Mon e-mail a-t-il été piraté ? Vérifier, quoi faire ?

Les vols de données sont nombreux, les médias en rapportent quotidiennement plusieurs cas. Ils ont pour origine des causes diverses : des mots de passe trop simples, une mauvaise configuration technique, des failles logicielles, des erreurs humaines, des piratages de sites, des phishings…

Les hackers rassemblent les informations volées dans des bases de données et les revendent sur le Dark Web. Ces informations permettent de collecter des données en masse. Ainsi les identifiants et les mots de passe vont autoriser des connections sur des sites bancaires ou de commerce pour voler des informations, réaliser des escroqueries ou encore des usurpations d'identité. Les adresses e-mail pourront aussi être revendues à des spammeurs.

Des chercheurs en sécurité ont récupéré ces bases de données et les ont mis sur des sites pour que les internautes puissent vérifier si leurs adresses e-mail ont été l'objet de fuites. Ces collections proviennent pour la plupart de sites piratés dans un passé récent comme Yahoo, LinkedIn, Orange et de nombreux autres.

Vous trouverez ci-après trois sites qui vous permettront de vérifier si vos adresses de courriel ont fait l'objet de fuites de données et si elles ont été ou risquent d'être piratées.

Notez que comme ces sites n'utilisent pas forcément les mêmes bases de données, les résultats peuvent être différents pour une adresse e-mail donnée.

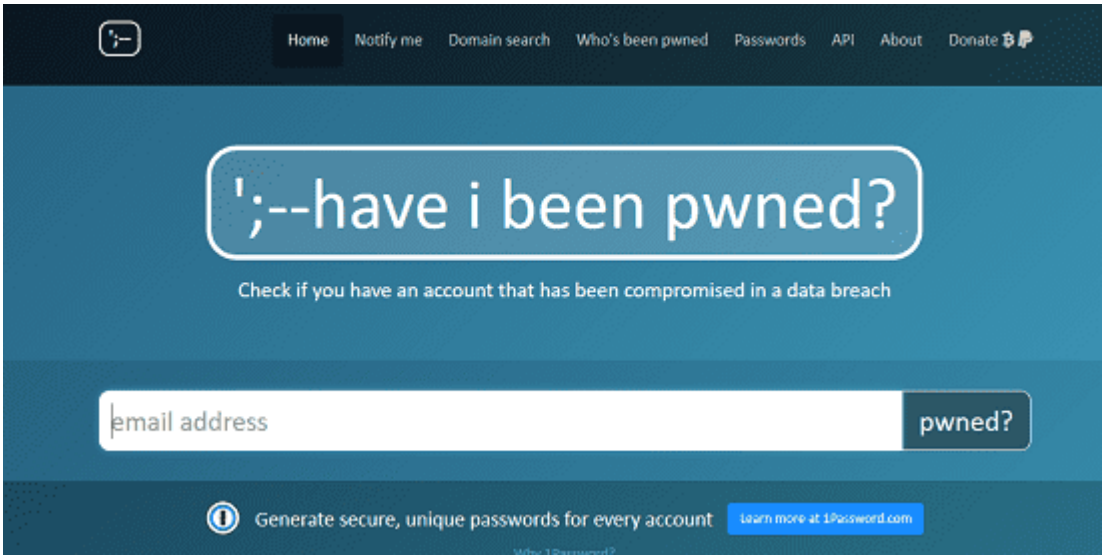
1 - Trois sites pour savoir si votre adresse est compromise

1.1 - Le 1er site est : « *Have I been pwned* »

Le site internet « *Have I been pwned*« , en français « *me suis-je fait avoir ?* » (HIBP) a été créé par Troy Hunt un expert en sécurité australien collaborateur de Microsoft. Ce site permet de **vérifier si votre email ou votre pseudo a été compromis sur plus d'une centaine de sites ou d'applications qui ont été un**

jour piratées (LinkedIn, Domino's pizzas, Minecraft, Yahoo, Snapchat, …). Le site recense plus d'un demi-milliard de comptes compromis.

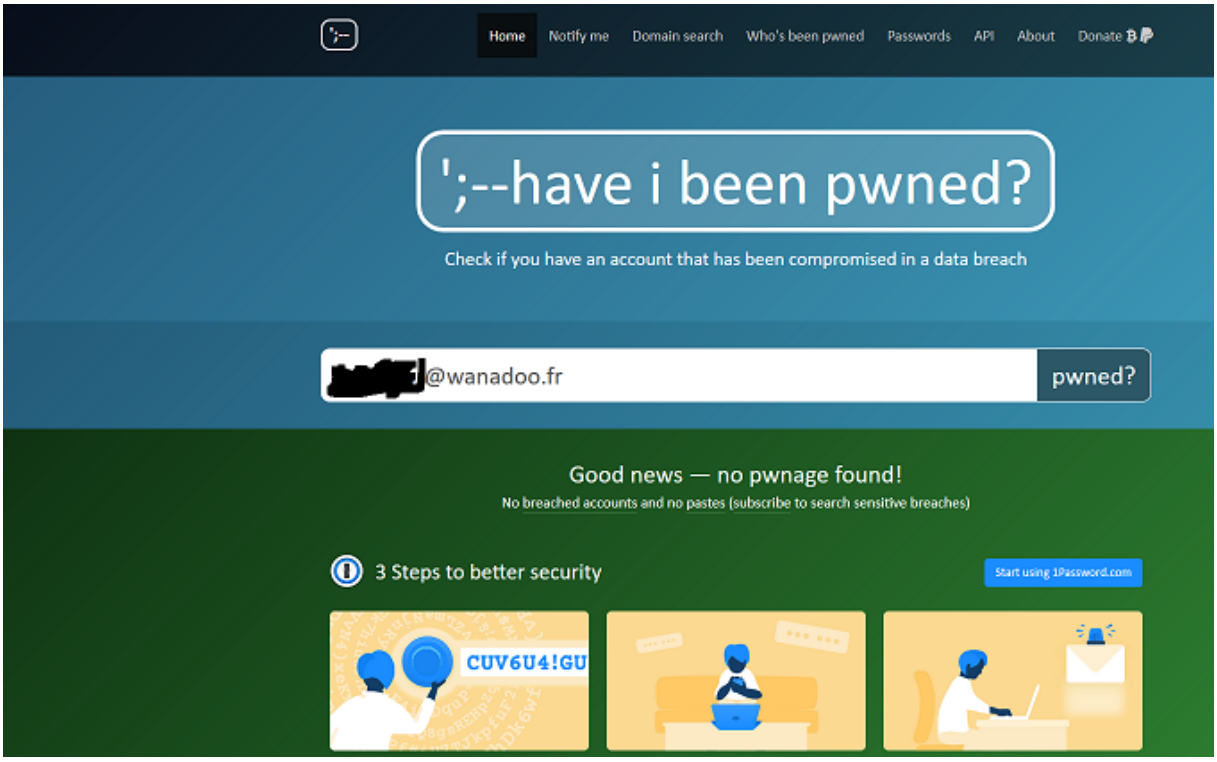
L'adresse du site est : https://haveibeenpwned.com/



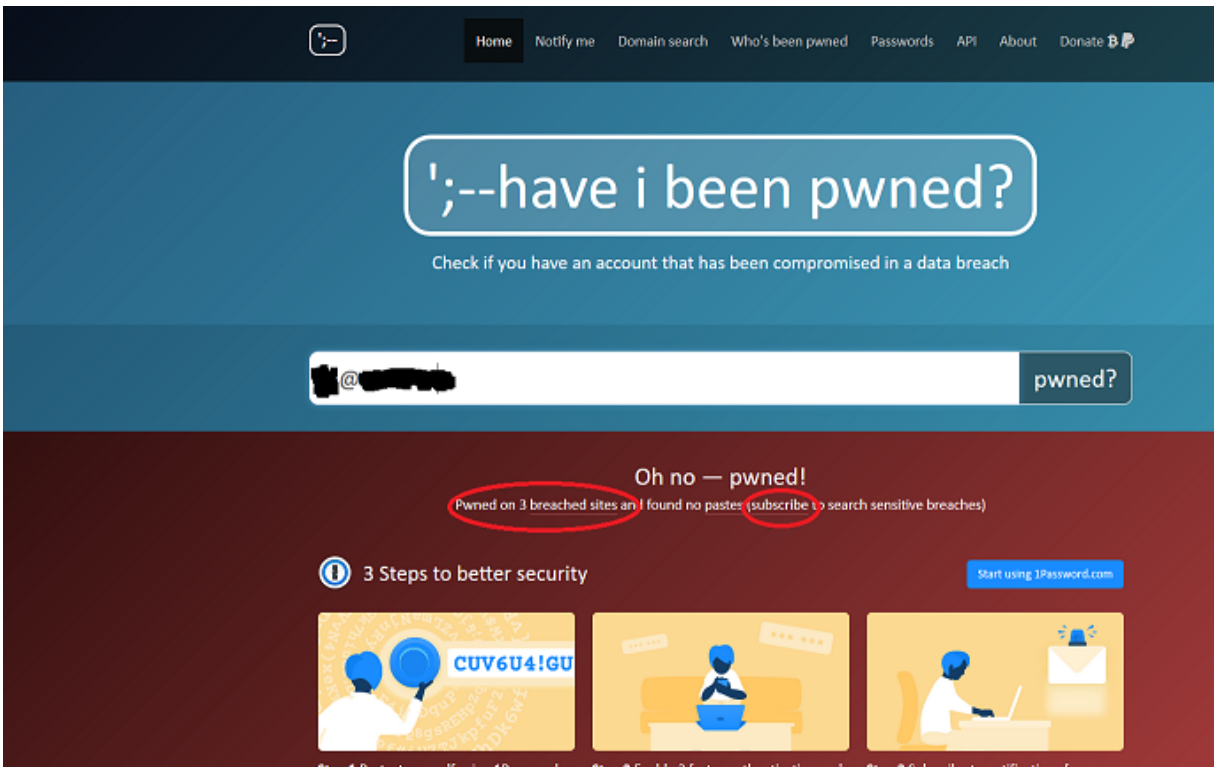
Ouvrez le site et entrez une adresse email puis cliquez sur le bouton « pwned ? »

Une nouvelle fenêtre s'ouvre.

Si cette fenêtre sous fond vert indique « Good news – no pwnage found ! » cela signifie que votre adresse email n'a pas été trouvée dans la base de données.

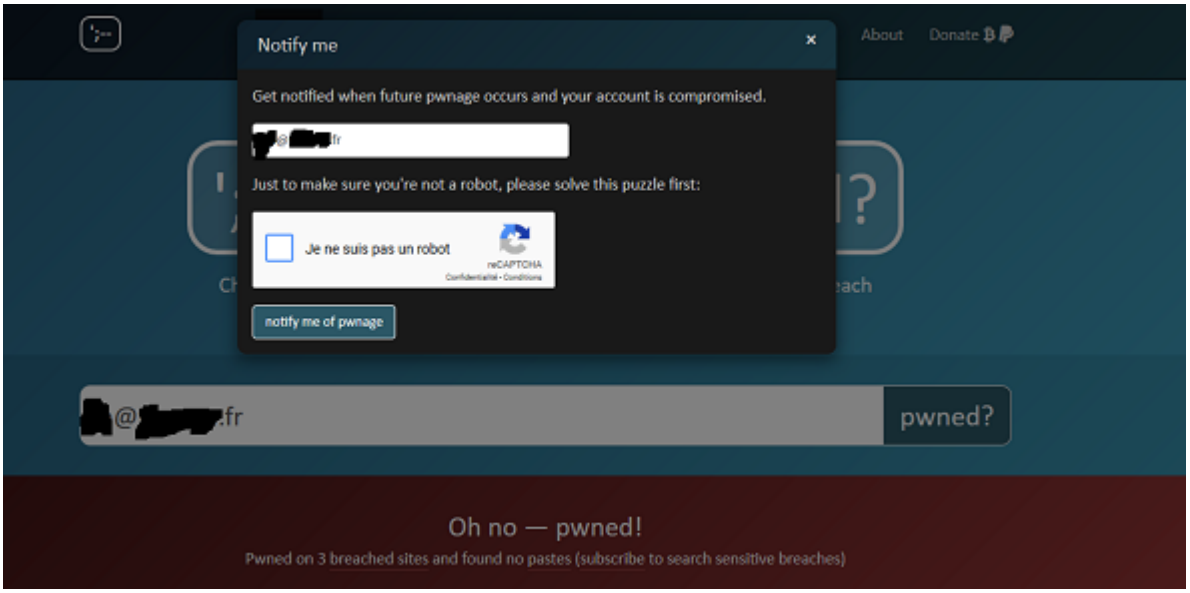


Si en revanche, c'est une fenêtre sur fond rouge comme celle-ci-dessous qui s'affiche, avec marqué : « Oh no – pwned ! » (Oh non - vous vous êtes fait avoir !), cela signifie que votre adresse a été compromise.

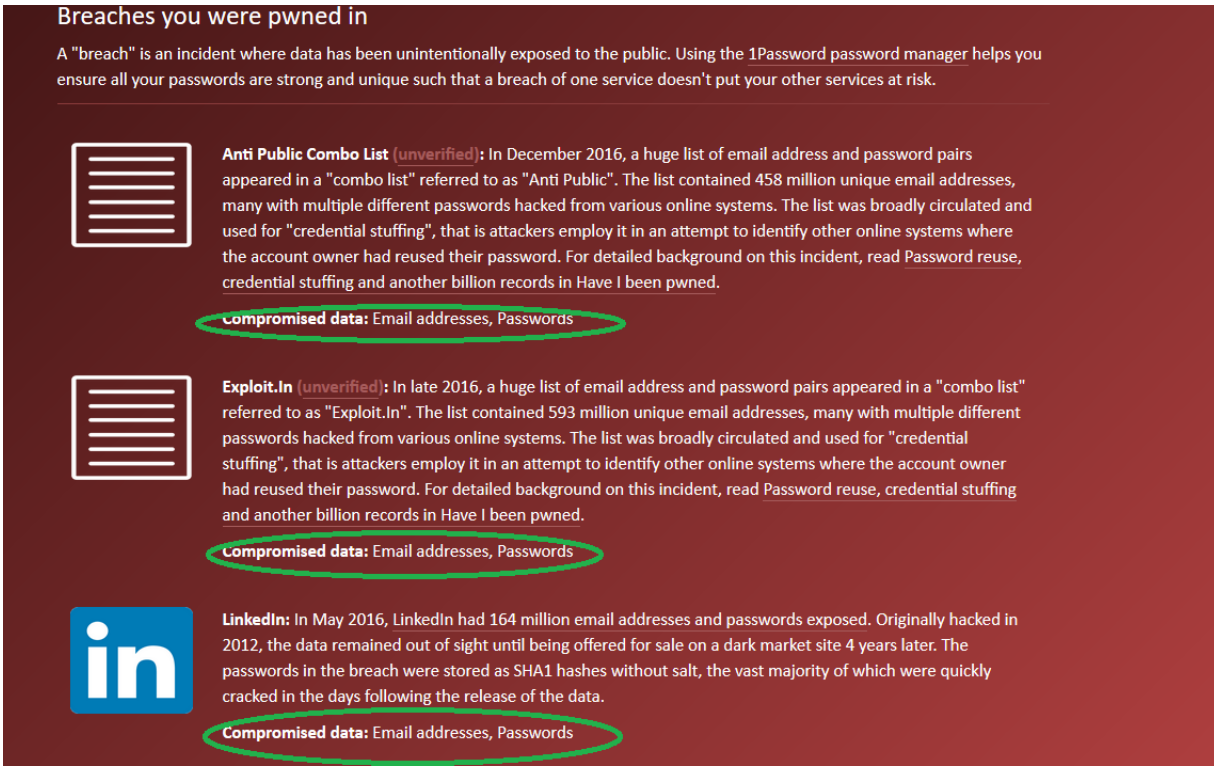


L’inscription sous : « Oh no – pwned ! » précise que dans cet exemple, trois brèches de sécurité ont été trouvées (Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches).

Cliquez sur le mot « subscribe » de cette phase, ressaisissez l’adresse email , renseignez le captcha (je ne suis pas un robot) et cliquez sur le bouton « notify me of pwnage ».



Vous allez recevoir un email (en anglais ☹) à cette adresse (vérifiez vos courriers indésirables le cas échéant). Dans le mail cliquez sur « Verify my email ». Le site s’ouvre avec des précisions complémentaires concernant les données compromises.



On peut lire notamment :

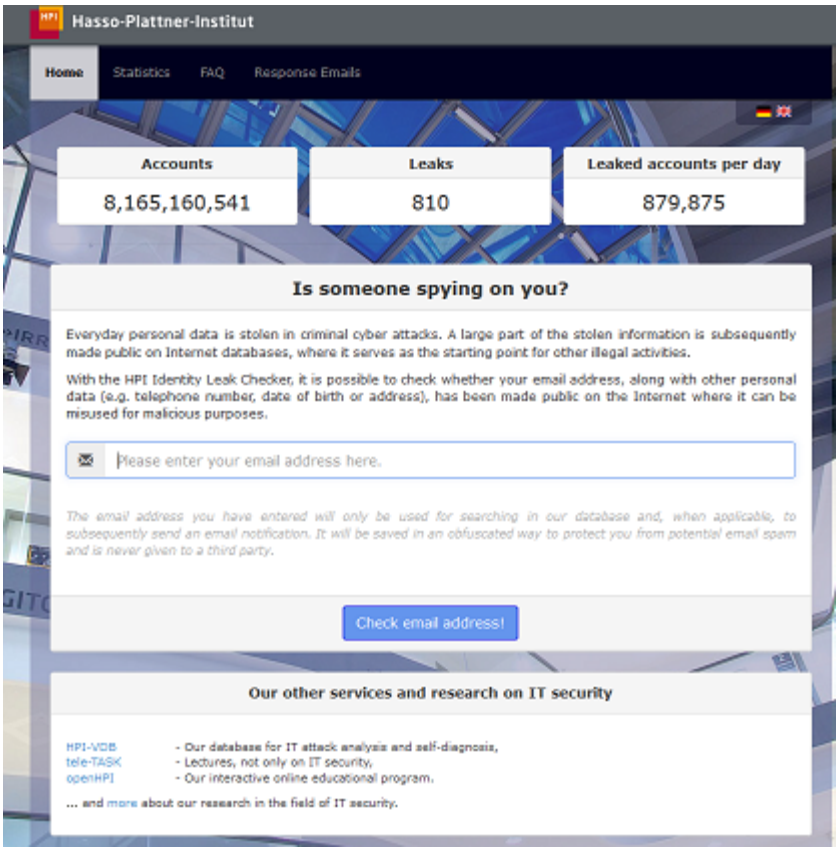
- Que ce sont à chaque fois l'adresse email et le mot de passe qui ont été volés,
- Qu'une des fuites vient du site Linkedln piraté en mai 2016,
- Que les 2 premières compromissions ont été détectées sur des listes concernant d'autres site piratés mais plus ou moins indéterminés.

1.2 - Le 2ème site est celui de Hasso-Platter-Institut

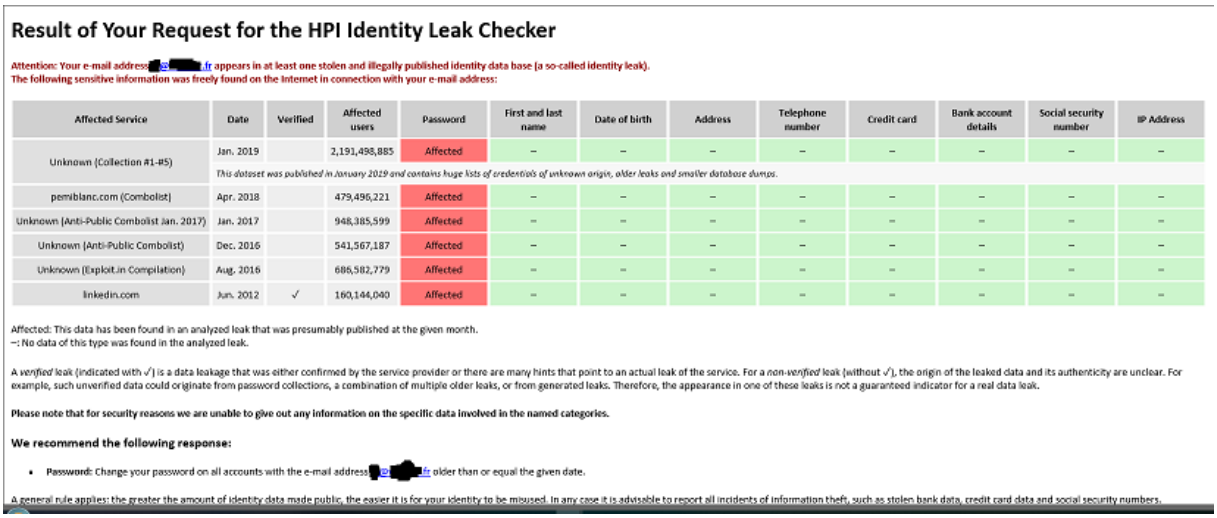
L'Identity Leak Checker est un site animé par l'institut Hasso-Plattner de Postdan, il permet aussi la recherche de données d'identification dérobées.

Son adresse est : https://sec.hpi.uni-potsdam.de/ilc/search?lang=en

Allez sur la page d'accueil d' Identity Leak Checker et renseignez l'adresse email à vérifier. Cliquez sur « Check email address ! ».



Quelques minutes plus tard vous recevrez à l'adresse e-mail renseignée le résultat des recherches qui ressemblera à la capture ci-après.



Result of Your Request for the HPI Identity Leak Checker

Attention: Your e-mail address [redacted].fr appears in at least one stolen and illegally published identity data base (a so-called identity leak).
The following sensitive information was freely found on the Internet in connection with your e-mail address:

Affected Service	Date	Verified	Affected users	Password	First and last name	Date of birth	Address	Telephone number	Credit card	Bank account details	Social security number	IP Address
Unknown (Collection #1-#5)	Jan. 2019		2,191,498,885	Affected	–	–	–	–	–	–	–	–
	This dataset was published in January 2019 and contains huge lists of credentials of unknown origin, older leaks and smaller database dumps.											
pemiblanc.com (Combolist)	Apr. 2018		479,496,221	Affected	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist Jan. 2017)	Jan. 2017		948,385,599	Affected	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist)	Dec. 2016		541,567,187	Affected	–	–	–	–	–	–	–	–
Unknown (Exploit.in Compilation)	Aug. 2016		686,582,779	Affected	–	–	–	–	–	–	–	–
linkedin.com	Jun. 2012	✓	160,144,040	Affected	–	–	–	–	–	–	–	–

Affected: This data has been found in an analyzed leak that was presumably published at the given month.
–: No data of this type was found in the analyzed leak.

A *verified* leak (indicated with ✓) is a data leakage that was either confirmed by the service provider or there are many hints that point to an actual leak of the service. For a *non-verified* leak (without ✓), the origin of the leaked data and its authenticity are unclear. For example, such unverified data could originate from password collections, a combination of multiple older leaks, or from generated leaks. Therefore, the appearance in one of these leaks is not a guaranteed indicator for a real data leak.

Please note that for security reasons we are unable to give out any information on the specific data involved in the named categories.

We recommend the following response:

- **Password:** Change your password on all accounts with the e-mail address [redacted].fr older than or equal the given date.

A general rule applies: the greater the amount of identity data made public, the easier it is for your identity to be misused. In any case it is advisable to report all incidents of information theft, such as stolen bank data, credit card data and social security numbers.

Identity Leak Checker en plus de vérifier si votre adresse email a été piratée ou risque de l'être, précise également si d'autres informations comme votre numéro de téléphone, votre date de naissance ou encore votre adresse postale ont aussi été volés. Il rajoutera la date et le site origine de la fuite.

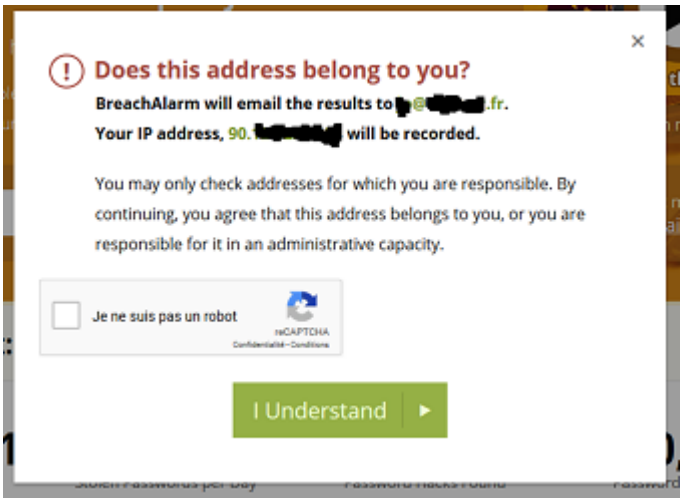
1.3 - Le 3ème site est [BreachAlarm]

BreachAlarm (que l'on peut traduire par « *alarme de brèche* ») est un site anglophone dont les fonctionnalités ressemblent à celles de Have I been pwned

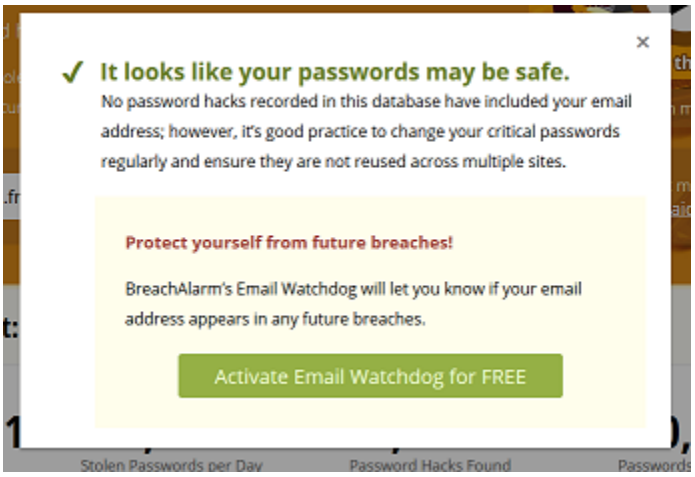
Son adresse est : https://breachalarm.com/

Comme pour les autres sites, entrez l'adresse email et cliquez sur le bouton « Check Now ».

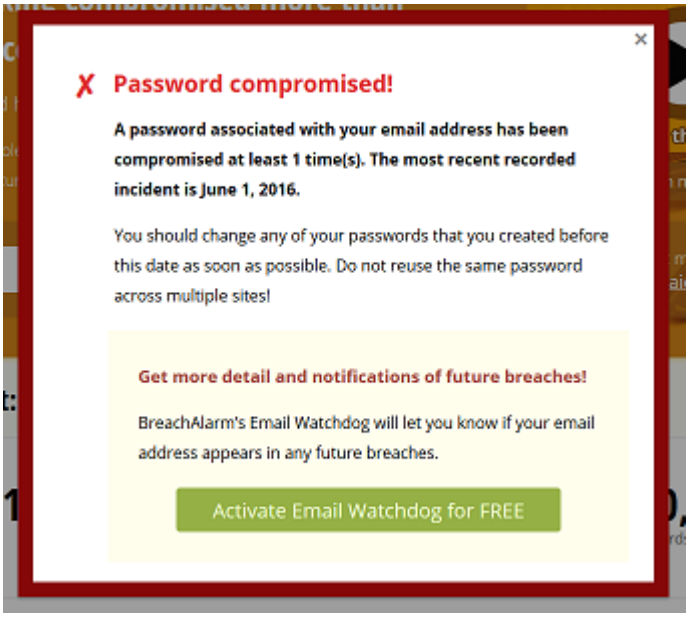
Une fenêtre vous pose la question « est-ce que cette adresse email vous appartient bien ? » et vous avertit que votre adresse IP sera enregistrée. Renseignez le captcha et cliquez sur le bouton « I understand ».



Si votre adresse n'est pas compromise une fenêtre du type ci-dessous s'ouvre avec l'inscription « It's looks like your passwords may be safe » (il semble que vos mots de passe ne sont pas compromis).



Dans le cas contraire, si votre adresse est compromise c'est une fenêtre du type ci-après qui va apparaitre (Mots de passe compromis). Elle précise la date la plus récente où a eu lieu la compromission (1er juin 2016).



En poursuivant (bouton Activate Email Watchdog for free), vous pouvez créer un compte et le site vous préviendra un suivi de cette adresse email.

2 - Que faire si mon e-mail est compromis?

Si votre adresse email apparait comme compromise, vous devez effectuer le plus rapidement possible les actions suivantes :

- **Changez votre mot de passe** sur le site concerné : prenez un mot de passe long (au moins 10 caractères et comprenant des majuscules et minuscules, des nombres et des caractères spéciaux.
- Si votre mot de passe est utilisé sur d'autres sites changez le également, sans reprendre le même.
- Si possible, **changez votre adresse email de contact** (si vous en avez plusieurs, sinon vous pouvez en créer une chez Gmail, Hotmail, Yahoo ou chez votre fournisseur internet. Utilisez des adresses différentes pour vos correspondances personnelles, professionnelles, vos achats, vos loisirs, …

Dans un deuxième temps sécurisez vos données sur les autres sites ou vous êtes inscrits :

- Vérifiez que les mots de passe soient toujours différents sur chaque site.
- Prenez toujours des mots de passe longs et forts. N'utilisez pas de mots du dictionnaire.
- Utilisez des logiciels qui gèrent, stockent et génèrent des mots de passe aléatoires.
- Optez chaque fois que possible pour une double authentification (par exemple un système qui vous demande en plus du mot de passe un code chiffré indépendant envoyé par mail ou SMS.
- Si vous stockez des données sensibles (données financières, papiers d'identité, etc…) dans le cloud, crypter-les. Vous pouvez vous servir pour cela de de nombreux logiciels gratuits
- Mettez régulièrement à jour votre ordinateur.

D'une façon générale, évitez de donner trop de renseignements sur vous quand vous vous inscrivez sur un site : date de naissance, adresse et téléphone, renseignement sur la famille, le travail, etc. quand elles ne sont pas obligatoires. Ces renseignements permettent souvent de cibler des publicités et d'espionner vos pérégrinations sur internet.

Si vous découvrez que votre adresse a été vraiment piratée est ou a été utilisée par quelqu'un d'autre, faites-la fermer et prenez en une autre. Même si vous récupérez le contrôle de votre messagerie, elle risque à terme d'être mise sur liste noire par plusieurs fournisseurs et devenir inutilisable.