



Une petite introduction au DNS

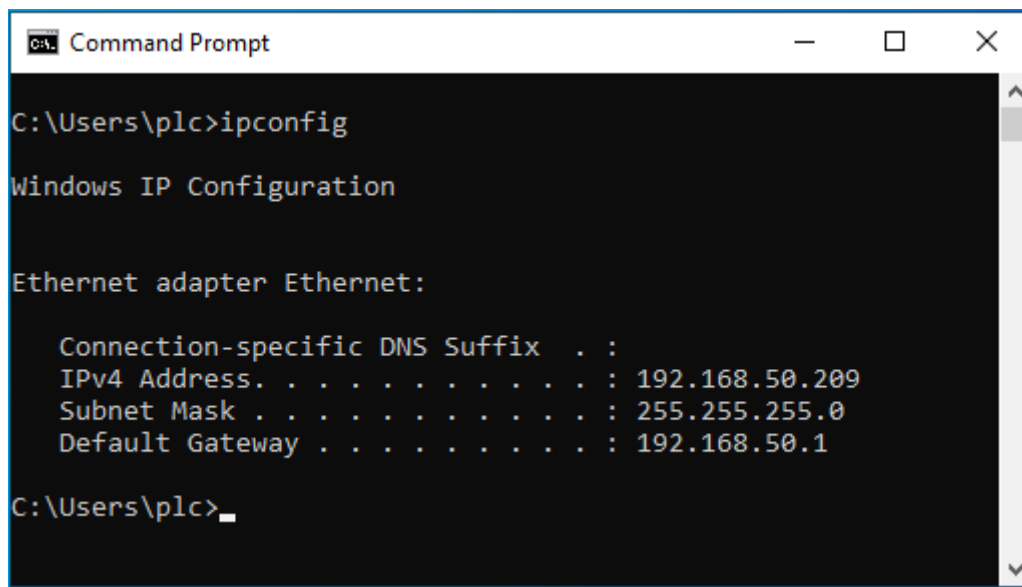
Qu'est-ce que le DNS

Qu'est-ce que le DNS, le Domain Name System ?

Le DNS est traditionnellement comparé à l'annuaire téléphonique d'un réseau; c'est le logiciel qui traduit les noms lisibles par l'homme en adresses réseau (IP).

Chaque interface réseau connectée à un réseau IP (Internet Protocol) possède une adresse, utilisée par les machines pour échanger des paquets de données. Il existe pour le moment 2 versions de l'adressage IP: IPv4 et IPv6. Une adresse IPv4 est une série de 4 chiffres entre 0 et 255, séparés par des points, par exemple 20.231.239.246. Une adresse IPv6 (totalement illisible) est un ensemble de 8 chiffres entre 0 et 65535 séparés par ':'.

Sous Windows, vous pouvez afficher votre adresse IP avec la commande suivante:
`ipconfig`.



```
C:\Users\plc>ipconfig

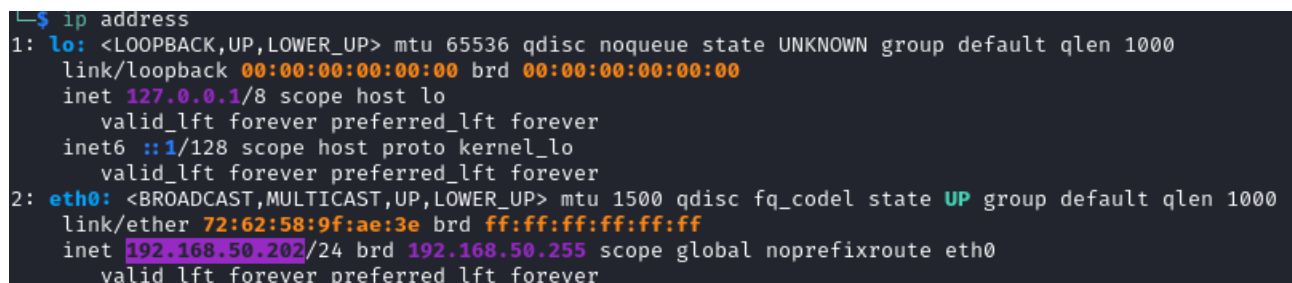
Windows IP Configuration

Ethernet adapter Ethernet:

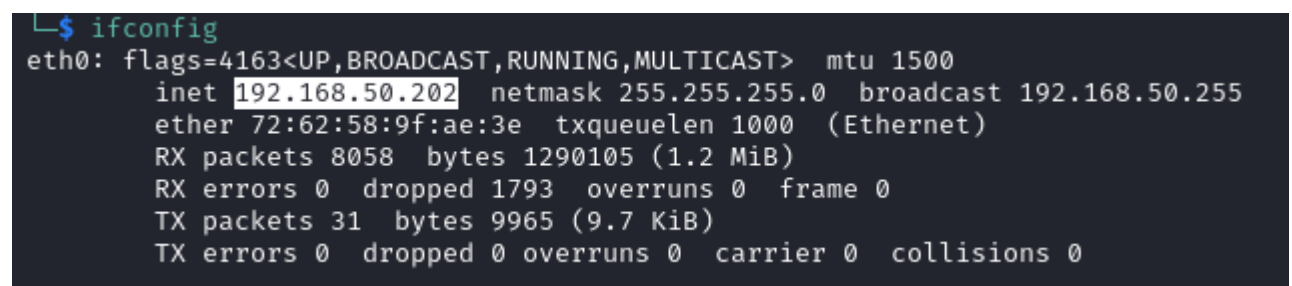
    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.50.209
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.50.1

C:\Users\plc>
```

Sous Linux, vous pouvez afficher vos adresses IP avec les commandes suivants: `ip address` ou `ifconfig`.



```
└─$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 72:62:58:9f:ae:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.202/24 brd 192.168.50.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
```



```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.202 netmask 255.255.255.0 broadcast 192.168.50.255
    ether 72:62:58:9f:ae:3e txqueuelen 1000 (Ethernet)
    RX packets 8058 bytes 1290105 (1.2 MiB)
    RX errors 0 dropped 1793 overruns 0 frame 0
    TX packets 31 bytes 9965 (9.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

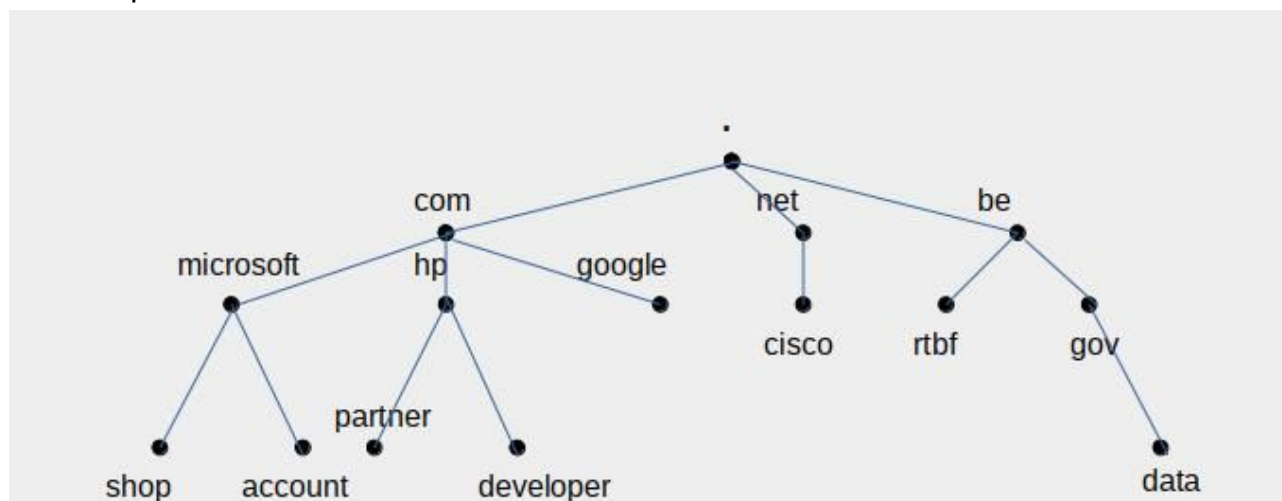
Vous pouvez constater par vous-même qu'il est impossible de se souvenir de telles adresses pour les multiples ressources que vous utilisez sur Internet. C'est la raison pour laquelle le DNS a été inventé.

Le DNS est une base de données *distribuée*. Cela signifie qu'aucune machine ne contient tous les noms et adresses, mais que les ressources sont réparties entre plusieurs ordinateurs. Un ordinateur qui détient une partie de la base de données d'adresses <-> noms est un serveur DNS.

Le DNS est également *hiérarchique*. Chaque nom peut être la racine d'un arbre en dessous de lui. Par exemple, prenons *shop.microsoft.com*. Ce nom contient 3 éléments.

- *.com* est le domaine de premier niveau (TLD).
- *microsoft.com* est le domaine appartenant à la société Microsoft.
- *shop* est un site web au sein du domaine *microsoft.com*.

Ce nom peut être schématisé comme un chemin dans une arborescence.



- En haut, vous avez la racine (``).
- Juste en dessous, vous avez les domaines de premier niveau (TLD). Les plus connus sont `.com`, `.net`, `.org`, `.edu`, et les domaines nationaux de premier niveau (`.us`, `.uk`, `.be`, `.fr`...).
- En-dessous, vous avez des domaines que les entreprises ou les particuliers peuvent acheter, par exemple `google.com`, `cisco.net`, `mit.edu`, `emmanuelmacron.fr`...
- - Au sein d'un domaine, vous pouvez trouver plusieurs ressources (comme des sites web) ou machines, qui recevront un nom de troisième niveau, comme `shop.microsoft.com`, `data.gov.be`... Il appartient au propriétaire du domaine de subdiviser davantage son domaine. Vous pourriez trouver, par exemple, `server1.brussels.belgium.entreprise.com`, si l'entreprise a décidé de diviser son espace de noms par pays (`belgium.entreprise.com`), puis par ville (`brussels.belgium.entreprise.com`). Notez que `server1.antwerp.belgium.entreprise.com`, même si son premier nom est le même que celui du serveur ci-dessus, représente une autre machine, avec une adresse IP différente, car son nom complet (son *nom de domaine entièrement qualifié*, ou *FQDN*) est différent.

Lorsque vous souhaitez savoir à qui appartient un serveur ou un site Web, généralement, seules les deux dernières parties du domaine sont pertinentes et définissent l'entité propriétaire. Des exceptions existent, par exemple au Royaume-Uni, où les entités commerciales ont souvent des noms de domaine comme `entreprise.co.uk`. Dans ce cas, vous devez tenir compte des 3 dernières parties.

DNS et URLs (ou liens web)

Une URL est le nom d'une ressource, locale ou sur Internet. Lorsqu'elle commence par `http://` ou `https://`, elle pointe vers une page ou une ressource sur un site Web.

L'adresse d'une page web est composée comme suit :

```
http://<nom de domaine complet>/<paramètres>
```

Ainsi, l'adresse du serveur qui publie la page est le nom de domaine complet DNS entre les deux slashes initiaux (//) et le slash suivant. Le reste de la chaîne est composé de chemins internes au serveur et/ou de paramètres qui peuvent être un emplacement de page sur le site web ou des valeurs utilisées par le serveur pour exécuter ses fonctions. Il peut également contenir d'autres slashes, mais seul le premier doit être pris en compte pour isoler le nom de domaine.

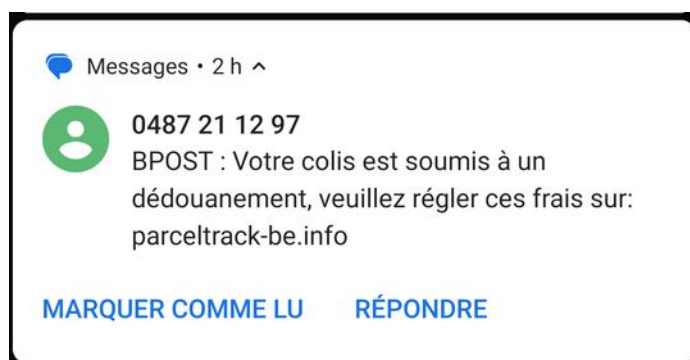
Évitez les liens suspects en analysant leurs noms DNS

Qu'est-ce que le DNS a à voir avec le phishing ?

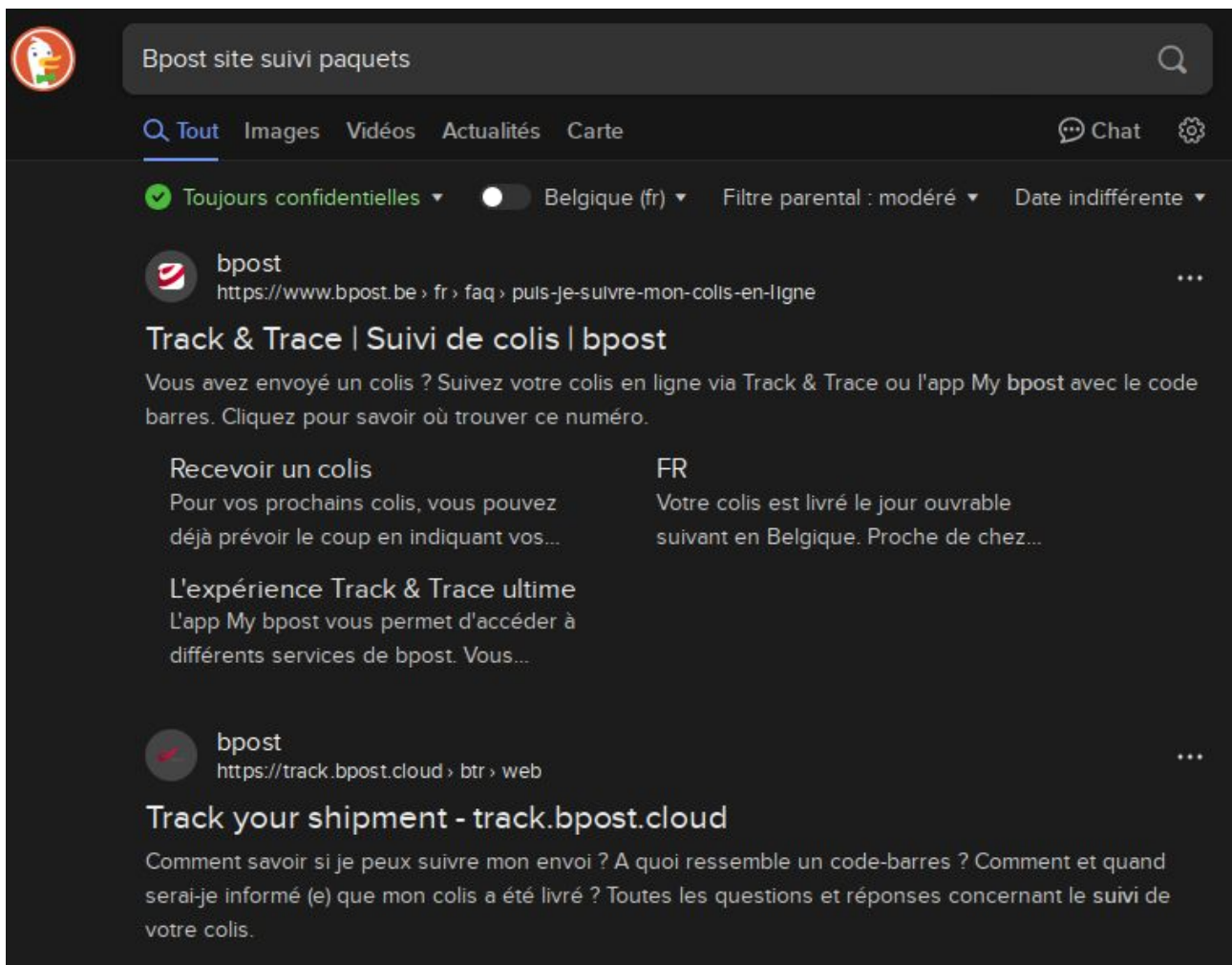
En analysant le nom de domaine complet de l'expéditeur d'un email, ou le lien sur lequel vous êtes censé cliquer dans un e-mail ou un SMS, vous pouvez détecter de nombreuses tentatives de phishing.

Un exemple de smishing

Vérifions le SMS suivant:



Hmm. Bpost (la poste belge) a des sites Web, la plupart se terminant par *bpost.be*. Elle a également un site de suivi de colis. Vérifions son nom DNS.



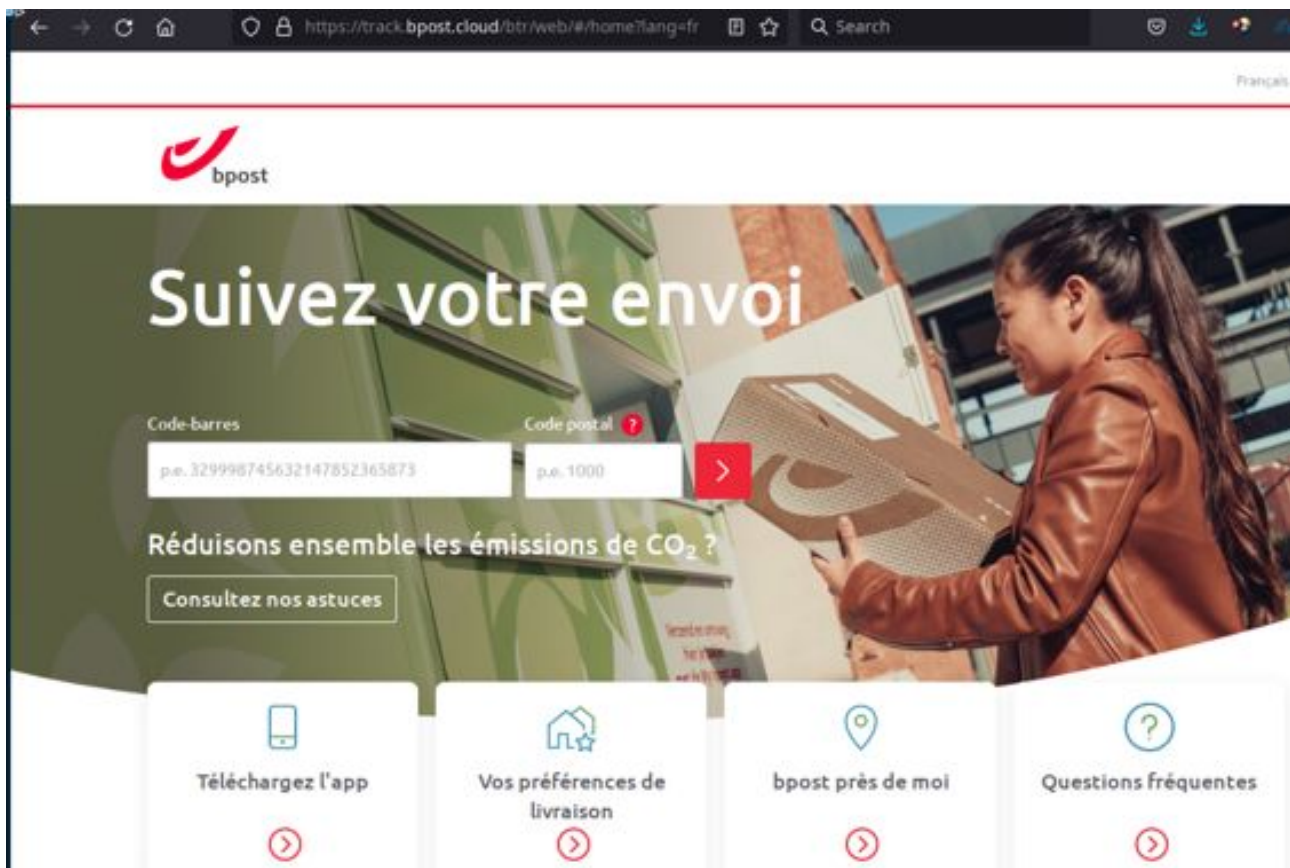
The screenshot shows a search engine interface with a search bar at the top containing the text "Bpost site suivi paquets". Below the search bar, there are tabs for "Tout", "Images", "Vidéos", "Actualités", and "Carte". To the right of these tabs are icons for "Chat" and settings. Below the tabs, there are filters: "Toujours confidentielles" (checked), "Belgique (fr)" (selected), "Filtre parental : modéré", and "Date indifférente".

The first search result is from "bpost" with the URL "https://www.bpost.be > fr > faq > puis-je-suivre-mon-colis-en-ligne". The title is "Track & Trace | Suivi de colis | bpost". The description says: "Vous avez envoyé un colis ? Suivez votre colis en ligne via Track & Trace ou l'app My bpost avec le code barres. Cliquez pour savoir où trouver ce numéro." Below the description, there are two columns of text:

- Recevoir un colis**
Pour vos prochains colis, vous pouvez déjà prévoir le coup en indiquant vos...
- FR**
Votre colis est livré le jour ouvrable suivant en Belgique. Proche de chez...

The second search result is also from "bpost" with the URL "https://track.bpost.cloud > btr > web". The title is "Track your shipment - track.bpost.cloud". The description says: "Comment savoir si je peux suivre mon envoi ? A quoi ressemble un code-barres ? Comment et quand serai-je informé (e) que mon colis a été livré ? Toutes les questions et réponses concernant le suivi de votre colis."

La recherche nous dit que le nom DNS est *track.bpost.cloud*. Allons-y.




Oui, c'est le bon.

Ha! *parceltrack-be.info* est un **faux**. On t'a eu, pirate! Nous ne tomberons pas dans le panneau. (Même si, honnêtement, celui-ci était plutôt facile à repérer).

Autre exemple de phishing


Le lien vers ce site était inclus dans un courrier de phishing qui vous informait qu'une mise à jour était disponible pour votre lecteur de carte, vous demandait de vous connecter à leur site Web et de saisir les informations de votre carte. Le site est une copie très crédible du site de connexion de la banque.

https://ing-banking.azurewebsites.net/login

ING 

NL | FR | EN

Se connecter avec ING Card Reader




Numéro de carte de débit


ING ID

☐ Sauvegarder vos données bancaires

[> Besoin d'aide ?](#) [Suivant](#)

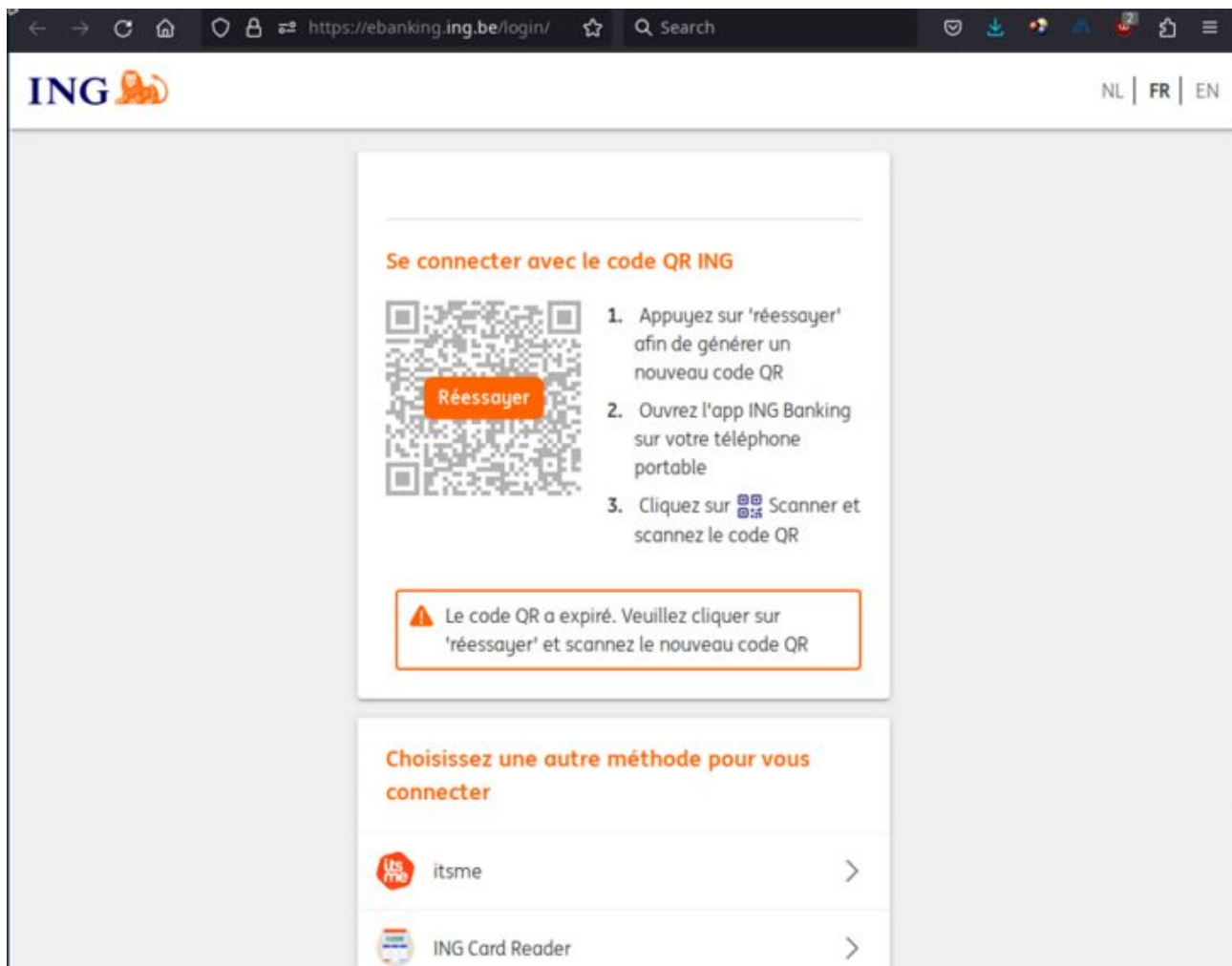
Choisissez une autre méthode pour vous connecter

 itsme

 ING Connectable Card Reader

Regardez le lien: ing-banking.azurewebsites.net

Une fois de plus, vérifions le site de la vraie banque:



URL: ebanking.ing.be

Verdict: azurewebsites.com \neq ing.be \rightarrow phishing!!

Conclusion

Vérifiez toujours les 2 (ou 3) derniers mots d'un nom de domaine.