

Annexes

1. Exemples de stratégie de réponse

Réponse initiale > Instructions > Conseils pour protéger ses identifiants

There are also several important steps that you can take to ensure that your data on any site, including Evernote, is secure:

- Avoid using simple passwords based on dictionary words
- Never use the same password on multiple sites or services
- Never click on 'reset password' requests in emails — instead go directly to the service

Evernote, 2013

La sécurité de votre compte est extrêmement importante pour nous et nous prenons toutes les mesures nécessaires afin d'identifier les failles éventuelles et y remédier. C'est pourquoi, par précaution, nous conseillons vivement à tous nos partenaires et utilisateurs de réinitialiser dès à présent leurs mots de passe. Lors de la saisie d'un nouveau mot de passe, nous recommandons d'utiliser au minimum huit caractères, d'éviter les mots de passe les plus évidents (ex: mot de passe1234) et de ne pas utiliser le même mot de passe sur plusieurs sites.

Dailymotion, 2016

At the same time, we strongly recommend you improve your online safety by setting a unique password for each website you use. Though it's easy to reuse the same password on different websites, this means if any one site is compromised, all your accounts are at risk. Tools like [1Password](#) can help you manage strong passwords across multiple sites.

Dropbox, 2012

We encourage our users to visit our [Safety Center page](#) for recommendations on how to stay secure online. Some important recommendations we're re-emphasizing today include the following:

- Change your passwords and security questions and answers for any other accounts on which you used the same or similar information used for your Yahoo account;
- Review all of your accounts for suspicious activity;
- Be cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information;
- Avoid clicking on links or downloading attachments from suspicious emails; and
- Consider using [Yahoo Account Key](#), a simple authentication tool that eliminates the need to use a password on Yahoo altogether.

Yahoo, 2016

[Réponse initiale](#) > [Instructions](#) > [Ingénierie sociale](#)

Nous vous rappelons donc les règles de sécurité que nous appliquons toujours :

- Nous ne vous adresserons jamais un e-mail mentionnant toute information confidentielle, mot de passe, coordonnées bancaires (cartes ou RIB), adresse postale...

Mediapart, 2013

Les intrusions de ce type servent principalement au « phishing ». Cette technique consiste à se faire passer pour des organismes officiels ou des entreprises et à utiliser des informations partielles vous concernant pour tenter de récupérer auprès de vous des informations plus sensibles.

C'est pourquoi nous vous invitons à la plus grande prudence en cas de sollicitation douteuse par email, sms, ou téléphone.

Pour en savoir plus sur le phishing, n'hésitez pas à consulter [l'assistance en ligne](#) sur orange.fr.

Orange, 2014

Réponse initiale > Instructions > Énumération des faits

Les faits se sont déroulés de la façon suivante :

16h05 : diffusion du premier faux communiqué aux rédactions.

16h06-16h07 : les agences Bloomberg et Dow Jones reprennent des éléments du faux communiqué.

A partir de 16h10 : le porte-parole du Groupe dément les fausses informations auprès des agences de presse. Ce démenti officiel est immédiatement repris par les agences.

16h15 : la cotation est suspendue après une baisse de plus de 18% du cours de bourse.

16h19 : la cotation de l'action reprend et le cours remonte à un niveau proche quoique inférieur à celui constaté avant la diffusion du premier faux communiqué.

16h27 : diffusion du deuxième faux communiqué de démenti partiel.

16h49 : VINCI publie un démenti écrit sur son site internet.

17h02 : diffusion du démenti écrit (à l'AMF, aux marchés financiers, à la presse).

17h15 : le directeur juridique du Groupe appelle l'AMF.

17h35 : diffusion du troisième et dernier faux communiqué de « pseudo-revendication ».

Vinci, 2016

Réponse initiale > Adaptation de l'information > Confiance des clients

At Albertsons, nothing is more important to us than your trust. Our team works hard to earn that trust through offering great value, service and quality products.

Albertsons, 2014

Information security and customer data protection are of paramount importance to eBay Inc., and eBay regrets any inconvenience or concern that this password reset may cause our customers. We know our customers trust us with their information, and we take seriously our commitment to maintaining a safe, secure and trusted global marketplace.

Ebay, 2014

To our loyal Neiman Marcus Group customers:

As the investigation into our cyber security incident continues, I want to provide you with an update. Your trust in us is our absolute priority.

Neiman Marcus, 2013

Consistent with our "Love It or Return It" policy, customer confidence and security remain our priority. As a result, we encourage any customer who is concerned about the security of their payment cards to call our Customer Service Hotline at 1-866-234-9442, so that we can assist them in addressing any potential concerns. Information will also be available on sallybeautyholdings.com. Sally Beauty will, as appropriate, provide updates as we learn more from our investigation.

Customer service is our top priority at Sally Beauty, and we will be responding to customer needs concerning this security incident.

Sally Beauty, 2015

Réponse initiale > Adaptation de l'information > Collaboration avec des experts

Safeguarding your personal information is important to us. We took immediate steps to remediate this security issue upon identifying it, and we are being assisted by outside cybersecurity experts. We have reported this issue to our credit card payment processor. We have also contacted and offered our full cooperation to federal law enforcement.

Acer, 2015

Law enforcement was immediately notified. Computer experts immediately began assisting us in determining the outside source of the issue and bringing our systems back online.

Centre médical presbytérien d'Hollywood, 2016

TORONTO, July 20, 2015 /PRNewswire/ -- We were recently made aware of an attempt by an unauthorized party to gain access to our systems. We immediately launched a thorough investigation utilizing leading forensics experts and other security professionals to determine the origin, nature, and scope of this incident.

Ashley Madison, 2015

Déni

- Pas de communication (silence)
- Nier l'existence d'une crise
- Nier ses responsabilités par rapport à la crise
- Nier ses responsabilités et désigner d'autres responsables

Recent news articles claiming that Dropbox was hacked aren't true. Your stuff is safe. The usernames and passwords referenced in these articles were stolen from unrelated services, not Dropbox.

Dropbox, 2014

« On ne communique pas sur le sujet »,
explique-t-on chez OVH où l'on se
retranche derrière les tweets du fondateur
de l'entreprise, Octave Klaba. **« Il informe
les clients qu'il se passe des choses. »**
Seul élément concret lâché par la société :
« On a l'infrastructure qui tient. »

OVH, 2013

Projet latéral

- Déplacer la communication vers un autre sujet
- Accepter certaines responsabilités mais impliquer d'autres responsables
- Accepter certaines responsabilités mais avec circonstances atténuantes
- Se positionner en tant que victime

Les cyber-attaques font malheureusement partie des tristes réalités du monde professionnel d'aujourd'hui. Étant donné le profil de nos produits et leur popularité, nous sommes devenus une cible privilégiée pour les pirates. Notre équipe en charge de la sécurité a récemment détecté sur notre réseau des attaques sophistiquées portant sur l'accès illégal aux informations de nos clients, ainsi qu'au code source de nombreux produits Adobe. Nous pensons que ces attaques pourraient être liées.

Adobe, 2013

We apologize for this unprovoked and criminal intrusion into our customers' information. The current business world has proven to be one in which no company's online assets are safe from cyber-vandalism, with Avid Life Media being only the latest among many companies to have been attacked, despite investing in the latest privacy and security technologies.

Ashley Madison, 2015

This attack has opened up an important conversation about internet security and volatility. Not only has it highlighted vulnerabilities in the security of "Internet of Things" (IOT) devices that need to be addressed, but it has also sparked further dialogue in the internet infrastructure community about the future of the internet. As we have in the past, we look forward to contributing to that dialogue.

Dyn, 2016

What happened?

Our company recently discovered a cyberattack that comprised a small number of employee log in credentials, allowing unauthorized access to eBay's corporate network.

Ebay, 2014

As recent events with other large services have demonstrated, this type of activity is becoming more common.

Evernote, 2013

The unauthorized access was in an isolated incident over a limited period of time. It included access to a server that contained personal information for consumers who applied for T-Mobile USA postpaid services between Sept. 1, 2013 and Sept. 16, 2015.

Experian, 2013

Hacking Team was the victim of a criminal act or acts sometime before July 6.

Hacking Team, 2015

As previously disclosed, the malware used in the attack had not been seen in any prior attacks and was designed to evade detection by antivirus software, according to Home Depot's security partners.

Home Depot, 2014

Based on the forensic investigation to date, no personal information, no debit card PIN numbers, no email addresses and no social security numbers were obtained by those criminally responsible. There is also no evidence that kmart.com customers were impacted.

Kmart, 2014

Ce vol de données confidentielles est, a priori, sans conséquence, la possession d'un RIB n'exposant pas aux mêmes possibilités de fraude qu'un numéro de carte de crédit.

Mediapart, 2013

As always, we want you to feel confident shopping at Neiman Marcus. What I said in my prior message to you remains the same: there is **NO** indication

- that Social Security numbers and birth dates were compromised
- that our Neiman Marcus cards have been used fraudulently
- that any online customers were impacted
- that any PINs were at risk since we do not use PIN pads in our stores

Neiman Marcus, 2013

However, since Telegram is based on phone contacts, any party can potentially check whether a phone number is registered in the system. This is also true for any other contact-based messaging app (WhatsApp, Messenger, etc.).

Telegram, 2016

As a precaution, we are alerting you that your Twitter account is one of a small group of accounts that may have been targeted by state-sponsored actors.

Twitter, 2015

It is important to note that our customer database does not contain any credit card information and VTech does not process nor store any customer credit card data on the Learning Lodge website. To complete the payment or check-out process of any downloads made on the Learning Lodge website, our customers are directed to a secure, third party payment gateway.

In addition, our customer database does not contain any personal identification data (such as ID card numbers, Social Security numbers or driving license numbers).

VTech, 2015

Reconnaissance < Accepter toutes les responsabilités et présenter ses excuses

We sincerely apologize for any inconvenience this may cause our members and customers.

Kmart, 2014

Nous vous présentons toutes nos excuses pour cette attaque que nous n'avons pas réussi à parer dans l'instant. [REDACTED]

Mediapart, 2013

Reconstruction

- Rappeler ses bonnes actions
- Dédommagement des victimes
- Prévention (mesures pour éviter que cela se reproduise)

What measures has Deutsche Telekom taken?

Firstly, we have applied filter measures in the network to prevent the remote maintenance interface from being accessed by the attackers in order to exclude a new infection of devices. In parallel, experts from the router manufacturers have begun developing software updates, and their installation on the affected routers began yesterday afternoon. We could already see signs of a clear stabilization during the course of yesterday morning, so our measures have taken effect. We also had to check whether or not all router types that were not affected were perhaps infected with malware. The fact that they were working was no proof of being free of malware.

Deutsche Telekom, 2016

Keeping Dropbox secure is at the heart of what we do, and we're taking steps to improve the safety of your Dropbox even if your password is stolen, including:

- [Two-factor authentication](#), a way to optionally require two proofs of identity (such as your password and a temporary code sent to your phone) when signing in. (Coming in a few weeks)
- New automated mechanisms to help identify suspicious activity. We'll continue to add more of these over time.
- A [new page](#) that lets you examine all active logins to your account.
- In some cases, we may require you to change your password. (For example, if it's commonly used or hasn't been changed in a long time)

Dropbox, 2012

Q: What are you doing to prevent this from happening again?

A: Experian is committed to building customers for life and is working tirelessly to improve our security systems and processes. We have taken immediate steps to harden our environment. To ensure our security measures and practices stand up to the high standards to which we hold ourselves.

Experian, 2013

The Home Depot is offering free identity protection services, including credit monitoring, to any customer who used a payment card at a Home Depot store in 2014, from April on. Customers who wish to take advantage of these services can learn more at www.homedepot.com or by calling 1-800-HOMEDEPOT (800-466-3337). Customers in Canada can call 800-668-2266.

Home Depot, 2014

LinkedIn a pris des mesures importantes depuis 2012 pour renforcer la sécurité des comptes. Nous avons ajouté des couches de protection supplémentaires au stockage des mots de passe et offrons la possibilité à nos membres d'activer la vérification en deux étapes pour plus de sécurité.

Linkedin, 2012

Mr. Rubin added, "Throughout our 40-year history, our customers have always been our number one priority and we deeply regret any inconvenience this may cause. The privacy and security of our customers' information is of critical importance to us and we are focused on addressing this issue."

Michaels store, 2013

As part of the major site re-launch in the summer of 2013, Myspace took significant steps to strengthen account security. The compromised data is related to the period before those measures were implemented. We are currently utilizing advanced protocols including double salted hashes (random data that is used as an additional input to a one-way function that "hashes" a password or passphrase) to store passwords. Myspace has taken additional security steps in light of the recent report.

MySpace, 2013

For over a century, our company's mission has been dedicated to delivering exceptional service to each of our customers, and responding properly to this attack is our top priority. Our goal is to do everything possible to restore your trust and to earn your loyalty.

Neiman Marcus, 2013

SOE will grant customers 30 days of additional time on their subscriptions, in addition to compensating them one day for each day the system is down. It is also in the process of outlining a "make good" plan for its PlayStation®3 MMOs (DC Universe Online and Free Realms). More information will be released this week.

Sony, 2011

Nous avons pris des dispositions pour renforcer nos systèmes de sécurité et pour nous aider à vous protéger ainsi que vos données – et nous continuerons de le faire. Nous prendrons d'autres dispositions dans les jours à venir pour améliorer la sécurité de nos utilisateurs.

Spotify, 2014

As a result, and in light of Staples' commitment to protecting its customers, Staples is offering free identity protection services, including credit monitoring, identity theft insurance, and a free credit report, to customers who used a payment card at any of the affected stores during the relevant time periods. Additional information about the incident, including dates of potential access and how to sign up for free credit monitoring, can be found at <http://staples.newsha.businesswire.com/statement>.

Staples, 2014

We understand that a situation like this creates stress and anxiety about the safety of your payment card data at Target. Our brand has been built on a 50-year foundation of trust with our guests, and we want to assure you that the cause of this issue has been addressed and you can shop with confidence at Target.

Target, 2013

For extra assurance, we will offer free credit monitoring services for everyone impacted. We'll be in touch with you soon on how and where to access the service.

Target, 2013

I understand that this will have caused some concern and inconvenience for our customers and for that I sincerely apologise.

understand that our customers will be concerned about this issue and I would like to apologise for this and any inconvenience this has caused.

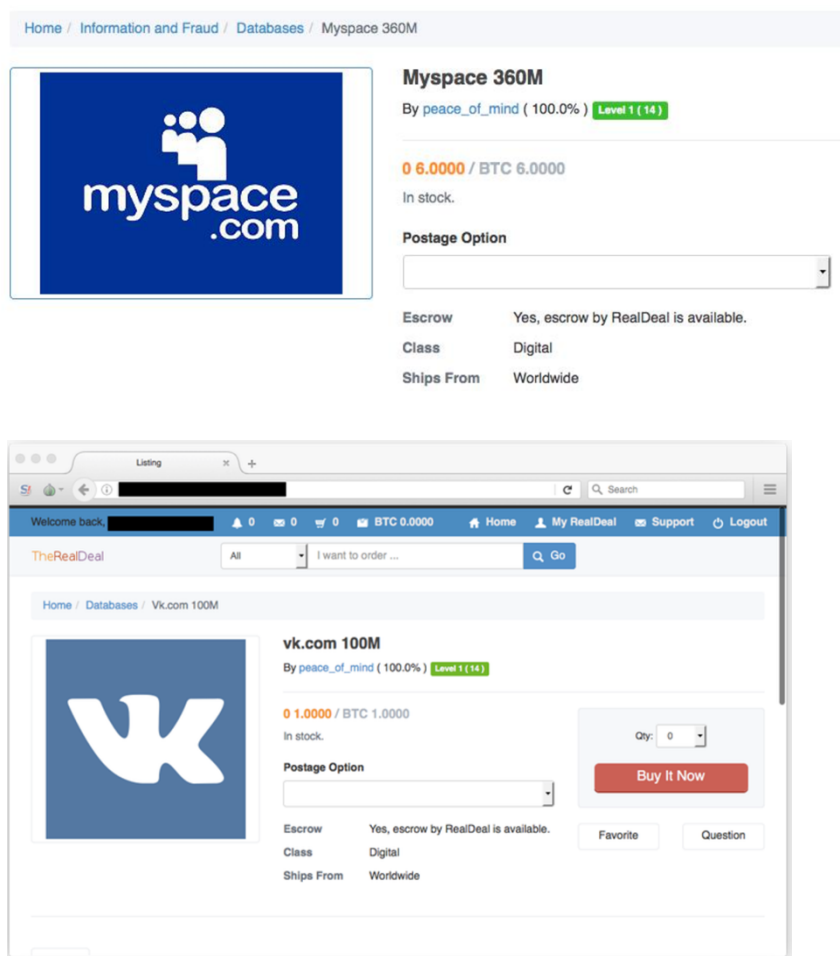
Three Mobile, 2016

We are offering **one year of complimentary fraud resolution and identity protection services**, to all affected cardholders. Enrollment information and additional information are on our website (<http://www.whitelodging.com/about/payment-card-issues>).

White Lodging, 2013

b) Vol de données

Une fois les données dérobées à une organisation, elles sont généralement revendues sur un marché parallèle. Le site spécialisé dans ce type de vente s'appelle TheRealDeal. Les images ci-dessous sont des captures d'écran d'annonces de la vente de données volées. Il s'agit des cas de MySpace¹ et de VK.com². Ici aussi, la monnaie utilisée est une crypto-monnaie, le bitcoin. Actuellement, un bitcoin vaut 2.000€ mais son cours varie.³



¹ https://motherboard.vice.com/en_us/article/427-million-myspace-passwords-emails-data-breach

² https://motherboard.vice.com/en_us/article/another-day-another-hack-100-million-accounts-for-vk-russias-facebook

³ <https://bitcoin.fr/cours-du-bitcoin/>

Parmi les données généralement volées, les mots de passe ne sont pas épargnés. Ils peuvent permettre à des personnes malveillantes de prendre le contrôle des comptes des internautes concernés. Régulièrement, les individus utilisent le même mot de passe pour tous leurs comptes et il n'est que faiblement sophistiqué. Voici une liste des mots de passe les plus fréquemment volés lors du piratage de VK.com⁴ et de MySpace⁵ (voir ci-dessous).

Rank	Password	Frequency
1	123456	709,067
2	123456789	416,591
3	qwerty	291,645
4	111111	189,151
5	1234567890	156,614
6	1234567	141,620
7	12345678	107,799
8	123321	93,048
9	000000	91,981
10	123123	89,461
11	777777	87,022

Rank	Password	Frequency
1	homelesspa	855,478
2	password1	585,503
3	abc123	569,825
4	123456	487,945
5	myspace1	276,915
6	123456a	244,641
7	123456789	191,016
8	a123456	165,132
9	123abc	159,700
10	(POSSIBLY INVALID)	158,462
11	qwerty1	141,110
12	passer2009	130,740
13	fuckyou1	125,302
14	iloveyou1	123,668

c) Usurpation d'identité

Ce type de cyberhacking se manifeste sous différentes formes. Ci-dessous, il s'agit d'un exemple de phishing ayant visé les clients de Colruyt. Un autre type d'usurpation d'identité est la publication de faux tweets sur le compte d'Auchan.



⁴ <http://thehackernews.com/2016/06/vk-com-data-breach.html>

⁵ https://motherboard.vice.com/en_us/article/427-million-myspace-passwords-emails-data-breach

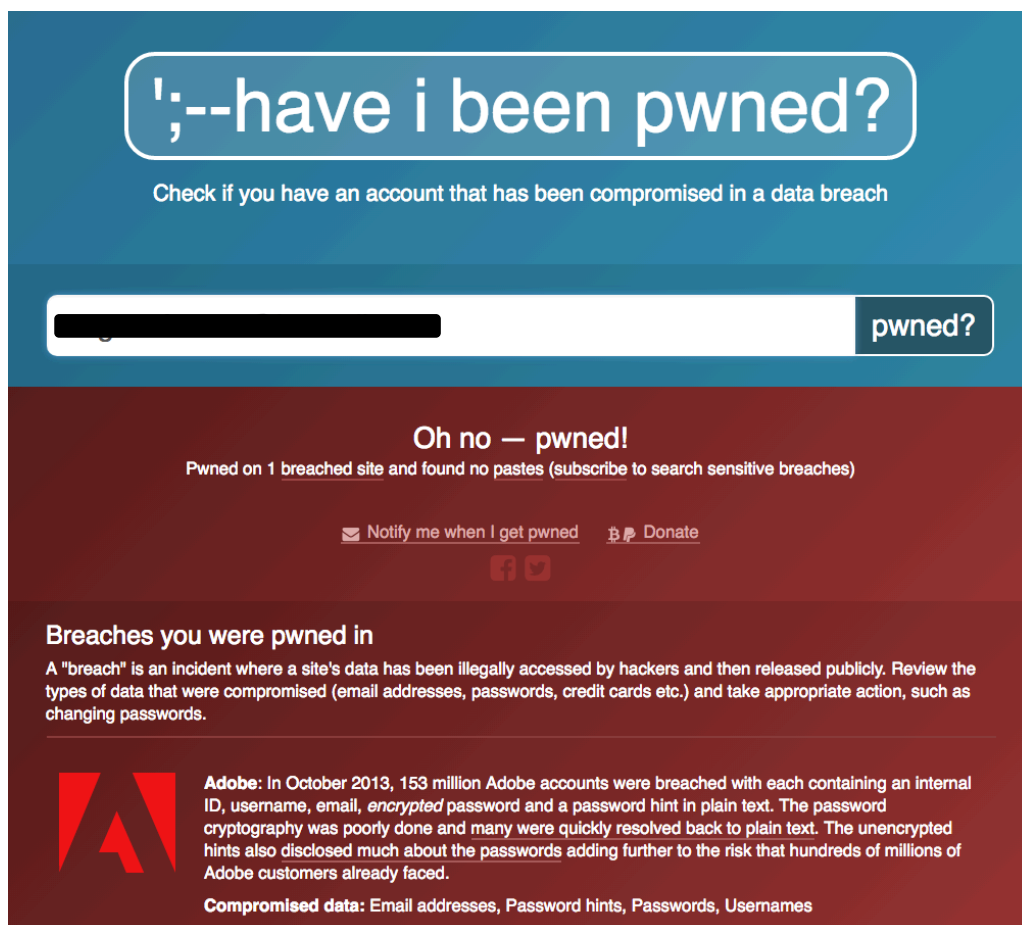


d) Défaçage

Le défaçage consiste généralement à détourner un site web, comme ce fut par exemple le cas du site de la Malaysia Airlines. Le groupe de hackers Lizard Squad a affiché cette page indiquant « 404 – Plane not found » en référence à un avion disparu. Le site du gouvernement wallon a également connu ce type de cyberhacking.



e) Illustrations du site HaveIbeenpwned



The screenshot shows the HaveIbeenpwned website interface. At the top, a blue header contains the site's logo and a search bar. The search bar has a redacted email address and a 'pwned?' button. Below the search bar, a red banner displays the message 'Oh no — pwned!' and indicates that the user's email was found in one breached site. It also provides links to subscribe for notifications and donate. The main content area, titled 'Breaches you were pwned in', explains what a breach is and lists the specific breach for Adobe in October 2013, detailing the types of data compromised.

';--have i been pwned?

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

pwned?

Oh no — pwned!

Pwned on 1 [breached site](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

[Notify me when I get pwned](#) [Donate](#)

[f](#) [t](#)

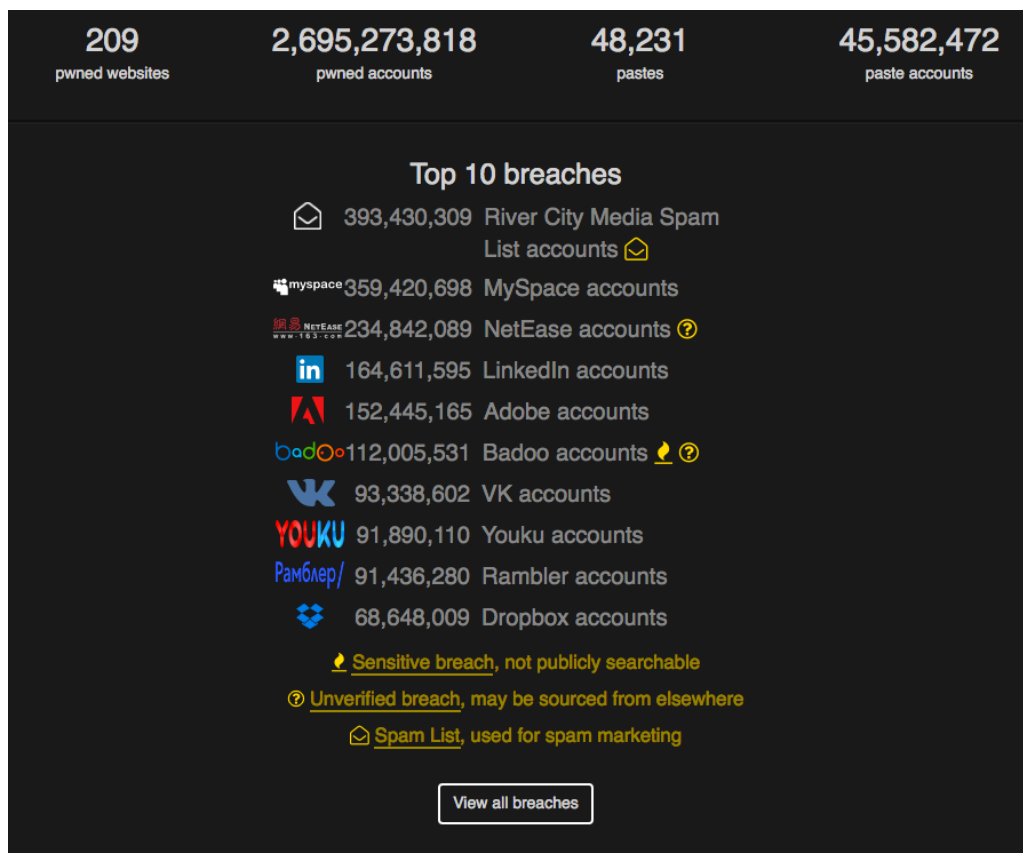
Breaches you were pwned in

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.

 **Adobe:** In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Lorsque vous entrez une adresse e-mail dans la barre de recherche, le site vous indique si votre adresse a fait l'objet d'un piratage. Mieux encore, il indique de quel piratage il s'agit. Dans ce cas-ci, il s'agit d'un test sur une de mes adresses e-mail. Elle a visiblement été piratée lors du cyberhacking d'Adobe en 2013.



Ce site récupère une copie des données mises en vente sur le darkweb et recense les plus grands vols. À la date du 20 avril 2017, voici les plus grandes brèches détectées. Certaines sont confirmées, d'autres doivent encore l'être. En ce qui concerne les données les plus sensibles, le site annonce le vol mais ne les communique pas.

3. Historique des cas par secteur

a) Grande distribution

Home Depot (Etats-Unis)	
Quand & Quoi	En 2014, 50 millions de données bancaires et d'adresses mail ont été compromises.
Par qui & Comment	Les hackers ont utilisé les identifiants d'un fournisseur pour entrer dans le réseau de Home Depot et répandre le logiciel malveillant dans les systèmes de caisses.
Observations	Le CEO a communiqué dans la semaine qui a suivi l'événement au travers d'un communiqué de presse en s'excusant et en précisant les étapes mises en place pour protéger les données des clients.

Target (Etats-Unis)	
Quand & Quoi	En 2013, 110 millions de données (nom, e-mail, numéros de cartes et codes pin etc.) ont été dérobés.
Par qui & Comment	Les pirates se sont infiltrés dans le réseau via un sous-traitant et ont profité que le type carte de crédit le plus répandu aux Etats-Unis ne soit pourvu que d'une simple bande magnétique, ce qui facilite le « skimming ».
Observations	Le CEO a communiqué dans le mois ayant suivi la crise au travers d'un communiqué sur le site. Par contre, ce sont les services secrets américains qui ont découvert des activités suspectes sur les comptes. Des mises à jour sur le déroulement et l'avancement de la crise ont été publiées

	très régulièrement. Ce piratage aurait coûté 1 milliard de dollars à l'entreprise.
--	--

Neiman Marcus (Etats-Unis)	
Quand & Quoi	En 2013, 350.000 cartes de crédit ont été compromises et 10% ont été utilisées frauduleusement.
Par qui & Comment	Le logiciel malveillant aurait circulé dans leur système pendant trois mois.
Observations	Le CEO a communiqué dans les mois qui ont suivi la crise au travers d'un article sur le blog et en insistant sur ce qui n'a pas été compromis. Une section entière est destinée à guider les clients dans le processus.

Albertsons (Etats-Unis)	
Quand & Quoi	Deux piratages visant des données bancaires ont été recensés en 2014 chez Albertsons. L'ampleur de la crise n'est pas connue.
Par qui & Comment	La méthode utilisée est l'infection via un malware mais aucune autre information n'a été précisée.
Observations	Dans les deux cas, un communiqué a été publié sur le site internet et différentes personnes ont pris la parole dans le mois suivant la crise. Une foire aux questions à destination des clients a été mise en place et Albertsons a expliqué les mesures qui éviteront que ce genre de scénario ne se reproduise.

Staples (Etats-Unis)	
Quand & Quoi	Un million de cartes de crédit ont été compromises dans 115 magasins de la chaîne Staples en 2014.
Par qui & Comment	Le mode opératoire utilisé est l'infection via un malware mais aucune autre information n'a été précisée.
Observations	Le responsable de la communication a publié un avis sur le site web cinq mois après les faits. La chaîne a offert une indemnisation aux victimes et a précisé collaborer avec des équipes d'experts.

Kmart (Etats-Unis)	
Quand & Quoi	Des données bancaires de 1.200 magasins ont été compromises en 2014.
Par qui & Comment	Un malware, soi-disant indétectable par leurs systèmes anti-virus, a infecté le système de paiement électronique.
Observations	Le propriétaire de la chaîne s'est excusé sur le site web un mois après les événements. Dans sa façon de dire les choses, l'importance de la réactivité apparaît régulièrement au travers de termes tels que « rapidement », « immédiatement » etc. Les victimes ont également reçu une protection gratuite.

Michaels Store (Etats-Unis)	
Quand & Quoi	En 2013, trois millions de cartes bancaires sont susceptibles d'avoir été compromises.
Par qui & Comment	La méthode utilisée est l'infection via un malware qui n'aurait jamais été rencontré auparavant.
Observations	La chaine ainsi que son CEO ont communiqué sur le site internet huit mois après les faits. Ils ont insisté sur les 40 ans de bons et loyaux services auprès des clients et ont minimisé l'ampleur des faits (« small percentage », « no evidence of other personal information »).

Sally Beauty (Etats-Unis)	
Quand & Quoi	280.000 numéros de cartes de crédit affectés en 2014.
Par qui & Comment	Les pirates ont utilisé les identifiants d'un responsable d'un des magasins avant de mettre les données en vente, au même endroit que celles de Home Depot et Target.
Observations	Le responsable des relations médias a pris la parole un mois après les événements via un communiqué posté sur le site web. Il met en avant le fait que ce genre d'incident est déjà arrivé à d'autres organisations pour avouer sa difficulté à évaluer l'ampleur des dégâts. La chaine avait annoncé un chiffre dix fois inférieur à l'ampleur réelle.

Auchan (France)	
Quand & Quoi	En 2013, le compte twitter a été piraté et de faux messages promotionnels ont été mis en ligne.
Par qui & Comment	Le community manager d'Auchan n'avait pas fait le nécessaire en matière de sécurité. Il n'avait pas activé la double authentification et avait choisi un mot de passe trop simple.
Observations	La marque a réagi dans les vingt-quatre heures à travers un e-mail, un message sur twitter et une interview. Les tweets ont été supprimés, mais la marque aurait gagné en visibilité et followers.

Colruyt (Belgique)	
Quand & Quoi	En 2017, une campagne de phishing ciblant les clients de Colruyt avec de fausses promotions a été mise en œuvre.
Par qui & Comment	À partir d'une adresse inventée et proche de la véritable adresse de Colruyt, les hackers ont piégé les clients du groupe Colruyt.
Observations	Le responsable marketing a alerté les clients par e-mail et sur les réseaux sociaux suite à de nombreuses plaintes.

b) Banques et assurances

JP Morgan (Etats-Unis)	
Quand & Quoi	En 2013, 465.000 détenteurs d'une carte prépayée UCard ont connu une fuite de données personnelles. Un an plus tard, 80 millions de données clients ont été dérobées.
Par qui & Comment	Les hackers sont entrés dans le système de la banque grâce à un ordinateur d'un employé infecté par un malware.
Observations	Un mois après l'événement, la porte-parole annonçait les faits en précisant qu'il s'agissait d'une fraude qui s'inscrit dans une attaque plus large contre d'autres banques. Les victimes seront indemnisées.

Tesco Bank (Royaume-Uni)	
Quand & Quoi	En 2016, 20.000 clients de cette banque ont été victimes d'un vol sur leurs comptes.
Par qui & Comment	La méthode n'est pas connue mais dans ce genre de cas, il est fort possible que les hackers se soient introduits dans le système bancaire en ligne grâce à un malware qui s'est répandu après une attaque de hameçonnage (« phishing »).
Observations	Le CEO s'est excusé dans un communiqué, à la radio et sur twitter avant de minimiser le phénomène en parlant de « montants modestes » sans révéler la somme exacte.

Banque centrale du Bangladesh (Bangladesh)	
Quand & Quoi	81 millions de dollars ont été dérobés à cette banque en 2016.
Par qui & Comment	Au total, 800 millions de dollars ont tenté d'être dérobés par des hackers originaires de Corée du Nord. Ils ont accédé à l'interface du gestionnaire des virements (SWIFT) après avoir dérobé les codes en infiltrant les ordinateurs de la banque.
Observations	Le gestionnaire de virements SWIFT, la réserve fédérale et la banque centrale s'accusent l'un après l'autre sans que personne ne reconnaisse sa culpabilité. Suite à cela, le directeur de la banque a démissionné et huit employés font l'objet d'une enquête.

The DAO (Allemagne)	
Quand & Quoi	En 2016, 50 millions de dollars en monnaie virtuelle ont été dérobés.
Par qui & Comment	Le hacker a profité d'une faille du code pour collecter la crypto-monnaie. Son objectif était de faire perdre la confiance dans ce projet.
Observations	Le fondateur a réagi sur le blog et dans la journée en précisant les méthodes du hacking, comment ils comptent l'arrêter, que peuvent faire les clients pour se protéger.

Morgan Stanley (Etats-Unis)	
Quand & Quoi	Les données de 730.000 comptes bancaires ont été postées sur internet (noms, adresse, numéro de téléphone etc.) à la suite d'un vol survenu entre 2011 et 2014.
Par qui & Comment	Un employé avait transféré ces données sur son ordinateur personnel. Ce dernier a ensuite été piraté.
Observations	L'organisation a profité de cette erreur pour attribuer l'entière responsabilité de l'incident à l'employé.

Bitfinex (Chine)	
Quand & Quoi	120.000 bitcoins, soit 64 millions d'euros ont été dérobés en 2016.
Par qui & Comment	L'origine et la méthode sont inconnues.
Observations	Bitfinex avait fait appel à une société de sécurité informatique qui s'est excusée de toute responsabilité en déclarant sur Twitter que ses serveurs ne présentaient aucune faille. Bitfinex a réagi dans la journée en expliquant utiliser toutes les ressources nécessaires pour régler le problème.

c) Internet

Ebay (Etats-Unis)	
Quand & Quoi	En 2014, 145 millions de membres eBay ont subi un vol massif de leurs données personnelles.
Par qui & Comment	eBay reste discret sur la méthode mais les hackers se seraient infiltrés dans le réseau grâce à des identifiants d'employés de l'organisation.
Observations	Deux mois après l'intrusion, la porte-parole d'eBay a annoncé qu'il ne s'agissait pas de données bancaires et que les utilisateurs sont leur plus grande priorité.

Yahoo Mail (Etats-Unis)	
Quand & Quoi	Yahoo a subi plusieurs vagues de piratage. En 2012, plus de 200 millions de comptes ont été piratés. En 2013 et 2014, 1 milliard et 500 millions de comptes ont également été compromis. En 2015-2016, il s'agit de 32 millions de comptes.
Par qui & Comment	Ces cas sont l'œuvre de hackers différents utilisant des cookies falsifiés et des données chiffrées de manière très faible.
Observations	Yahoo n'a communiqué sur ces piratages qu'en 2016, soit plusieurs années plus tard. Yahoo a d'ailleurs été poursuivi pour « négligence grave » à la suite d'une plainte d'un utilisateur.

Linkedin (Etats-Unis)	
Quand & Quoi	En 2012, 167 millions de données d'utilisateurs ont été mises en vente sur un site spécialisé pour environ 2000€.
Par qui & Comment	Le hacker Peace of Mind a infiltré le réseau de Linkedin car l'algorithme utilisé pour chiffrer les données était obsolète et peu fiable.
Observations	Ce vol n'a été rendu public que 4 ans après les faits par le directeur de la sécurité, d'abord au travers d'un mail adressé aux utilisateurs.

Dyn (Etats-Unis)	
Quand & Quoi	Des sites web tels que Netflix, Twitter, Spotify, Amazon etc. ont été rendus inaccessibles pendant plusieurs heures en octobre 2016.
Par qui & Comment	Les hackers n'ont pas été formellement identifiés mais ils ont utilisé un réseau d'objets connectés (caméras de surveillance etc.) pour perpétrer une attaque par déni de service.
Observations	Immédiatement, le vice-président a placé ses clients au centre de la communication.

Adobe (Etats-Unis)	
Quand & Quoi	En 2013, des informations (y compris bancaires) concernant 153 millions de clients et les codes sources de certains produits Adobe ont été mis en ligne.

Par qui & Comment	Les hackers ont attaqué un serveur de secours contenant une énorme base de données.
Observations	Adobe a mis 3 mois avant de communiquer sur les mesures prises, de s'excuser et de réfuter la dernière estimation du nombre de clients touchés.

Tumblr (Etats-Unis)	
Quand & Quoi	Après un premier piratage en 2012, 65 millions d'identifiants ont été dérobés en 2013.
Par qui & Comment	Les données étaient faiblement protégées, ce qui a facilité le travail au groupe de hackers Peace of Mind qui les a revendues en ligne pour 3000€.
Observations	L'organisation a communiqué sur ce piratage 3 ans après les faits et n'a pas souhaité donner le nombre exact de comptes concernés. Elle a conseillé aux internautes de changer leurs mots de passe.

MySpace (Etats-Unis)	
Quand & Quoi	427 millions de comptes (mails, noms d'utilisateurs, mots de passe) ont été compromis, la date exacte du vol n'est pas confirmée.
Par qui & Comment	Comme Tumblr, les données étaient faiblement protégées, ce qui a facilité le travail au groupe de hackers Peace of Mind qui les a revendues en ligne pour 2500€.

Observations	L'organisation n'a communiqué que plusieurs années après les faits, lors de la mise en vente des données sur le web. Elle recommande de changer de mot de passe, s'excuse et présente les mesures mises en place.
---------------------	---

Ashley Madison (Canada)

Quand & Quoi	Des données liées à 32 millions de comptes ont été mises en ligne en juillet 2015. Un mois plus tard, un second fichier a été publié et concerne des données internes à l'entreprise.
Par qui & Comment	The Impact Team est à l'origine du piratage et reprochait au site de rencontres extraconjugales d'avoir menti sur la suppression définitive de certains comptes. Ces hackers souhaitaient la fermeture du site, sans quoi ils publieraient les données. Le deuxième piratage a servi à prouver la crédibilité du hacker auprès du directeur général.
Observations	Avid Life Media a communiqué dans les deux premières semaines au travers d'un communiqué. L'entreprise n'a pas tout de suite confirmé l'authenticité des fichiers. Ils ont d'abord opté pour une stratégie de déni avant de se positionner en tant que victimes dans un environnement de plus en plus atteint par le piratage.

Friend Finder Network (Etats-Unis)

Quand & Quoi	En 2015, un premier piratage de 4 millions d'utilisateurs a eu lieu. En 2016, il s'agissait de 420 millions de comptes du site de rencontres.
-------------------------	---

Par qui & Comment	Le mode opératoire du premier piratage est inconnue mais dans le deuxième cas, le site de rencontres utilisait une technologie de protection des données dépassée.
Observations	Le site a toujours communiqué par le biais d'autres médias, avec des interviews. Le piratage de 2016 n'a ni été confirmé, ni démenti, bien que le site ait affirmé qu'il existait une vulnérabilité dans ses codes, qui a été réparée.

Dropbox	
Quand & Quoi	En 2012, 68 millions d'identifiants ont été mis en ligne sur internet. Deux ans plus tard, 7 autres millions d'adresses électroniques et de mots ont été dérobés.
Par qui & Comment	Les hackers ont utilisé les identifiants d'un employé pour accéder aux informations. Ils ont obtenu les informations de cet employé après le piratage de LinkedIn. Le salarié utilisait le même mot de passe sur les deux plateformes. Cependant, la technique pour protéger les mots était assez robuste.
Observations	En 2012, une première communication avait été faite au sujet d'un faible nombre de comptes. Ce n'est qu'en 2016 que Dropbox a révélé l'ampleur de la fraude qui remontait à 2012. En ce qui concerne le piratage de 2014, Dropbox nie les faits.

Twitter (Etats-Unis)	
Quand & Quoi	Entre 2013 et 2016, Twitter a connu des piratages chaque année. En 2013, cela concernait des données de 250.000 utilisateurs. En 2014, des messages publicitaires ont été publiés à partir de milliers de comptes. L'année suivante, des adresses mail, adresses IP et numéros de téléphones étaient concernés. Et en 2016, il s'agissait de 32 millions de comptes.
Par qui & Comment	L'origine des deux premiers piratages est inconnue. En 2015, Twitter soupçonnait des acteurs soutenus par un Etat ayant profité d'une faille de sécurité. En 2016, Peace of Mind a utilisé une campagne de malware et a ensuite revendu les informations sur le dark web.
Observations	En 2013, le directeur de la sécurité a insisté sur le fait que d'autres piratages du même type avaient touché d'autres organisations. L'année suivante, Twitter s'est excusé et a réinitialisé les mots de passe. En 2015, Twitter pointait la responsabilité d'un acteur soutenu par un Etat. Et en 2016, Twitter a reporté la faute sur les particuliers en précisant que leurs systèmes n'avaient pas été piratés.

Twitter Counter (Pays-Bas)	
Quand & Quoi	En 2017, les comptes piratés affichaient un message en référence au référendum en Turquie. Il s'agissait par exemple du compte d'Amnesty International, du ministère français de l'Économie ou de la BBC.

Par qui & Comment	Pas d'information.
Observations	Sur le réseau social, le porte-parole a réagi dans la journée. Ils ont imputé ce piratage à une application tierce.

Hacking Team (Italie)	
Quand & Quoi	Vol de 400 gigaoctets de données confidentielles, compte twitter piraté et diffusion en ligne de documents volés.
Par qui & Comment	Pas d'information.
Observations	Ils affirment les informations révélées par les pirates sont fausses.

xHamster (Etats-Unis)	
Quand & Quoi	En 2016, 380.000 comptes ont été compromis et rendus public.
Par qui & Comment	Ces informations étaient chiffrées à l'aide d'un système qui n'était plus adapté.
Observations	Interrogé par le site spécialisé Motherboard, le porte-parole de xHamster a nié et a assuré que les mots de passe étaient correctement chiffrés et impossibles à pirater.

Plenty of Fish (Canada)	
Quand & Quoi	Le piratage de 28 millions d'utilisateurs remonte à 2011. Les informations n'ont pas été mises en ligne.
Par qui & Comment	Un pirate argentin nommé Chris Russo a récupéré les informations facilement car elles étaient faiblement protégées. Cependant, il ne les a pas publiées mais souhaitait uniquement avertir les administrateurs du site de la faible protection et a proposé de travailler pour eux.
Observations	Un article sur le blog a été posté dans la semaine. Plenty of Fish a réinitialisé tous les mots de passe et parlait d'une « attaque bien planifiée et très sophistiquée »

Pirate Bay (Suède)	
Quand & Quoi	En 2010, les données de 4 millions d'utilisateurs ont été compromises.
Par qui & Comment	Il s'agit du même « Grey Hat » que pour le cas de Plenty of Fish. Il a alerté la toile des problèmes de sécurité du site. Il a profité d'une faille informatique.
Observations	Ils minimisent les faits en disant que leurs données ont été volées, mais « are not insecured ». Nous sommes tous humains, et l'erreur est humaine, ont-ils ajouté.

eHarmony (Etats-Unis)	
Quand & Quoi	Une liste d'un million et demi de mots de passe a été dérobée au site et mise en ligne.
Par qui & Comment	Le mode de chiffrement utilisé était dépassé, Peace of Mind en a profité.
Observations	Ils minimisent les faits en disant que seule une petite fraction des utilisateurs est concernée.

Cupid Media (Australie)	
Quand & Quoi	En 2013, 42 millions de données (adresses électroniques, mots de passe en « clair » et dates d'anniversaire) ont été publiées sur le web.
Par qui & Comment	Les mots de passe étaient stockés « en clair », c'est-à-dire sans protection.
Observations	Le site a communiqué dix mois après les événements et a envoyé un mails aux internautes concernés et a engagé un expert en sécurité informatique.

Top Face (Russie)	
Quand & Quoi	Top Face s'est fait dérober 20 millions d'adresses mails en 2015.
Par qui & Comment	Le pirate nommé Mastermind a profité d'une vulnérabilité dans le système. Son intention n'était pas de vendre les informations mais de mettre en avant les millions de faux profils utilisés par les sites de rencontres.

Observations	L'organisation a payé le pirate pour qu'il ne publie pas les adresses e-mail sur le web. Pourquoi payer le hacker s'il ne s'agit que d'adresses e-mail ?
---------------------	--

Vkontakte (Russie)	
Quand & Quoi	Entre 2011 et 2012, le site s'est fait dérober des informations concernant 100 millions de comptes.
Par qui & Comment	Le site n'utilisait pas les normes de sécurité pour le stockage de mots de passe, le groupe de hacker Peace of Mind en a profité.
Observations	Les premières communications ont eu lieu en 2016, lorsque les données ont été rendues publiques. Les victimes ont été prévenues par e-mail. L'organisation nie l'existence d'une faille de sécurité, elle rappelle aux internautes qu'installer des logiciels non certifiés peut mettre leurs données en danger.

Brazzers (Canada)	
Quand & Quoi	En 2012, 790.000 données ont été mises en ligne.
Par qui & Comment	Une faille dans une plateforme qui permet de créer des forums (vBulletin) a été exploitée.
Observations	L'organisation a réagi 4 ans après. Elle a reporté la responsabilité de l'incident sur la plateforme de création de forums. Néanmoins, elle a expliqué les mesures mises en place pour que cela ne se reproduise pas.

Avast (République Tchèque)	
Quand & Quoi	Les données de 400.000 comptes ont été compromises en 2014 mais les mots de passe étaient chiffrés.
Par qui & Comment	Pas d'information.
Observations	Les premières communications ont eu lieu deux jours après les événements. Après avoir conseillé aux internautes de ne pas utiliser le même mot de passe sur d'autres sites, Avast a tenté de les rassurer en précisant que seulement 0,2% d'entre eux étaient concernés. L'organisation a reporté la responsabilité du piratage à une tierce partie.

Spotify (Suède)	
Quand & Quoi	Dropbox s'est fait dérober des données à deux reprises. Dans un premier temps, il s'agissait de données internes et d'informations liées à un seul utilisateur. En 2016, cela concernait plusieurs milliers d'identifiants.
Par qui & Comment	Pas d'information.
Observations	Lors du premier vol, l'organisation a demandé à ses utilisateurs de renouveler leurs identifiants même si cela ne concernait qu'un internaute. En 2016, Spotify nie le piratage de son service et indique que les données proviennent d'une vieille liste correspondant à un ancien service.

Telegram (Russie)	
Quand & Quoi	Des pirates iraniens ont pris le contrôle d'une douzaine de comptes et ont obtenu 15 millions de numéros de téléphone en 2016.
Par qui & Comment	Il s'agit de pirates iraniens nommés Rocket Kitten. Ils ont intercepté des codes de vérification par SMS grâce à une faille dans la messagerie pourtant réputée très sécurisée.
Observations	Ils nuancent la gravité en admettant que des comptes ont été compromis mais par des vulnérabilités dont ils ne sont pas responsables. Ils impliquent également d'autres plateformes de messagerie telles que WhatsApp et Messenger. La sécurité de cette application est essentielle et réputée pour son haut niveau de confidentialité car il s'agit du seul canal de discussion qui n'est pas censuré par le gouvernement.

Evernote (Etats-Unis)	
Quand & Quoi	50 millions de mots de passe ont été volés en 2013.
Par qui & Comment	Pas d'information.
Observations	Ils parlent d'une cyberattaque sophistiquée et ont contacté les victimes par e-mail. Ils impliquent également d'autres plateformes : « <i>as recent events with other large services have demonstrated, this type of activity is becoming more common</i> ».

Steam (Etats-Unis)	
Quand & Quoi	En 2011, des pirates ont eu accès aux noms, mots de passe, adresses e-mail ainsi que des informations bancaires.
Par qui & Comment	Le vol est dû à une faille dans vBulletin, plateforme de création de forum, tout comme pour le cas de Brazzers.
Observations	Un message a été publié sur le forum quatre jours plus tard sur les forums de Steam.

Netflix (Etats-Unis)	
Quand & Quoi	De nombreux programmes ont été dérobés et la nouvelle saison d' « Orange is the new black » a été rendue publique en 2017, avant la sortie officielle.
Par qui & Comment	TheDarkOverlord a profité d'une vulnérabilité de Larson Studios pour récupérer les fichiers. Ils réclamaient une rançon de 66.000€ que Netflix n'a pas payé, la saison a donc été mise en ligne.
Observations	Netflix a collaboré avec les autorités et accuse la sécurité du fournisseur de production d'être compromise.

Dailymotion (France)	
Quand & Quoi	Plus de 80 millions d'adresses et d'identifiants ont été dérobés, ainsi qu'un mot de passe sur cinq.
Par qui & Comment	Pas d'information.

Observations	Un billet de blog a été écrit et envoyé par mail aux utilisateurs en expliquant comment procéder pour résoudre le problème de sécurité. L'information a d'abord été révélée par un site spécialisé et publiée dans les médias avant que Dailymotion ne réagisse.
---------------------	--

OVH (France)	
Quand & Quoi	En 2013, les données de ses clients ont été dérobées. Trois ans plus tard, l'hébergeur a dû faire face à une série d'attaques de plus de 100 gigabits par seconde qui ont mis ses serveurs hors service.
Par qui & Comment	En 2013, le hacker a obtenu le mot de passe d'un employé et s'est ainsi introduit dans le réseau pour s'emparer de dossiers internes concernant 700.000 clients. En 2016, c'est le malware Mirai qui a mis hors service les serveurs d'OVH grâce à un bonnet de 150.000 caméras de sécurité infectées et détournées par des hackers.
Observations	Dans les deux cas, il n'a fallu que quelques jours pour que le fondateur prenne la parole. Cependant, ses communications n'ont pas été très complètes ni visibles (sur un blog peu fréquenté pour le premier cas, uniquement sur twitter pour le second).

AlieExpress (Chine)	
Quand & Quoi	En 2014, une faille aurait permis aux pirates de dérober des informations sur les clients et de modifier les informations de certaines marchandises du site.

Par qui & Comment	Pas d'information.
Observations	L'organisation a pris la parole par le biais d'un e-mail en rappelant que la sécurité de la vie privée des clients est leur priorité.

d) Loisir

Sony Online Entertainment (Japon)	
Quand & Quoi	En 2011, des données personnelles et bancaires de 77 millions d'utilisateurs ont été volées. La même année, la plateforme avait été rendue inaccessible pendant vingt-trois jours. Un an plus tard, un groupe de hackers a mis en ligne l'intégralité du catalogue de films et de musique de Sony.
Par qui & Comment	Lulz Security serait à l'origine de la mise en ligne des données de 2011. Anonymous aurait mis en téléchargement gratuit les films et musiques pour défendre le droit à la liberté d'expression après la fermeture du site Megaupload.
Observations	Pour le vol de données, le chef de la division des activités grand public s'est excusé et a souligné l'absence de preuves liées au vol de comptes bancaires mais sans en exclure la possibilité. Il offre également une compensation de trente jours de temps supplémentaire aux victimes. En ce qui concerne le cas de 2012, Sony n'a pas communiqué.

Sony Pictures Entertainment (Japon)

Quand & Quoi	100 terabytes de données concernant 47.000 employés et tiers ont été volées en 2014. Cinq films du studio ont également été mis en ligne illégalement.
Par qui & Comment	La Corée du Nord est suspectée d'avoir commandité les faits par le biais du groupe de hackers Guardian of Peace suite à la diffusion du film « The interview » par Sony.
Observations	L'organisation n'a pas été très joignable. La première réaction officielle du CEO est arrivée deux mois après la mise en ligne des données volées. Entretemps, les pirates faisaient pression pour annuler la sortie du film.

Sony Playstation Network (Japon)

Quand & Quoi	En 2014, les réseaux Playstation et Xbox Live ont été mis hors service pendant trois jours.
Par qui & Comment	Le groupe de hackers Lizard Squad, qui avait déjà perturbé le réseau, avait prévenu d'une nouvelle attaque pour Noël. L'objectif étant de démontrer « l'incompétence » de Sony et de Microsoft en matière de sécurité.
Observations	Peu d'information ont été communiquées par Sony autrement que via Twitter.

VTech (Chine)	
Quand & Quoi	Onze millions de comptes d'enfants et de parents ont été dérobés en 2015. En plus de cela, des prénoms, genres et dates de naissance de 200.000 enfants sont concernés.
Par qui & Comment	Les données étaient faiblement protégées mais le pirate n'a pas vendu les données.
Observations	VTech a contacté chaque personne pour les alerter mais la marque a minimisé l'acte de piratage en assurant qu'aucune donnée sensible n'est concernée. Elle reconnaît tout de même que sa base de données n'était pas aussi sécurisée qu'elle aurait dû l'être.

Spiral Toys (Etats-Unis)	
Quand & Quoi	Les données de 800.000 propriétaires de peluches connectées ont été piratées en 2016.
Par qui & Comment	La base de données n'était pas du tout protégée et était stockée sur des appareils facilement piratables. Les clients ont reçu un message proposant d'échanger leurs données contre un bitcoin.
Observations	Dans un premier temps l'organisation était sous silence. Elle a ensuite opté pour le déni en niant le piratage de messages vocaux.

e) Transports

San Fransisco Municipal Railway (Etats-Unis)	
Quand & Quoi	Pendant tout un week-end de 2016, les distributeurs de cette compagnie de transports ont été mis hors services.
Par qui & Comment	Un ransomware a verrouillé l'accès aux données. Il s'est exécuté après une campagne d'hameçonnage destiné à récupérer le mot de passe d'un administrateur du réseau. Un rançon de 73.000 dollars étaient demandée.
Observations	Le porte-parole a déclaré que la compagnie avait pris la décision de bloquer les distributeurs pour minimiser l'impact. Ils travaillent avec les forces de l'ordre. Il a précisé qu'il s'agissait du premier piratage de la compagnie.

Malaysia Airlines (Malaisie)	
Quand & Quoi	Le message « 404 – avion non trouvé » s'affichait sur le site web de la compagnie.
Par qui & Comment	Lizard Squad est le groupe de hackers responsable.
Observations	La compagnie a réagi dans la journée et a assuré qu'aucune donnée client n'a été compromise et que son site serait bientôt opérationnel.

f) Télécommunication

Three Mobile (Royaume-Uni)	
Quand & Quoi	Les informations de 133.000 clients ont été volées (pas d'information bancaire) en 2016.
Par qui & Comment	Le compte d'un employé s'est fait pirater par le biais d'une campagne d'hameçonnage, ce qui a permis aux pirates de s'introduire dans les systèmes de Three Mobile.
Observations	La communication de Three Mobile fut très axée sur les clients, avec de nombreuses mises à jour et en présentant des excuses.

Orange (France)	
Quand & Quoi	Deux piratages ont eu lieu en 2014. D'abord les e-mails, numéros de mobile et coordonnées postales de 800.000 clients ont été compromises. Ensuite, les données de plus d'un million de clients ont été volées.
Par qui & Comment	Lors du premier piratage, une faille a été exploitée. Lors du second, les mesures de sécurité d'Orange lors de transferts d'informations étaient trop légères.
Observations	Orange précise que lors du premier piratage, aucune donnée bancaire n'était concernée mais a attendu deux semaines avant de reconnaître l'effraction informatique. Après le deuxième piratage, Orange a contacté individuellement ses clients un mois plus tard.

Deutsche Telekom (Allemagne)	
Quand & Quoi	En 2015, 900.000 clients allemands ont rencontré des pannes de réseau pendant une journée.
Par qui & Comment	Le malware Mirai infecte les objets connectés et a exploité une faille dans les routeurs internet de la marque. L'objectif était de transformer ces routeurs en éléments d'un botnet, mais la tentative a échoué.
Observations	Une foire aux questions a été créée dans la journée sur le site de la marque pour accompagner les victimes. L'opérateur précise que des équipes ont pris en charge le problème et qu'ils n'ont jamais fait d'économies sur les coûts en matière de sécurité. L'opérateur dit également que le hacking n'aurait pas pu être anticipé.

Talk Talk (Grande Bretagne)	
Quand & Quoi	Un fichier de 4 millions de clients et concernant des données bancaires a été dérobé.
Par qui & Comment	Talk Talk ne respectait pas les standards en matière de protection des données bancaires.
Observations	Après avoir tenté d'expliquer les événements par une attaque par déni de service, l'entreprise a admis qu'elle aurait pu faire plus en matière de sécurisation des données de ses clients. Le régulateur britannique des télécommunications a condamné Talk Talk à une amende de 70 millions d'euros pour négligence car il estime que

	l'entreprise aurait pu empêcher le hacking avec des précautions minimales.
--	--

Vodafone (Royaume-Uni)	
Quand & Quoi	Piratage de 1800 clients de l'opérateur en 2015, comprenant des données bancaires.
Par qui & Comment	En utilisant des identifiants issus d'autres piratages.
Observations	Trois jours après le piratage, Vodafone a assuré que ses systèmes n'ont pas été compromis, qu'aucune donnée bancaire n'a été obtenue et que seulement 1800 clients sont concernés.

g) Santé

Centre médical presbytérien d'Hollywood	
Quand & Quoi	Les données de 900 patients ont été inaccessibles pendant 10 jours en février 2016. Le centre médical a payé 15.000 euros pour récupérer ces informations.
Par qui & Comment	Le ransomware à l'origine de ce piratage s'appelle Locky.
Observations	Selon un interview du CEO, payer la rançon était « le moyen le plus rapide et efficace ».

Laboratoires de biologie médicale (France)	
Quand & Quoi	En 2015, des pirates réclamaient 20.000 euros contre la non publication de 40.000 identifiants et des centaines de bilans médicaux.
Par qui & Comment	Les pirates se nomment Rex Mundi et ont agi pour leur plaisir.
Observations	Les laboratoires ont décidé de ne pas payer la rançon pour éviter une incitation au renouvellement de telles pratiques. Ils n'ont pas énormément communiqué sur le sujet.

h) Médias

Libération (France)	
Quand & Quoi	En 2013 et 2014, Libération a connu deux piratages similaires. Le site a été indisponible pendant une heure en 2013 et pendant une vingtaine de minutes en 2014.
Par qui & Comment	En 2013, aucune information sur le pirate n'est donnée. En 2014, il s'agit du franco-israélien Ulcan.
Observations	Dans les deux cas, Libération a communiqué dans l'heure pour prévenir de l'indisponibilité de ses services.

Rue 89 (France)	
Quand & Quoi	En 2014, le site était inaccessible pendant plusieurs heures.
Par qui & Comment	Il s'agit d'Ulcan, le même pirate que lors du piratage du site de Libération, Mediapart et Arrêt sur Images.

Observations	Le rédacteur en chef positionne Rue89 comme victime d'Ulcan qui s'amuserait à faire tomber des sites qu'il perçoit comme pro-Palestiniens.
---------------------	--

Mediapart (France)	
Quand & Quoi	En 2013, des relevés d'identités bancaires (RIB) ont été extraits du site. Un an plus tard, l'accès au site a été bloqué pendant plusieurs heures.
Par qui & Comment	Il n'y pas d'information concernant le piratage de 2013. En 2014, il s'agissait de l'œuvre du hacker Ulcan. Il demandait de stopper les mensonges à propos d'Israël.
Observations	La rédaction de Mediapart a rapidement communiqué sur les événements. Dans un premier temps, le site n'a pas précisé le nombre de RIB volés. Le site s'est néanmoins excusé de ne pas avoir su contrer l'attaque. En 2014, le site a qualifié le hacking d'atteinte à la liberté d'information.

Radio France (France)	
Quand & Quoi	En 2014, les sites de France Inter et de France Info étaient inaccessibles pendant plusieurs heures.
Par qui & Comment	Le hacker est Ulcan, le même que pour le cyberhacking qui a concerné Mediapart. Le pirate accusait le média de ne pas respecter la présomption d'innocence, ni les droits de réponse. Il s'agit d'une vengeance personnelle.
Observations	Le porte-parole de Radio France a communiqué instantanément et s'en est tenu aux faits et au déroulement

	des événements. Aucune réponse supplémentaire n'a été donnée.
--	---

Le Parisien (France)	
Quand & Quoi	En 2014, le site du Parisien a été rendu inaccessible pendant vingt minutes.
Par qui & Comment	La Ligue de défense juive (LDJ) s'est félicitée de l'action sur son compte Twitter mais sans réellement la revendiquer.
Observations	Pas d'information.

Arrêt sur Images (France)	
Quand & Quoi	Le site était inaccessible pendant plusieurs heures le 23 août 2014.
Par qui & Comment	Soupçonné de s'en être pris à Rue 89 et Mediapart, Ulcan est de nouveau impliqué dans ce piratage. Une émission lui avait été dédiée la veille.
Observations	Le site a annoncé sur les réseaux sociaux qu'en réaction au piratage, l'émission serait disponible gratuitement sur Dailymotion.

TV5 Monde (France)	
Quand & Quoi	Les outils de production, le site internet et les réseaux sociaux de la chaîne ont été piratés. Le compte Facebook

	et Twitter de TV5 Monde affichait des messages de propagande djihadiste.
Par qui & Comment	Les auteurs sont notamment connus sous le nom de ATP28. Ils ont pu accéder au réseau informatique de la chaîne grâce à un mot de passe peu protégé d'un des prestataires.
Observations	Le chaîne a tout de suite réagi sur son compte Twitter et le CEO a publié un message vidéo qui explique les faits, les mesures pour que tout revienne à la normale etc. « On avait anticipé ce genre d'attaques et nous disposons de systèmes de sécurité puissants et audités régulièrement. Sur le principe, nous étions prêts. Mais cette attaque était très puissante, ils en savaient visiblement beaucoup. »

Le Monde (France)	
Quand & Quoi	Le compte Twitter du Monde qui comptait 3 millions d'utilisateurs en 2015 a été piraté. Après s'être introduit dans les outils de publication du média, les hackers ont publié des messages de propagande.
Par qui & Comment	L'Armée électronique syrienne utilise toujours le même mode opératoire. Elle choisit des cibles à très grande visibilité et lance une campagne d'hameçonnage.
Observations	De manière générale, lorsqu'un employé se fait voler ses identifiants et permet ainsi aux pirates de s'introduire dans le système de l'entreprise pour laquelle il travaille, celle-ci lui incombe les responsabilités. Dans ce cas-ci, Le Monde défend cet employé en scénarisant le déroulement, à la façon du storytelling : « les gens sont affolés », « ils courent

	dans les couloirs », « un coup de fil d'un confrère réveille des personnes de la rédaction ». Le Monde pointe également d'autres médias ayant subi le même type de hacking.
--	--

Associated Press (Etats-Unis)	
Quand & Quoi	Un faux tweet annonçant que Barack Obama avait été blessé dans une explosion a été publié sur le compte Twitter de l'agence de presse (2 millions d'abonnés en 2013). Cette information a été retweetée des centaines de fois.
Par qui & Comment	L'Armée électronique syrienne est connue pour pirater des médias internationaux.
Observations	L'agence a mis quelques minutes pour démentir l'information. Un peu plus tard, elle a annoncé que son site venait d'être piraté. Elle a travaillé avec Twitter pour enquêter sur l'affaire.

BBC (Royaume-Uni)	
Quand & Quoi	Le site internet a été perturbé pendant plusieurs heures en 2015 par une attaque par déni de service.
Par qui & Comment	À l'origine de ce piratage, un groupe de hacker nommé New World qui dit lutter contre le terrorisme.
Observations	Le porte-parole s'est contenté d'expliquer les faits de façon chronologique.

TF1 (France)	
Quand & Quoi	En 2013, les données de deux millions de clients du service d'abonnement ont été dérobées, y compris des données bancaires.
Par qui & Comment	Le groupe de hackers Linker Squad en serait à l'origine et aurait exploité une faille dans le site de TF1. « Les données que nous détenons (...) seront sûrement revendues »
Observations	Selon la chaîne, les données bancaires sont cryptées et ne craignent rien. Elle annonce également qu'il ne s'agit pas d'un piratage de TF1 mais d'un partenaire commercial, Viapresse : « Nous réglerons nos différends avec le partenaire défaillant dans le cadre du secret des affaires. Il va sans dire que TF1 défendra ses intérêts à la hauteur du préjudice subi ».

Canal + (France)	
Quand & Quoi	En 2016 et pendant plusieurs heures, les sites internet de Canal Plus et Canal Play étaient inaccessibles. Les sites redirigeaient les internautes vers des pages de propagande sur les conflits armés en Syrie.
Par qui & Comment	AMAR^SHG, un groupe de hackers d'Afrique du nord qui souhaitait faire passer un message en dénonçant le silence sur les massacres en Syrie.
Observations	La réaction fut instantanée sur Twitter mais très limitée : « On est dessus », « Bonsoir, c'est en cours de résolution,

	nous sommes dessus. En attendant, myCANAL fonctionne ».
--	---

i) Sécurité

US Central Command (Etats-Unis)	
Quand & Quoi	Les comptes Twitter et Youtube ont été détournés en 2015 pour afficher ce message : « Soldats américains, nous arrivons, prenez garde ! ». Des documents ont également été publiés mais pouvaient déjà être trouvés en ligne.
Par qui & Comment	Les hackers se nomment CyberCaliphate, ils ont déclaré : « Au nom d'Allah, le Tout Miséricordieux, le Très Miséricordieux, le CyberCaliphate sous les auspices de ISIS continue son CyberDjihad ».
Observations	Le CentCom a confirmé le piratage de ses comptes mais rappelle qu'aucun document classifié n'a été compromis. Il reporte les responsabilités sur Twitter : "Twitter a été piraté, pas le Centcom", ajoute le Pentagone

j) Politique

OSCE (Autriche)	
Quand & Quoi	En 2016, des pirates ont eu accès aux courriers électroniques, dossiers et mots de passe.

Par qui & Comment	Il s'agit de l'œuvre d'ATP28 qui s'est introduit dans le réseau grâce à une faille dans le système d'exploitation utilisé par l'organisation.
Observations	La porte-parole a communiqué par le biais d'une enquête du média Le Monde, deux mois après le piratage. Elle parle de spéculations, qu'ils n'auraient pas les capacités de mener une enquête et reste très vague dans son discours.

Mairie de Toulon (France)	
Quand & Quoi	En 2011, des photos d'un drapeau algérien accompagnées d'un texte propagandiste apparaissaient lors de la connexion sur le site.
Par qui & Comment	Pas d'information.
Observations	Selon le ministre de l'intérieur, tous les moyens du ministère ont été mobilisés pour retrouver les coupables.

k) Energie

Prikarpattiaoblenergo (Ukraine)	
Quand & Quoi	En 2015, plus d'un million d'habitants ukrainiens ont rencontré une coupure d'électricité pendant plusieurs heures.
Par qui & Comment	Il s'agit d'un logiciel malveillant (KillDisk) envoyé par e-mail à des personnes ciblées afin d'infecter certaines machines.

Observations	La compagnie a réagi rapidement auprès des clients mais les communications publiques viennent essentiellement d'une société informatique et de sources locales.
---------------------	---

Korea Hydro and Nuclear Power (Corée du Sud)	
Quand & Quoi	En 2014, des pirates ont accédé à 11.000 données d'employés et aux plans de réacteurs. Certaines informations ont été publiées sur Naver, Nate et Twitter.
Par qui & Comment	Le malware utilisé ressemble à celui de Sony Pictures. La compagnie soupçonne le président d'une organisation antiréacteur nucléaire d'Hawaï qui voulait faire fermer les trois réacteurs le jour de Noël.
Observations	Pas d'information.

1) Bâtiment et Immobilier

Vinci	
Quand & Quoi	En 2016, un faux communiqué de presse annonçant de mauvaises nouvelles à propos de la société de construction a été envoyé à de nombreuses rédactions. L'information a été rapidement relayée par ces rédactions entraînant une chute de l'action de Vinci pendant quelques minutes.
Par qui & Comment	Le mode opératoire relève de l'ingénierie sociale. Les escrocs se sont fait passer pour Vinci. Ils revendiquaient

	leur mécontentement par rapport à certains projets de la société.
Observations	Un mail de démenti a été envoyé peu de temps après ainsi qu'un communiqué assez incomplet. La société ne se dit pas victime d'un piratage mais d'une usurpation d'identité.

m) Hôtellerie et restauration

White Lodging (Etats-Unis)	
Quand & Quoi	En 2013 et 2014, la chaine d'hôtels a rencontré deux piratages. Dans les deux cas, les données bancaires de milliers de clients ont été compromises.
Par qui & Comment	Pas d'information.
Observations	Dans le premier cas, la porte-parole n'a pas souhaité faire de commentaire. Dans le deuxième cas, il a fallu plusieurs mois pour que la chaine réagisse. La chaine a mis l'accent sur les mesures de sécurité prises depuis la crise. Elle a également offert une compensation.

n) Technologie & Electronique

Acer (Taiwan)	
Quand & Quoi	En 2015, les données personnelles et bancaires de 34.500 clients ont été volées.

Par qui & Comment	Il s'agit d'un forum géré par une tierce partie qui a été attaqué mais il n'y a pas d'autre information.
Observations	Le service clientèle a envoyé un courrier aux clients de la marque un an après les faits. L'entreprise assure que moins de 0,2% de la clientèle a été affectée.

o) Service

Experian (Irlande)	
Quand & Quoi	En 2013, des informations d'identité de 15 millions de clients T-Mobile (opérateur téléphonique) ont été volées.
Par qui & Comment	Les pirates ont exploité une faille chez Experian, société avec laquelle T-Mobile entretenait une collaboration.
Observations	Experian a contacté chaque personne affectée et offre un dédommagement. T-Mobile renvoie la responsabilité sur Experian et a remis en cause le partenariat.

p) ONG

q) Automobile

r) Alimentaire

s) Textile

4. Corpus

[http://www.lemondeinformatique.fr/actualites/lire-home-depot-le-vol-de-ses-donnees-lui-a-coute-43-m\\$-sur-le-trimestre-59406.html](http://www.lemondeinformatique.fr/actualites/lire-home-depot-le-vol-de-ses-donnees-lui-a-coute-43-m$-sur-le-trimestre-59406.html)
<https://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm>
https://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm?_ga=1.261057101.1927114899.1492004317
<http://www.lalibre.be/economie/digital/des-hackers-arretes-pour-le-piratage-de-la-banque-jpmorgan-55af94933570b54652da5386>
http://www.lemonde.fr/entreprises/article/2014/10/03/les-comptes-de-plusieurs-millions-de-clients-de-jpmorgan-pirates_4499719_1656994.html?xtmc=jpmorgan&xtcr=171
<http://www.lalibre.be/economie/digital/ebay-recommande-de-changer-de-mot-de-passe-537ca9ee35704f05d6990a61>
http://www.liberation.fr/eclairs/2014/05/21/ebay-victime-d-une-cyberattaque_1023330
http://www.lemonde.fr/economie/article/2014/05/21/ebay-victime-d-une-vaste-cyberattaque_4423060_3234.html?xtmc=ebay&xtcr=221
<http://www.lefigaro.fr/secteur/high-tech/2014/05/21/32001-20140521ARTFIG00249-victime-d-une-cyberattaque-ebay-recommande-de-changer-de-mot-de-passe.php>
<http://www.francesoir.fr/tendances-eco-monde/yahoo-un-piratage-de-plusieurs-centaines-de-millions-de-comptes-en-2012-la>
http://www.lemonde.fr/economie/article/2016/09/23/yahoo-vise-par-un-acte-de-piratage-d-une-ampleur-inedite_5002310_3234.html#Z2eTKu5lkZW6KBQU.99
<http://geeko.lesoir.be/2016/08/03/200-millions-de-comptes-yahoo-en-vente-sur-le-darkweb/>
http://www.lemonde.fr/pixels/article/2017/03/02/32-millions-d-utilisateurs-affectes-par-les-faux-cookies-utilises-contre-yahoo_5088090_4408996.html?xtmc=yahoo&xtcr=9
http://www.lemonde.fr/pixels/video/2016/12/15/un-milliard-de-comptes-yahoo-pirates-quels-sont-les-risques-et-comment-s-en-proteger_5049714_4408996.html?xtmc=yahoo&xtcr=25
http://www.lemonde.fr/pixels/article/2016/12/15/le-piratage-de-yahoo-revele-de-graves-defaillances_5049486_4408996.html?xtmc=yahoo&xtcr=28
<https://yahoo-security.tumblr.com/>
<http://www.lefigaro.fr/flash-eco/2017/01/23/97002-20170123FILWWW00009-la-sec-examine-les-attaques-informatiques-contre-yahoo.php>
<http://geeko.lesoir.be/2016/12/15/plus-dun-milliard-de-comptes-yahoo-ont-ete-pirates/>
http://www.liberation.fr/eclairs/2014/01/31/les-mails-yahoo-victimes-d-une-attaque-informatique_976806
http://www.lemonde.fr/pixels/article/2016/09/22/500-millions-de-comptes-d-utilisateurs-de-yahoo-ont-ete-pirates_5002118_4408996.html
http://www.lemonde.fr/pixels/article/2016/09/22/500-millions-de-comptes-d-utilisateurs-de-yahoo-ont-ete-pirates_5002118_4408996.html
http://www.lemonde.fr/pixels/article/2016/09/23/piratage-de-yahoo-les-reponses-a-vos-questions_5002273_4408996.html#kh6ccjPBoykVb9z1.99
<http://www.lemonde.fr/pixels/article/2016/11/10/piratage-massif-de-yahoo-des-employes-etaient-au-courant-des-2014-d-une->

[intrusion_5028842_4408996.html#bKkVMdJgVuZqbv2z.99](#)
http://www.lemonde.fr/ameriques/article/2016/09/24/piratage-massif-yahoo-poursuivi-pour-negligence-par-un-utilisateur_5002731_3222.html?xtmc=yahoo&xtcr=59
<https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security>
<http://www.lefigaro.fr/flash-eco/2016/09/29/97002-20160929FILWWW00385-yahoo-pirate-par-des-professionnels.php>
<http://geeko.lesoir.be/2016/09/23/qui-se-cache-derriere-lattaque-de-yahoo/>
<http://geeko.lesoir.be/2016/12/15/plus-dun-milliard-de-comptes-yahoo-ont-ete-pirates/>
http://www.lemonde.fr/pixels/article/2017/02/16/de-faux-cookies-ont-ete-utilises-pour-pirater-des-comptes-e-mail-yahoo_5080592_4408996.html
http://www.lemonde.fr/pixels/article/2017/03/02/la-patronne-de-yahoo-renonce-a-son-bonus-suite-aux-faillies-de-securite_5087825_4408996.html?xtmc=yahoo&xtcr=10
<http://www.lefigaro.fr/flash-eco/2017/02/15/97002-20170215FILWWW00388-cyberattaques-yahoo-alerte-encore-les-victimes.php>
<http://www.lefigaro.fr/secteur/high-tech/2017/03/02/32001-20170302ARTFIG00208-yahoo-avoue-un-troisieme-piratage-massif.php>
<http://www.lefigaro.fr/flash-eco/2016/11/10/97002-20161110FILWWW00011-yahoo-impact-de-la-cyberattaque-plus-etendu.php>
<http://geeko.lesoir.be/2016/09/23/qui-se-cache-derriere-lattaque-de-yahoo/>
https://www.lesechos.fr/22/09/2016/lesechos.fr/0211319146141_yahoo--victime-d-une-nouvelle-fuite-massive-de-donnees.htm
https://blog.linkedin.com/2016/05/18/protecting-our-members?trk=li_tw_corp_coreyscott_protectingourmembers&sf26502733=1
http://www.lemonde.fr/pixels/article/2016/12/15/le-piratage-de-yahoo-revele-de-graves-defaillances_5049486_4408996.html#7mAs2YcT0iHFe7dX.99
<http://www.lefigaro.fr/secteur/high-tech/2016/12/28/32001-20161228ARTFIG00145-yahoo-deutsche-telekom-linkedin8230-2016-un-grand-millesime-pour-le-piratage.php>
<http://www.lefigaro.fr/secteur/high-tech/2016/05/18/32001-20160518ARTFIG00292-plus-de-100-millions-de-mots-de-passe-linkedin-dans-la-nature.php>
<https://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised>
http://www.lemonde.fr/pixels/article/2016/10/21/piratage-de-linkedin-arrestation-du-principal-suspect_5017979_4408996.html?xtmc=linkedin&xtcr=71
http://www.lemonde.fr/pixels/article/2016/05/18/des-millions-d-identifiants-linkedin-pirates-a-vendre_4921784_4408996.html?xtmc=linkedin&xtcr=33
<http://geeko.lesoir.be/2016/05/19/apres-un-piratage-linkedin-demande-a-ses-utilisateurs-de-changer-de-mot-de-passe/>
<http://geeko.lesoir.be/2016/12/15/plus-dun-milliard-de-comptes-yahoo-ont-ete-pirates/>
<https://blog.linkedin.com/2011/05/23/user-security>
<https://blog.linkedin.com/2012/06/06/updating-your-password-on-linkedin-and-other-account-security-best-practices>
<https://blog.linkedin.com/2012/06/07/taking-steps-to-protect-our-members>
<http://www.lalibre.be/economie/digital/usa-une-cyberattaque-massive-perturbe-de-nombreux-sites-internet-580a6891cd70fdfb1a55dedf>
<http://www.lefigaro.fr/flash-eco/2016/10/21/97002-20161021FILWWW00260-twitter-ebay-perturbes-par-une-cyberattaque.php>
<http://www.lefigaro.fr/secteur/high-tech/2016/12/28/32001-20161228ARTFIG00145-yahoo-deutsche-telekom-linkedin8230-2016-un-grand-millesime-pour-le-piratage.php>

<http://www.lefigaro.fr/secteur/high-tech/2016/10/21/32001-20161021ARTFIG00343-des-grands-sites-web-perturbes-par-une-immense-cyberattaque.php>
<http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>
<http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>
http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html#BhQoJg0i0tdlqIH99
<https://helpx.adobe.com/fr/x-productkb/policy-pricing/security-blog-en.html>
<http://geeko.lesoir.be/2013/10/04/29-millions-de-comptes-adobe-pirates-le-cloud-remis-en-question/>
<http://www.lalibre.be/economie/digital/sony-a-nouveau-victime-de-piratage-549cf3f6357028b5e9adbe61>
<http://www.lalibre.be/economie/digital/sony-va-bientot-redemarrer-playstation-network-51b8d22ee4b0de6db9c10f4c>
<https://www.sony.net/SonyInfo/News/Press/201105/11-0503E/>
http://www.lemonde.fr/a-la-une/article/2011/06/03/sony-a-nouveau-victime-de-piratage-informatique_1531431_3208.html#Jo1HwyZW0UJ3EC2699
<http://www.lalibre.be/economie/digital/anonymous-rend-le-catalogue-de-sony-en-acces-gratuit-51b8e443e4b0de6db9c52ebb>
<http://www.lalibre.be/economie/digital/sony-a-nouveau-victime-de-piratage-549cf3f6357028b5e9adbe61>
<https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>
http://www.lemonde.fr/pixels/article/2014/11/25/sony-pictures-paralyse-par-un-piratage-informatique_4529273_4408996.html#v5rqsasPB020i34D99
http://www.lemonde.fr/economie/article/2014/12/13/sony-pictures-face-a-un-piratage-historique_4540084_3234.html#ELqd7MHRHAOQjmjU99
http://www.lemonde.fr/pixels/article/2014/12/15/sony-pictures-exige-des-medias-qu-ils-detruisent-les-documents-pirates_4540425_4408996.html#HoRDr33KQzYxPEAm99
http://www.lemonde.fr/economie/article/2015/02/02/quand-le-crime-envahit-la-toile_4568029_3234.html#vCsGq1THQmqyKPgs99
<http://www.lalibre.be/economie/digital/les-services-playstation-retablis-apres-la-cyber-attaque-de-noel-54a01aaa357028b5e9b7b4c3>
<http://www.lalibre.be/economie/digital/les-services-de-playstation-perturbes-pour-le-3e-jour-consecutif-549fb381357028b5e9b65d43>
<http://www.lalibre.be/economie/digital/sony-a-nouveau-victime-de-piratage-549cf3f6357028b5e9adbe61>
<http://www.lalibre.be/economie/libre-entreprise/cyber-attaque-contre-une-filiale-de-sony-nous-plantons-le-drapeau-de-l-ei-sur-les-serveurs-53fad5f235708a6d4d516483>
http://www.lemonde.fr/pixels/article/2014/12/27/le-playstation-network-et-le-xbox-live-restent-perturbes-apres-une-possible-cyberattaque_4546734_4408996.html#EuX0k0ZHKFF6f1o599
http://www.lemonde.fr/pixels/article/2014/12/26/les-serveurs-de-la-xbox-et-de-la-playstation-en-panne_4546182_4408996.html#ztlv134kEos2EXqDD99
https://www.lesechos.fr/07/11/2016/lesechos.fr/0211469816937_tesco-bank-victime-d-une-attaque-informatique-sans-precedent.htm#4dy8sWjcGQ3uCTMB99
<http://corporate.tescobank.com/25/news/news-releases/an-updated-statement-for-current-account-customers-from-benny-higgins/?newsid=290>
<http://corporate.tescobank.com/25/news/news-releases/tesco-bank-announces-full-service-has-resumed-for-customers/?newsid=291>
<http://www.lefigaro.fr/secteur/high-tech/2013/07/23/32001-20130723ARTFIG00240-l-hebergeur-francais-ovh-victime-d-un-piratage.php>
<http://travaux.ovh.net/?do=details&id=8998>
<http://www.numerama.com/magazine/26577-ovh-victime-d-un-piratage-massif-de-ses-donnees-clients.html>

http://www.lemonde.fr/technologies/article/2013/07/23/ovh-se-fait-pirater-les-donnees-de-ses-clients-europeens_3452455_651865.html
<http://www.lefigaro.fr/secteur/high-tech/2016/09/26/32001-20160926ARTFIG00338-ovh-subit-la-premiere-attaque-menee-par-des-objets-connectes.php>
http://www.lemonde.fr/pixels/article/2016/09/26/derriere-une-serie-d-attaques-informatiques-tres-puissantes-un-reseau-d-objets-connectes-pirates_5003470_4408996.html#7U6YrDzglBrxCrRh.99
http://www.lemonde.fr/pixels/article/2016/09/26/derriere-une-serie-d-attaques-informatiques-tres-puissantes-un-reseau-d-objets-connectes-pirates_5003470_4408996.html?xtmc=ovh&xtcr=1
<http://www.leparisien.fr/high-tech/etats-unis-le-tramway-de-san-francisco-pirate-et-rendu-gratuit-28-11-2016-6386652.php>
<http://www.numerama.com/politique/213198-le-pirate-des-transports-de-san-francisco-est-un-habitué-du-ransomware.html>
<https://www.sfmta.com/about-sfmta/blog/update-sfmta-ransomware-attack>
<http://www.numerama.com/tech/212228-les-tramways-de-san-francisco-victimes-dun-piratage-massif.html>
<http://www.numerama.com/business/210357-un-operateur-britannique-se-fait-deroiber-les-donnees-de-133-000-clients.html>
<http://www.threemediacentre.co.uk/news/2016/handset-fraud-investigation.aspx>
http://www.lemonde.fr/pixels/article/2016/12/06/dailymotion-victime-d-un-vol-de-donnees_5044028_4408996.html#oy3EZG1rXJD2KTjO.99
<http://www.numerama.com/tech/214529-dailymotion-victime-dun-piratage-85-millions-de-comptes-concernees.html>
<http://blog.dailymotion.com/2016/12/06/8886/>
http://www.francetvinfo.fr/internet/les-donnees-du-service-de-videos-en-ligne-dailymotion-piratees_1956069.html
<http://geeko.lesoir.be/2016/12/07/dailymotion-victime-dun-vol-de-donnees-plus-de-80-millions-de-comptes-sont-concernees/>
http://www.lemonde.fr/economie/article/2014/01/22/aux-etats-unis-piratage-geant-des-clients-de-target_4352310_3234.html
http://www.lemonde.fr/economie/article/2015/02/02/du-crime-sur-la-toile_4568059_3234.html#dr7BqCj4e7EMoBYw.99
<https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car>
<https://corporate.target.com/article/2013/12/important-notice-unauthorized-access-to-payment-ca>
http://www.lemonde.fr/pixels/article/2016/02/24/des-hopitaux-francais-eux-aussi-victimes-de-chantage-informatique_4870885_4408996.html?xtmc=adobe&xtcr=48
<http://www.lefigaro.fr/secteur/high-tech/2016/02/16/32001-20160216ARTFIG00205-un-hopital-americain-paralyse-par-des-pirates-informatiques.php>
http://www.lemonde.fr/pixels/article/2016/02/16/un-hopital-americain-paralyse-par-des-pirates-informatiques_4866243_4408996.html

<http://www.leparisien.fr/faits-divers/los-angeles-un-hopital-verse-une-rancon-a-des-hackers-qui-le-pirataient-18-02-2016-5557129.php>
http://www.francetvinfo.fr/monde/un-hopital-de-los-angeles-ranconne-par-des-hackers_1706701.html
https://www.rtbf.be/info/monde/detail_usa-un-hopital-verse-une-rancon-a-des-pirates-informatiques?id=9216538
<http://www.lalibre.be/economie/placements/de-nouvelles-cyberattaques-sophistiquees-possibles-contre-le-systeme-financier-57945d71357086b3e0d7d9c8>
http://www.lemonde.fr/pixels/article/2017/03/23/la-coree-du-nord-accusee-du-piratage-de-la-banque-centrale-du-bangladesh_5099182_4408996.html

https://www.lesechos.fr/19/03/2016/lesechos.fr/021774994706_l-incroyable-cyber-braquage-de-la-banque-centrale-du-bangladesh.htm
<http://www.lefigaro.fr/secteur/high-tech/2016/03/11/32001-20160311ARTFIG00172-la-banque-centrale-du-bangladesh-se-fait-derober-81-millions-de-dollars.php>
<http://www.lalibre.be/economie/placements/de-nouvelles-cyberattaques-sophistiquees-possibles-contre-le-systeme-financier-57945d71357086b3e0d7d9c8>
<https://www.swift.com/insights/press-releases/swift-comments-on-malware-reports>
<https://www.newyorkfed.org/newsevents/statements/2016/0311-2016>
<http://www.la-croix.com/Economie/Monde/La-Banque-centrale-Bangladesh-victime-pirates-informatiques-2016-03-13-1200746334>
<http://www.europe1.fr/international/des-hackers-aurait-pu-voler-1-milliard-de-dollars-sils-naient-pas-fait-une-faute-dorthographe-2690758>
<https://www.newyorkfed.org/newsevents/statements/2016/0311-2016>
http://www.lemonde.fr/pixels/article/2016/12/15/le-piratage-de-yahoo-revele-de-graves-defaillances_5049486_4408996.html#7mAs2YcT0iHFe7dX.99
http://www.lemonde.fr/economie/article/2015/12/01/les-jouets-vtech-victimes-d-un-cybercriminel_4821275_3234.html?xtmc=sony_piratage&xtcr=21
https://www.vtech.com/en/press_release/2015/statement/
<http://geeko.lesoir.be/2015/12/01/les-profilis-de-milliers-denfants-touchees-par-une-cyber-attaque-contre-vtech/>
https://www.lesechos.fr/31/05/2016/lesechos.fr/021981878356_tumblr--myspace---des-millions-de-donnees-piratees-et-en-vente-sur-le-dark-web.htm
http://www.lemonde.fr/pixels/article/2016/12/01/tous-pirates_5041576_4408996.html?xtmc=yahoo&xtcr=37
 En savoir plus sur http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html#CEfpHOHLbbhhgKCM.99
<https://staff.tumblr.com/post/144263069415/we-recently-learned-that-a-third-party-had>
<http://geeko.lesoir.be/2016/05/31/65-millions-didentifiants-tumblr-en-vente-sur-internet/>
http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html#CEfpHOHLbbhhgKCM.99
<https://myspace.com/pages/blog>
http://www.lemonde.fr/pixels/article/2016/05/30/les-informations-de-millions-de-comptes-myspace-en-vente-en-ligne_4928733_4408996.html
<http://www.lemondeinformatique.fr/actualites/lire-blockchain-l-attaque-contre-the-dao-conduit-ethereum-a-proposer-un-fork-65194.html>
<https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/>
<http://www.lefigaro.fr/secteur/high-tech/2016/06/27/32001-20160627ARTFIG00068-dans-la-blockchain-le-code-ne-fait-plus-la-loi.php>
http://www.lemonde.fr/pixels/article/2015/12/10/suicides-demission-chantage-les-consequences-tragiques-du-piratage-du-site-de-rencontres-ashley-madison_4828391_4408996.html
http://www.lemonde.fr/pixels/article/2015/08/19/les-sites-de-rencontre-cibles-privilegiees-des-piratages_4730294_4408996.html#hMJAToTLiFkDloVV.99
http://www.lemonde.fr/pixels/article/2015/08/19/les-donnees-piratees-du-site-de-rencontres-adulteres-ashley-madison-publiees-en-ligne_4729818_4408996.html#KsIWSUJ3kqJeS8js.99
<http://madame.lefigaro.fr/societe/des-hackers-menacent-de-reveler-lidentite-des-utilisateurs-dun-site-de-rencontres-extra>
http://www.prnewswire.com/news-releases/statement-from-avid-life-media-inc-300115394.html?tc=eml_cleartime
<http://www.lefigaro.fr/flash-eco/2015/08/28/97002-20150828FILWWW00191-le-pdg->

d-ashley-madison-demissionne.php
<http://geeko.lesoir.be/2015/08/19/les-donnees-personnelles-de-37-millions-dinfideles-publiees-sur-la-toile/>
<http://geeko.lesoir.be/2015/07/20/des-pirates-menacent-de-devoiler-les-noms-et-details-de-37-millions-dinfideles/>
http://www.lemonde.fr/pixels/article/2015/05/22/les-informations-de-millions-d-utilisateurs-du-site-de-rencontres-adultfriendfinder-publiees_4638637_4408996.html
http://www.lemonde.fr/pixels/article/2016/12/15/le-piratage-de-yahoo-est-le-plus-important-vol-de-donnees-de-l-histoire_5049326_4408996.html#fmkL1LyL90vFvtW6.99
http://www.lemonde.fr/pixels/article/2016/11/14/le-site-de-rencontres-adultfriendfinder-pirate-412-millions-de-comptes-compromis_5031019_4408996.html#jWxBLt5qzBmoAtYd.99
http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html#CEfpHOHLbbhhgKCM.99
https://motherboard.vice.com/en_us/article/dropbox-forces-password-resets-after-user-credentials-exposed
http://www.lemonde.fr/pixels/article/2016/08/31/les-donnees-piratees-de-dropbox-en-2012-refont-surface_4990293_4408996.html?xtmc=dropbox&xtcr=8
<https://blogs.dropbox.com/dropbox/2012/07/security-update-new-features/>
<https://blogs.dropbox.com/dropbox/2016/08/resetting-passwords-to-keep-your-files-safe/>
https://www.lesechos.fr/31/08/2016/lesechos.fr/0211243940340_dropbox---plus-de-68-millions-d-identifiants-voles-circulent-sur-internet.htm
http://www.lemonde.fr/pixels/article/2016/08/31/les-donnees-piratees-de-dropbox-en-2012-refont-surface_4990293_4408996.html?xtmc=dropbox&xtcr=8
<https://blogs.dropbox.com/dropbox/2014/10/dropbox-wasnt-hacked/>
<http://www.numerama.com/magazine/30911-piratage-dropbox-7-millions-comptes.html>
http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html?xtmc=yahoo&xtcr=63
<http://geeko.lesoir.be/2015/12/14/twitter-previent-certains-utilisateurs-que-leur-compte-a-pu-etre-pirate/>
<https://blog.twitter.com/2010/ftc-announcement>
<https://blog.twitter.com/2013/keeping-our-users-secure>
<http://geeko.lesoir.be/2014/04/22/piratage-massif-de-comptes-sur-twitter/>
<https://blog.twitter.com/2014/keeping-your-twitter-account-safe>
<http://geeko.lesoir.be/2015/12/14/twitter-previent-certains-utilisateurs-que-leur-compte-a-pu-etre-pirate/>
<http://www.lalibre.be/economie/digital/twitter-previent-certains-utilisateurs-que-leur-compte-a-pu-etre-pirate-566e7c953570b38a5795ebcd>
<http://www.leparisien.fr/high-tech/twitter-previent-certains-utilisateurs-que-leur-compte-a-pu-etre-pirate-14-12-2015-5370581.php>
<http://www.lefigaro.fr/secteur/high-tech/2016/06/09/32001-20160609ARTFIG00161-un-hacker-russe-pretend-avoir-derobe-des-millions-de-mots-de-passe-twitter.php>
<https://blog.twitter.com/2016/keeping-your-account-safe>
<http://www.lesoir.be/1460778/article/actualite/fil-info/fil-info-monde/2017-03-15/twitter-confirme-piratage-comptes-du-une-application-tierce>
https://www.rtf.be/info/medias/detail_twitter-confirme-le-piratage-de-comptes-du-a-une-application-tierce?id=9554877
<http://www.lefigaro.fr/flash-actu/2017/03/15/97001-20170315FILWWW00113-twitter-confirme-le-piratage-de-comptes.php>
<http://www.lalibre.be/dernieres-depeches/afp/l-application-twitter-counter-confirme-un-piratage-58c90d7fcd705cd98df4ab95>

http://www.lemonde.fr/pixels/article/2017/02/28/les-donnees-personnelles-de-800-000-proprietaires-d-ours-en-peluche-connectes-accessibles-sur-internet_5087012_4408996.html?xtmc=spiral_toys&xtcr=1
http://www.lemonde.fr/technologies/article/2014/01/12/plusieurs-groupes-de-distribution-americains-victimes-de-pirates-informatiques_4346625_651865.html?xtmc=neiman_marcus&xtcr=21
<http://www.neimanmarcus.com/en-be/NM/Security-Info/cat49570732/c.cat>
<http://www.albertsons.com/ab-acquisition-llc-confirms-incident-involving-payment-card-data-processing/>
<http://www.albertsons.com/recent-update/>
<http://www.lsa-conso.fr/nouvelle-cyber-attaque-contre-deux-enseignes-americaines,182052>
<http://www.albertsons.com/ab-acquisition-llc-announces-discovery-of-separate-criminal-incident-involving-payment-card-data-processing/>
<http://www.albertsons.com/recent-update/>
<http://www.lefigaro.fr/flash-eco/2014/10/21/97002-20141021FILWWW00380-des-pirates-informatiques-volent-les-clients-de-staples.php>
<http://staples.newshq.businesswire.com/press-release/corporate/staples-provides-update-data-security-incident>
<http://bfmtv.com/01-business-forum/etats-unis-le-groupe-de-discount-kmart-victime-dune-cyber-attaque-628588.html>
<http://searsholdings.com/press-releases/pr/143>
<http://hightech.bfmtv.com/internet/les-palaces-du-groupe-hilton-victimes-de-piratage-de-cartes-bancaires-918192.html>
<http://hightech.bfmtv.com/internet/les-palaces-du-groupe-hilton-victimes-de-piratage-de-cartes-bancaires-918192.html>
<http://www.prnewswire.com/news-releases/white-lodging-releases-information-about-data-breach-investigation-at-select-food-and-beverage-outlets-300062065.html>
<http://www.michaels.com/payment-card-notice-faqs/payment-card-notice-faqs.html>
<http://www.businesswire.com/news/home/20140417006352/en/Michaels-Identifies-Previously-Announced-Data-Security-Issue#.U1A3P2fhf7w>
<http://www.lsa-conso.fr/michaels-stores-a-son-tour-victime-de-piratage-informatique-3-millions-de-cartes-de-credits-concernees,170868>
<http://www.sallybeautyholdings.com/investor-relations/press-releases/2014/03-05-2014-014510832>
<http://www.sallybeautyholdings.com/investor-relations/press-releases/2014/03-17-2014-014510723>
https://www.washingtonpost.com/business/economy/sally-beauty-confirms-data-breach/2014/03/17/c644049a-adf5-11e3-96dc-d6ea14c099f9_story.html
<http://www.lsa-conso.fr/le-distributeur-sally-beauty-nouvelle-victime-de-la-cybercriminalite,168224>
<http://www.sallybeautyholdings.com/investor-relations/press-releases/2015/05-04-2015-014508867>
<http://www.sallybeautyholdings.com/investor-relations/press-releases/2015/05-14-2015-014508648>
<http://www.sallybeautyholdings.com/investor-relations/press-releases/2015/05-28-2015-014508539>
<http://www.lalibre.be/economie/placements/de-nouvelles-cyberattaques-sophistiquees-possibles-contre-le-systeme-financier-57945d71357086b3e0d7d9c8>
http://www.morganstanley.com/pub/content/msdotcom/en/press-releases/morganstanley-says-employee-misappropriated-wealth-management-data_7f189537-f51c-40b0-a963-fc0dc6c65861.html

https://www.lesechos.fr/09/06/2016/lesechos.fr/0211012427508_morgan-stanley-n-a-pas-assez-protege-les-donnees-de-ses-clients.htm#vPG8bKzPsDmQPB13.99
http://www.lemonde.fr/economie/article/2014/05/07/orange-de-nouveau-victime-d-une-cyberattaque-massive_4412779_3234.html
http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html#CEfpHOHLbbhhgKCM.99
<http://www.lefigaro.fr/secteur/high-tech/2014/05/07/32001-20140507ARTFIG00167-orange-une-cible-privilegiee-pour-les-pirates.php>
<http://www.lefigaro.fr/secteur/high-tech/2014/02/03/32001-20140203ARTFIG00003-les-donnees-personnelles-de-800000-clients-orange-pirates.php>
<http://www.numerama.com/magazine/28219-orange-avait-promis-la-securite-des-donnees-persos-rate.html>
<http://www.numerama.com/magazine/30336-donnees-de-clients-pirates-la-cnill-juge-orange-coupable-et-puis-c-est-tout.html>
http://www.liberation.fr/ecrans/2013/11/19/deni-de-service-attaque-par-saturation_948075
http://www.lemonde.fr/societe/article/2013/11/18/le-site-de-liberation-bloque-par-une-attaque-informatique_3515786_3224.html
<http://tempsreel.nouvelobs.com/faits-divers/20131118.OBS5890/le-site-internet-de-liberation-victime-d-une-attaque-informatique.html>
<http://www.rtl.fr/actu/coups-de-feu-a-liberation-le-site-internet-du-quotidien-pirate-7766957027>
<http://tempsreel.nouvelobs.com/rue89/rue89-making-of/20140730.RUE5123/au-sujet-des-difficultes-rencontrees-sur-rue89-mardi-et-mercredi.html>
<http://www.numerama.com/magazine/25641-mediapart-pirate-des-donnees-bancaires-derobees.html>
<https://blogs.mediapart.fr/la-redaction-de-mediapart/blog/100413/nos-abonnes>
<http://www.numerama.com/magazine/25641-mediapart-pirate-des-donnees-bancaires-derobees.html>
<http://www.lefigaro.fr/flash-actu/2013/04/10/97001-20130410FILWWW00760-le-site-de-mediapart-pirate.php>
<http://www.ouest-france.fr/europe/france/piratage-les-sites-de-mediapart-le-parisien-france-info-attaques-3119224>
http://www.lemonde.fr/actualite-medias/article/2014/08/22/plainte-de-mediapart-apres-une-attaque-informatique-contre-son-site_4475529_3236.html?xtmc=ulcan&xtcr=17
<https://www.mediapart.fr/journal/france/220814/apres-rue89-et-mediapart-la-police-sur-les-traces-du-hacker-ulcan>
http://www.lemonde.fr/pixels/article/2014/10/09/ulcan-revendique-des-attaques-contre-les-sites-de-france-inter-et-france-info_4503864_4408996.html?xtmc=ulcan&xtcr=13
<http://tvmag.lefigaro.fr/le-scan-tele/polemiques/2014/10/10/28003-20141010ARTFIG00096-le-hacker-ulcan-revendique-le-piratage-des-sites-web-de-france-info-et-france-inter.php>
http://www.liberation.fr/societe/2014/10/09/ulcan-revendique-un-nouveau-piratage-de-sites-d-info_1118579
http://www.lemonde.fr/pixels/article/2014/10/02/le-site-internet-du-parisien-vise-par-une-attaque_4499621_4408996.html?xtmc=ulcan&xtcr=14
http://www.lemonde.fr/actualite-medias/breve/2014/08/24/le-site-arret-sur-images-a-son-tour-vise-par-des-attaques-informatiques_4475815_3236.html
http://www.lemonde.fr/pixels/article/2016/12/15/le-piratage-de-yahoo-est-le-plus-important-vol-de-donnees-de-l-histoire_5049326_4408996.html?xtmc=yahoo&xtcr=30
<http://www.hackingteam.it/news/2015/07/22/statement-from-hackingteam.html>

<http://www.lefigaro.fr/secteur/high-tech/2015/07/06/32001-20150706ARTFIG00097-le-spectaculaire-piratage-d-une-societe-de-surveillance-des-internautes.php>
http://www.lemonde.fr/pixels/article/2015/08/10/une-faille-de-securite-de-hacking-team-a-ete-utilisee-par-un-important-groupe-de-pirates_4719735_4408996.html
<https://www.nextinpact.com/news/95703-surveillance-masse-hacking-team-piratee-400-go-donnees-seraient-dans-nature.htm>
http://www.lemonde.fr/pixels/article/2016/11/30/les-identifiants-de-milliers-d-utilisateurs-du-site-pornographique-xhamster-publies-en-ligne_5040806_4408996.html#Om71mZ49kDvgXQRI.99
<http://www.numerama.com/tech/213109-plus-de-380-000-comptes-xhamster-derobes-et-mis-en-vente-par-des-pirates.html>
http://www.lemonde.fr/pixels/article/2015/08/19/les-sites-de-rencontre-cibles-privilegiees-des-piratages_4730294_4408996.html#hMJAtLiFkDloVV.99
http://www.lemonde.fr/technologies/article/2010/07/08/le-site-de-partage-the-pirate-bay-pirate_1385387_651865.html
<http://www.france24.com/fr/20100709-the-pirate-bay-hacking-russo-argentin-sql-download-telechargement-illegal>
<http://www.ouest-france.fr/high-tech/telechargement-illegal-pirate-bay-ferme-copie-ressuscite-3057624>
http://www.lemonde.fr/pixels/article/2015/08/19/les-sites-de-rencontre-cibles-privilegiees-des-piratages_4730294_4408996.html#hMJAtLiFkDloVV.99
http://www.lemonde.fr/pixels/article/2015/08/19/les-sites-de-rencontre-cibles-privilegiees-des-piratages_4730294_4408996.html#hMJAtLiFkDloVV.99
http://www.lemonde.fr/technologies/article/2013/11/20/42-millions-d-adresses-electroniques-volees-sur-des-sites-de-rencontre_3517437_651865.html#rSLvCvgixPI23pmd.99
http://www.lemonde.fr/pixels/article/2015/08/19/les-sites-de-rencontre-cibles-privilegiees-des-piratages_4730294_4408996.html#hMJAtLiFkDloVV.99
<https://topface.com/user-data/>
<http://www.numerama.com/tech/174614-171-millions-de-mots-de-passe-du-clone-russe-de-facebook-pirates.html>
<http://www.lefigaro.fr/actualite-france/2015/06/09/01016-20150609ARTFIG00401-cyberattaque-contre-tv5-monde-la-piste-russe-envisagee.php>
<http://www.lefigaro.fr/secteur/high-tech/2015/04/09/32001-20150409ARTFIG00231-les-medias-cibles-de-choix-des-hackeurs.php>
http://www.lemonde.fr/pixels/article/2015/06/09/piratage-de-tv5-monde-l-enquete-s-oriente-vers-la-piste-russe_4650632_4408996.html
<http://tvmag.lefigaro.fr/programme-tv/article/television/86345/la-chaine-tv5-monde-piratee-par-des-militants-de-l-etat-islamique.html>
<http://www.lefigaro.fr/actualite-france/2015/06/09/01016-20150609ARTFIG00401-cyberattaque-contre-tv5-monde-la-piste-russe-envisagee.php>
http://www.lemonde.fr/pixels/article/2015/04/13/tv5-monde-les-pirates-ont-infiltre-la-chaine-plusieurs-semaines-avant-l-attaque_4614813_4408996.html
http://www.lemonde.fr/pixels/article/2015/04/09/tv5-monde-un-piratage-d-ampleur-et-de-nombreuses-zones-d-ombre_4613300_4408996.html
http://www.lemonde.fr/international/article/2016/12/28/l-osce-victime-d-une-attaque-informatique_5054744_3210.html
http://www.lemonde.fr/pixels/article/2017/02/24/arrestation-d-un-britannique-suspecte-d-etre-responsable-des-attaques-informatiques-massives-de-2016_5084777_4408996.html?xtmc=deutsche%20telekom&xtcr=1
<http://www.lefigaro.fr/secteur/high-tech/2016/11/28/32001-20161128ARTFIG00268-des-pirates-auraient-reussi-a-priver-900000-foyers-allemands-d-internet.php>
<http://www.lefigaro.fr/flash-eco/2016/11/28/97002-20161128FILWWW00143-allemande-1-million-de-foyers-prives-d-internet.php>

<https://www.telekom.com/en/media/media-information/archive/13-answers-to-attack-on-routers-445148>
<https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862>
<http://www.lefigaro.fr/societes/2016/11/22/20005-20161122ARTFIG00358-vinci-victime-d-une-attaque-de-pirates-informatiques.php>
<http://www.numerama.com/tech/211306-ingenierie-sociale-piratage-vinci-une-inattention-qui-coute-cher.html>
<http://www.europe1.fr/societe/vinci-histoire-dun-piratage-eclair-2909114>
<https://www.vinci.com/vinci.nsf/fr/communiqués/pages/20161123-1845.htm>
http://www.lemonde.fr/economie-francaise/article/2016/11/23/comment-le-groupe-vinci-victime-d-un-hoax-a-chute-en-bourse_5036269_1656968.html
http://www.lemonde.fr/pixels/article/2016/02/24/des-hopitaux-francais-eux-aussi-victimes-de-chantage-informatique_4870885_4408996.html#AmW4bUgozArxIH8h.99
<http://info.arte.tv/fr/hacking-medical>
<http://www.numerama.com/business/128037-grave-piratage-de-loperateur-talktalk-4-millions-de-clients-concernees.html>
<http://www.lefigaro.fr/flash-eco/2015/10/23/97002-20151023FILWWW00213-les-donnees-de-millions-de-britanniques-menacees.php>
<http://www.lefigaro.fr/flash-actu/2015/10/26/97001-20151026FILWWW00338-piratage-de-talktalk-un-ado-de-15-ans-arrete.php>
http://www.lemonde.fr/pixels/article/2016/12/13/un-adolescent-de-17-ans-condamne-pour-le-piratage-du-fai-britannique-talktalk_5048318_4408996.html
http://www.lemonde.fr/pixels/article/2015/10/27/un-adolescent-de-15-ans-arrete-pour-le-piratage-du-fai-britannique-talktalk_4797566_4408996.html
<http://www.ab-consulting.fr/blog/tag/talk-talk>
<http://help.talktalk.co.uk/>
<http://www.numerama.com/politique/129106-loperateur-vodafone-touche-par-un-piratage.html>
<https://mediacentre.vodafone.co.uk/pressrelease/statement-on-unauthorised-account-access/>
<http://www.lefigaro.fr/secteur/high-tech/2016/09/07/32001-20160907ARTFIG00063-plus-de-790000-utilisateurs-d-un-site-pornographique-americain-touchees-par-un-piratage.php>
https://motherboard.vice.com/en_us/article/nearly-800000-brazzers-porn-site-accounts-exposed-in-forum-hack
<https://blog.avast.com/2014/05/26/avast-forum-offline-due-to-attack/>
<https://www.nextinpact.com/news/87788-avast-forum-pirate-4-millions-comptes-touchees-mots-passe-en-danger.htm>
<http://www.lefigaro.fr/secteur/high-tech/2016/08/03/32001-20160803ARTFIG00143-des-pirates-volent-72-millions-de-dollars-a-une-plateforme-de-bitcoin.php>
<http://www.numerama.com/business/187125-le-bitcoin-devisse-apres-un-piratage-a-65-millions-de-dollars.html>
<https://bitfinex.statuspage.io/incidents/6174rk4zpyv8>
<https://bitfinex.statuspage.io/incidents/hx2vb8jngghb>
<https://www.nextinpact.com/news/100914-bitfinex-apres-vol-119-756-bitcoins-clients-en-seront-leur-poche.htm>
<http://geeko.lesoir.be/2016/06/21/les-donnees-bancaires-de-34500-clients-dacer-ont-ete-derobees/>
<http://geeko.lesoir.be/2015/01/21/le-compte-twitter-du-journal-le-monde-pirate-par-larmee-electronique-syrienne/>
<http://www.lefigaro.fr/secteur/high-tech/2015/01/21/32001-20150121ARTFIG00134-le-compte-twitter-du-monde-pirate-par-l-armee-electronique-syrienne.php>
<http://www.lemonde.fr/pixels/article/2015/01/24/comment-notre-compte-twitter-a>

[ete-pirate_4562506_4408996.html](#)
http://www.lemonde.fr/pixels/article/2015/01/21/le-compte-twitter-du-monde-pirate_4560072_4408996.html
http://www.lemonde.fr/pixels/article/2015/01/20/comment-le-monde-a-ete-pirate-par-l-armee-electronique-syrienne_4559393_4408996.html
<http://www.lefigaro.fr/flash-eco/2014/05/27/97002-20140527FILWWW00282-spotify-victime-d-un-piratage.php>
<https://news.spotify.com/fr/2014/05/27/important-notice-to-our-users/>
<http://geeko.lesoir.be/2016/04/26/des-milliers-de-comptes-spotify-pirates/>
<http://www.lesoir.be/230956/article/economie/2013-04-23/piratage-du-compte-twitter-l-ap-fait-chuter-dow-jones>
<http://geeko.lesoir.be/2013/04/24/twitter-va-relever-dun-cran-la-securite-de-ses-comptes/>
http://www.lemonde.fr/technologies/article/2013/04/23/le-compte-twitter-de-l-agence-associated-press-pirate_3165036_651865.html#QJaziz7DqrlXzI0.99
<http://www.lefigaro.fr/secteur/high-tech/2016/08/03/32001-20160803ARTFIG00151-telegram-victime-du-piratage-de-15-millions-de-comptes-en-iran.php>
http://www.liberation.fr/futurs/2016/08/03/piratage-de-telegram-en-iran-qui-se-cache-derriere-les-hackers_1470054
http://www.lemonde.fr/pixels/article/2016/08/03/telegram-dement-le-piratage-de-son-service-en-iran_4977934_4408996.html
<http://www.numerama.com/tech/187387-telegram-conteste-le-piratage-de-son-application-mobile-en-iran.html>
<http://www.lefigaro.fr/flash-actu/2016/01/02/97001-20160102FILWWW00077-un-groupe-anti-daech-revendique-le-piratage-de-la-bbc.php>
<http://www.bbc.com/news/technology-35204915>
<http://www.bfmtv.com/international/l-ei-pirate-le-compte-twitter-du-commandement-militaire-americain-au-moyen-orient-857036.html>
https://motherboard.vice.com/en_us/article/some-docs-leaked-by-centcom-twitter-hackers-were-not-public-army-says
http://www.lemonde.fr/proche-orient/article/2015/01/12/un-groupe-se-reclamant-de-l-etat-islamique-pirate-un-compte-twitter-de-l-armee-americaine_4554711_3218.html
<http://www.numerama.com/magazine/31846-des-hackers-de-l-etat-islamique-pirant-l-armee-americaine-maj.html>
<http://www.numerama.com/magazine/26238-auchan-se-fait-pirater-son-compte-twitter.html>
http://www.lemonde.fr/pixels/article/2015/01/03/le-site-de-tf1-pirate-les-donnees-de-2-millions-de-personnes-derobees_4548802_4408996.html
<http://www.leparisien.fr/high-tech/tf1-pirate-des-hackers-derobent-les-donnees-de-1-9-millions-de-clients-03-01-2015-4416577.php>
http://www.lemonde.fr/technologies/article/2013/03/04/pirate-evernote-reinitialise-les-mots-de-passe-de-ses-membres_1842613_651865.html
<http://blog.evernote.com/blog/2013/03/02/security-notice-service-wide-password-reset/>
https://www.lesechos.fr/02/10/2015/lesechos.fr/021374129195_les-donnees-de-15-millions-de-clients-de-t-mobile-piratees.htm
<https://www.t-mobile.com/landing/experian-data-breach>
<http://www.experian.com/data-breach/t-mobilefacts.html>
https://www.lesechos.fr/15/03/2016/lesechos.fr/021767694479_les-sites-de-canal-et-canal-play-pirates.htm
<http://tvmaq.lefigaro.fr/le-scan-tele/actu-tele/2016/03/15/28001-20160315ARTFIG00068-les-sites-internet-de-canal-et-canalplay-pirates.php>
http://www.lepoint.fr/high-tech-internet/les-sites-de-canal-et-canal-play-un-court-instant-pirates-15-03-2016-2025525_47.php

<https://www.nextinpact.com/archive/66872-steam-forum-piratage-defacage-ferme.htm>
<http://www.lefigaro.fr/flash-actu/2016/08/14/97001-20160814FILWWW00080-le-site-internet-de-la-ville-de-toulon-pirate.php>
https://www.rtb.be/info/medias/detail_ukraine-un-black-out-cause-par-une-cyberattaque-une-premiere-mondiale?id=9178147
<http://www.lefigaro.fr/flash-actu/2016/01/05/97001-20160105FILWWW00381-ukraine-une-cyberattaque-coupe-l-electricite.php>
http://www.lemonde.fr/pixels/article/2016/01/05/un-piratage-soupconne-d-etre-a-l-origine-d-une-coupure-electrique-en-ukraine_4841756_4408996.html
<http://www.numerama.com/tech/137182-un-piratage-serait-a-lorigine-dune-coupure-delectricite-en-ukraine.html>
<http://www.rtl.be/info/belgique/societe/attention-un-faux-concours-colruyt-circule-917303.aspx>
https://www.rtb.be/info/medias/detail_le-site-economie-wallonie-be-hacke-par-des-pirates-tunisiens?id=8953280
<http://www.lesoir.be/847882/article/economie/vie-du-net/2015-04-10/un-site-du-gouvernement-wallon-pirate-par-des-hackers-tunisiens>
<http://www.lefigaro.fr/secteur/high-tech/2016/12/21/32001-20161221ARTFIG00223-le-compte-twitter-de-netflix-a-ete-pirate.php>
<http://geeko.lesoir.be/2016/12/21/le-compte-twitter-de-netflix-a-ete-pirate/>
<http://www.lefigaro.fr/secteur/high-tech/2016/12/21/32001-20161221ARTFIG00223-le-compte-twitter-de-netflix-a-ete-pirate.php>
<http://geeko.lesoir.be/2017/05/02/netflix-pirate-par-un-groupe-de-hackers/>
<http://geeko.lesoir.be/2015/01/26/le-site-de-malaysia-airlines-pirate-avec-beaucoup-dhumour/>
<http://www.lemondeinformatique.fr/actualites/lire-alibaba-piege-par-une-banale-faille-de-securite-59565.html>
http://www.lemonde.fr/asie-pacifique/article/2014/12/23/le-nucleaire-sud-coreen-vise-par-un-piratage_4545388_3216.html
<http://www.lemondeinformatique.fr/actualites/lire-le-geant-du-nucleaire-coreen-victime-de-cyber-pirates-59712.html>