



FORUM CYBERSECURITE

*C'est quoi la Sécurité des Systèmes
d'Information / Cybersécurité ?*

Mercredi 3 Mars 2021

Lycée Bellepierre

Matthieu DRUILHE / Président CLUSIR-ROI / RSSI&DPD

Présentation



- Matthieu DRUILHE
- D.U. Ingénierie des Réseaux et Télécommunications
- Management des Opérations
- RSSI depuis 2007 et DPD depuis le 25 Mai 2018
- Parenthèse « Responsable des Infrastructures »
- Président























C'est quoi la cybersécurité ?

- A) Le sujet principal de la dernière série à la mode sur votre plateforme préférée de vidéo à la demande souveraine.
- B) Un enjeu de société à l'ère du « tout-dématérialisé ».
- C) Une piste à étudier pour votre avenir ?
- D) Le bon dosage de mesures de sécurité technique/organisationnelle/juridique adapté au besoin.

PREAMBULE

clario.

The companies that know most about you

#	Company	% of personal data collected	Email	Name	Age	Gender	Sexual	Marital	Race	Religious	Live Loc	Home A	Employ	Job Title	Pet/Anim	Mobile	Landline	Type of	Hobbies	Interest	Height	Weight	Next of	Mother	Current	Past Em	Bank Ac	Salary	Social P	Social P	Social P	Country	Allergie	Health &
1	 Facebook	70.59%	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			•		•	•			•	•	•			
2	 Instagram	58.82%	•	•	•	•					•	•	•	•	•	•		•	•	•	•	•			•	•			•	•	•			
3	 Tinder	55.88%	•	•	•	•	•	•			•		•	•	•	•		•	•	•	•					•		•	•	•	•			
4	 Grindr	52.94%	•	•	•	•	•	•			•		•	•	•	•		•	•	•	•							•	•	•	•			
5	 Uber	52.94%	•	•	•	•					•	•	•	•		•	•	•	•	•					•	•		•	•	•	•			
6	 Strava	41.18%	•	•	•	•					•	•				•		•			•	•				•		•	•	•	•			
7	 Tesco	38.24%	•	•	•	•		•				•				•	•	•								•		•	•	•	•			
8	 Spotify	35.29%	•	•	•							•				•	•	•		•						•		•	•	•	•			
9	 MyFitnessPal	35.29%	•	•	•							•				•	•	•			•	•				•							•	
10	 Jet2	35.29%	•	•	•	•		•	•			•				•	•	•								•							•	
11	 Credit Karma	32.35%	•	•	•								•	•		•		•		•	•					•	•							
12	 Lidl Plus	32.35%	•	•	•						•	•			•	•	•	•								•								•
13	 Netflix	26.47%	•	•	•							•				•	•	•		•						•								
14	 Nike	26.47%	•	•	•	•						•						•			•	•				•								
15	 Asos	26.47%	•	•	•							•				•		•			•	•				•								
16	 Depop	26.47%	•	•	•							•				•		•			•	•				•								
17	 Ryanair	26.47%	•	•	•							•				•	•	•								•							•	
18	 Ocado	26.47%	•	•	•							•				•	•	•								•								•
19	 Airbnb	26.47%	•	•	•	•						•			•	•		•								•								
20	 American Airlines	26.47%	•	•	•							•				•	•	•								•								•

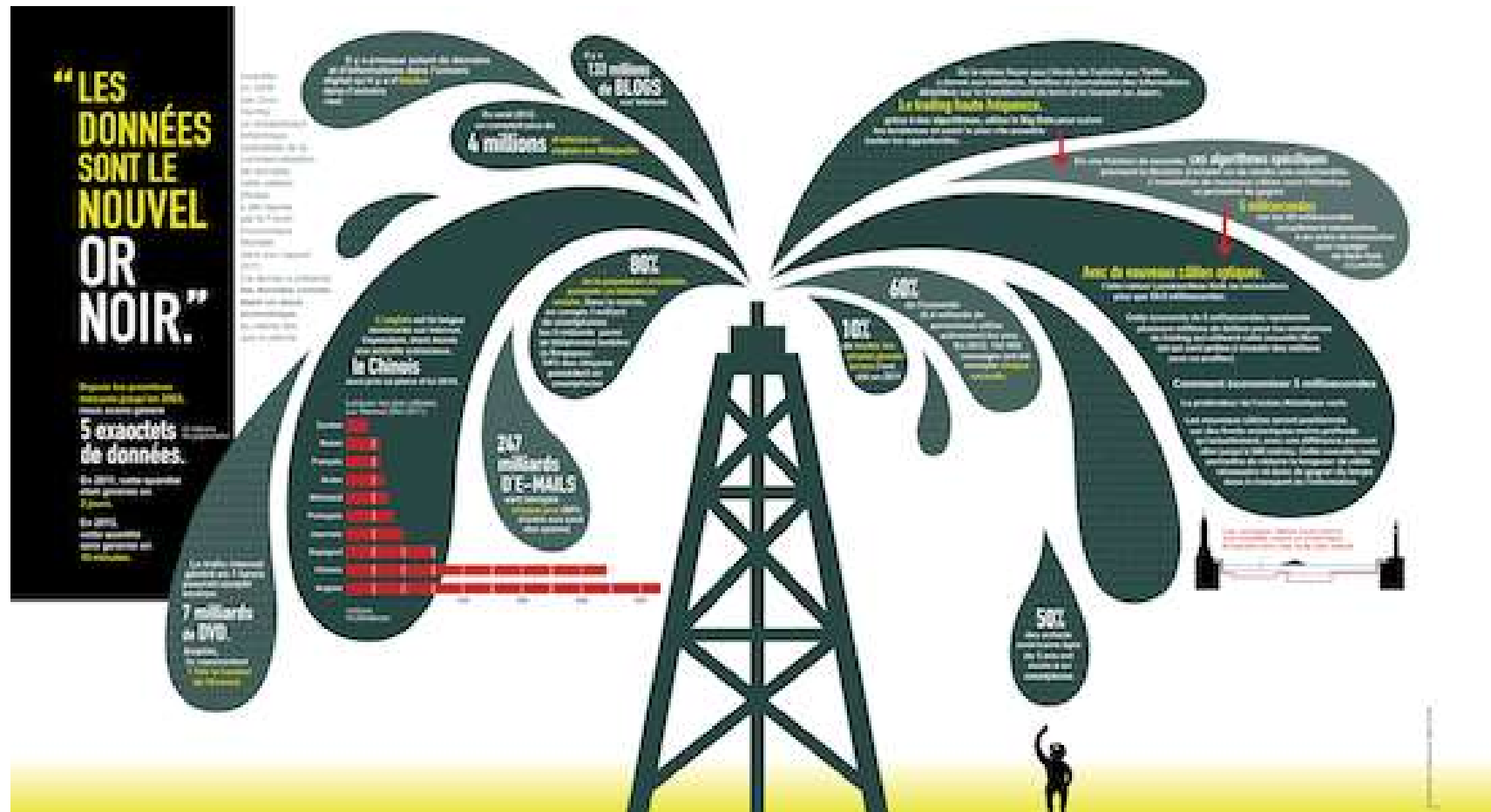
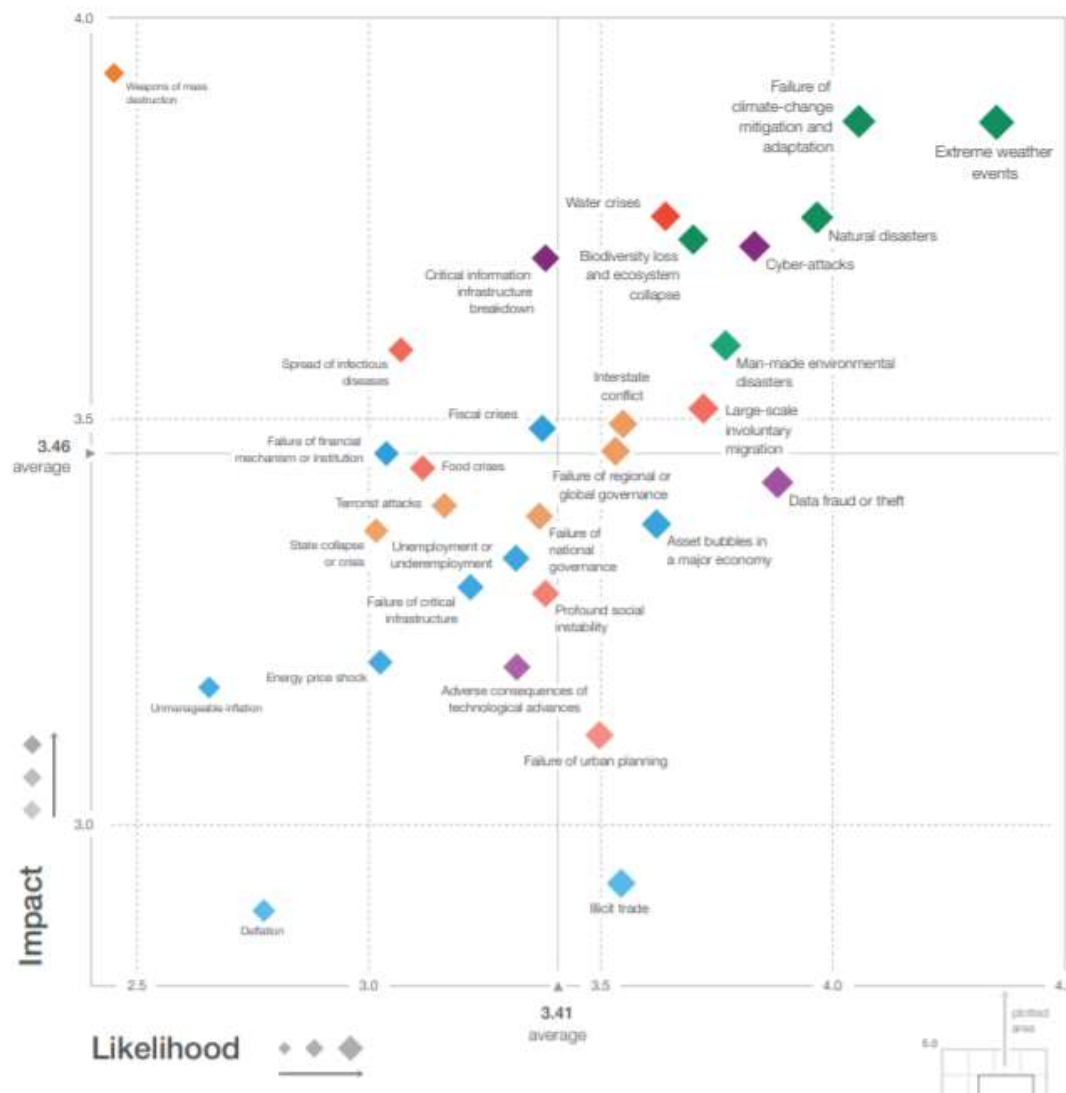


Figure I: The Global Risks Landscape 2019



The Global Risks Report 2019

14th Edition

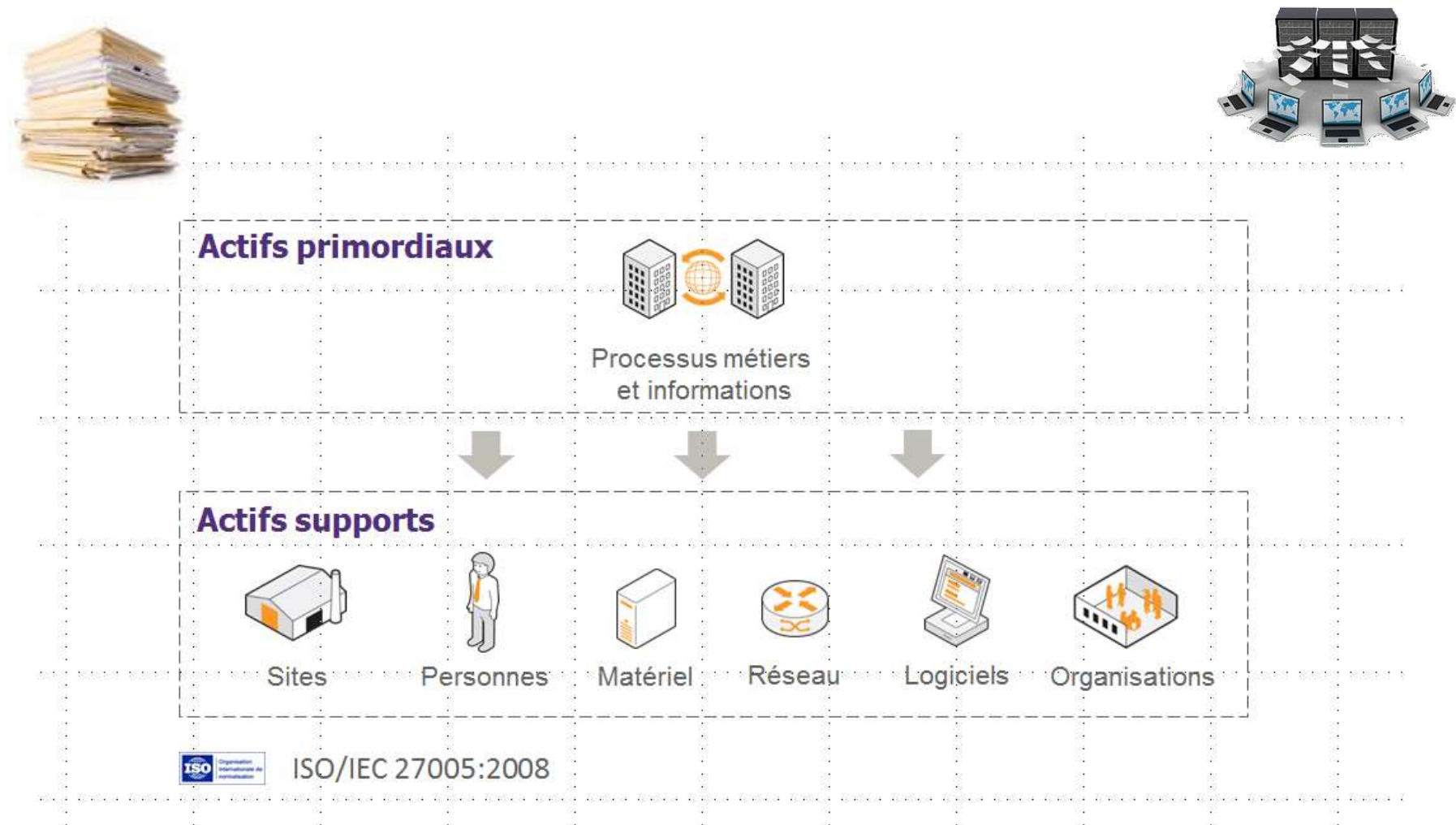
WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

KéZaKo ?

un système d'information ?

Un système d'information est constitué d'



The logo for KéZaKo? is displayed in a playful, rounded font. Each letter is a different color: 'K' is orange, 'é' is red, 'Z' is purple, 'a' is blue, 'K' is green, 'o' is yellow, and the question mark is grey.

la sécurité d'un système
d'information ?

Les critères de sécurité : de quoi parle t'on ?

- La SSI recouvre l'ensemble des moyens techniques et organisationnels pour garantir, **au juste niveau requis**, la sécurité des informations

24H/24HJ



7J//7J

Disponibilité



Intégrité



Confidentialité

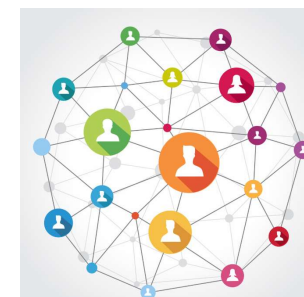
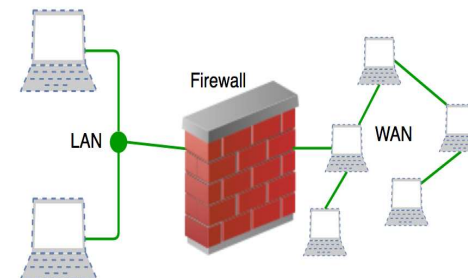


Tracabilité

les mesures de sécurité « traditionnelles » :



les mesures de sécurité « numériques » :



CONTEXTE

Exigences, contexte et enjeux



Pourquoi faire de la protection des données ?



RGPD

Genèse et évolution



10 chapitres
99 articles
173 considérants



A+2
M+9
J+9

1978

**Loi Informatique
Et Libertés et CNIL**

1995

Directive 95/46/CE

2004

**Loi Informatique
Et Libertés modifiée**

2016

Loi République Numérique et RGPD

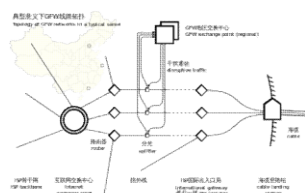
2018

Application du RGPD

1974

Révélation sur SAFARI

Le Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus désignait un projet d'interconnexion des fichiers nominatifs de l'administration française, notamment par le biais du numéro INSEE. Le projet est révélé le 21 mars 1974 par le quotidien *Le Monde*, dans l'article intitulé «SAFARI ou la chasse aux Français de Philippe Boucher»



Champ d'application

- 1 Un **traitement** de **données personnelles** ...
- 2 ...effectués par un **RT** ou un **ST**...



établie sur le
territoire de l'UE
**critères de
l'établissement**

ou

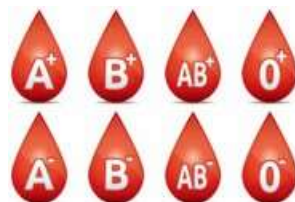
visant des
résidents de l'UE
critères du ciblage



C'est quoi une donnée personnelle ?



- **Définition** : Toute information identifiant **directement** ou **indirectement** une personne physique



Relevé d'Identité Bancaire				
Code Banque	Code Guichet	Numéro de compte	Clé RIB	Domiciliation
12345	12345	1234567891A	12	Banque-ville-agence
IBAN FR00 1234 5123 4512 3456 7891 A12				
BIC ABCDEFGH				
Titulaire Monsieur ou Madame Jean NEAUE				



C'est quoi un traitement de données personnelles ?



- **Définition** : Tout opération ou tout ensemble d'opérations effectués **ou non** à l'aide de procédés automatisés et appliqués à des **données** ou des **ensembles de données à caractère personnel**.
- **Précisions** : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction



IMPORTANT

Chaque manipulation de données est un traitement !

Les données sensibles



La conformité

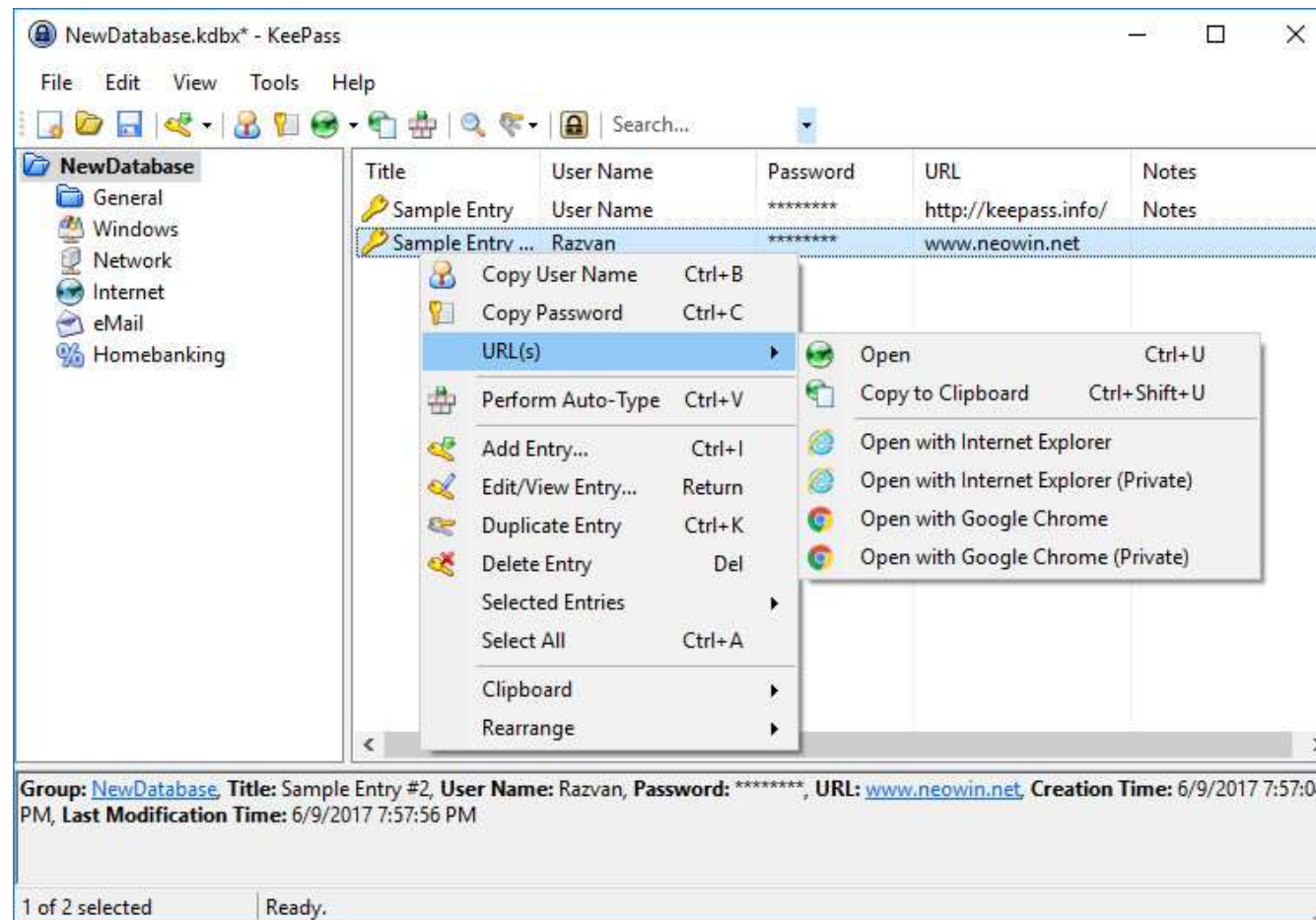


Bonnes pratiques

Hygiène et prophylaxie



De l'utilité d'un coffre fort sécurisé



<https://keepass.info/>

HaveUbeenpwned?

The screenshot shows the Have I Been Pwned website interface. At the top is a dark navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below this is a large blue banner with the text "';--have i been pwned?" and a subtext "Check if you have an account that has been compromised in a data breach". A search bar contains a blurred domain name followed by ".com" and a "pwned?" button. The results section, on a dark red background, states "Oh no — pwned!" and "Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)". It includes links for "Notify me when I get pwned" and "Donate". Below this is a section titled "Breaches you were pwned in" with a definition of a breach. Two breaches are listed: Dropbox (mid-2012) and Last.fm (March 2012). At the bottom, a dark bar displays statistics: 233 pwned websites, 4,729,225,727 pwned accounts, 54,390 pastes, and 51,474,803 paste accounts.

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

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

.com pwned?

Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)

Notify me when I get pwned Donate

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

lost.fm: In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.

Compromised data: Email addresses, Passwords, Usernames, Website activity

233 pwned websites

4,729,225,727 pwned accounts

54,390 pastes

51,474,803 paste accounts

<https://haveibeenpwned.com/>

Alors, c'est quoi la cybersécurité ?

- A) Le sujet principal de la dernière série à la mode sur votre plateforme préférée de vidéo à la demande souveraine.
- B) Un enjeu de société à l'ère du « tout-dématérialisé ».
- C) Une piste à étudier pour votre avenir ?
- D) Le bon dosage de mesures de sécurité technique/organisationnelle/juridique adapté au besoin.

Pour aller plus loin

- MOOC CNIL : <https://atelier-rgpd.cnil.fr>
- MOOC ANSSI : <https://secnumacademie.gouv.fr/>
- Assistance et prévention du risque numérique :
 - <https://www.cybermalveillance.gouv.fr/> et kit de sensibilisation
<https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/>
- Vérifier si votre adresse courriel ou les adresses de votre organisation (macollectivite.re) ont fait l'objet d'une fuite de données :
<https://haveibeenpwned.com>
- Cahier de vacances pour les enfants : <https://securitytuesday.com/wp-content/uploads/2018/10/ISSA.Cahier.SecNum777.pdf>



« Les tuiles qui protègent de la pluie ont toutes été posées par beau temps »

Proverbe chinois

VOS QUESTIONS ?



MERCI
POUR VOTRE
ATTENTION

KeepCalmAndPassion.com



: CLUSIR ROI



<http://clusir-roi.org/>