OUTIL - LE HACKING OU PIRATAGE INFORMATIQUE

SÉCURITÉ > 4.2 PROTÉGER LES DONNÉES PERSONNELLES ET LA VIE PRIVÉE

CONVIENT POUR	AGE	NIVEAU DE COMPÉTENCE	FORMAT	DROITS D'AUTEUR	LANGUE(S)
Animateurs	N/A	Niveau 1	Fiche de préparation	Creative Commons (BY-SA)	Français

Cette fiche complète la fiche outil sur l’identité numérique et les données personnelles. Il s’agit ici de donner une définition précise du hacking, de sensibiliser sur quelques dangers qui peuvent exister sur le web et de fournir des outils pour s’en prémunir

Objectif général	Connaissances
Temps de préparation pour l'animateur	moins d'une 1 heure
Domaine de compétence	4 - Protection de l’identité et des données personnelles
Nom de l'auteur	Khera Rida
Ressource originellement créée	Français

DÉROULÉ

1 Qu’est-ce que le hacking ?

Le hacking ou piratage informatique est une pratique qui permet aux hackers de voler et échanger nos données personnelles de manière illégale. Le hackeur va utiliser tous les moyens possibles pour subtiliser mots de passe, identité bancaire etc…

Laisser de trop nombreuses traces visibles multiplie les risques de se trouver confronté aux attaques informatiques et à l’usurpation d’identité. En effet, ces dernières années, les hackers informatiques ont élaboré de nombreuses techniques pour récupérer les informations présentes en ligne :

- Les virus : souvent cachés dans des pièces jointes d’e-mail, soit vous recevrez de nombreuses publicités et messages frauduleux soit le virus attaque tout le disque dur !
- Le phishing : un mail de votre banque vous invitant à vous connecter sur leur site pour récupérer vos données de cartes bancaires par exemple. Il s’agit en réalité d’un faux site construit à l’identique pour créer l’illusion
- Le pharming : les hackers vont profiter des failles de certains sites pour récupérer les données personnelles des utilisateurs. Pas de panique, cela arrive rarement !

2 Comment s’en prémunir ?

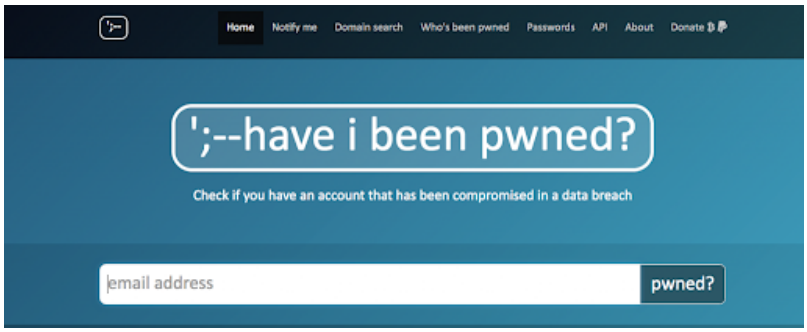
Nous vous invitons à consulter la fiche outil données personnelles et identité numérique qui explique comment protéger ses données personnelles et ne pas être la cible de ce genre d’attaque.

Les cyberattaques se multiplient, non plus seulement à l'encontre des particuliers, mais également des grandes entreprises, administrations et des plateformes. Il existe des outils en ligne spécialement dédiés à ces vérifications. Les entreprises se veulent rassurantes, mais régulièrement des hackers réussissent à compromettre et diffuser des bases de données comprenant des milliers voire des millions de données : nom, prénom, adresse email, etc. Ces fuites massives d'informations facilitent et entraînent de nombreuses conséquences : campagne de phishing, usurpation d'identité ou tentative de compromission de compte… Si quelques firmes jouent la transparence en avertissant les utilisateur.rice.s de brèches et fuites dont elles ont été victimes, toutes ne sont pas aussi bienveillantes et préfèrent taire leurs propres défaillances.

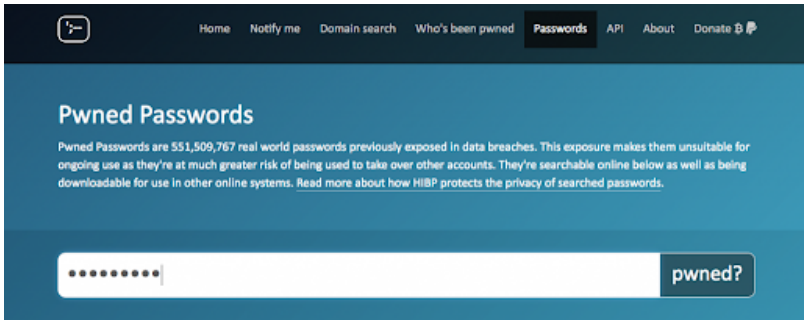
Exemples d'outils permettant de faire face à ces attaques

C'est là que le site « Have i been pwned » (« Est-ce que je me suis fait avoir ? ») ou l'outil Firefox monitor sont utiles. Ils rendent publics l'ensemble des sites qui ont été hackés et dont les données ont fuité. Permettant aux utilisateur.rice.s de s'assurer que nos adresses e-mail ne font pas partie des comptes potentiellement compromis.

→ Ecrire son adresse e-mail et cliquer sur **pwned**

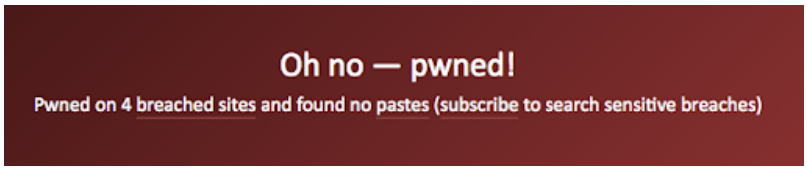


→ Ou écrire son mot de passe



→ La nouvelle n'est pas réjouissante, si ce n'est déjà fait, il devient urgent de vérifier ses comptes et de rehausser leur sécurité. Have I Been pwned précise le site attaqué, la date de la fuite et la nature des

données compromises



→ Pas de problème ici, vos comptes sont sécurisés

3 Pour aller plus loin :

le site internet Safe on the web recense les risques actuels de phishing etc. Tout en donnant des conseils pour se protéger du piratage.