RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

mémo

COMPRENDRE LES RISQUES

LES **FAUX SUPPORTS TECHNIQUES**

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.).

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

Info Escroqueries
0 805 805 817 (gratuit)

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

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

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

mémo

COMPRENDRE LES RISQUES

L'HAMEÇONNAGE

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…

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

Phishing-initiative.fr

Info Escroqueries
0 805 805 817 (gratuit)

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

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 ?

- PARTICULIERS
- COLLECTIVITÉS TERRITORIALES
- ENTREPRISES

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

LES RANÇONGICIELS

Un rançongiciel (***ransomware*** en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

BUT RECHERCHÉ

Extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Certaines attaques visent juste à endommager le système de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.

SI VOUS ÊTES VICTIME

DÉBRANCHEZ LA MACHINE D'INTERNET ou du réseau informatique.

En entreprise, **ALERTEZ IMMÉDIATEMENT VOTRE SERVICE OU PRESTATAIRE INFORMATIQUE.**

NE PAYEZ PAS LA RANÇON réclamée car vous n'êtes pas certain de récupérer vos données et vous alimenteriez le système mafieux.

CONSERVEZ LES PREUVES: message piégé, fichiers de journalisation (logs) de votre pare-feu, copies physiques des postes ou serveurs touchés. À défaut, conservez les disques durs.

DÉPOSEZ PLAINTE au commissariat de police ou à la gendarmerie ou en écrivant au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

Professionnels : **NOTIFIEZ L'INCIDENT À LA CNIL** s'il y a eu une violation de données personnelles.

IDENTIFIEZ LA SOURCE DE L'INFECTION et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

APPLIQUEZ UNE MÉTHODE DE DÉSINFECTION ET DE DÉCHIFFREMENT, lorsqu'elle existe*. En cas de doute, effectuez une restauration complète de votre ordinateur. Reformatez les postes et/ou serveurs touchés et réinstallez un système sain puis restaurez les copies de sauvegarde des fichiers perdus lorsqu'elles sont disponibles.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS. Vous trouverez sur www.cybermalveillance.gouv.fr des professionnels en sécurité informatique susceptibles de pouvoir vous apporter leur assistance.

** Le site suivant peut fournir des solutions dans certains cas: https://www.nomoreransom.org/fr/index.4html*

MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Tenez à jour l'antivirus et configurez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.

N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.

N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses.

Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

Utilisez des mots de passe suffisamment complexes et changez-les régulièrement, mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés (tous nos conseils pour gérer vos mots de passe).

Éteignez votre machine lorsque vous ne vous en servez pas.

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- De tels procédés relèvent de l'**extorsion de fonds** et non de l'escroquerie. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou de ses fichiers – obligeant à une remise de fonds non volontaire. L'article 312-1 du code pénal dispose que : « *l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende* ».

- L'infraction d'**atteinte à un système de traitement automatisé de données (STAD)** peut aussi être retenue. Les articles 323-1 à 323-7 du code pénal disposent notamment que « *le fait d'accéder ou de se maintenir frauduleusement* » *dans un STAD,* « *la suppression ou la modification de données contenues dans le système* », « *le fait [...] d'extraire, de détenir, de reproduire, de transmettre [...] les données qu'il contient* » ou « *l'altération du fonctionnement de ce système* » sont passibles de trois à sept ans d'emprisonnement et de 100 000 à 300 000 euros d'amende.
  – La tentative de ces infractions est punie des mêmes peines (article 323-7 du code pénal).
  – Lorsque ces infractions ont été commises en bande organisée (article 323-4-1 du code pénal), la peine peut être portée à dix ans d'emprisonnement et à 300 000 euros d'amende.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

V230417

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

mémo

COMPRENDRE LES RISQUES

LES **RANÇONGICIELS**

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.

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

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

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 ?

- PARTICULIERS
- COLLECTIVITÉS TERRITORIALES
- ENTREPRISES

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LE PIRATAGE DE COMPTE

COMPRENDRE LES RISQUES

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne. En pratique, les attaquants ont pu avoir accès à votre compte de plusieurs manières : le mot de passe était peut-être trop simple, vous avez précédemment été victime d'hameçonnage (***phishing*** en anglais) où vous avez communiqué votre mot de passe sans le savoir, ou bien vous avez utilisé le même sur plusieurs sites dont l'un a été piraté.

BUT RECHERCHÉ

Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.).

SI VOUS ÊTES VICTIME

Si vous ne pouvez plus vous connecter à votre compte, **CONTACTEZ LE SERVICE CONCERNÉ POUR SIGNALER VOTRE PIRATAGE ET DEMANDEZ LA RÉINITIALISATION DE VOTRE MOT DE PASSE.**

Dans vos paramètres de récupération de compte, **ASSUREZ-VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS**. Si ce n'est pas le cas, changez-les immédiatement.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE et choisissez-en un solide (voir notre fiche sur la gestion des mots de passe). Et si possible, **ACTIVEZ LA DOUBLE AUTHENTIFICATION.**

CHANGEZ SANS TARDER LE MOT DE PASSE PIRATÉ SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.

PRÉVENEZ TOUS VOS CONTACTS DE CE PIRATAGE pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

VÉRIFIEZ QU'AUCUNE PUBLICATION OU COMMANDE N'A ÉTÉ RÉALISÉE avec le compte piraté.

Si vos coordonnées bancaires étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

En fonction du préjudice subi, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

MESURES PRÉVENTIVES

Utilisez des mots de passes différents et complexes pour chaque site et application utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.

Lorsque le site ou le service le permettent, **activez la double authentification** pour augmenter le niveau de sécurité.

Ne communiquez jamais d'informations sensibles (mots de passe) par messagerie, par téléphone ou sur Internet.

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Maintenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

N'ouvrez pas les courriels ou leurs pièces jointes et ne cliquez jamais sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont le contenu du message est inhabituel ou vide.

Évitez les sites non sûrs ou illicites, tels ceux hébergeant des contrefaçons dont ces dernières peuvent contenir des logiciels malveillants (musique, films, logiciels, etc.) ou certains sites pornographiques.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

Si le site le permet, **vérifiez les date et heure de la dernière connexion à votre compte** afin de repérer d'éventuelles connexions anormales.

Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics. Non maîtrisés, ils peuvent être contrôlés par un pirate.

Déconnectez-vous systématiquement de votre compte après utilisation pour éviter que quelqu'un puisse y accéder après vous.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal)** : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de trois ans d'emprisonnement et de 100 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine encourue est de cinq ans d'emprisonnement et de 150 000 euros.

Dans le cas d'un piratage d'un compte de messagerie :
- **Atteinte au secret des correspondances (article 226-15 du code pénal)** : délit passible d'une peine d'emprisonnement d'un an et de 45 000 euros d'amende.

Dans le cas de collecte de données à caractère personnel quel que soit le compte :
- **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal)** : le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Si le compte a été détourné pour usurper votre identité :
- **Usurpation d'identité par voie de télécommunication (article 226-4-1 du code pénal)** : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

V230417

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CHANTAGE À L'ORDINATEUR OU À LA WEBCAM PRÉTENDUMENT PIRATÉS

COMPRENDRE LES RISQUES

Le chantage à l'ordinateur ou à la webcam prétendus piratés (ou « **cryptoporno** ») désigne un type d'escroquerie qui vise à vous faire croire que vos équipements ont été piratés. Il prend généralement la forme d'un message reçu, essentiellement par courriel (mail), de la part d'un inconnu qui se présente comme un pirate informatique. Ce « hacker » prétend avoir pris le contrôle de l'ordinateur de la victime suite à la consultation d'un site pornographique et annonce avoir obtenu des vidéos compromettantes avec sa webcam. Le cybercriminel menace de les publier aux contacts (personnels et/ou professionnels) de la victime si elle ne lui paie pas une rançon, souvent réclamée en monnaie virtuelle (généralement en Bitcoin). Parfois, pour attester de la prise de contrôle de l'ordinateur auprès de la victime, les cybercriminels vont jusqu'à lui écrire avec sa propre adresse mail ou lui dévoiler l'un de ses mots de passe.

BUT RECHERCHÉ

Soutirer de l'argent sous la menace de divulguer des vidéos compromettantes de la victime à ses contacts.

SI VOUS ÊTES VICTIME

NE PANIQUEZ PAS. En effet, vous n'avez sans doute rien de réellement compromettant à vous reprocher.

NE RÉPONDEZ PAS. Il ne faut jamais répondre à de telles menaces de chantage qui montrent aux cybercriminels que votre adresse de messagerie est « valide » et que vous portez de l'intérêt au message de chantage qu'ils vous ont envoyé.

NE PAYEZ PAS LA RANÇON. Et ce, même si vous aviez un doute. En effet, aucune mise à exécution des menaces n'a été démontrée jusqu'à présent et vous alimenteriez donc inutilement ce système criminel.

CONSERVEZ LES PREUVES. Faites des captures d'écran, conservez les messages qui pourront vous servir pour signaler cette tentative d'extorsion aux autorités.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE partout où vous l'utilisez s'il a été divulgué ou au moindre doute et choisissez-en un solide (tous nos conseils pour gérer vos mots de passe).

CONTACTEZ VOTRE BANQUE si vous avez payé la rançon pour essayer de faire annuler la transaction.

DÉPOSEZ PLAINTE au commissariat de police ou à la gendarmerie ou en adressant votre plainte au procureur de la République du tribunal judiciaire dont vous dépendez.

MESURES PRÉVENTIVES

Faites régulièrement les mises à jour de sécurité de tous vos appareils (tous nos conseils pour gérer vos mises à jour).

Utilisez un antivirus et tenez-le à jour.

Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels, etc.) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

Utilisez des mots de passe suffisamment complexes et **changez-les au moindre doute** (tous nos conseils pour gérer vos mots de passe).

N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.

Masquez votre webcam quand vous ne vous en servez pas (un simple morceau de ruban adhésif opaque sur l'objectif peut suffire).

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

LES **INFRACTIONS**

L'incrimination principale qui peut être retenue est l'**extorsion de fonds**. **L'article 312-1 du Code pénal** dispose que « *l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ». L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.

Licence Ouverte v2.0 (ETALAB)

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LE SPAM TÉLÉPHONIQUE

COMPRENDRE LES RISQUES

Le spam téléphonique désigne une communication non sollicitée à des fins publicitaires, commerciales ou malveillantes. Il peut prendre différentes formes : SMS, MMS ou bien appel téléphonique. Dans bien des cas, il s'agit de messages publicitaires adressés à des fins de prospection commerciale. Mais le spam téléphonique peut également revêtir un caractère malveillant : incitation à rappeler un numéro surtaxé, envoyer un SMS à un numéro payant ou encore tentatives d'hameçonnage (***phishing*** en anglais) pour récupérer des données personnelles et/ou confidentielles. D'après la loi, la prospection commerciale n'est autorisée que si les personnes concernées ont donné leur accord pour être démarchées par téléphone.

BUT RECHERCHÉ

- **Vente de produits ou de services,** publicité virale, propagande, etc.
- **Vol de données** personnelles et/ou professionnelles
- **Escroquerie à caractère financier**, etc.

SI VOUS ÊTES VICTIME

En cas d'appels non sollicités, **DEMANDEZ À CE QUE VOS DONNÉES SOIENT RETIRÉES DES FICHIERS DE COORDONNÉES DE L'APPELANT.**

Pour bloquer les SMS ou MMS indésirables, **ENVOYEZ LE MOT « STOP » PAR SMS** au numéro expéditeur du message.

S'il s'agit d'une société commerciale vous contactant par SMS, vous pouvez obtenir les coordonnées du service client de l'expéditeur et ainsi faire valoir votre droit au retrait de consentement en les contactant. **ENVOYEZ LE MOT « CONTACT » PAR SMS** au numéro expéditeur du message.

Si vous avez reçu un spam téléphonique (SMS, MMS ou appel), **SIGNALEZ-LE SUR LA PLATEFORME 33 700** (www.33700.fr) **OU PAR SMS AU 33700**.

BLOQUEZ LES SMS OU APPELS INDÉSIRABLES SUR VOTRE TÉLÉPHONE MOBILE. Votre appareil dispose en effet de fonctionnalités permettant de bloquer des numéros de téléphone (voir documentation du téléphone).

En cas de sollicitations répétées ou abusives et si vous êtes inscrit sur la liste d'opposition Bloctel, **FAITES UNE RÉCLAMATION DEPUIS VOTRE ESPACE PERSONNEL SUR LE SITE INTERNET DE BLOCTEL.** Votre signalement sera transmis à la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) pour investigation et sanction si la pratique commerciale abusive est avérée.

Si vous avez demandé à ne plus être sollicité mais que les appels téléphoniques continuent, **DÉPOSEZ PLAINTE AUPRÈS DE LA CNIL.**

Si les sollicitations s'apparentent à du harcèlement, **DÉPOSEZ PLAINTE** au commissariat de police ou à la brigade de gendarmerie ou en écrivant au procureur de la République dont vous dépendez.

MESURES PRÉVENTIVES

Soyez vigilant lorsque vous communiquez votre numéro de téléphone fixe ou mobile à des tiers.

Inscrivez-vous sur la liste d'opposition Bloctel qui enregistre les numéros de téléphone des personnes qui ne souhaitent pas être sollicitées dans le cadre de prospections commerciales et que des sociétés doivent consulter avant de vous contacter.

Certains opérateurs téléphoniques proposent **des systèmes de filtrage de numéros. N'hésitez pas à les utiliser.**

Soyez vigilant lorsque vous répondez à des formulaires d'inscription, des bons de commande ou participez à des jeux concours : certains acteurs n'appliquent pas toujours les bonnes pratiques et votre numéro de téléphone pourrait figurer dans des bases de données à votre insu. Vérifiez la fiabilité d'une marque avant d'accorder votre consentement par téléphone pour éviter que votre numéro ne soit communiqué à des tiers.

Désabonnez-vous ou supprimez les comptes que vous n'utilisez plus pour limiter toute diffusion de données à des tiers.

Si vous recevez un appel en absence provenant d'un numéro surtaxé ou passé depuis l'étranger sans qu'un message ne soit laissé, **ne rappelez pas.** Il peut s'agir d'une arnaque vous incitant à rappeler ce numéro pour vous faire payer les frais liés à la communication téléphonique.

Si vous recevez un message vous invitant à envoyer un SMS à un numéro payant (numéro à 5 chiffres commençant par 6, 7 ou 8), **ne répondez pas.**

Si vous recevez un message SMS incitant à cliquer sur un lien Internet, soyez vigilant car ce lien pourrait vous rediriger vers un service payant ou malveillant.

En cas de doute, **utilisez un annuaire inversé des numéros**, comme infosva.org, pour identifier à qui appartient le numéro et son coût.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- **Prospection sans consentement préalable (article L121-20-5 du Code de la consommation et article L34-5 du Code des postes et communications électroniques)** : « *est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen. Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services* ». Selon l'article L470-1 du Code du commerce, « *lorsque le professionnel concerné n'a pas déféré dans le délai imparti à une injonction qui lui a été notifiée à raison d'une infraction ou d'un manquement passible d'une amende administrative, l'autorité administrative chargée de la concurrence et de la consommation peut prononcer à son encontre, dans les conditions et selon les modalités prévues à l'article L. 470-2, une amende administrative dont le montant ne peut excéder 3 000 € pour une personne physique et 15 000 € pour une personne morale* ». Par ailleurs, selon l'article R10-1 du Code des postes et des communications électroniques, « *le fait d'utiliser, dans des opérations de prospection directe, des données à caractère personnel relatives à des personnes ayant exprimé leur opposition, par application des dispositions du 4 de l'article R.10, quel que soit le mode d'accès à ces données, est puni, pour chaque correspondance ou chaque appel, de l'amende prévue pour les contraventions de la quatrième classe, sans préjudice de l'application du premier alinéa de l'article 226-18 du code pénal* ». En outre, l'article 226-18-1 stipule que « *le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.* »

- **Pratique commerciale trompeuse (article L121-2 du Code de la consommation)** : « *une pratique commerciale est trompeuse lorsqu'elle crée une confusion avec un autre bien ou service, une marque, un nom commercial, ou un autre signe distinctif d'un concurrent, lorsqu'elle repose sur des allégations, indications ou présentations fausses ou de nature à induire en erreur ou bien encore lorsque la personne pour le compte de laquelle elle est mise en œuvre n'est pas clairement identifiable.* » Selon l'article L121-6 du Code de la consommation, les pratiques commerciales trompeuses sont punies d'un emprisonnement de deux ans et d'une amende de 300 000 €. Le montant de l'amende peut être porté, de manière proportionnée aux avantages tirés du manquement, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits, ou à 50 % des dépenses engagées pour la réalisation de la publicité ou de la pratique constituant le délit.

Lorsque le spam a pour fonction ou objet de tromper dans un but de captation de données ou de fonds :

- **Escroquerie (article 313-1 du code pénal)** : « *l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge* ». L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

- **Tromperie en matière commerciale (article L213-1 du Code de la consommation)** : « *sera puni d'un emprisonnement de deux ans au plus et d'une amende de 300 000 euros quiconque, qu'il soit ou non partie au contrat, aura trompé ou tenté de tromper le contractant, par quelque moyen ou procédé que ce soit, même par l'intermédiaire d'un tiers, soit sur la nature, l'espèce, l'origine, les qualités substantielles, la composition ou la teneur en principes utiles de toutes marchandises, soit sur la quantité des choses livrées ou sur leur identité par la livraison d'une marchandise autre que la chose déterminée qui a fait l'objet du contrat ou bien soit sur l'aptitude à l'emploi, les risques inhérents à l'utilisation du produit, les contrôles effectués, les modes d'emploi ou les précautions à prendre* ». Le montant de l'amende peut être porté, de manière proportionnée aux avantages tirés du manquement, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits.

S'il s'agit d'un harcèlement caractérisé (répétition et volonté de nuire à la victime / ne comprend pas le démarchage publicitaire) :

- **Harcèlement téléphonique (article 222-16 du code pénal)** : « *les appels téléphoniques malveillants réitérés, les envois réitérés de messages malveillants émis par la voie des communications électroniques ou les agressions sonores en vue de troubler la tranquillité d'autrui sont punis d'un an d'emprisonnement et de 15 000 euros d'amende.* »

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

LE SPAM ÉLECTRONIQUE

Le spam électronique, également appelé courrier indésirable ou pourriel, désigne une communication électronique non sollicitée à des fins publicitaires, commerciales ou malveillantes. Dans bien des cas, il s'agit de messages de prospection commerciale ne respectant pas les obligations légales en matière de consentement des destinataires, mais il peut également revêtir un caractère malveillant : astuces pour gagner de l'argent, sollicitation pour transférer des fonds ou encore tentatives d'hameçonnage (***phishing*** en anglais) pour récupérer des données personnelles et/ou confidentielles. Les expéditeurs de spams ciblent essentiellement les comptes de messagerie, mais peuvent aussi utiliser les messageries instantanées ou les réseaux sociaux. Un spam peut parfois même contenir un logiciel malveillant ou un virus (un rançongiciel par exemple) qui pourrait permettre d'utiliser ou de bloquer votre appareil à votre insu.

BUT RECHERCHÉ

- **Vente de produits ou de services,** publicité virale, propagande, etc.
- **Diffusion de virus**
- **Vol de données** personnelles et/ou professionnelles
- **Escroquerie à caractère financier**, etc.

SI VOUS ÊTES VICTIME

Si vous avez reçu un message douteux, **N'Y RÉPONDEZ PAS.**

Si l'émetteur vous semble légitime, **CLIQUEZ SUR LE LIEN DE DÉSINSCRIPTION OU DE DÉSABONNEMENT** figurant dans les messages électroniques (sollicitations commerciales, lettres d'information) pour faire valoir votre droit au retrait du consentement.

Pour lutter plus activement contre le spam, **SIGNALEZ-LE À SIGNAL SPAM** (Signal-spam.fr). Vous aurez la possibilité d'installer une extension à votre navigateur Internet et/ou votre client de messagerie qui vous permettra de signaler facilement tout message ou site Internet suspects.

Dans la boîte de réception de votre messagerie, **MARQUEZ LES SPAMS COMME « INDÉSIRABLES »**. Cette fonctionnalité existe dans la majorité des clients de messagerie et webmails, et dans le module de Signal Spam.

Vous pouvez également **BLOQUER LES EXPÉDITEURS DE SPAM** dans les paramètres de configuration de votre client de messagerie.

Si vous avez demandé à ne plus être sollicité mais que vous continuez à recevoir des spams, **DÉPOSEZ PLAINTE AUPRÈS DE LA CNIL.**

MESURES PRÉVENTIVES

Soyez vigilant lorsque vous communiquez votre adresse de messagerie à des tiers.

Ne répondez pas aux messages dont vous ne connaissez pas l'expéditeur. Vous éviterez ainsi de le renseigner sur la validité de votre adresse de messagerie.

N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le message est inhabituel ou vide.

Utilisez un filtre ou un logiciel anti-spam pour limiter la réception de spams. Certains antivirus proposent ce type de protection.

Soyez vigilant lorsque vous répondez à des formulaires d'inscription, des bons de commande ou quand vous participez à des jeux-concours : certains acteurs n'appliquent pas toujours les bonnes pratiques et votre adresse pourrait figurer dans des bases de données à votre insu. Vérifiez la fiabilité d'une marque (recherche sur Internet ou d'avis par exemple) avant d'accepter l'envoi de communications publicitaires ou de lettres d'information pour éviter que votre messagerie ne soit vite submergée.

Désabonnez-vous ou supprimez les comptes (services, applications, sites Internet) que vous n'utilisez plus pour limiter toute diffusion de données à des tiers.

Créez des règles dans votre boîte de messagerie pour filtrer et/ou supprimer certains types de messages indésirables.

Créez différentes adresses de messagerie en fonction de vos besoins (échanges personnels, sites marchands etc.) afin de préserver votre adresse principale.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- **Prospection sans consentement préalable (article L121-20-5 du Code de la consommation et article L34-5 du Code des postes et communications électroniques)** : « *est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen. Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services* ». Selon l'article L470-1 du Code du commerce, « *lorsque le professionnel concerné n'a pas déféré dans le délai imparti à une injonction qui lui a été notifiée à raison d'une infraction ou d'un manquement passible d'une amende administrative, l'autorité administrative chargée de la concurrence et de la consommation peut prononcer à son encontre, dans les conditions et selon les modalités prévues à l'article L. 470-2, une amende administrative dont le montant ne peut excéder 3 000 € pour une personne physique et 15 000 € pour une personne morale* ». Par ailleurs, selon l'article R10-1 du Code des postes et des communications électroniques, « *le fait d'utiliser, dans des opérations de prospection directe, des données à caractère personnel relatives à des personnes ayant exprimé leur opposition, par application des dispositions du 4 de l'article R.10, quel que soit le mode d'accès à ces données, est puni, pour chaque correspondance ou chaque appel, de l'amende prévue pour les contraventions de la quatrième classe, sans préjudice de l'application du premier alinéa de l'article 226-18 du code pénal* ». En outre, l'article 226-18-1 stipule que « *le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.* »

- **Pratique commerciale trompeuse (article L121-2 du Code de la consommation)** : « *une pratique commerciale est trompeuse lorsqu'elle crée une confusion avec un autre bien ou service, une marque, un nom commercial, ou un autre signe distinctif d'un concurrent, lorsqu'elle repose sur des allégations, indications ou présentations fausses ou de nature à induire en erreur ou bien encore lorsque la personne pour le compte de laquelle elle est mise en œuvre n'est pas clairement identifiable.* » Selon l'article L121-6 du Code de la consommation, les pratiques commerciales trompeuses sont punies d'un emprisonnement de deux ans et d'une amende de 300 000 €. Le montant de l'amende peut être porté, de manière proportionnée aux avantages tirés du manquement, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits, ou à 50 % des dépenses engagées pour la réalisation de la publicité ou de la pratique constituant le délit.

Lorsque le spam a pour fonction ou objet de tromper dans un but de captation de données ou de fonds :

- **Escroquerie (article 313-1 du code pénal)** : « *l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge* ». L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

- **Tromperie en matière commerciale (article L213-1 du Code de la consommation)** : « *sera puni d'un emprisonnement de deux ans au plus et d'une amende de 300 000 euros quiconque, qu'il soit ou non partie au contrat, aura trompé ou tenté de tromper le contractant, par quelque moyen ou procédé que ce soit, même par l'intermédiaire d'un tiers, soit sur la nature, l'espèce, l'origine, les qualités substantielles, la composition ou la teneur en principes utiles de toutes marchandises, soit sur la quantité des choses livrées ou sur leur identité par la livraison d'une marchandise autre que la chose déterminée qui a fait l'objet du contrat ou bien soit sur l'aptitude à l'emploi, les risques inhérents à l'utilisation du produit, les contrôles effectués, les modes d'emploi ou les précautions à prendre* ». Le montant de l'amende peut être porté, de manière proportionnée aux avantages tirés du manquement, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

Version 3.0