Lexicon of the perfect hacker

In an environment marked by constant technological development and the digitalisation of practices, computer attacks are on the increase, whether in the professional or private sphere, often with very serious consequences for personal data.

Behind these attacks lie mysterious little creatures known as « *hackers* », who seem to demonstrate a constantly renewed inventiveness, so much so that the question for businesses and individuals is no longer « *Will I be attacked one day* » but rather « *When will I be attacked ?* ».

So, to help you to navigate these dangerous waters and to better understand the terms used by the experts in cyber security, we are offering you this small lexicon of the most common terms used during these « *cyber attacks* ».

Backdoor: Unauthorized means of access, hidden in a program that allows a malicious user to break into a computer system.

> **Example**: creation of a new administrator account with a password chosen by a hacker

Hoax: False, obsolete, or unverifiable information that is propagated spontaneously by internet users. Essentially in written form, like an electronic mail, inviting the internet user to forward the information to all his or her contacts, resulting in a chain reaction.

Examples:

- Alerts about viruses or missing children
- promise of happiness
- solidarity chains

Trojan horse: Malicious software with reference to Homer's Lliade, who under a legitimate appearance performs harmful actions without the knowledge of the user. By introducing a backdoor on the computer, the Trojan horse allows a hacker to take control of the computer via a remote connection, to steal registered passwords, to copy data, and to execute harmful actions.

> **Example:** a hacker sends a mail to the person he is trying to infiltrate and encloses his « *Trojan* » in an attachment. If the user opens the file, the cookie is installed discretely on the computer, often hidden in a file or program that functions perfectly legitimately, like a game for instance.

Denied service: An attack by saturation that consists of sending thousands of messages from dozens of computers in order to overwhelm the servers of a company. Although this technique does not modify the content of a company's internet site, it does paralyse it for several hours, thus blocking its access to users.

Deepfake: Very realistic fake video produced using artificial intelligence. Similar to fake news (see below), this technique involves superimposing existing video images over others.

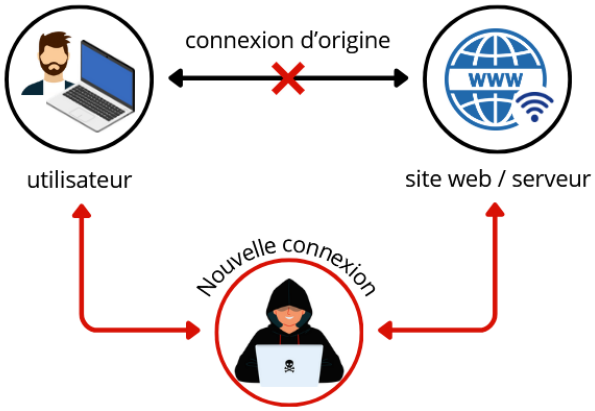
Drive by Download: Unwanted downloading, carried out without the user's knowledge, for example when visiting a website, opening an attachment in an email, or clicking on a pop-up on a malicious site.

Flaw: Vulnerability in a computer system that allows a hacker to compromise the normal operations of the system, its confidentiality or the integrity of the data it contains.

Fake technical support: This type of fraud consists of scaring victims into believing that their equipment is faulty or suffering from a serious technical problem.
Very often, the fake technician will install remote software that will allow him/her to take control of his victims' devices and steal their passwords and documents.

Man-in-the-middle attack: An attack in which a hacker places himself/herself in an interception position on the network

Example: recovery of the router's MAC address in order to recover communications



Fake news: False information disseminated with the aim of manipulating or misleading public opinion.

Malware: Program developed for the purpose of harming, or using, a computer system or network. It can take the form of a virus or a computer worm.

Mail bombing: Sending a massive amount of emails (for example, several thousands) to a single recipient with malicious intent. It generally results in either saturating the victim's mailbox or making it impossible for the victim to use his email address.

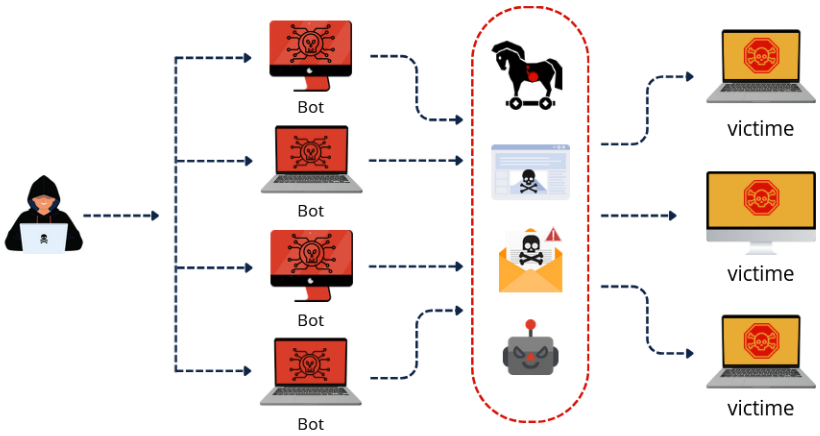
Patch: A piece of code that is added to a software to fix a problem (for example, a bug fix).

Account hacking: Access to an account (bank, administrator, social networking profile, etc.) after « *cracking* » the password protecting it.

Phishing: Theft of identity or confidential information (access codes, bank details) by subterfuge. The scammers are most often considered a trusted organization (banking, PayPal, ...) and invite users, by email, to visit a fraudulent site - which looks like the authentic site - and share sensitive information.

Ransomware: Malicious software that hijacks the data contained in a computer system by encrypting and blocking the files contained on the computer and sending the key for decryption only when the user has paid the ransom.

Botnet: A network of infected machines controlled by a remote hacker. The latter can then transmit orders to the machines of the botnet and operate them as he/she pleases.



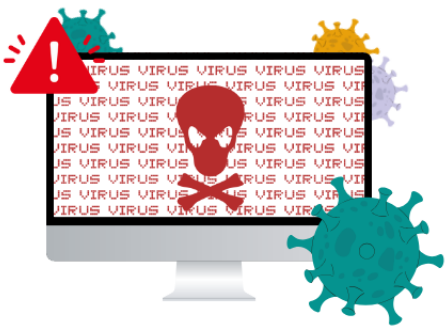
Scan: Fraudulent practice, most often from West Africa and Nigeria, which consists of extorting money from Internet users by dangling (promising) money.

> **Example**: an email from a so-called rich African heir who finds himself in distress or in an emergency situation claiming his bank account is blocked. If the user agrees to help him get his money, then he promises in exchange to credit the helper's account with a huge sum of money.

Spamming: Massive sending of electronic messages for promotional or advertising purposes to persons with whom the sender has never had contact but whose information has been unlawfully retrieved.

Account theft: A form of identity theft in which hackers gain access to an account, application or online service by pretending to be someone else after successfully stealing that person's credentials.

Computer virus: A malicious program or piece of code that attaches itself to a legitimate file in the hope that the user or the system will execute it, to allow it to spread across a computer system (computer, server, mobile device, etc.) and often to attain the data, the memory, and / or the network.



The propagation from one machine to another is done by the exchange of infected files through a messaging system, backdoors, a fraudulent internet page, memory sticks, and file sharing.

Computer worm: A virus that spreads almost autonomously (without direct human intervention) via the network. It uses a flaw in the system to copy itself where it shouldn't and then spread its code, without the knowledge of users, to the largest number of targets, and infect the network (address book recovery, sending copies, ...).

Vishing: Derived from the contraction of '*voice'* and *'phishing'*, this phone call or voicemail scam aims to obtain the victim's banking or personal details by pretending to be a reliable source.

> **Example**: calls from a number displaying the name of a bank or service to obtain authorisation codes for making a transfer