TOOL - HACKING AND CYBERCRIME

SAFETY > 4.2 PROTECTING PERSONAL DATA AND PRIVACY

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
Facilitators	N/A	Level 1	Preparatory guide	Creative Commons (BY-SA)	English, French

This document contains background information for facilitators before they run the workshop with participants. It gives an understanding of dangers of hacking online and how to protect oneself against them.

General Objective	Knowledge acquisition
Preparation time for facilitator	less than 1 hour
Competence area	4 - Safety
Name of author	Khera Rida
Resource originally created in	French

WORKSHOP DIRECTIONS

1 What is hacking?

Hacking is a practice used by certain programmers to steal and exchange personal data illegally. Hackers use all means available to steal passwords, bank account details, etc.

Leaving too many detectible traces multiplies the risks of becoming victims of cybercrime and identity theft. Indeed, in recent years, hackers have developed many ways to appropriate personal data left by users online:

- Viruses: often hidden in email attachments, they often either attack your hard drive or cause you to receive a multitude of illicit advertisements and false messaging.
- Phishing: for example, a mail from your bank encouraging you to connect to your account. These are actually false sites that appear identical to the real thing in order to trick you into handing over your account information.
- Pharming: hackers sometimes manage to take advantage of weaknesses in certain websites to redirect their traffic to a replica, thereby being able to appropriate large amounts of user data. This remains a rare occurrence.

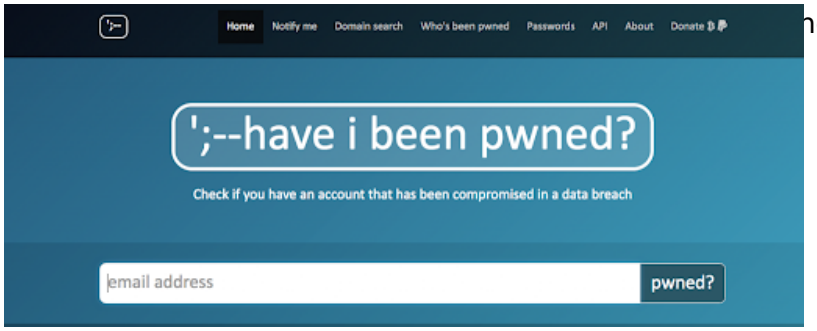
2 How can we protect ourselves from hacking?

We recommend you have a look at personal data and digital identity which explains how to protect our personal data and how not protect ourselves from cybercrime.

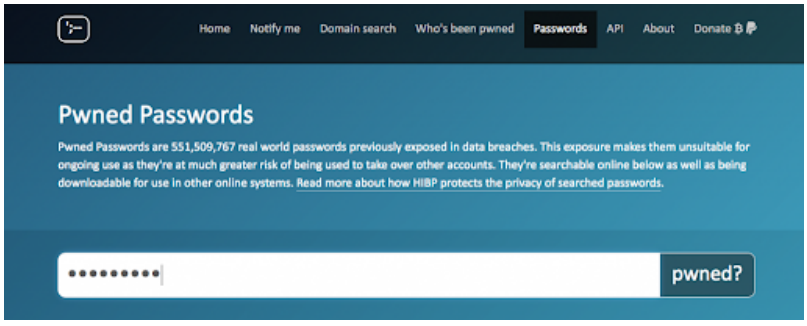
Cyberattacks are becoming more common, not only against individuals but also against big corporations, platforms and organisations. There are many available tools to combat this. Companies want reassurance, but hackers regularly manage to affect their operations, managing to access databases containing thousands if not millions of data: names, addresses, bank account details, etc. These massive information breaches lead to many consequences, including phishing campaigns, identity theft or account takeovers. While some companies who fall victim to data breaches will warn the individual victims, others many tend to keep quiet, in which case the information comes out independently at a later point (as in the case of the Facebook-Cambridge Analytica data breach scandal) or never comes out at all.

Here are some examples of tools that can help to prevent such attacks.

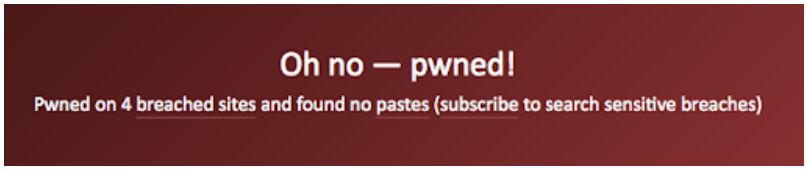
The website Have i been pwned or the tool Firefox monitor serve a similar useful function in that they make public all sites that have been hacked and whose information has been leaked. Users can therefore reassure themselves that their email addresses have not been part of the list of potentially compromised data.



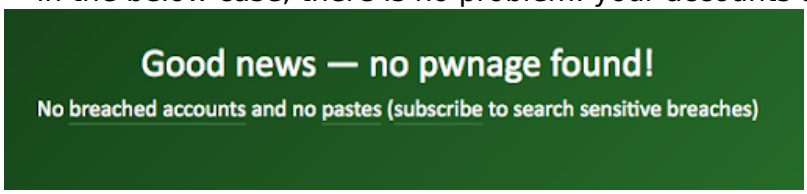
nd click ‘pwned?’



→ Here the news is not good. If you haven’t done this already, it should now be urgent to verify your accounts and change your password. The website will specify the affected site, the date of the breach



→ In the below case, there is no problem: your accounts are secure.



3 Going further

The website staysafeonline contains a lot of resources on cybercrime activity as well as advice on how to stay alert and protect ourselves.