

# JE SUIS VICTIME ?

# À QUI JE M'ADRESSE ?

Vous souhaitez signaler :

✓ un Spam



[www.signal-spam.fr](http://www.signal-spam.fr)



[www.gendarmerie.interieur.gouv.fr/conseils](http://www.gendarmerie.interieur.gouv.fr/conseils)

✓ un contenu  
illicite  
sur internet



[www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr)



[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

✓ une fraude  
à la carte  
bancaire

PERCEV@L

[www.service-public.fr/  
particuliers/vosdroits](http://www.service-public.fr/particuliers/vosdroits)



[www.cybermalveillance.gouv.fr/17cyber](http://www.cybermalveillance.gouv.fr/17cyber)

## EN CAS D'URGENCE

Composer le 17 ou le 112

Déposer plainte sur [plainteenligne.fr](http://plainteenligne.fr)  
ou à la brigade de gendarmerie locale

L'application  
Ma sécurité

[www.masecurite.interieur.gouv.fr/fr](http://www.masecurite.interieur.gouv.fr/fr)



# ARNAQUES EN LIGNE ?

# AYEZ LES BONS RÉFLEXES !



# “ Des Arnaques en ligne, mais lesquelles ? ”



Les plus courantes...

Usurpation d'identité, fausses annonces, faux RIB, escroquerie aux sentiments, numéros surtaxés, arnaques thématiques, hameçonnage regroupant les phishing, smishing, vishing, quishing...



## Adoptez LES BONS RÉFLEXES !

### Petites annonces et offres d'emploi

- Attention aux documents que vous transmettez
- Apposez un filigrane sur l'image du document en indiquant sa destination : <https://filigrane.beta.gouv.fr>
- Privilégier la rencontre physique



# Conseils...

### Mot de passe

- 4 sortes de **caractères différents** : minuscule, majuscule, chiffre, signe, caractère spécial...
- Minimum **16 caractères**
- **Anonyme**
- **1 mot de passe** par application ou site



### Les faux investissements

- Site REGAFI pour vérifier le droit d'exercice en France : [www.regafi.fr/spip.php?rubrique1](http://www.regafi.fr/spip.php?rubrique1)
- Site de l'AMF qui tient une liste noire des faux sites de trading : [www.amf-france.org/fr/espace-epargnants/proteger-son-epargne/listes-noires-et-mises-en-garde](http://www.amf-france.org/fr/espace-epargnants/proteger-son-epargne/listes-noires-et-mises-en-garde)



# Prévenir...

### Ordinateur et téléphone

- Faire la **mise à jour régulière** du système d'exploitation (Linux, Android, iOS, Windows ) ainsi que des applications installées
- **Éteindre complètement** l'appareil au moins 1 fois par semaine
- Fin de vie de l'appareil : **attention à vos données !** Pensez soit à effacer celles-ci ( a minima en réinitialisant l'appareil aux paramètres d'usine ) soit à détruire l'appareil



### Je me protège...

- Il y a toujours urgence : le but recherché par les malfaiteurs est de stresser la victime pour qu'elle agisse de manière irraisonnée
- Attention aux chèques volés : attendre 3 jours
- Vérifier l'adresse des sites en tapant sur internet : nom du site + arnaque
- Se méfier des demandes de paiement en mandat cash, transfert Western Union, carte PCS...



# Que faire ?

### En cas d'hameçonnage...

- Ne pas cliquer sur les liens dans les messages ou mails
- Contacter ou rappeler l'interlocuteur en utilisant le moyen habituel
- Attention à qui vous communiquez votre mail et/ou numéro de téléphone
- Faire la plupart des opérations sur ordinateur plutôt qu'un smartphone, notamment pour lire et répondre aux mails.

