

Particuliers, entreprises, collectivités locales rester vigilants et signaler les escroqueries

SIGNALER LES SPAMS, LES MAILS FRAUDULEUX OU E-MAILS DE PHISHING

www.33700.fr les spams (mails indésirables)

mails : www.signal-spam.fr

SMS : 33 700

SMS et SMS vocaux : 33700.fr

www.internet-signalement.gouv.fr

ou www.phishing-initiative.com

SIGNALER LES ESCROQUERIES EN LIGNE

via la plate-forme gouvernementale Info escroquerie :
0 805 805 817

SIGNALER LES CONTENUS CHOQUANTS CYBERMALVEILLANTS OU ILLICITES

www.cybermalveillance.gouv.fr

www.stop-djihadisme.gouv.fr

www.pointdecontact.net

VICTIME D'UNE CYBER-ATTAQUE ?

Si vous êtes victime d'une cyber-atteinte (piratage informatique de système ou de données, escroquerie via Internet, etc.) vous pouvez vous rapprocher d'un commissariat ou d'une brigade de gendarmerie sur toute la France.

à Paris et dans les départements 92, 93 et 94, en fonction du lieu de commission des faits ou du domicile de l'auteur ou du lieu de son arrestation, le commissariat de Police traitera votre dossier ou le transmettra au service spécialisé de la police judiciaire compétent.

informer
et protéger



prefecturedepolice.paris

[prefpolice](https://twitter.com/prefpolice)

[prefecturedepolice](https://www.facebook.com/prefecturedepolice)

[prefpolice](https://www.instagram.com/prefpolice)

[prefecture-de-police-de-paris](https://www.linkedin.com/company/prefecture-de-police-de-paris)

3430

Service gratuit
+ prix appel

INFORMER ET PROTÉGER

**cybersécurité
cybervigilance**
Conseils de sécurité
informatique

S'approprier une culture de cybervigilance pour sa cybersécurité

MOTS DE PASSE

- Choisissez des mots de passe ne figurant dans aucun dictionnaire, ils sont plus difficiles à pirater.
- Mélangez lettres, chiffres et caractères spéciaux dans vos mots de passe.
- Évitez les mots de passe relatifs à des informations personnelles (date de naissance, nom du chien, etc.).
- Ne laissez pas d'aide-mémoire (post-it ou autre) à proximité de l'ordinateur.
- Évitez les gestionnaires de mot de passe sur votre navigateur si vous êtes plusieurs à l'utiliser chez vous.
- Ne jamais retenir de mot de passe dans l'ordinateur ou le téléphone.
- Ne choisissez pas de questions secrètes que d'autres personnes pourraient deviner (par les réseaux sociaux par exemple) ou apportez-y une fausse réponse.

FOCUS

Changez toujours les mots de passe par défaut (après installation d'un réseau Wi-Fi par exemple).

FOCUS

Sécurisez votre réseau Wi-Fi (préférer la protection par clé WPA2 plutôt que par clé WEP).

PROTECTION CONTRE LES INTRUSIONS ET LES ESCROQUERIES

- Assurez-vous de disposer pour votre système d'exploitation (Windows, Linux, MacOS etc.), et pour vos logiciels (navigateur Internet par exemple), d'un pare-feu et d'un anti-virus et mettez les régulièrement et automatiquement à jour.
- N'exécutez jamais de programme dont vous ne connaissez pas la finalité ou l'expéditeur. Scannez-les à l'aide d'un anti-virus à jour en cas de doute.
- N'hésitez pas à vous faire aider d'une personne de confiance ayant des connaissances en informatique pour l'installation de vos logiciels de sécurité.
- Ne jamais cliquer sur un lien reçu par mail, y compris s'il provient d'une personne que vous connaissez. Préférez copier le lien dans la barre d'adresse de votre navigateur pour rechercher le site où vous serez conduit s'il existe bien.
- Dès constatation d'une infraction, cessez l'utilisation du poste pour éviter d'effacer des preuves à durée de vie limitée utiles à l'enquête et coupez l'alimentation électrique.

ESCOQUERIES

- Ne répondez pas aux e-mails douteux en provenance d'inconnus et ne cliquez jamais sur un lien et/ou une pièce jointe proposés dans de tels mails.
- En cas de doute sur le contenu d'un mail envoyé par un proche, demandez-lui par un autre moyen de communication s'il a bien envoyé ce mail.
- Ne relayez jamais par mail ou SMS les chaînes, ne partagez ni photos, ni MMS, ni rumeurs, vérifiez sur les sites tel **www.hoaxbuster.com**
- Aucun service ne vous demandera jamais par mail ou par téléphone, vos identifiants et mots de passe, même pour de prétendues raisons de sécurité.
- Pour les transactions sur Internet, vérifiez que la page de paiement est sécurisée (souvent une adresse commençant par https:// et repérez le cadenas vert).
- Méfiez-vous des « affaires du siècle » proposées sur les sites de vente et évitez les paiements auprès des sociétés de transferts d'argent si ceux-ci vous sont demandés par une personne inconnue ou rencontrée sur Internet. Ces solutions sont conçues pour un transfert d'argent entre personnes de confiance.



CONSULTEZ LES SITES D'INFORMATION

www.prefecturedepolice.paris

www.ssi.gouv.fr (Agence Nationale de Sécurité des Systèmes d'Information ANSSI)

www.cert.ssi.gouv.fr (CERT-FR de l'ANSSI)

www.cybermalveillance.gouv.fr

www.internet-signalement.gouv.fr (plate-forme PHAROS)

www.cnil.fr (site de la CNIL) et **www.jeunes.cnil.fr**