

## Données personnelles exposées : quels sont les principaux risques ?

La CNIL décrit les deux principaux risques liés à l'exposition de données personnelles

### L'hameçonnage (*phishing*)

L'[hameçonnage](#) consiste à vous envoyer un courriel ou SMS frauduleux qui vous paraîtra plus réaliste du fait de l'utilisation des données récupérées grâce à la fuite de données (un soi-disant courriel de votre médecin ou de la sécurité sociale par exemple).

### Que faire en cas de message suspect ?

- N'ouvrez surtout pas les pièces jointes.
- Ne répondez pas au message.
- Ne consultez pas les liens et supprimez le message immédiatement.

Notons que les adresses email et les numéros de téléphone n'ont pas été exposés : c'est donc un facteur limitant du risque.

### L'usurpation d'identité

Si vous pensez être victime d'une [usurpation d'identité](#) à la suite de la divulgation d'informations vous concernant, vous pouvez :

- vous rendre sur le site [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr) pour obtenir des conseils pour vous prémunir d'usurpation ;
- porter **plainte** au plus vite auprès d'un commissariat de police ou de gendarmerie.

Si l'usurpation est confirmée, demandez auprès des services de la CNIL une consultation du [fichier des comptes bancaires](#) (FICOBA) afin de savoir si des comptes ont été ouverts à votre nom par l'escroc.

Source : site de la CNIL