

LANQUETIN Alexis
GONZALEZ Jules

WEB BROWSER FINGERPRINTING

- I - Que sont les Web Browser Fingerprint**
- II - Comment fonctionnent-elles ?**
- III - Quelques cas d'utilisation**
- IV - Comment limiter les informations récoltées ?**
- V - Demonstration**



Identifier les utilisateurs

- Éléments HTTP
- Configuration du navigateur
- Configuration machine
- Adresse IP



Identification à 99% de certitude

Cookies vs Fingerprints

Peuvent être supprimés, bloqués

Utilisent des informations
personnelles

Sont stockés sur l'appareil

Ne peuvent pas être bloquées

Utilisent seulement des
données matérielles et software

Ne sont pas stockées

Comment sont récupérées les fingerprint

Passif fingerprinting

- User Agent
- HTTP ACCEPT headers
- System platform
- Encoding
- IP Adress

Actif fingerprinting

- JavaScript
 - Screen resolution, color depht
 - Canvas, WebGL
 - Extension, plugin
 - Timezone
 - File formats
- Cookies, DoNotTrack, ...
- Device (peripherals, sensors...)
- Audio

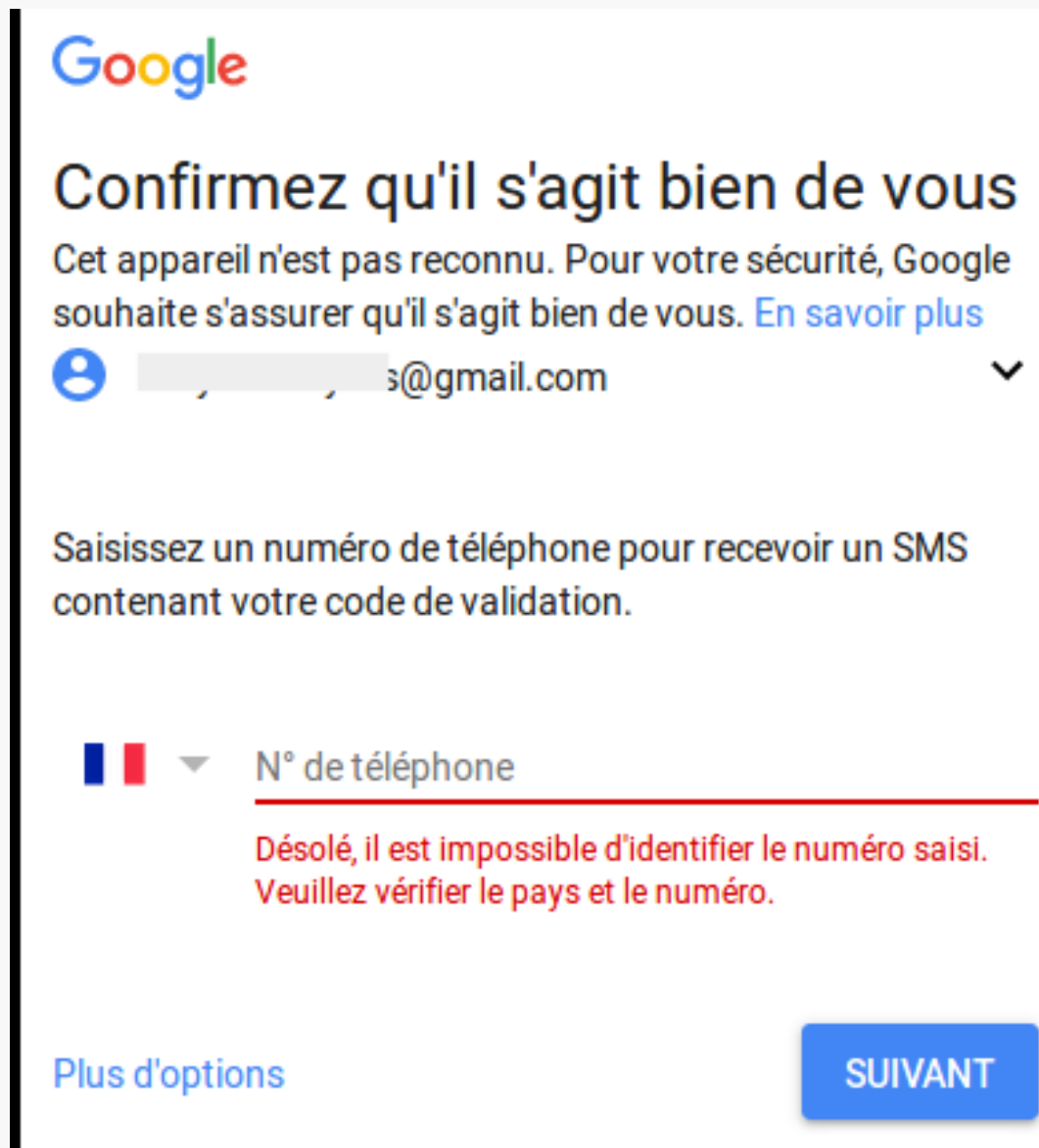
Cas d'utilisation

Sécurité

Publicité

Agences de surveillance


Statistiques




Google

Confirmez qu'il s'agit bien de vous

Cet appareil n'est pas reconnu. Pour votre sécurité, Google souhaite s'assurer qu'il s'agit bien de vous. [En savoir plus](#)

 [redacted]@gmail.com

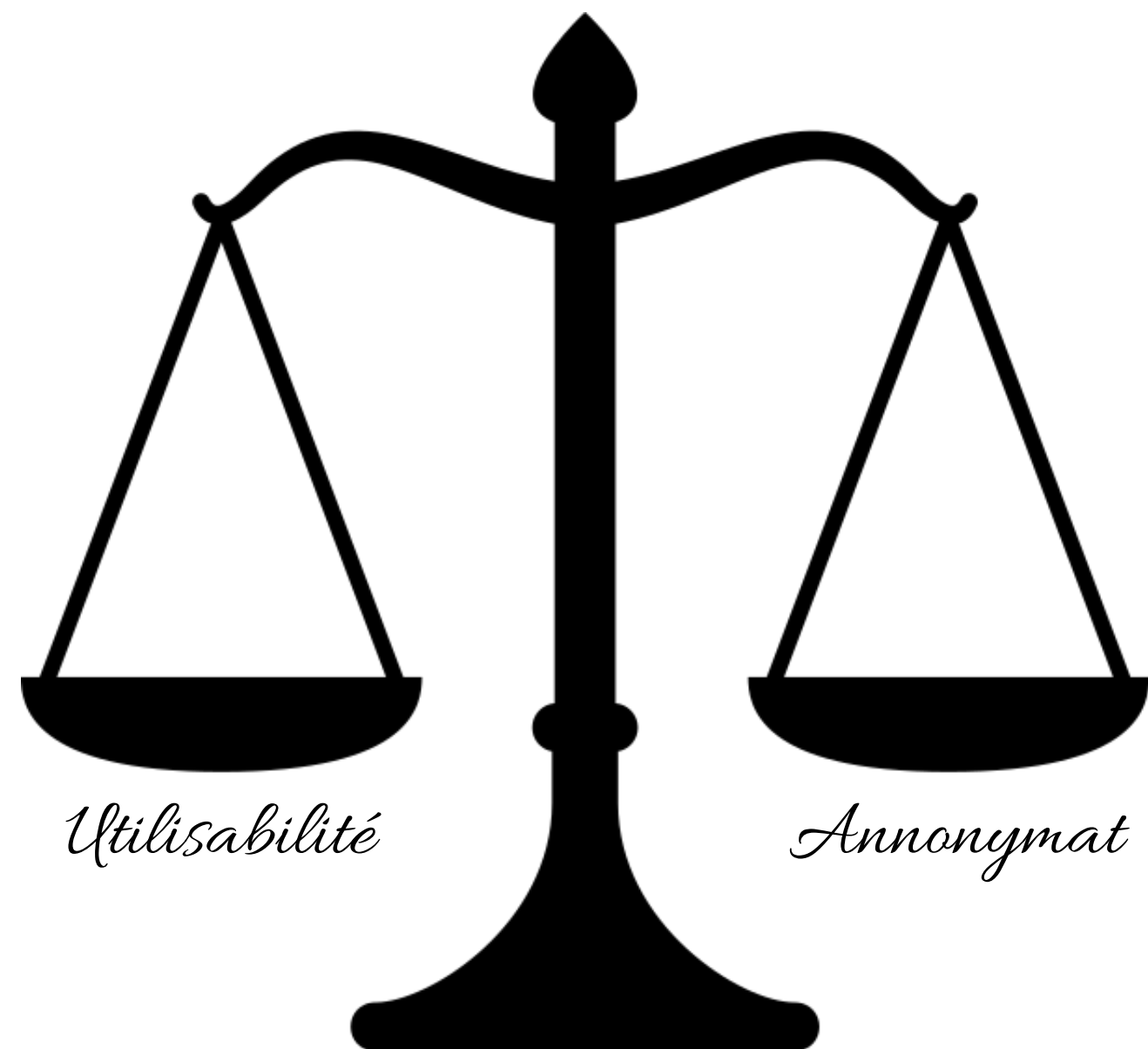
Saisissez un numéro de téléphone pour recevoir un SMS contenant votre code de validation.

 N° de téléphone

Désolé, il est impossible d'identifier le numéro saisi.
Veuillez vérifier le pays et le numéro.

[Plus d'options](#) [SUIVANT](#)

Comment se protéger ?





navigation privée



Bloqueurs de trackers et scripts



Utiliser une VM

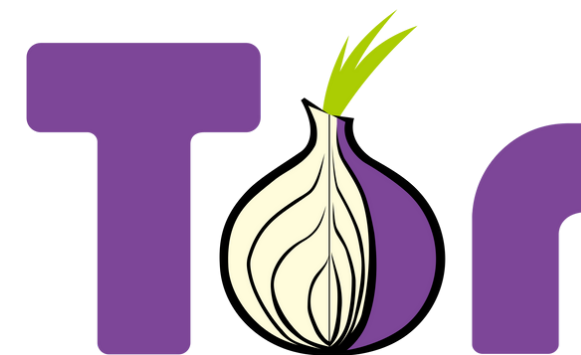


Désactiver les scripts



NordVPN®

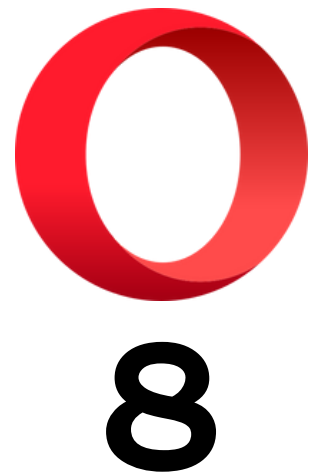
Utiliser un VPN



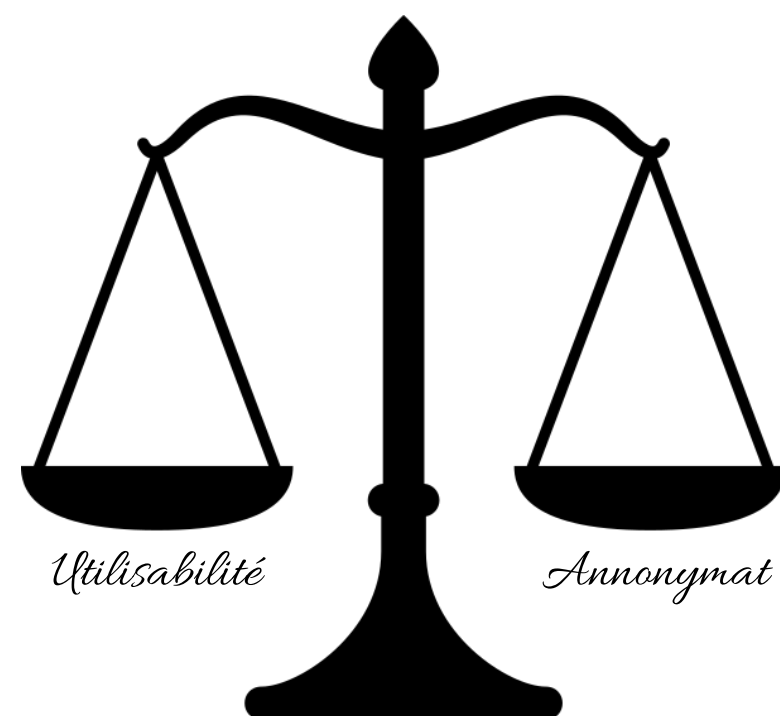
Utiliser des navigateurs résistants aux fingerprints



<https://www.expressvpn.com/blog/best-browsers-for-privacy/>



Démonstration



Pour conclure



**Merci pour
votre attention**