



## 10 CONSEILS POUR GÉRER VOS MOTS DE PASSE

mémo

1

Utilisez un mot de passe différent pour chaque service



6

Ne communiquez jamais votre mot de passe à un tiers



2

Utilisez un mot de passe suffisamment long et complexe



7

N'utilisez pas vos mots de passe sur un ordinateur partagé



3

Utilisez un mot de passe impossible à deviner



8

Activez la double authentification lorsque c'est possible



4

Utilisez un gestionnaire de mots de passe



9

Changez les mots de passe par défaut des différents services auxquels vous accédez



5

Changez votre mot de passe au moindre soupçon



10

Choisissez un mot de passe particulièrement robuste pour votre messagerie



Pour en savoir plus ou vous faire assister, rendez-vous sur [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)

## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1 ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2 INFORMATION ET SENSIBILISATION  
SUR LA SÉCURITÉ NUMÉRIQUE** 
- 3 OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR :  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)





## 10 CONSEILS POUR VOTRE SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

mémo

1

Protégez l'accès  
à vos comptes



6

Évitez les ordinateurs et  
les réseaux Wi-Fi publics



2

Vérifiez vos paramètres  
de confidentialité



7

Vérifiez régulièrement  
les connexions à votre  
compte



3

Maîtrisez vos publications



8

Faites preuve de  
discernement avec les  
informations publiées



4

Faites attention  
à qui vous parlez



9

Utilisez en conscience  
l'authentification avec  
votre compte de réseau  
social sur d'autres sites



5

Contrôlez les applications  
tierces



10

Supprimez votre compte  
si vous ne l'utilisez plus



Pour en savoir plus ou vous faire assister, rendez-vous sur [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)

## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1 ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2 INFORMATION ET SENSIBILISATION  
SUR LA SÉCURITÉ NUMÉRIQUE** 
- 3 OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR :  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)





## 10 CONSEILS POUR SÉCURISER VOS APPAREILS MOBILES

1

Mettez en place les  
codes d'accès



6

N'installez des applications  
que depuis les sites ou  
magasins officiels



2

Chiffrez les données  
de l'appareil



7

Contrôlez les autorisations  
de vos applications



3

Appliquez les mises à jour  
de sécurité



8

Ne laissez pas votre  
appareil sans surveillance



4

Faites des sauvegardes



9

Évitez les réseaux Wi-Fi  
publics ou inconnus



5

Utilisez une solution de  
sécurité contre les virus  
et autres attaques



10

Ne stockez pas d'informations  
confidentielles sans  
protection



## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1 ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2 INFORMATION ET SENSIBILISATION  
SUR LA SÉCURITÉ NUMÉRIQUE** 
- 3 OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR:  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)





## 10 CONSEILS POUR FAIRE VOS SAUVEGARDES

1

Effectuez des sauvegardes régulières de vos données



2

Identifiez les appareils et supports qui contiennent des données



3

Déterminez quelles données doivent être sauvegardées



4

Choisissez une solution de sauvegarde adaptée à vos besoins



5

Planifiez vos sauvegardes



6

Déconnectez votre support de sauvegarde après utilisation



7

Protégez vos sauvegardes (perte, vol, casse...)



8

Testez vos sauvegardes



9

Vérifiez le support de sauvegarde



10

Pro

Sauvegardez les logiciels indispensables à l'exploitation de vos données



## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1 ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2 INFORMATION ET SENSIBILISATION  
SUR LA SÉCURITÉ NUMÉRIQUE** 
- 3 OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR:  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)





## 10 CONSEILS POUR GÉRER VOS MISES À JOUR

1

Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels



6

Planifiez les mises à jour lors de périodes d'inactivité



2

Téléchargez les mises à jour uniquement depuis les sites officiels



7

Méfiez-vous des fausses mises à jour sur Internet



3

Identifiez l'ensemble des appareils et logiciels utilisés



8

Informez-vous sur la publication régulière des mises à jour de l'éditeur



4

Activez l'option de téléchargement et d'installation automatique des mises à jour



9

Testez les mises à jour lorsque cela est possible et faites des sauvegardes



5

Définissez les règles de réalisation des mises à jour



10

Protégez autrement les appareils qui ne peuvent pas être mis à jour



Pour en savoir plus ou vous faire assister, rendez-vous sur [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)

## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1 ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2 INFORMATION ET SENSIBILISATION  
SUR LA SÉCURITÉ NUMÉRIQUE** 
- 3 OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR:  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)





## 10 CONSEILS POUR SÉCURISER VOS USAGES PRO ET PERSO

1

Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez



2

Ne mélangez pas votre messagerie professionnelle et personnelle



3

Ayez une utilisation raisonnable d'Internet au travail



4

Maîtrisez vos propos sur les réseaux sociaux



5

N'utilisez pas de service de stockage en ligne personnel à des fins professionnelles



6

Faites les mises à jour de sécurité de vos équipements



7

Utilisez une solution de sécurité contre les virus et autres attaques



8

N'installez des applications que depuis les sites ou magasins officiels



9

Méfiez-vous des supports USB



10

Évitez les réseaux Wi-Fi publics ou inconnus



Pour en savoir plus ou vous faire assister, rendez-vous sur [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)

## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1 ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2 INFORMATION ET SENSIBILISATION  
SUR LA SÉCURITÉ NUMÉRIQUE** 
- 3 OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR:  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)





## L'HAMEÇONNAGE

mémo

**CYBERCRIMINEL**



### VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

#### BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

#### TECHNIQUE

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce...



**VICTIME**



### COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir ci-dessous)

**LIENS UTILES**

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

[Phishing-initiative.fr](https://www.phishing-initiative.fr)

[Info Escroqueries](https://www.info-escroqueries.gouv.fr)  
0805805817 (gratuit)

Pour en savoir plus ou vous faire assister, rendez-vous sur [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)

## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1 ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2 INFORMATION ET SENSIBILISATION  
À LA SÉCURITÉ NUMÉRIQUE** 
- 3 OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR:  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)





## LES RANÇONGIELS

mémo

CYBERCRIMINEL



### EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

#### BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

#### TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.



VICTIME



### COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

LIEN UTILE [www.nomoreransom.org/fr/index.4html](http://www.nomoreransom.org/fr/index.4html)

Pour en savoir plus ou vous faire assister, rendez-vous sur [Cybermalveillance.gouv.fr](http://Cybermalveillance.gouv.fr)

## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1** **ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2** **INFORMATION ET SENSIBILISATION  
À LA SÉCURITÉ NUMÉRIQUE** 
- 3** **OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR:  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)





## LES FAUX SUPPORTS TECHNIQUES

mémo

CYBERCRIMINEL



### ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique? Vous êtes victime d'une arnaque au faux support!

#### BUT

Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants.

#### TECHNIQUE

Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).



VICTIME



### COMMENT RÉAGIR ?

- Ne répondez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
- Désinstallez tout nouveau programme suspect
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

LIENS UTILES

[Internet-signalement.gouv.fr](https://internet-signalement.gouv.fr)

[Info Escroqueries](#)  
0805 805 817 (gratuit)

Pour en savoir plus ou vous faire assister, rendez-vous sur [Cybermalveillance.gouv.fr](https://Cybermalveillance.gouv.fr)

## DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

### SES MISSIONS

- 1 ASSISTANCE AUX VICTIMES  
D'ACTES DE CYBERMALVEILLANCE** 
- 2 INFORMATION ET SENSIBILISATION  
À LA SÉCURITÉ NUMÉRIQUE** 
- 3 OBSERVATION ET ANTICIPATION  
DU RISQUE NUMÉRIQUE** 

### QUI EST CONCERNÉ ?



RETROUVEZ TOUTES NOS PUBLICATIONS SUR:  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

