# A small introduction to DNS

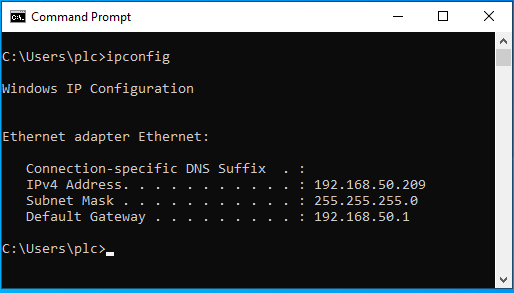
## **What is** DNS?

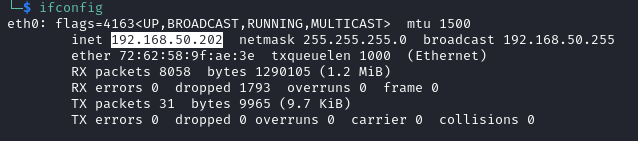
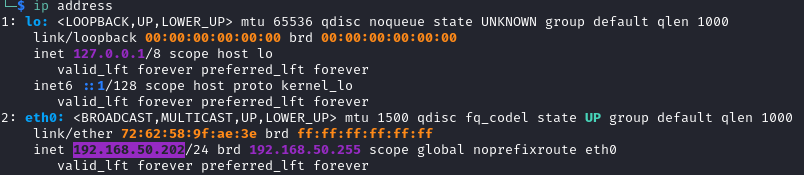
What is DNS, the Domain Name System?

DNS is traditionally compared with the phone book of a network; it's the software that translates human readable names to network (IP) addresses.

Each network interface connected to an Internet Protocol (IP) network has an address, used by machines to exchange data packets. There are for the moment 2 versions of the IP addressing: IPv4 and IPv6. An IPv4 address is a series of 4 numbers between 0 and 255, separated by dots, for example 20.231.239.246. An IPv6 address (totally unreadable) is a set of 8 numbers between 0 and 65535 separated by ':'.

On Windows, you can display your IP address with the following command: ipconfig

On Linux, you can display your IP addresses with the following commands: ip address or ifconfig.

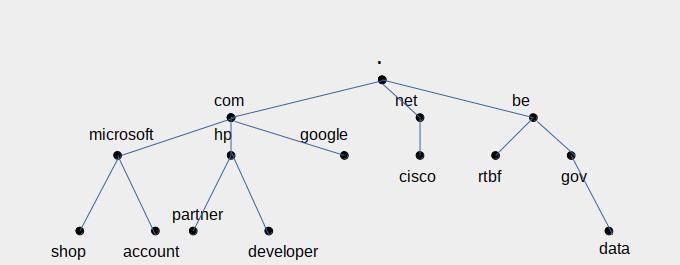
You can see by yourself that it is impossible to remember such addresses for the multiple resources you use on the Internet. That is the reason why DNS was invented.

DNS is a *distributed database*. It means that no single machine holds all the names and addresses, but that resources are split among many computers. A computer holding a part of the address <-> name database is a DNS server.

DNS is also *hierarchical*. Each name can be the root of a tree below it. For example, let's take shop.microsoft.com. This name contains 3 elements.

* .com is the top level domain (TLD).
* microsoft.com is the domain belonging to the Microsoft company.
* shop is a website within the microsoft domain.

This name can be schematized as a path in a tree.

At the top, you have the root (.).

Just below, you have the top level domains (TLDs). The most known are .com, .net, .org, .edu, and the national top domains (.us, .uk, .be, .fr...).

Below, you have domains that enterprises or private persons can buy, for example google.com, cisco.net, mit.edu, emmanuelmacron.fr...

Within a domain, you can find several resources (like websites) or machines, which will receive a third level name, like shop.microsoft.com, data.gov.be... It is up to the domain owner to further subdivide his domain. You could find, for example, server1.brussels.belgium.entreprise.com, if the company has decided to divide its namespace by country (belgium.enterprise.com), then by city (brussels.belgium.enterprise.com). Note that server1.antwerp.belgium.enterprise.com, even if its first name is the same as the former server, represents another machine, with a different IP address, because its complete name (its *fully qualified domain name*, or FQDN) is different.

When you want to know who is owning a server or a website, usually, only the two last parts of the domain are relevant and define the owning entity. Exceptions exist, for example in the United Kingdom, where the commercial entities often have domain names like enterprise.co.uk. In this case, you have to consider the 3 last parts.

## DNS and URLs (or w**e**b links)

An URL is the name of a resource, local or on the Internet. When it begins with http:// or https://, it points to a page or resource on a website.

The address of a web page is composed like follows:

http://<fully qualified domain name>/<parameters>

So, the address of the server publishing the page is the DNS fully qualified domain name between the two leading slashes (//) and the next slash. The remaining of the string is composed of parameters that can be a page location on the web site or values used by the server to perform its functions. It can also contain other slashes, but only the first one should be considered to isolate the domain name.

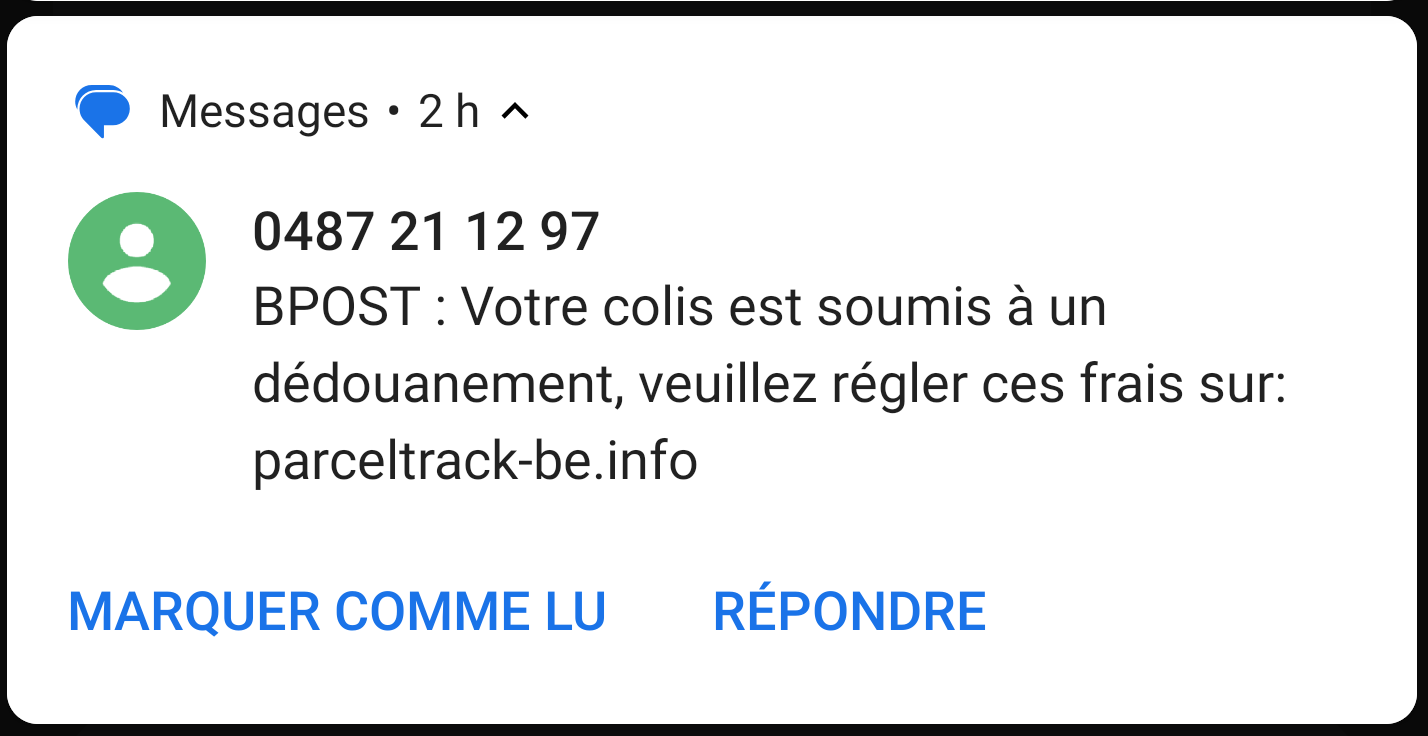
## Avoid suspicious links by analyzing their DNS names

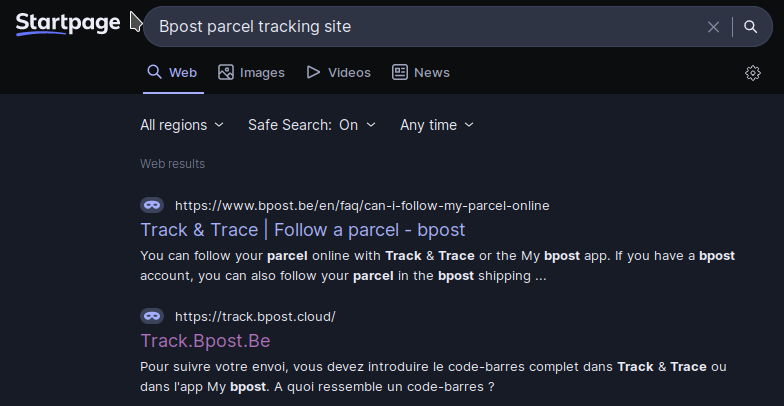
What does DNS have to do with phishing?

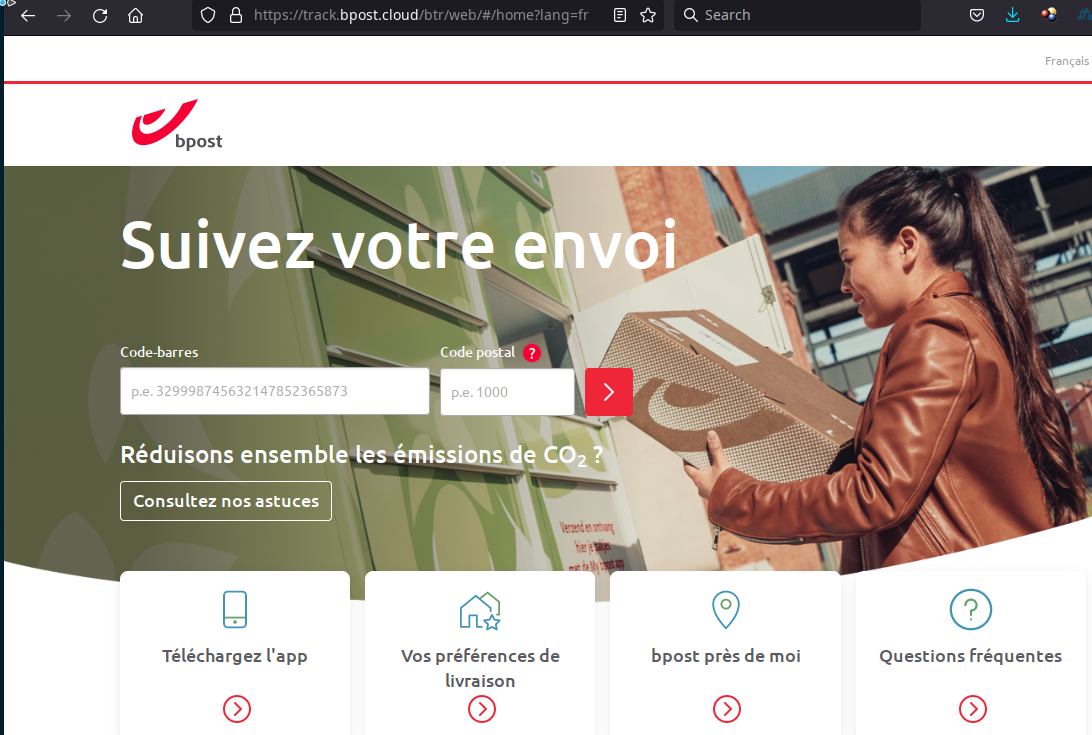
By analyzing the fully qualified domain name of the sender of an email, or the link you are supposed to click in a mail or SMS, you can detect many phishing tentatives.

### **A s**mishing example

Let's check the following SMS (in French; the translation is: "BPOST: your parcel is subject to customs clearance, please pay the fee on parceltrack-be.info"):

Hmm. Bpost (Belgian post) has websites, most of them ending with bpost.be. It has also a parcel tracking site. Let's check its DNS name.

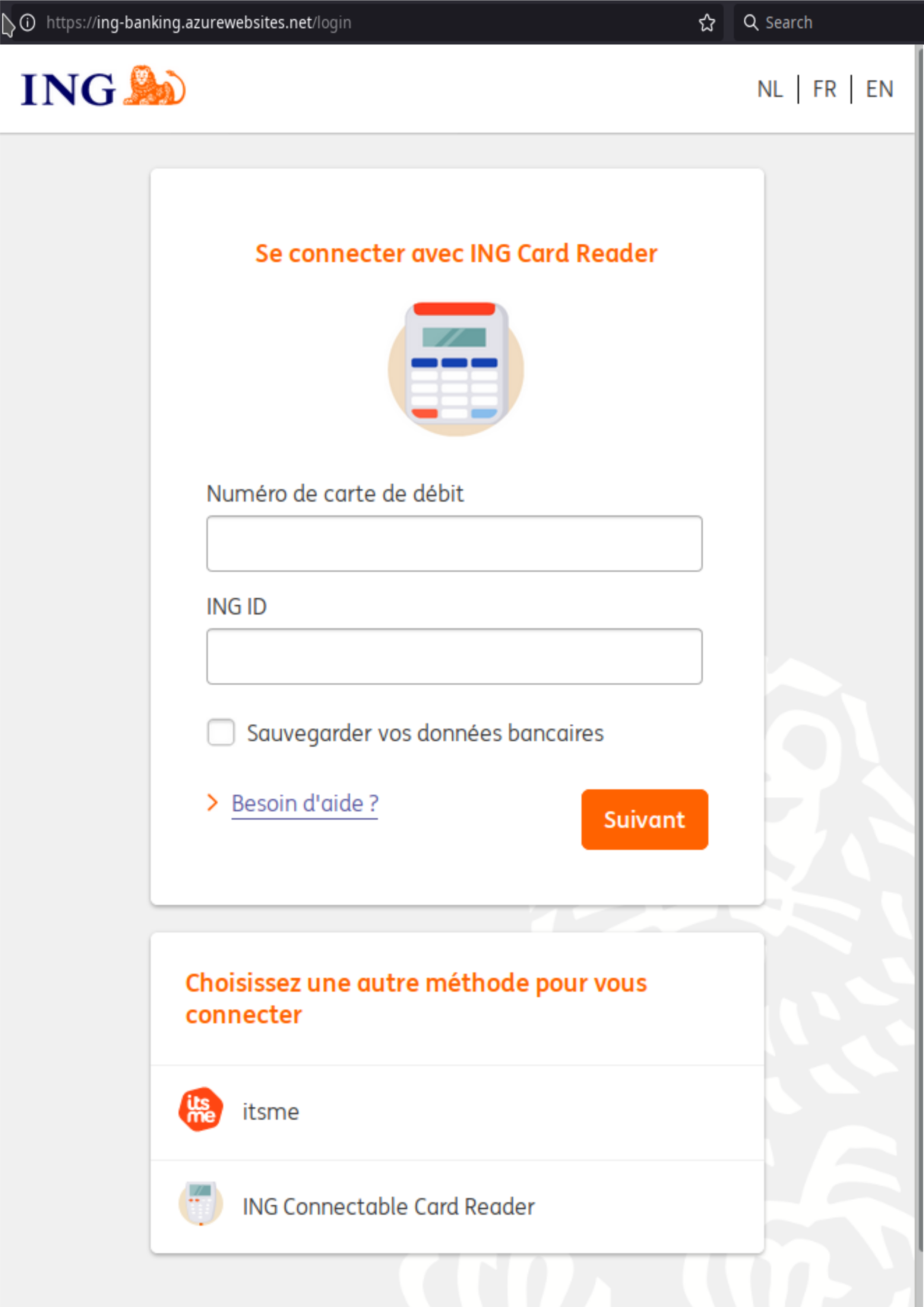
Google says that the DNS name is track.bpost.cloud. Let's go to it.

Yes, this is the right one.

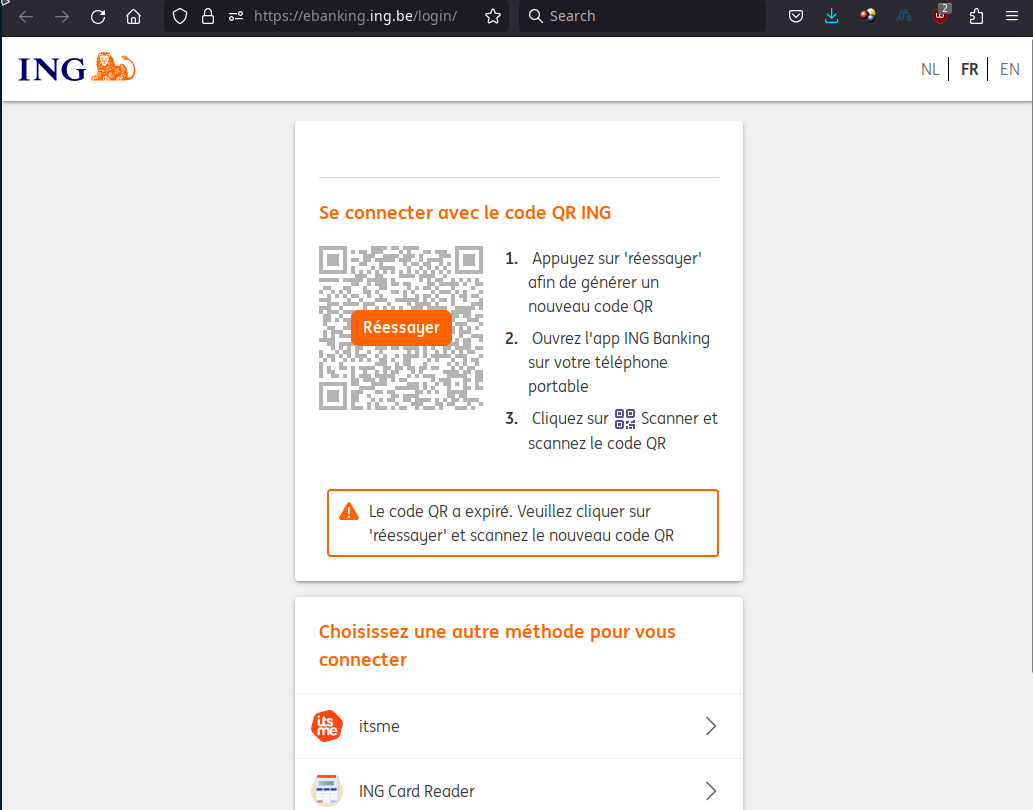
Ha! parceltrack-be.info is a fake. Gotcha, pirate! We will not fall for this. (Although, honestly, this one was rather easy to spot).

### **Another ph**ishing example

The link to this site was included in a phishing mail that informed you there was an update for your card reader, asked you to login to their website and fill your card information . The site is a very credible copy of the bank's login site.

Look at the link: ing-banking.azurewebsites.net

Once again, let's check the real bank's site:

URL: ebanking.ing.be

Verdict: azurewebsites.com ≠ ing.be → phishing!!

## Conclusion

Always check the 2 (or 3) last words in a domain name.