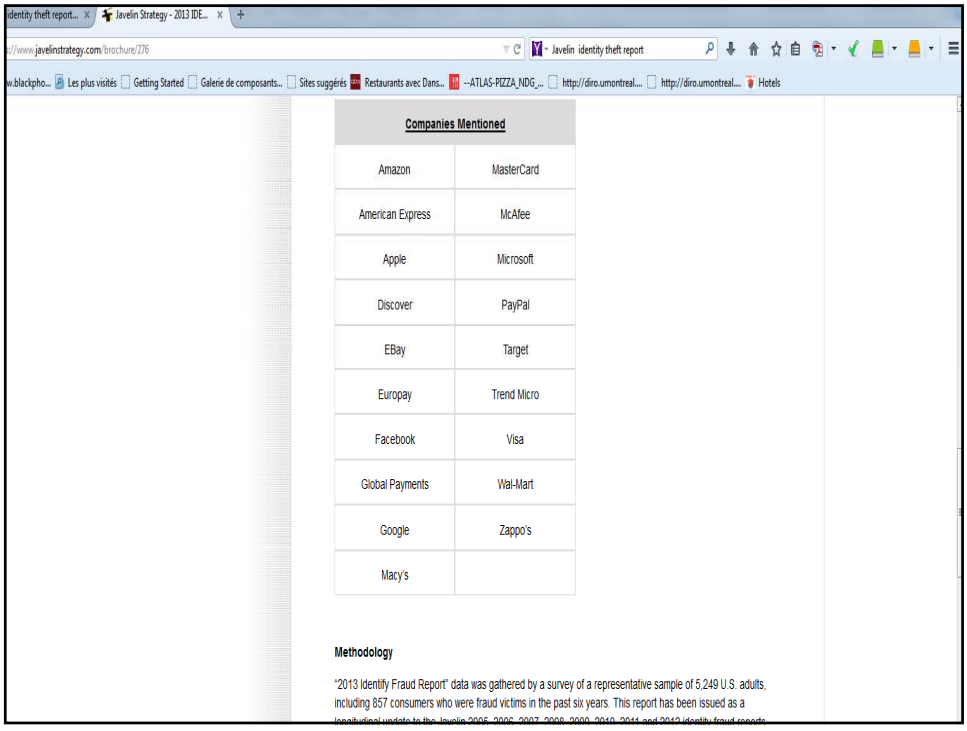


12 sur 14 — 140%

Figure 34: Fraud Incidence by Ownership of Tech Products

Q39A: Please indicate which of the following products do you personally own and use. Q5: How long ago did you DISCOVER that your personal or financial information had been misused?

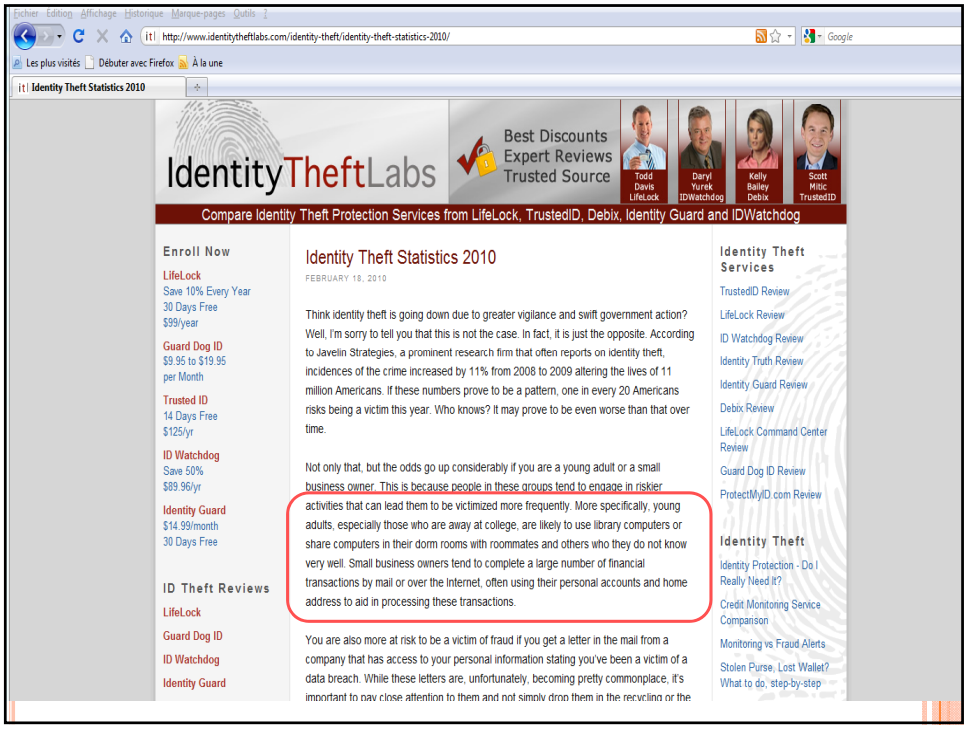
October 2012, n = varies 1,062 to 5,249.
Base: All consumers, owners of various products.

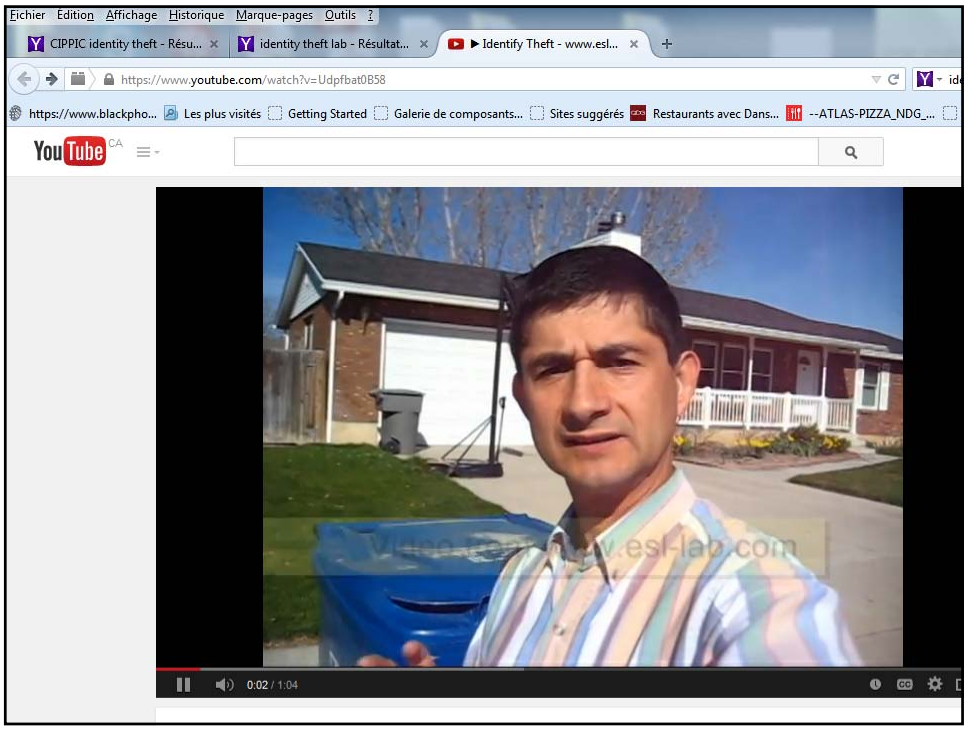


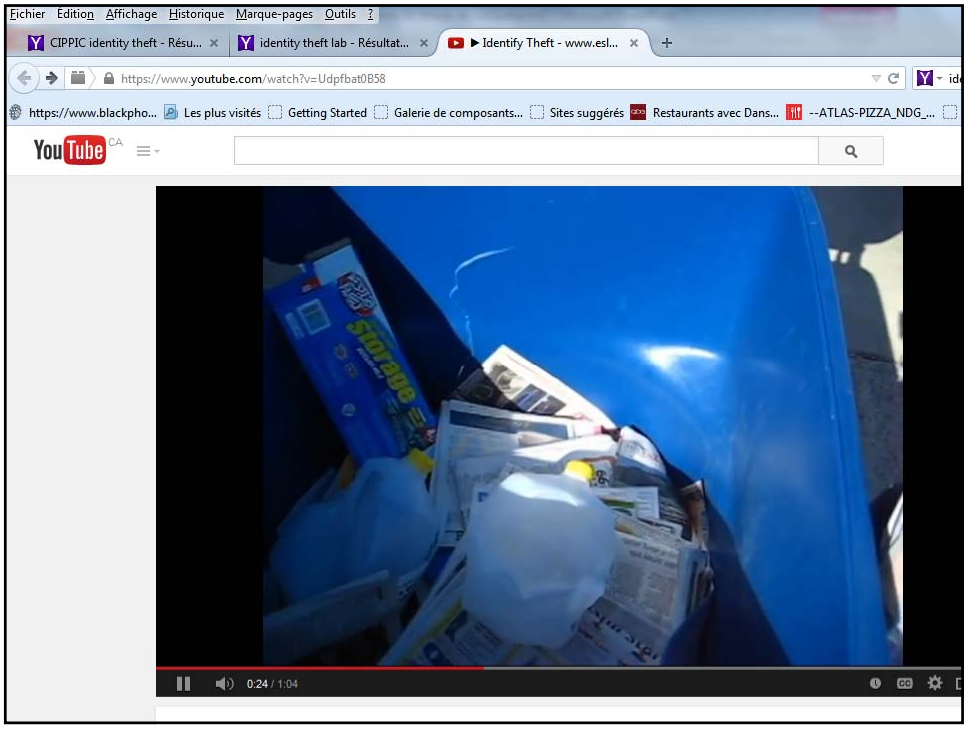
Companies Mentioned	
Amazon	MasterCard
American Express	McAfee
Apple	Microsoft
Discover	PayPal
EBay	Target
Europay	Trend Micro
Facebook	Visa
Global Payments	Wal-Mart
Google	Zappo's
Macy's	

Methodology

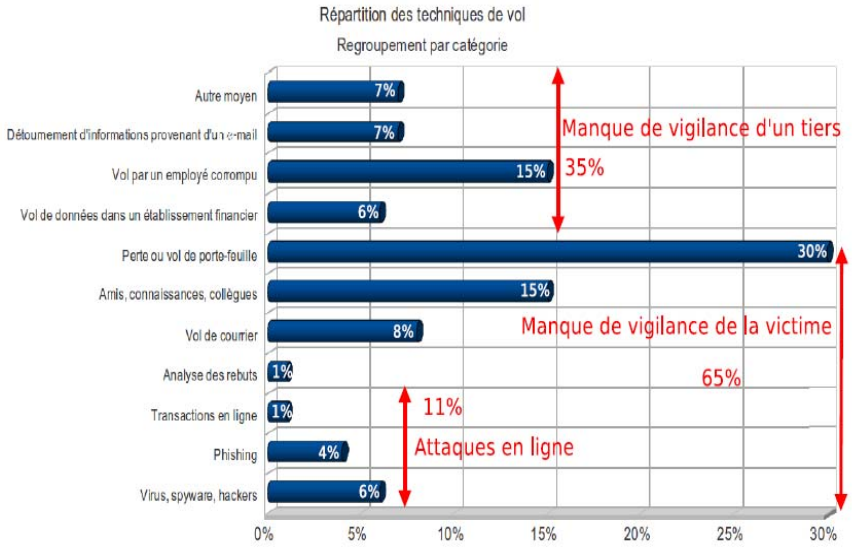
"2013 Identify Fraud Report" data was gathered by a survey of a representative sample of 5,249 U.S. adults, including 857 consumers who were fraud victims in the past six years. This report has been issued as a


http://www.identitytheftlabs.com/identity-theft/identity-theft-statistics-2010/
Identity Theft Statistics 2010
IdentityTheftLabs
Best Discounts
Expert Reviews
Trusted Source
Compare Identity Theft Protection Services from LifeLock, TrustedID, Debix, Identity Guard and IDWatchdog
Enroll Now
LifeLock
Save 10% Every Year
30 Days Free
$99/year
Guard Dog ID
$9.95 to $19.95
per Month
Trusted ID
14 Days Free
$125/yr
ID Watchdog
Save 50%
$89.96/yr
Identity Guard
$14.99/month
30 Days Free
ID Theft Reviews
LifeLock
Guard Dog ID
ID Watchdog
Identity Guard
Identity Theft Statistics 2010
FEBRUARY 18, 2010
Think identity theft is going down due to greater vigilance and swift government action? Well, I'm sorry to tell you that this is not the case. In fact, it is just the opposite. According to Javelin Strategies, a prominent research firm that often reports on identity theft, incidences of the crime increased by 11% from 2008 to 2009 altering the lives of 11 million Americans. If these numbers prove to be a pattern, one in every 20 Americans risks being a victim this year. Who knows? It may prove to be even worse than that over time.
Not only that, but the odds go up considerably if you are a young adult or a small business owner. This is because people in these groups tend to engage in riskier activities that can lead them to be victimized more frequently. More specifically, young adults, especially those who are away at college, are likely to use library computers or share computers in their dorm rooms with roommates and others who they do not know very well. Small business owners tend to complete a large number of financial transactions by mail or over the Internet, often using their personal accounts and home address to aid in processing these transactions.
You are also more at risk to be a victim of fraud if you get a letter in the mail from a company that has access to your personal information stating you've been a victim of a data breach. While these letters are, unfortunately, becoming pretty commonplace, it's
Identity Theft Services
TrustedID Review
LifeLock Review
ID Watchdog Review
Identity Truth Review
Identity Guard Review
Debix Review
LifeLock Command Center Review
Guard Dog ID Review
ProtectMyID.com Review
Identity Theft
Identity Protection - Do I Really Need It?
Credit Monitoring Service Comparison
Monitoring vs Fraud Alerts
Stolen Purse, Lost Wallet? What to do, step-by-step


CIPPIC identity theft - Résu...
identity theft lab - Résultat...
Identify Theft - www.esl...
https://www.youtube.com/watch?v=Udpfbat0B58
YouTube
0:02 / 1:04



(CIPPIC, "Techniques of identity theft", 2007)



Hackers

109

110

Acteurs dans le domaine

- *Black Hat*
  - Criminels
  - Électrons libres (indonésien a créé un virus pour le plaisir)
  - *Script kiddies* (des enfants utilisent des applications/outils pour faire des dommages)
- *Gray Hat* (organisme mandaté)/*White Hat* (employé)
  - Consultants en sécurité
  - Auditeurs (*Penetration-Testers*)
- Universités
- Entreprises
- Gouvernements

111

Hackers

- Dans les années 1980, des groupes de pirates informatiques comme le *Chaos Computer Club* (CCC) se sont auto-proclamés hackers, ce qui signifie : « experts dans leur domaine ». Ce terme a alors été repris par la presse et même parfois dans le milieu de la sécurité informatique.
- Le mot **hacker**, parfois traduit par *bidouilleur*, désigne simplement en Outre-Atlantique une personne apte à modifier astucieusement un objet pour le destiner à un autre usage que celui prévu initialement. Le terme ne comporte pas de connotation péjorative, et n'est pas nécessairement associé à la sécurité informatique, encore moins à des activités illégales.

Finalité des Hackers

- Pour le plaisir
- Par curiosité
- Pour la gloire
- Pour faire des dommages
- Pour demander des rançons
- Pour se venger
- Pour menacer des organisations
- Pour l'appât du gain
- Idéologie et justice

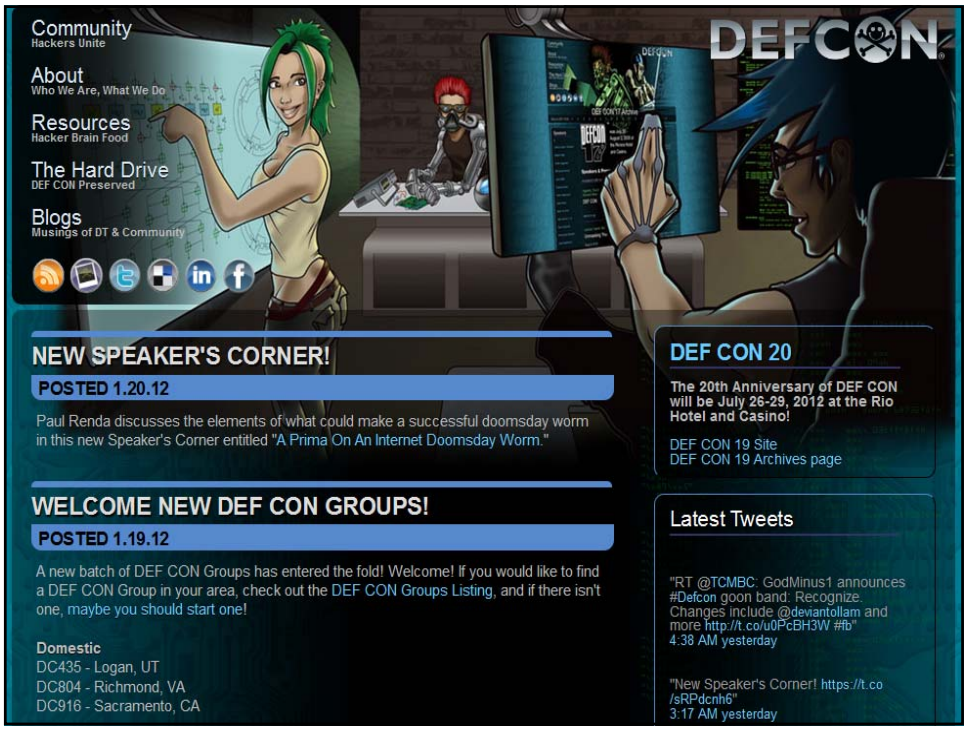
Sociologiquement…

- Sentiment d'impunité «derrière son PC»
- Syndrome du «pas vu pas pris»
- Me-too (mon voisin le fait)
- Nouvelle culture «hippie» : libre, gratuit…
- Refus des institutions

DEF CON

- DEF CON est la convention hacker la plus connue à travers le monde. Elle est tenue chaque année à Las Vegas, aux États-Unis. La première convention DEF CON s'est déroulée en juin 1993.
- Le public de cette convention est pour la plupart composé de professionnels de la sécurité des systèmes d'information, de crackers, et de hackers intéressés par la programmation et l'architecture.

115



Evitez les pièges du vol d'identité pour votre entreprise

0 | 30 nov 2012 - Par *Le mag'Pro*

Sur Internet, certaines informations concernant votre entreprise (logos, photos, adresses mail, organigramme…) se retrouvent en certaines circonstances librement accessibles à tous… voire à certaines personnes mal intentionnées. Quelques conseils pour protéger ces données.

Que risquez-vous ?

L'usurpation d'identité intervient lorsqu'un tiers utilise le nom d'une entreprise ou ses détails d'identification (numéro de Siret par exemple) à des fins frauduleuses.

- Il peut s'agir de **nuire à la réputation de l'entreprise** en se servant de son identité pour créer un faux site Internet, un faux blog, de faux profils sur les réseaux sociaux, de faux comptes ou commentaires sur les forums… Ce qui peut conduire à ruiner votre e-réputation.
- Autre conséquence de l'usurpation d'identité : **le vol de données confidentielles** (fichiers clients, contacts mail, coordonnées bancaires). Le risque est alors de voir les opérations frauduleuses se multiplier : virements bancaires, commandes réalisées au nom et aux frais de votre entreprise, voire sollicitation de services à crédit auprès de vos fournisseurs.
  Les pirates peuvent notamment recourir à la technique du "phishing" pour accéder à vos informations personnelles. Ce qu'on appelle en français le " **hameçonnage** " est une technique qui vise à voler des données confidentielles et des mots de passe. La technique est simple : le pirate se fait passer pour votre banquier par exemple. Dans un mail, il vous incite, via un lien frauduleux, à vous rendre sur le site de la banque et à y entrer vos identifiants. En fait, vous n'êtes pas connecté au bon site mais à un faux, créé par le pirate, qui peut ensuite utiliser les données que vous avez communiquées.
- L'usurpateur peut également **se faire passer pour vous auprès de vos clients** : les pirates créent une adresse mail proche de la vôtre, avec votre logo, votre adresse postale, voire le nom de vos employés, et ils réclament de l'argent, en proposant le plus souvent à la victime de payer immédiatement par virement. A noter que ce type d'arnaques touche principalement les grosses entreprises.

Reconstitution de profils

Même quand vous pensez que tout est “safe”

118

Déclaration en fevrier 2011

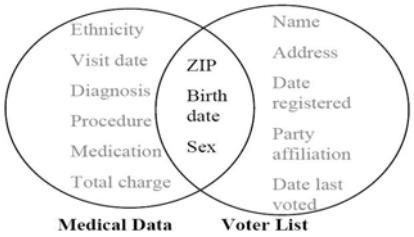
- Des renseignements qui, à première vue, semblent anonymisés ou dépersonnalisés peuvent parfois avoir été combinés à des renseignements tirés d'autres sources, puis manipulés à l'aide de bases de données puissantes en vue de la production de données pouvant être associées à des personnes identifiables.

http://www.priv.gc.ca/parl/2011/parl_20110214_f.cfm

119

Institutions and private companies

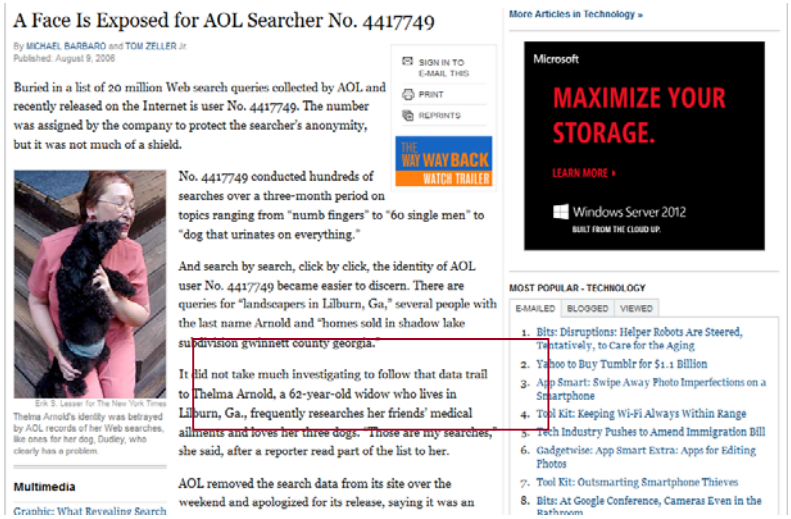
Institutions and governments are also vulnerable to data leakage (Wikileaks)



Latanya Sweeney (2002): only three pieces of information (ZIP code, gender and date of birth) suffice to uniquely identify 87% of the population in the United States.

120

Data breach by AOL



A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

SIGN IN TO E-MAIL THIS
PRINT
REPRINTS

THE WAY BACK
WATCH TRAILER

Erik S. Lesser for The New York Times
Thelma Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an

Multimedia

Graphic: What Revealing Search

More Articles in Technology »

Microsoft
MAXIMIZE YOUR STORAGE.
LEARN MORE »
Windows Server 2012
BUILT FROM THE CLOUD UP.

MOST POPULAR - TECHNOLOGY

E-MAILED | BLOGGED | VIEWED

1. Bits: Disruptions: Helper Robots Are Steered, Tentatively, to Care for the Aging
2. Yahoo to Buy Tumblr for $1.1 Billion
3. App Smart: Swipe Away Photo Imperfections on a Smartphone
4. Tool Kit: Keeping Wi-Fi Always Within Range
5. Tech Industry Pushes to Amend Immigration Bill
6. Gadgetwise: App Smart Extra: Apps for Editing Photos
7. Tool Kit: Outsmarting Smartphone Thieves
8. Bits: At Google Conference, Cameras Even in the Bathroom

121

Impacts sur les victimes

122

Who are the victims?

Young people: 20-40 represent 50% of cases
(Federal Trade Commission, 2011)

- Less vigilant (SNS, etc.)
- Overuse of online services

High incomes: (Dupont, 2008)

- Use financial services more often
- Hackers want to maximise their gain

123
123

Impact on victims

- Financial impact
- Legal impact: crime committed on their behalf
- Psychological impact: 50% of the victims do not know how the data were stolen
- (Non)Impact on the behaviour:
  - Victims remain just equally vulnerable and ineffective in securing their personal information online (Ponemon Institute, 2012)
  - Only 8% are more careful and aware (PrinceMarket, 2012)

124
124

Quand la victime devient “coupable”

- Outre les conséquences dramatiques que ces fraudes à l’identité peuvent entraîner, il appartient à **la victime de démontrer son innocence à défaut de prouver la culpabilité de l’usurpateur.**

- Certaines victimes se retrouvent embourbées dans une cascade d’ennuis sans réussir à convaincre l’administration de leur véritable identité. Un enfer qui **dure parfois des années sans véritable recours juridique.**

125

Regrets on Twitter and Facebook

- Do not think about their reason for posting or consequences of their posts
- Misjudge the culture and norms within their social circles
- “Hot” state of high emotion when posting
- Postings are seen by an unintended audience
- Do not foresee how posts could be perceived by people within their intended audience
- Misunderstand or misuse the social network platform

126

"I read my Twitter the next morning and was astonished" A Conversational Perspective on Twitter Regrets

Manya Sleeper*, Justin Cranshaw*, Patrick Gage Kelley†, Blase Ur*,
Alessandro Acquisti*, Lorrie Faith Cranor*, Norman Sadeh*

*Carnegie Mellon University
{msleeper, jcransh, bur, acquisti, lorrie, sadeh}@cmu.edu

†University of New Mexico
pgk@unm.edu

ABSTRACT

We present the results of an online survey of 1,221 Twitter users, comparing messages individuals regretted either saying during in-person conversations or posting on Twitter. Participants generally reported similar types of regrets in person and on Twitter. In particular, they often regretted messages that were critical of others. However, regretted messages that were cathartic/expressive or revealed too much information were reported at a higher rate for Twitter. Regretted messages on Twitter also reached broader audiences. In addition, we found that participants who posted on Twitter became aware of, and tried to repair, regret more slowly than those reporting in-person regrets. From this comparison of Twitter and in-person regrets, we provide preliminary ideas for tools to help Twitter users avoid and cope with regret.

Author Keywords

Twitter; regrets; messaging; conversation; survey

Thus it is worthwhile to investigate regret both on Twitter and for in-person conversations. Past studies of in-person regret have identified factors that lead to regret, methods for becoming aware of regret, and strategies for repairing harm [8, 15, 16]. However, Twitter presents different features and limitations than offline conversation. Beyond offering wider audiences and increased message persistence, Twitter lacks face-to-face channels, such as body language, for transmitting apologies or indicating offense.

We explore regretted messages Twitter users posted on Twitter or said during in-person conversations. We aim to improve understanding of regrets on Twitter by comparing them with in-person regrets. By examining these regrets, as well as how people became aware of regrets in person and on Twitter, we also identify preliminary design directions for preventing and ameliorating regrets on Twitter.

Specifically, we examine four research questions:

Technological solutions

Anti-spam filters: more efficient (rules-based filtering, statistical content analysis, etc.)

Anti-virus software

Intrusion detection systems

Biometric authentication

Cryptographic methods: mails, etc.

Privacy Enhanced Technologies (P.E.T.s)

Browsing anonymously: Mixnet, TOR

128

128

Privacy Enhanced technologies

PETs for Anonymisation

(Goldschlag *et al.*, 1996; Reiter and Rubin, 1998; Sweeney, 2002; Dingledine *et al.*, 2004 Machanavajjhala et al., 2006; M. Atzori, Pedreschi, 2005;)

PETs for Identity Management

(Brands 2002, Herzberg and Mass, 2004; Chaum, 1992, 1986, Cameron and Jones, 2007).

PETs for Data Processing

(Agrawal and Srikant, 2000; Evfimevski et al., 2003; Chen and Liu, 2005; Kargupta et al., 2003; Pinkas, 2002, Gambs et al, 2007; Du et al., 2004;Yang et al., 2004; Jacquemont et al., 2006; Matwin et al., 2005; Cuzzocrea et al., 2008; Fung et al., 2007; Zheleva and Getoor, 2007; Domingo-Ferrer, 2007).

129

PETs for Anonymisation

Some anonymous Communication Techniques

First generation Onion Routing (Goldschlag et al., 1996)

Crowds (Reiter and Rubin, 1998)

Hordes (Levine and Shields, 2002)

TOR (Dingledine, 2004)

130

Re-identification

Linkage (Sweeney, 2000)

Merge two databases to find common information

Inference (Acquisti and Gross, 2009)

deduce new information from other information (e.g. guess the person's tastes from their habits).

131

Homogeneity (Machanavajjhala et al, 2006)

showing a subject's belonging to a homogeneous group in order to deduce all, or part of his or her identity

(e.g. anonymous users are classified into groups according to their age)

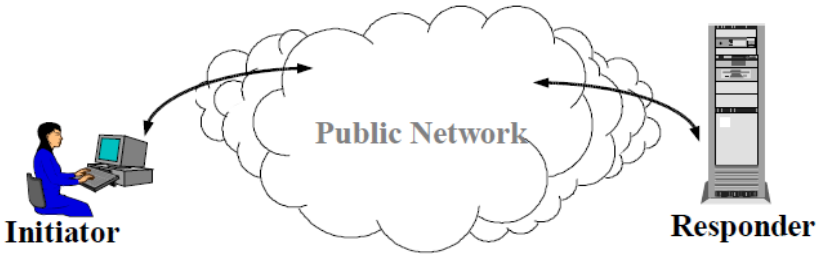
Graphs and machine learning (Narayanan and Shmatikov, 2009) An algorithm uses the structure of social networks, that is to say, relations between users

(e.g. the "follow" relationships on Twitter, "friend" on Facebook).

132

Public Networks are Vulnerable to Traffic Analysis

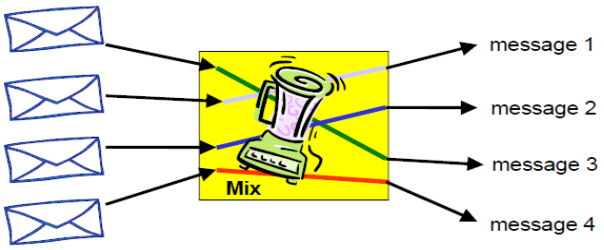
- In a Public Network (Internet):
- Packet (message) headers identify recipients
- Packet routes can be tracked



Encryption does *not* hide routing information.

MIXNET

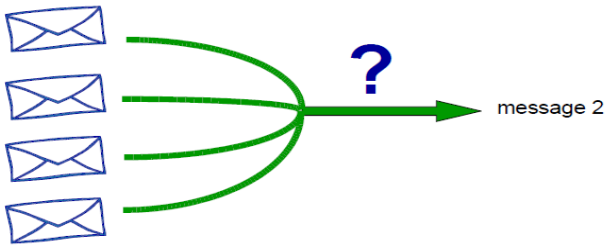
What does a mix do?



Randomly permutes and decrypts inputs

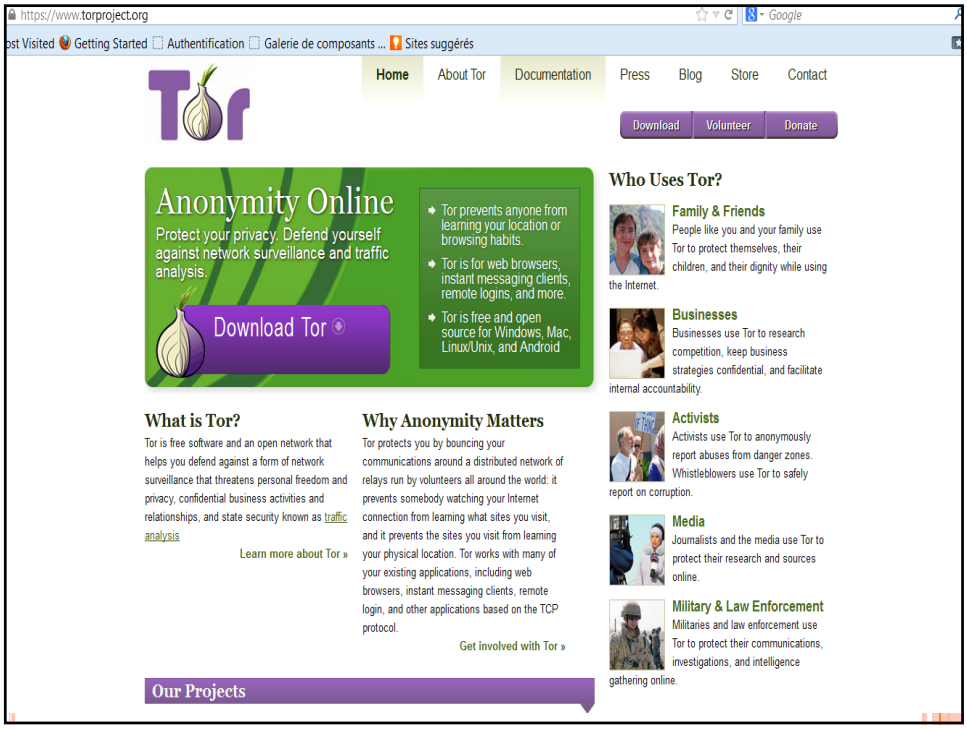
134

What does a mix do?



Key property: Adversary can't tell which ciphertext corresponds to a given message

135



Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.

Tor (The Onion Router) is free software for enabling online anonymity.

137

Why we need Tor

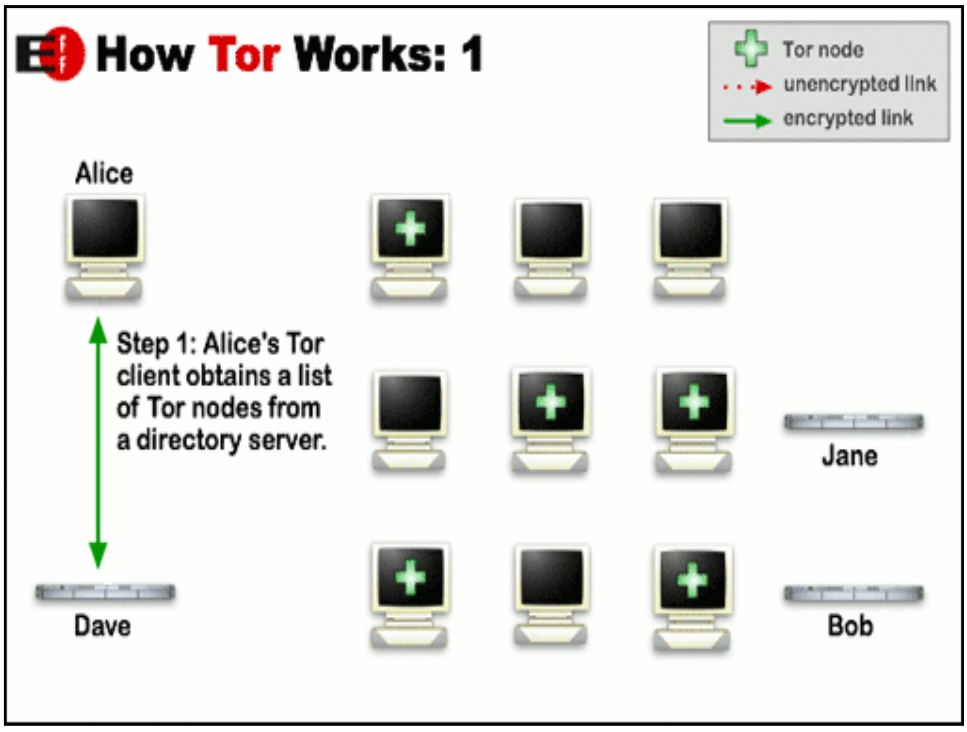
- Using Tor protects you against traffic analysis can be used to infer who is talking to whom over a public network.
- Knowing the source and destination of your Internet traffic allows others to track your behavior and interests.
- This can impact your checkbook if, for example, an e-commerce site uses price discrimination based on your country or institution of origin. It can even threaten your job and physical safety by revealing who and where you are.
- For example, if you're travelling abroad and you connect to your employer's computers to check or send mail, you can inadvertently reveal your national origin and professional affiliation to anyone observing the network, even if the connection is encrypted.

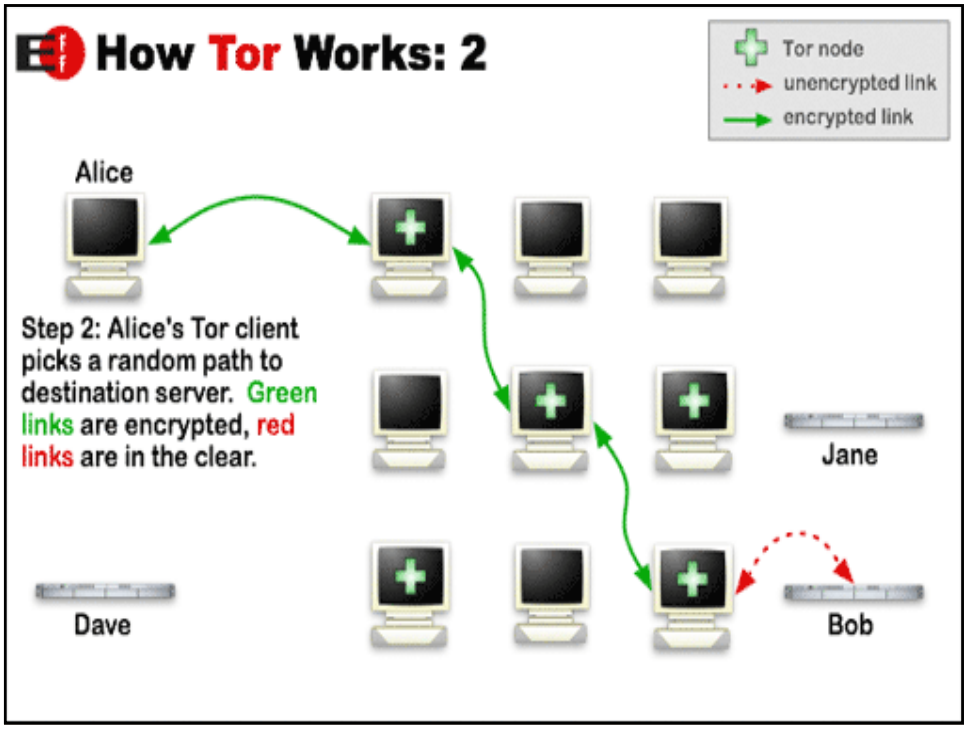
138

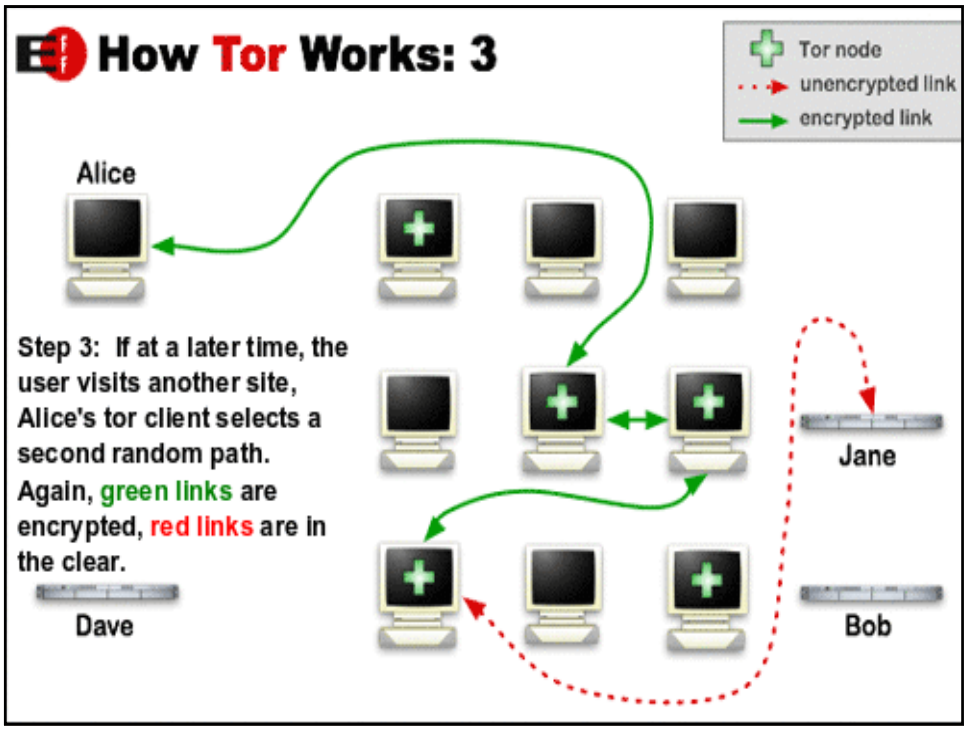
How does traffic analysis work?

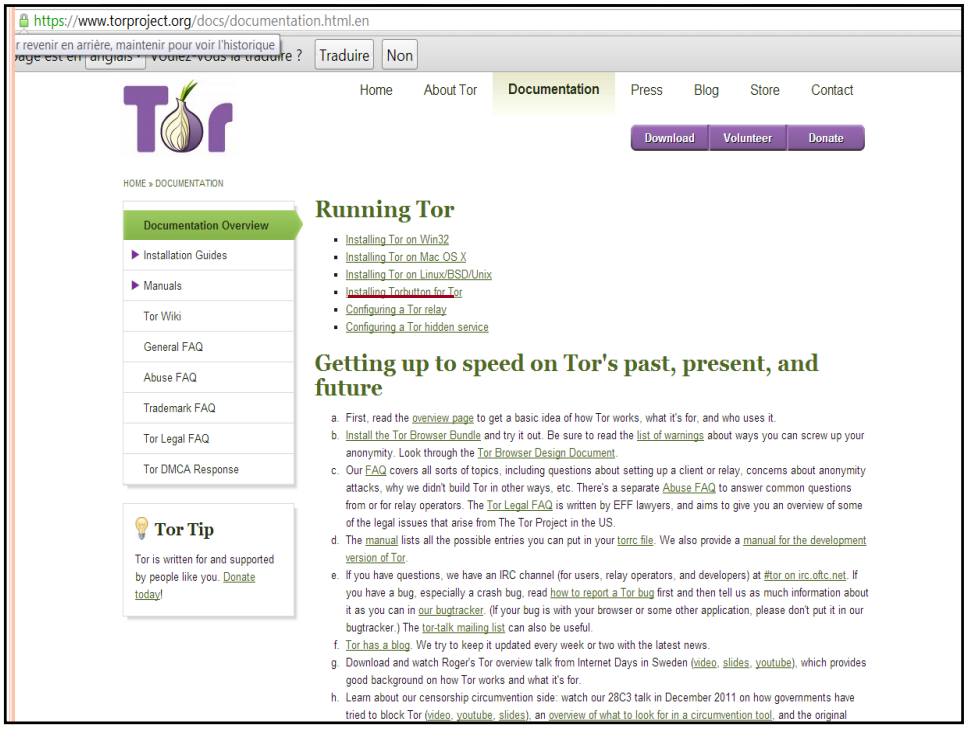
- Internet data packets have two parts: a **data payload and a header** used for routing. The data payload is whatever is being sent, whether that's an email message, a web page, or an audio file.
- Even if you encrypt the data payload of your communications, traffic analysis still reveals a great deal about what you're doing and, possibly, what you're saying. That's because it focuses on the **header, which discloses source, destination, size, timing, and so on.**
- So can authorized intermediaries like Internet service providers, and sometimes unauthorized intermediaries as well. A very simple form of traffic analysis might involve sitting somewhere between sender and recipient on the network, looking at headers.

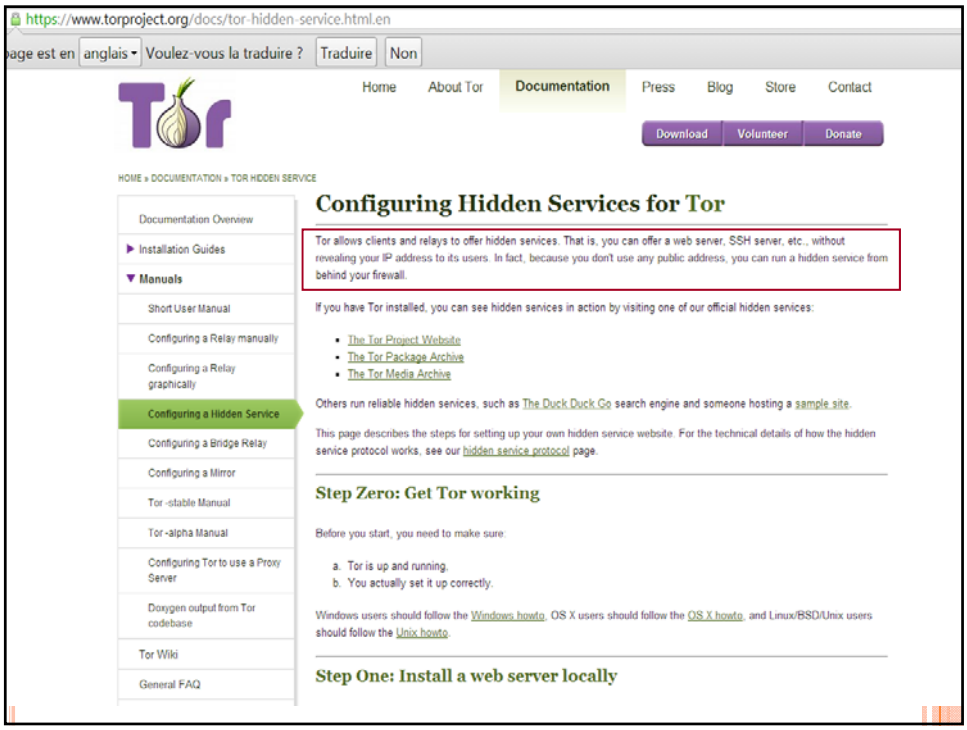
139




How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

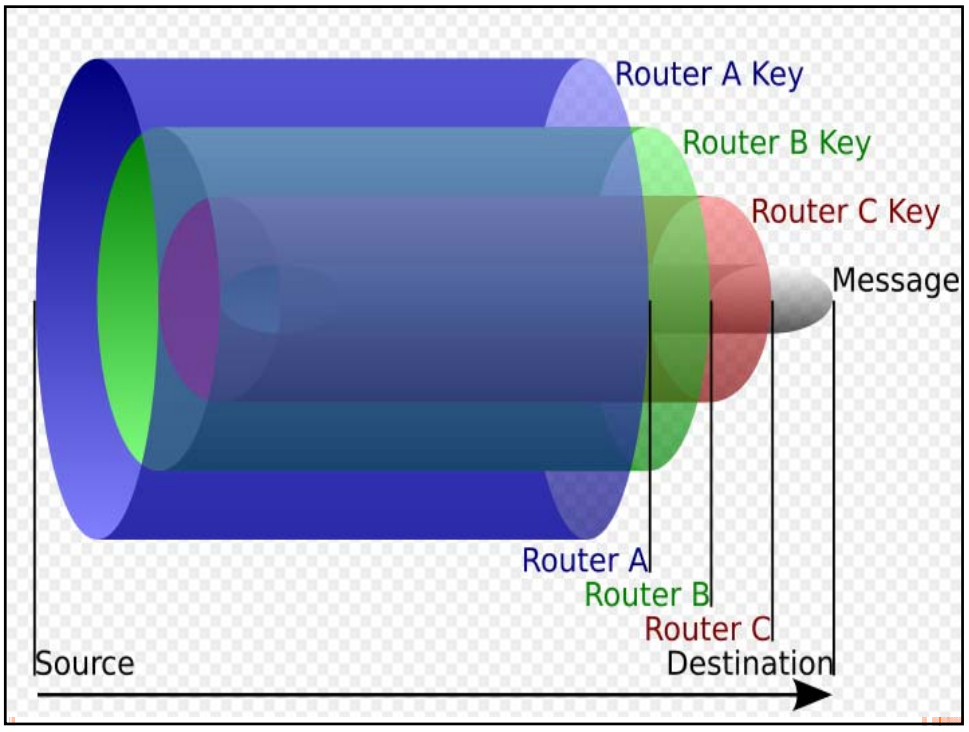

https://www.torproject.org/docs/documentation.html.en
Traduire
Non
Home
About Tor
Documentation
Press
Blog
Store
Contact
Download
Volunteer
Donate
HOME » DOCUMENTATION
Documentation Overview
Installation Guides
Manuals
Tor Wiki
General FAQ
Abuse FAQ
Trademark FAQ
Tor Legal FAQ
Tor DMCA Response
Tor Tip
Tor is written for and supported by people like you. Donate today!
Running Tor
Installing Tor on Win32
Installing Tor on Mac OS X
Installing Tor on Linux/BSD/Unix
Installing Torbutton for Tor
Configuring a Tor relay
Configuring a Tor hidden service
Getting up to speed on Tor's past, present, and future
a. First, read the overview page to get a basic idea of how Tor works, what it's for, and who uses it.
b. Install the Tor Browser Bundle and try it out. Be sure to read the list of warnings about ways you can screw up your anonymity. Look through the Tor Browser Design Document.
c. Our FAQ covers all sorts of topics, including questions about setting up a client or relay, concerns about anonymity attacks, why we didn't build Tor in other ways, etc. There's a separate Abuse FAQ to answer common questions from or for relay operators. The Tor Legal FAQ is written by EFF lawyers, and aims to give you an overview of some of the legal issues that arise from The Tor Project in the US.
d. The manual lists all the possible entries you can put in your torrc file. We also provide a manual for the development version of Tor.
e. If you have questions, we have an IRC channel (for users, relay operators, and developers) at #tor on irc.oftc.net. If you have a bug, especially a crash bug, read how to report a Tor bug first and then tell us as much information about it as you can in our bugtracker. (If your bug is with your browser or some other application, please don't put it in our bugtracker.) The tor-talk mailing list can also be useful.
f. Tor has a blog. We try to keep it updated every week or two with the latest news.
g. Download and watch Roger's Tor overview talk from Internet Days in Sweden (video, slides, youtube), which provides good background on how Tor works and what it's for.
h. Learn about our censorship circumvention side: watch our 28C3 talk in December 2011 on how governments have tried to block Tor (video, youtube, slides), an overview of what to look for in a circumvention tool, and the original


https://www.torproject.org/docs/tor-hidden-service.html.en
anglais
Voulez-vous la traduire ?
Traduire
Non
Home
About Tor
Documentation
Press
Blog
Store
Contact
Download
Volunteer
Donate
HOME » DOCUMENTATION » TOR HIDDEN SERVICE
Documentation Overview
Installation Guides
Manuals
Short User Manual
Configuring a Relay manually
Configuring a Relay graphically
Configuring a Hidden Service
Configuring a Bridge Relay
Configuring a Mirror
Tor -stable Manual
Tor -alpha Manual
Configuring Tor to use a Proxy Server
Doxygen output from Tor codebase
Tor Wiki
General FAQ
Configuring Hidden Services for Tor
Tor allows clients and relays to offer hidden services. That is, you can offer a web server, SSH server, etc., without revealing your IP address to its users. In fact, because you don't use any public address, you can run a hidden service from behind your firewall.
If you have Tor installed, you can see hidden services in action by visiting one of our official hidden services:
The Tor Project Website
The Tor Package Archive
The Tor Media Archive
Others run reliable hidden services, such as The Duck Duck Go search engine and someone hosting a sample site.
This page describes the steps for setting up your own hidden service website. For the technical details of how the hidden service protocol works, see our hidden service protocol page.
Step Zero: Get Tor working
Before you start, you need to make sure:
a. Tor is up and running.
b. You actually set it up correctly.
Windows users should follow the Windows howto. OS X users should follow the OS X howto, and Linux/BSD/Unix users should follow the Unix howto.
Step One: Install a web server locally

Onion Routing

- "Onion Routing" refers to the layers of the encryption used.
- The original data, including its destination, are encrypted and re-encrypted multiple times, and sent through a virtual circuit comprising successive, randomly selected Tor relays.
- Each relay decrypts a "layer" of encryption to reveal only the next relay in the circuit in order to pass the remaining encrypted data on to it.
- The final relay decrypts the last layer of encryption and sends the original data, without revealing or even knowing its sender, to the destination.

145



PLAN

- Introduction vie privée
- Domaines de collecte des données
- Perte de données
- Techniques
- Vol identité et Reconstitution de profils
- **Recommandations**

147

Utiliser des “Passphrase” faciles à mémoriser

- Mardi matin j’ai donné une présentation à l’université à 9 h 30
- Première lettre de chaque mot et le mot ne doit pas figurer dans le dictionnaire
- MMjdupau930??

148

Effacer ses traces

En effaçant régulièrement les traces stockées sur son ordinateur tel que le cache du navigateur web et cookies.

En demandant l'application de son droit de rectification et du droit à l'oubli auprès de l'entreprise qui stocke ses traces.

En limitant les traces qu'on laisse par l'utilisation de technologies respectueuses de la vie privée tel que anonymisateurs et réseaux de communication anonyme.

En noyant vos traces dans du bruit.
Exemple : génération de milliers de page web comportant des informations anodines.

149

Lisez attentivement les politiques de vie privée des sites que vous visitez

POLITIQUES DE VIE PRIVÉE

1. Les usagers ne lisent pas les politiques de vie privée

2. Ils ne comprennent pas le contenu

3. Manque d'expertise => difficulté de prendre une décision

4. Décisions biaisées à cause de la difficulté du processus decisionnel

151

Quelques recommandations pour les réseaux sociaux

- ✓ Ne pas diffuser d'informations sensibles
- ✓ Vérifier régulièrement ses paramètres de confidentialité
- ✓ Ne pas utiliser ou ponctuellement la géolocalisation (désactiver le GPS de son smartphone)
- ✓ Rester discret sur ses activités professionnelles
- ✓ Respecter ses obligations vis à vis de son employeur
- ✓ Faire preuve de réserve dans ses opinions et croyances (religieuses, philosophiques ou politiques)
- ✓ Utiliser avec beaucoup de précaution la fonction "j'aime" permettant également d'integrer un goupe

152

Getting Started | Authentification | Galerie de composants ... | Sites suggérés

KrebsonSecurity
In-depth security news and investigation

21 Privacy 101: Skype Leaks Your Location

MAR 13

The events of the past week reminded me of a privacy topic I've been meaning to revisit: That voice-over-IP telephony service **Skype** constantly exposes your Internet address to the entire world, and that there are now numerous free and commercial tools that can be used to link Skype user account names to numeric Internet addresses.

The fact that Skype betrays its users' online location information is hardly news. For example, *The Wall Street Journal* and other news outlets warned last year about research showing that it was possible to coax Skype into revealing the IP addresses of individual Skype users. But I believe most Skype users still have no clue about this basic privacy weakness.

A Skype resolver service in action.

What's changed is that over the past year, a number of services have emerged to help snoops

www.skype.com/en/legal/privacy/?intsrc=client-_-windows-_-6.3-_-go-privacy#collectedInformation

1. WHAT INFORMATION DOES SKYPE COLLECT AND USE?

Skype may gather and use information about you, including (but not limited to) information in the following categories:

(a) Identification data (e.g. name, username, address, telephone number, mobile number, email address);

(b) Profile information (e.g. age, gender, country of residence, language preference and any information that you choose to make available to others as part of your Skype user profile as further described in Section 6);

(c) Electronic identification data (e.g. IP addresses, cookies);

(d) Banking and payment information (e.g. credit card information, account number);

(e) Call quality and survey results;

(f) Information about your usage of and interaction with Skype software, products, and websites (including computer, platform, device and connection information, client performance information, error reports, device capability, bandwidth, statistics on page views, and traffic to and from our websites, browser type and Skype WiFi enabled hotspot detection and usage statistics;

(g) Products or services ordered and delivered;

(h) The URL of videos that you have selected to appear in your mood message;

(i) Skype test calls made to ECHO123 (which are recorded and played back to the user and deleted thereafter);

(j) List of your contacts and related data (we will give you a choice as to whether you want Skype to use contact lists from other services to populate your Skype contacts);

(k) Your username and password for other email accounts where you have provided this to us and requested us to search for your friends on Skype (please note that Skype does not retain this information after completing the search or use it for any other purpose);

(m) Traffic data (data processed for the purpose of the conveyance of communications or the billing thereof, including, but not limited to, the duration of the call, the number calling and the number called); and

(n) Content of instant messaging communications, voicemails, and video messages (please see section 12);

(o) Location information, derived from your mobile carrier or from the mobile device that you use. In connection with the Qik products, you control when your location is shared with others. Your location is displayed and shared with other Qik users only in accordance with your privacy settings. You also may create location information by "geo-tagging" your submitted content with location information. Please manage your privacy settings for location information carefully;

(p) Mobile device information, such as manufacturer's name, device model number, operating system, carrier network;

(q) Location information and device identifiers, derived from your device, when you search for or connect to a Skype WiFi compatible hotspot. This information may be used to improve detection of eligibility to connect using Skype WiFi and for the purposes of offering, providing and marketing Skype WiFi to you;

(r) Access tokens for other accounts you associate with your Skype account (such as Microsoft account or Facebook), which are like an electronic key provided by the service that acts in place of a password for authentication.

Publié le 27 février 2013 à 05h00 | Mis à jour le 27 février 2013 à 13h46

Médias sociaux et réputation: les entreprises appelées à la vigilance

Les entreprises n'ont plus le choix et doivent se doter d'une politique de gestion des risques à l'égard de la réputation, d'une politique portant sur les réseaux sociaux ainsi qu'une réglementation interne sur l'utilisation des médias sociaux.

QUAND VOTRE SYNDICAT S'INVITE DANS VOTRE E-REPUTATION

Le blog d'un des syndicats de l'entreprise est placé en deuxième position sur Google lorsque l'on fait une recherche sur elle.

L'algorithme Google valorise les blogs qui sont très actifs. Les syndicats alimentaient très régulièrement leur blog ce qui leur confère une certaine « puissance ».

Il faut développer les relations presse en ligne, ne pas hésiter à créer des sous-sites sur des thématiques importantes pour l'entreprise, de produire du contenu régulièrement

Est-ce grave pour l'image de l'entreprise ?

Oui parce que ce n'est pas l'information la plus pertinente pour un client, un fournisseur ou à un banquier. Il serait préférable que ces personnes découvrent d'abord votre expertise, avant un article relatant avec virulence la fermeture d'une de vos usines en 2006 lorsque votre société faisait face à des difficultés financières.

Ce n'est pas tant que le contenu en lui-même qui pose problème, que son ordre d'apparition et l'absence de contre-argumentaire.

158

Deux conseils très importants

Evitez d'employer directement la voie juridique contre les personnes concernées, car cela peut être mal perçu par les salariés et *certains n'ont pas toujours conscience de l'impact de ce qu'ils écrivent*. Prenez le temps d'expliquer l'impact que certaines déclarations publiques peuvent avoir sur l'activité de l'entreprise et l'emploi.

N'attendez pas trop avant de réagir, il existe de nombreux vides juridiques sur ces questions et les délais de prescription pour diffamation sont de 3 mois après la première publication.

159

Quelques conseils pour surveiller et gérer votre réputation sur internet

- Vérifier sur Google ce qui apparaît en saisissant votre nom et celui de votre entreprise
- Surveiller ce qui se dit sur votre entreprise (google alerte)
- Distinguer vie personnelle et vie professionnelle
- Respecter la confidentialité de vos données professionnelles (données clients, fournisseurs...)
- Se construire une présence numérique professionnelle (création d'un site web, blog, présence sur les réseaux sociaux, forums,…)

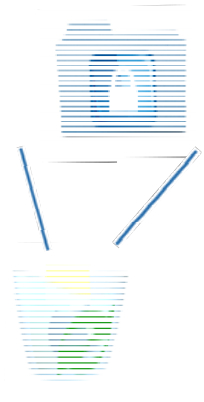
160

Deux solutions en cas d'atteinte à la réputation

- Une demande de retrait du contenu par lettre recommandée à l'hébergeur du site. Cette technique s'avère généralement assez efficace.
- Procéder au « noyage » des propos malveillants par la création de contenus. Cette action vise à rendre peu visibles les informations gênantes (repoussées en page 3 ou en page 4 des moteurs de recherche) noyées par des contenus positifs ou neutres.

161

Même vos poubelles peuvent contenir de l'information personnelle !!!



Service	Trusted ID	ProtectMyID	Lifelock	ID Watchdog	IDENTITY GUARD®
Website Screenshot					
Overview	Our Pick	Trusted Service	Popular	Recovery	Feature packed
Credit Monitoring	Yes	Yes	No	No	Yes
Credit Reports	3	1	No	No	3
Credit Score	No	No	No	No	Yes
Internet Monitoring	Yes	Yes	Yes	Yes	Yes
Getting Reports	Mail / Email	Email / Online	Mail / Email / Online	Email / Online	Email / Online
Public Records Monitoring	Yes	No	Yes	Yes	Yes
Software Solutions	Yes	No	No	No	Yes
Lost Wallet Service	Yes	Yes	Yes	No	Yes
Resolution Service	Yes – in-house	Yes – in-house	Yes	Yes	Yes
Insurance or Guarantee	$1 Million Warranty	$1 Million Insurance	$1 Million Guarantee	100% Recovery	$1 Million Insurance
Our Review	Most purchased family and individual plans. They offer a wealth of features for the cheapest price. Full Review	Although new to the ID theft scene, Experian created an effective, cheap id theft and credit monitoring service. Full Review	Well-known for their commercials. Offers effective fraud protection and monitoring services. Full Review	Advertises itself as a comprehensive identity theft solution. Expensive for the features they provide. Full Review	Offers the most protection features, however they cost more. Also offers Internet protection and software. Full Review
Trial Period	14 Days	1 Month ($1)	None	None	1 Month
Price (w/ discount)	$7.01/mo View Offer	$11.65/mo View Offer	$9/mo View Offer	$19.95/mo View Offer	$17.99/mo View Offer

- **Scroogle** was a web service that allowed users to perform Google searches anonymously. It focused heavily on searcher privacy by blocking Google cookies and not saving log files.
- The service was launched in 2003 by Daniel Brandt. After 2005, the service encountered rapid growth before running into a series of problems starting in 2010.
- In February 2012, the service was permanently shut down by its creator due to a combination of throttling of search requests by Google and a denial-of-service attack by an unknown person or group.

165

Tweet preservation at Library of Congress

The Library's primary mission is research and it receives copies of every book, pamphlet, map, print, and piece of music registered in the United States.

It's very exciting that tweets are becoming part of history.

Only after a six-month delay can the Tweets be used for internal library use, for non-commercial research, public display by the library itself, and preservation.

166

What should vulnerable users do?

167

PREVENTION

- Pay attention to waste: shred all documents from sensitive institutions (bank, government), use the recycling industry specializing in old electronic devices
- Prevention among young people (students):
  - 40% leave their room unlocked
  - 9% share passwords online (IdTheftSecurity)

169

PREVENTION (CONTINUED)

- Online:
  - An antivirus is necessary but not sufficient
  - Avoid opening suspect attachments
  - Secure WiFi access point
  - Avoid installing SNS extra applications
  - Control cookies, browse anonymously
  - Use strong encryption
- Monitor your bank accounts regularly
- "Google" your name regularly or use services like ReputationDefender to take care of your e-reputation

170

PREVENTION (CONTINUED)

- Use tools that seek data leak prevention such as Proofpoint.com, CodegreenNetwork.com, Reconnex.com Verdasys.com, etc.
- Develop prevention campaigns to raise awareness
- In case of identity theft:
  - Alert the banks and credit agencies to block the accounts.
  - File a report with a anti fraud centre such as phonebuster.
  - Complain to the police.

171

INSURANCE

(http://identity-theft-protection-services-review.toptenreviews.com/)

172

Privacy by Design

Ann Cavoukian (Assistant Privacy Commissioner of Ontario): to take the problem of privacy into account from the outset when designing systems, and not as an afterthought.

- Proactive anonymisation of data within the institutions
- Impossibility to find correlations between different sources of information
- Difficult compromise between transparency of institutions and privacy of individuals

173

Prevention: some recommendations from Javelin 2013 and Symantec 2014 reports

- Install mobile software only from trusted sources and official app stores.
- Make sure all operating systems are the latest versions.
- Install or enable a passcode lock on your smartphone.
- Do not reveal sensitive or personal information on SNS Facebook, Flickr, Tumblr, LinkedIn, MySpace, Google+ and Twitter.
- Use and recognize secure websites. Look for the padlock symbol and an “s” after the “http” in your browser’s address bar.
- Avoid accessing websites that display personal or account information using unsecured Wi-Fi connections (cafes, public libraries, or airports).
- Turn off Bluetooth and Wi-Fi when they are not being used.

Prevention: some recommendations from Javelin 2013 and Symantec 2014 reports (continued)

- Watch out for email and attachments from convincing imitations of banks, card companies, charities and government agencies.
- Do not click on embedded links in any email or SMS.
- Avoid re-using same passwords (change them every 90 days).
- Do not access unsecure websites or type in PII using public Wi-Fi on mobile devices, laptops or computers.
- Wipe clean electronic devices, such as smartphones, tablets and computers, before disposing of, turning in or selling them.
- Stay Safe Offline.
- Shred paper documents that contain sensitive information

Prevention: some recommendations from Javelin 2013 and Symantec 2014 reports (continued)

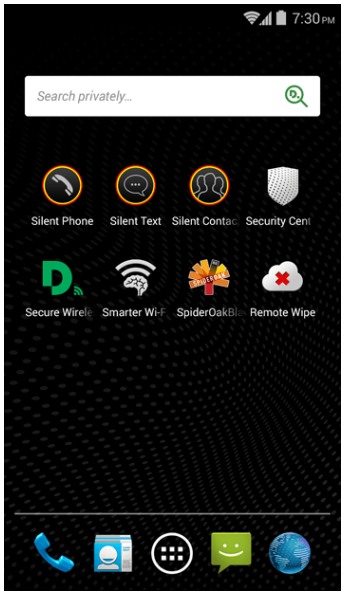
- Restrict email attachments (block or remove .VBS, .BAT, .EXE, .PIF, .SCR files)
- Use reputation tools for files or websites
- Be wary of scareware tactics (infected computers)
- Be aware of sharing files on public sites (gaming, bitTorrent, P2P exchanges)
- Keep Dropbox and Evernote to a minimum for pertinent information only
- Avoid Shopping online or banking from public computers (libraries, Internet cafes, or unencrypted Wi-fi connections)
- Configure your home, Wi-fi network for strong authentication (require a unique password)

OUTLINE

- Introduction about privacy
- Internet data collection techniques
- Identity theft
- Privacy Enhanced Technologies
- Re-identification
- Legal issues
- Recommendations
- **Challenges and Future Trends**

WEB CLEANER

BLACK PHONE



EPHEMERAL APPS

Ephemeral messaging apps such as Snapchat, Wickr and Frankly, advertise that your photo, message or update will only be accessible for a short period, are on the rise.

Snapchat and Frankly claim they permanently delete messages, photos and videos after 10 seconds. After that, there's no record.

CHALLENGES

(SYMANTEC CORPORATION, 2014)

Public: **insatiable appetite** for personal lifestyle apps.

Traditional malware threats **« ported»** to mobile devices

Internet of Things (TVs, telephones, security cameras, baby monitors, wearable technology, motor cars …) next battleground in the threat landscape

DATA DEALER

Data Dealer, the gleefully sarcastic game about data privacy

"Privacy? Screw that. Turn the tables! Become a data dealer and get all the dirty details on your friends, neighbors and the rest of the world. Learn how to trick your users and make cash out of their personal info! Legal? Illegal? Whatever."

DATA DEALER

Data Dealer is an online game about collecting and selling personal data - full of irony and gleeful sarcasm.

It is a browser/serious/edu/impact game about digital culture and surveillance and aims to raise awareness about online privacy in a new and fun way. The English version was released in May 2013. It is also available on Facebook!.

OPEN DATA

the Open data" movement will lead to the release of a huge amount of dataset

"Ethical Hacker": Job with a Future?

Ethical hackers are working at improving cyber security.
Their technique: they put themselves in the shoes of a hacker in order to assess the vulnerability of companies when attacked from the outside.
As the Internet grows, the need for security increases. *Ethical Hackers: a job with a future!*

185

Conclusion

- ✓Une formation à la sensibilisation des menaces à l'attention des utilisateurs
- ✓Faire de la veille technologique
- ✓Se doter d'un "data privacy officer"
- ✓La protection de la vie privée doit constituer un choix par défaut plutôt qu'un ajout effectué pendant ou après le processus d'élaboration: *Privacy by design*
- ✓*Opt in au lieu de Opt out*
- ✓*Ne pas oublier que rien ne s'efface !*

186

Merci pour votre Attention !

Professeur Esma Aïmeur

Université de Montréal

Email : aimeur@iro.umontreal.ca

http://www.iro.umontreal.ca/~aimeur

187