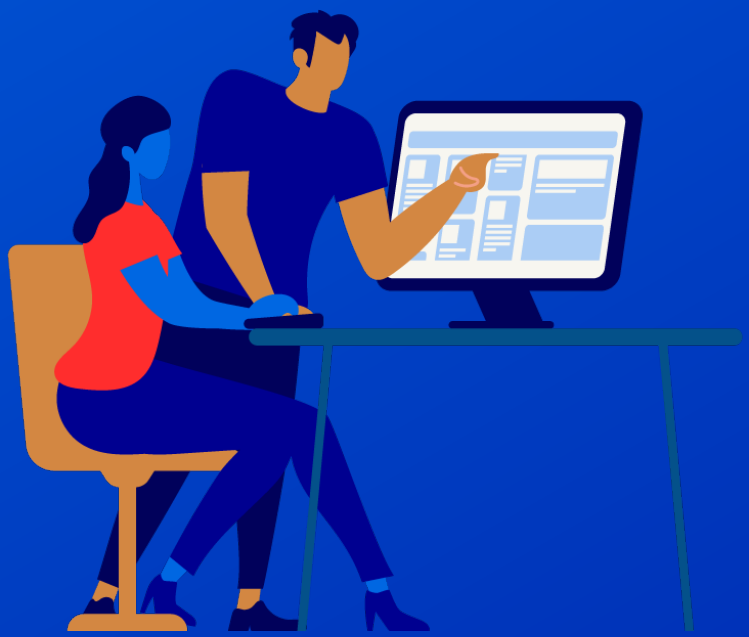
Les premiers pas de la sécurité en ligne

La fiche ***Les premiers pas de la sécurité en ligne*** est la première d'une série de trois fiches conçus pour aider les Français à comprendre les principes de base de la cybersécurité. Découvrez comment vous pouvez agir pour vous protéger contre les cybermenaces les plus courantes.



Rédacteurs : TelesCoop (Quentin MADURA, Maxime BELLEC)

Mise en forme : TelesCoop (Quentin MADURA)

Coordination

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CONSEILLER NUMÉRIQUE

Sécuriser ses comptes

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe.

Comment créer un mot de passe sécurisé ?

Pour créer un mot de passe sécurisé, il existe quelques bonnes pratiques à respecter :

1. utiliser un mot de passe différent pour chaque compte
2. utiliser un mot de passe suffisamment long et complexe avec au minimum 12 caractères comprenant des majuscules, des minuscules et des caractères spéciaux.
3. ne pas utiliser qu'un seul mot (par exemple, "princesse") ou une phrase couramment utilisée (par exemple, "Iloveyou").
4. faire en sorte que votre mot de passe soit difficile à deviner.

Soyez particulièrement attentif à la sécurité de votre mot de passe utilisé pour votre adresse e-mail. Si un cybercriminel peut accéder à votre compte de courrier électronique, il pourrait : accéder à des informations privées vous concernant (coordonnées bancaires), réinitialiser les mots de passe de tous vos autres comptes (et accéder à tous vos autres comptes en ligne) ou encore écrire des courriels et des messages prétendant provenir de vous (et les utiliser pour tromper d'autres personnes)

Quelques astuces pour créer un mot de passe solide :

- La méthode des premières lettres : Un tiens vaut mieux que deux tu l'auras
  > 1tvmQ2tl'A
- La méthode phonétique : J'ai acheté huit CD pour cent euros cet après-midi
  > ght8CD%E7am

Le mieux est encore d'inventer sa propre méthode mnémotechnique !

Où les stocker ?

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. Vous pouvez choisir de conserver vos mots de passe sur un carnet que vous conservez uniquement à la maison ou sur un fichier sur votre ordinateur avec un nom qui n'attire pas l'attention (exemple : liste de courses).

Pour aller plus loin

Pourquoi et comment bien gérer ses mots de passe ?
cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

Reconnaître les messages frauduleux

Les messages frauduleux (ou technique d'hameçonnage ou *phishing* en anglais) sont destinés à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

Apprendre à reconnaître les messages frauduleux

Il n'est cependant pas toujours facile de détecter les messages d'hameçonnage, car ils ressemblent souvent à s'y méprendre à des messages tout à fait légitimes. Cela dit, les cybercriminels aussi font des erreurs : fautes d'orthographe, adresse courriel mal écrite ou qui ne correspond pas à l'identité réelle de la personne ou de l'organisation que l'auteur dit représenter.

Les messages frauduleux courants

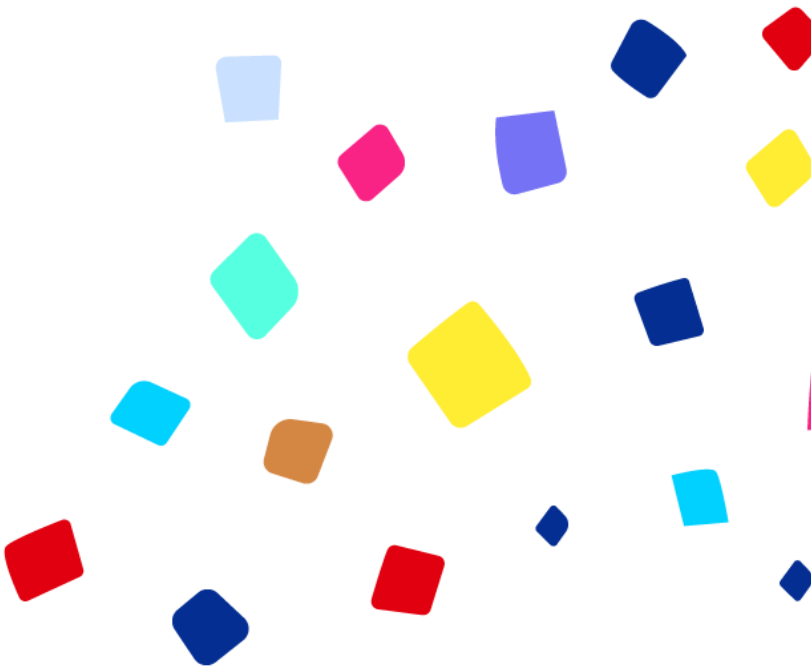
Ces types de messages sont souvent frauduleux, donc soyez particulièrement vigilants quand vous les recevez même s'ils peuvent correspondre à des sollicitations qui sont réellement pertinentes.

1. SMS ou email relatif à un colis - ne suivez pas le lien
2. Appel à l'aide d'un proche - vérifiez auprès du proche
3. Email de votre banque / la CAF vous demandant de mettre à jour vos coordonnées (éventuellement bancaires) - ne suivez jamais ces liens, au besoin allez sur le site de votre banque ou de la CAF pour vérifier une demande
4. Demandes d'aide venant d'une rencontre en ligne - les sites de rencontre donnent lieu à de nombreuses arnaques, ne donnez pas d'argent à une personne que vous n'avez jamais rencontré en vrai, quelle que soit la prétendue urgence.
5. Demande d'argent pour débloquer des dons qui vous seraient destinés ou que vous auriez gagné - si une personne que vous ne connaissiez pas devait vous léguer de l'argent, elle passerait par un notaire.
6. Appel de votre banque / de la police / des impôts - quelle que soit la prétendue urgence, ne donnez aucune information personnelle et aucun argent. Ces organismes publics ont d'autres moyens de vous contacter (courrier, venir chez vous si c'est si urgent)... Ou contactez ces organismes vous-même en vous déplaçant ou en les contactant via les numéros indiqués sur les sites officiels.

Pour aller plus loin

Comment reconnaître un mail de phishing ou d'hameçonnage ?

cybermaveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage



Se protéger des arnaques

N'achetez qu'auprès des sites dans lesquels vous avez confiance.

Le plus sûr est d'utiliser le site internet d'un magasin ou d'une chaîne de magasin.

Éviter de réagir trop rapidement

Certains messages frauduleux misent sur la peur ou l'intimidation pour tromper leurs victimes afin que celles-ci, apeurées, réagissent sans réfléchir. Il est important d'être prudent lorsqu'on reçoit un message qui semble suspect et d'éviter de réagir trop rapidement.

Ne pas communiquer d'informations sensibles

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration, banque ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

Réfléchissez avant de partager des informations sur les médias sociaux

Les cybercriminels peuvent utiliser les informations que vous avez publiées sur votre/vos compte(s) de médias sociaux dans leurs escroqueries et cyberattaques. Il s'agit donc d'éviter de partager certains types d'informations comme :

- Lieu et date de naissance
- Adresse et numéro de téléphone
- Votre employeur et vos antécédents professionnels
- L'endroit où vous êtes allé à l'école
- Toute autre information personnelle susceptible d'être utilisée pour vous cibler.

N'oubliez pas que les informations publiées sur Internet sont souvent permanentes et que vous ne pourrez peut-être jamais effacer complètement ce qui a été publié.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si elle ne correspond pas exactement au site concerné (par exemple, magasin-leroy-merlin.fr à la place de leroymerlin.fr), il s'agit très certainement d'un site frauduleux. Parfois, un seul caractère dans l'adresse du site peut vous tromper. Vérifiez que l'adresse commence par "https://" et qu'un petit cadenas sécurisé est visible à côté de l'adresse dans la barre d'adresse, ce qui indique une connexion sécurisée. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante, puis utilisez un moteur de recherche pour être sûr d'aller sur le vrai site.

Pour aller plus loin

10 mesures essentielles pour assurer votre sécurité numérique. cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

Que faire en cas de phishing ou hameçonnage ? cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Les acteurs de référence en matière de cybersécurité

Agence nationale de la sécurité des systèmes d'information (ANSSI)

C'est l'agence gouvernementale chargée de la cybersécurité en France. L'ANSSI est responsable de la protection des systèmes d'information stratégiques du gouvernement et des entreprises.

En savoir plus : https://cyber.gouv.fr/

cybermalveillance.gouv.fr

Incubé par l'ANSSI cette référence gouvernementale est incontournable sur les sujets de cybersécurité en France. Ce site s'adresse principalement à toutes les victimes d'attaques informatiques qui ne disposent pas des compétences ou des ressources suffisantes en sécurité numérique.
Ils diffusent régulièrement des informations et des bonnes pratiques et accompagnent également ces victimes en cas d'actes de cyber malveillance.

En savoir plus : cybermalveillance.gouv.fr

SecNumEdu

Initiative de l'ANSSI visant à sensibiliser les citoyens aux enjeux de la cybersécurité. Elle propose des ressources pédagogiques pour différents publics, y compris le grand public. Elle édite notamment le site secnumacademie.gouv.fr, un MOOC pour s'initier au sujet ou approfondir ses compétences sur la cybersécurité.

En savoir plus : https://secnumacademie.gouv.fr/

La Commission nationale de l'informatique et des libertés (CNIL)

Créée en 1978, la CNIL veille à ce que les entreprises et institutions respectent les lois sur la protection des données. La CNIL informe et conseille les citoyens sur leurs droits et les bonnes pratiques. Elle intervient en cas de violation des données et impose des sanctions si nécessaire. Son site, cnil.fr, offre des ressources et des guides pour aider les individus et les organisations à protéger leurs informations personnelles.

Autres initiatives

En plus des conseillers numérique France Service, d'autres acteurs de la médiation numérique proposent aussi des initiations à la cybersécurité. De manière non exhaustive, on peut citer les Espaces Publics Numériques, Emmaüs Connect, Les Bons Clics ou les acteurs locaux.

Les indispensables de la sécurité en ligne

La fiche ***Les indispensables de la sécurité en ligne*** est la seconde d'une série de trois fiches conçus pour aider les Français à comprendre les principes de base de la cybersécurité. Découvrez comment vous pouvez agir pour vous protéger contre les cybermenaces les plus courantes.

Rédacteurs : TelesCoop (Quentin MADURA, Maxime BELLEC)

Mise en forme : TelesCoop (Quentin MADURA)

Coordination

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CONSEILLER NUMÉRIQUE

Notion de base sur les virus

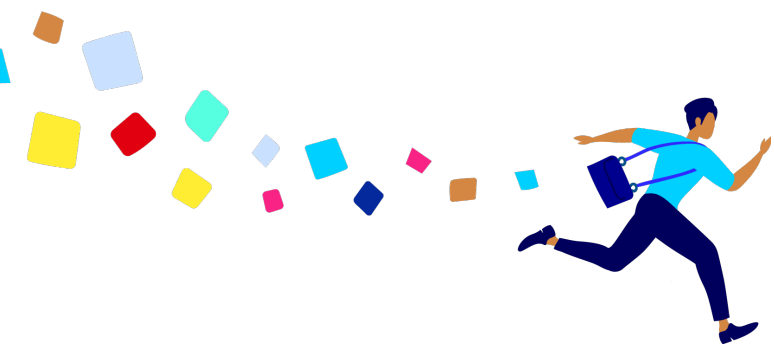
Les virus sont un type de logiciel malveillant qui peut endommager des appareils tels que les ordinateurs, les ordinateurs portables, les smartphones et les tablettes. Une fois sur votre appareil infecté, ces logiciels malveillants peuvent voler vos données, les effacer partiellement ou complètement, voire vous empêcher d'utiliser complètement votre appareil.

Les méthodes courantes d'infections

Une machine est souvent infectée par messages courriels (mail), par un partage de fichiers, via une faille du système ou par un élément extérieur comme une clef USB.

Le téléchargement et l'installation d'un logiciel font partie des principales méthodes d'infections. Il est donc très important de télécharger un logiciel depuis une source sûre.

Vérifier d'abord si le logiciel que vous voulez installer est disponible sur le magasin d'application de votre environnement - Microsoft Store sur Windows, App Store sur iOS ou macOS, Play Store sur Android. Si ce n'est pas le cas, identifier l'éditeur de l'application en cherchant par exemple "éditeur [nom du logiciel]" sur un moteur de recherche, et téléchargez le logiciel depuis le site officiel de l'éditeur. De nombreux autres sites proposent des liens de téléchargement, mais ils peuvent présenter un risque.



Les effets des virus

Les effets d'un virus sur un appareil peuvent être très différents : certains vont exploiter vos données, d'autres (appelés les rançongiciels) vont les rendre inaccessibles dans le but de vous faire payer une rançon. Il existe également des virus qui peuvent permettre de prendre le contrôle de votre ordinateur, de votre tablette ou de votre téléphone mobile pour vous voler vos données.

Identifier un virus informatique

Pour identifier la présence d'un virus, voici une liste des effets que peuvent provoquer ces logiciels malveillants :

- Ralentissement de l'appareil,
- Blocage,
- Fenêtres qui s'affichent sans raison,
- Modification de logiciels ou programmes, comme votre navigateur Internet, logiciel de traitement de texte, etc.
- Boîte de dialogue ou messages inconnus,
- Sites Internet qui apparaissent automatiquement.

Des messages non sollicités, par SMS ou mail par exemple, ne sont pas forcément un signe de virus et touchent malheureusement tout le monde

Pour aller plus loin

Virus informatique, que faire ?
cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/virus-informatiques

Quels sont les différents types de piratage informatique ?
cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/quels-sont-les-differents-types-de-piratage-informatique

Se protéger des virus informatiques

Le meilleur antivirus, c'est vous

Le meilleur antivirus est souvent soi-même, car la sécurité informatique dépend en grande partie de ses actions et de ses comportements. La vigilance et l'éducation continue de l'utilisateur en matière de cybersécurité sont des composantes clés pour maintenir un environnement informatique sûr. Éviter donc de cliquer sur des liens ou des pièces jointes suspects dans les emails, de télécharger des logiciels de sources inconnues et méfiez-vous des offres trop alléchantes sur Internet.

Mettre à jour son appareil

Il est important d'installer les mises à jour de vos applications et du logiciel de vos appareils dès qu'elles sont disponibles. Les mises à jour corrigent les failles de sécurité qui empêchent les virus d'infecter le système et apportent des améliorations et de nouvelles fonctionnalités. Si vous recevez une invitation à mettre à jour votre appareil (ou vos applications), ne l'ignorez pas. L'application de ces mises à jour est l'une des choses les plus importantes (et les plus rapides) que vous puissiez faire pour assurer votre sécurité en ligne.

À noter : la mise à jour de votre appareil peut prendre un certain temps et nécessite une connexion internet fiable, il est donc préférable de le faire à la maison où vous pouvez accéder à votre wi-fi (et de laisser votre appareil branché).

En matière de protection, les antivirus en version gratuite sont globalement aussi efficaces que les versions payantes mais ils intègrent moins de services annexes. Les antivirus en version gratuite ont tendance à être très incitants pour acheter leur produit, ce qui peut être pénible. Comme antivirus gratuit, nous recommandons BitDefender Antivirus Free ou Avast One Essential (malgré un mauvais historique sur les données personnelles). Si vous disposez d'un budget, les versions payantes offrent des fonctionnalités utiles et qui sont pertinentes.

Installer un logiciel antivirus

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté. Être vigilant contre les liens douteux

Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

… et contre les messages suspects.

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.

Évitez les sites non sûrs ou illicites.

Comme les sites qui hébergent des contrefaçons (musique, films, logiciels, etc.) ou de nombreux sites pornographiques gratuits.

Pour aller plus loin

Comment se protéger sur Internet ?
cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-se-proteger-sur-internet

Pourquoi est-il dangereux de négliger les mises à jour ?
cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/pourquoi-est-il-dangereux-de-negliger-les-mises-a-jour

Comment choisir son antivirus ?
QueChoisir.org, https://www.quechoisir.org/guide-d-achat-antivirus-n11017/

L'indispensable de l'achat en ligne

Identifier les menaces possibles

En faisant des achats en ligne, vous vous exposez au vol d'identité, au piratage et à des pertes financières. Voici quelques exemples des méthodes auxquelles les auteurs de menace peuvent avoir recours pour voler vos informations sensibles et pirater vos comptes :

- De faux sites marchands recueillent vos renseignements lorsque vous faites un achat que vous croyez réel
- Des sites frauduleux de traitement des paiements collectent votre argent lorsque vous croyez faire une véritable transaction
- Des sites Web non chiffrés exposent vos renseignements à de possibles attaques malveillantes

Identifier la fiabilité d'un site

Quelques indices qui permettent de détecter si un site n'est pas fiable :

- Le site semble mal conçu et/ou peu professionnel.
- Le prix des articles est étonnamment bas ou on vous propose des aubaines qui semblent trop belles pour être vraies.
- Pour un site professionnel, il ne comporte pas les mentions obligatoires avec les informations sur l'identité de l'entreprise, le numéro d'immatriculation au RCS, mail et numéro de téléphone, l'identité de l'hébergeur, etc.). Pour un site marchand, les conditions générales de vente ne sont pas présentes.
- On vous demande de donner les justificatifs d'identité associés à votre carte de crédit pour d'autres raisons que pour faire des achats.
- Les frais d'expédition, les droits de douane et les frais supplémentaires semblent anormaux.

Adopter les bons réflexes

Lorsque vous faites des achats en ligne, vous pouvez vous protéger en adoptant certains réflexes.

Ne suivez pas les liens reçus par mail ou SMS.

Ils pourraient renvoyer vers des faux liens. Consultez directement le site si vous connaissez l'adresse, ou utiliser un moteur de recherche.

N'achetez qu'auprès des sites dans lesquels vous avez confiance.

Le plus sûr est d'utiliser le site internet d'un magasin ou d'une chaîne de magasin ou un site en ligne spécialisé ayant une grande réputation.

Ne pas enregistrer le numéro de sa carte bancaire sur le site internet ou dans votre navigateur

Conserver votre numéro de carte bancaire sur des sites ou dans des navigateurs augmente le risque de fraude et de piratage, car ces données peuvent être volées lors de cyberattaques. Cela peut conduire à des achats non autorisés ou à des abonnements involontaires si d'autres personnes ont accès à votre appareil ou si vous oubliez les renouvellements automatiques.

Vérifier la réputation du professionnel.

Pour vous renseigner et choisir un site de confiance vous pouvez utiliser les moteurs de recherche et taper "le nom du site" avec "avis" ou "forum". Si des clients ont eu des problèmes avec un site, ils pourraient en avoir parlé dans les forums de discussion, dans les avis Google ou sur les réseaux sociaux, ou même sur le site lui-même.

Faire ses achats sur des sites sécurisés

Faites vos achats sur des sites Web dont l'adresse commence uniquement par HTTPS. Assurez-vous que les sites Web affichent un cadenas vert dans la barre d'adresse (un cadenas ouvert ou manquant signifie que les données du site Web ne sont pas sécurisées).

Pour aller plus loin

Les achats en ligne
cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/zoom-sur-les-achats-en-ligne

Le guide des achats en ligne.
Fevad et l'INC, édition 2019. https://www.cybermalveillance.gouv.fr/medias/2020/01/2019_GUIDE_Achats-en-ligne.pdf

Pratiques avancées

La fiche ***Pratiques avancées*** est la dernière d'une série de trois fiches conçus pour aider les français à comprendre les principes de base de la cybersécurité.

Rédacteurs : TelesCoop (Quentin MADURA, Maxime BELLEC)

Mise en forme : TelesCoop (Quentin MADURA)

Coordination

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CONSEILLER NUMÉRIQUE

Pratiques avancées

Utilisez un gestionnaire de mots de passe pour mémoriser vos mots de passe

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. C'est là qu'un gestionnaire de mots de passe peut s'avérer utile : il peut stocker tous vos mots de passe en toute sécurité, de sorte que vous n'ayez pas à vous en souvenir. Cela vous permet d'utiliser des mots de passe uniques et forts pour tous vos comptes importants.

KeePaas

KeePass, un gestionnaire de mots de passe sécurisé et gratuit

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. KeePass dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.

Activer la double authentification

La double authentification, également connue sous le nom de validation en deux étapes ou "2FA", est une mesure de sécurité qui renforce la protection des comptes en exigeant une vérification supplémentaire au-delà du nom d'utilisateur et du mot de passe habituels.

Elle vise à prévenir les tentatives d'accès non autorisées en alertant l'utilisateur lorsqu'une connexion est tentée à partir d'un nouvel appareil.

Comment activer la double authentification ?

Les étapes pour activer la double authentification dépendent des comptes, appareils et des applications : elle peut nécessiter un code provisoire envoyé par SMS, e-mail, une application spécifique, une clé physique ou une reconnaissance biométrique.

Le plus important est de l'activer sur les comptes les plus importants : comptes bancaires et sur vos adresses emails (e.g. Gmail, Outlook, Hotmail, Yahoo!)

Installez un bloqueur de publicités

Les publicités, quel que soit leur format et le site sur lequel elles se trouvent, peuvent cacher des arnaques ou des virus potentiels. Les plugins bloqueurs de publicités pour les navigateurs web permettent de limiter l'exposition à ces publicités potentiellement malveillance. Certains navigateurs offrent déjà des fonctionnalités de ce type, mais l'ajout d'un tel plugin vous assurera un second moyen de protection.

uBlock Origine

uBlock Origin est une extension libre pour les navigateurs Mozilla Firefox, Google Chrome, Opera et Microsoft Edge chargée de filtrer le contenu des pages web afin d'en bloquer certains éléments, en particulier les bannières de publicité. Il est aussi possible de configurer ses propres listes de bloquage DNS pour filtrer certains malveillants, sites adultes, etc.

Pour aller plus loin

Pourquoi et comment bien gérer ses mots de passe ? cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

Comment protéger ses comptes en ligne avec la double authentification ? cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/double-authentification

Pratiques avancées

Créer une sauvegarde régulière de vos appareils

Une sauvegarde est une copie numérique de vos informations. Il peut s'agir de données auxquelles vous accordez une importance particulière ou considérées comme essentielles dans le cadre de vos activités personnelles ou professionnelles (photos, vidéos, documents personnels ou de travail, etc.). La sauvegarde de vos informations est une mesure de précaution qui permet de les récupérer en cas de perte, de vol ou d'endommagement.

Il est recommandé de réaliser des sauvegardes régulières de l'ensemble de vos appareils en ayant au préalable identifié les données que vous estimez importantes. Pensez à en conserver une copie sur un support externe (clé USB ou disque dur externe). Par ailleurs, il existe des services en ligne, appelés « Cloud », qui offrent des fonctionnalités de sauvegarde de données. Ces solutions peuvent être gratuites ou payantes en fonction de la capacité de stockage dont vous avez besoin.

Chiffrer les données de vos appareils

Le cryptage d'un disque complet signifie que l'intégralité du contenu du disque dur de votre ordinateur est crypté et n'est accessible qu'à l'aide d'un mot de passe. Même si votre appareil est protégé par un mot de passe unique et fort, les cybercriminels peuvent toujours accéder au disque dur et voler vos données s'il n'est pas encrypté.

Comment puis-je crypter le disque dur de mon ordinateur ?

La plupart des systèmes d'exploitation les plus récents sont équipés d'une forme de cryptage de disque intégré.

Pour les ordinateurs sous Windows 10 ou 11, suivez les indications suivantes :

- Ouvrez une session Windows avec un **compte d'administrateur**.
- **Paramètres** > **Confidentialité & sécurité** > **Chiffrement de l'appareil**. Ouvrir le chiffrement de l'appareil dans Paramètres.
- Si le Chiffrement de l'appareil est désactivé, sélectionnez **Activez**.

Sur Apple macOS, le chiffrement des disques est connu sous le nom de FileVault. Pour l'activer, suivez les indications suivantes :

- Ouvrez les "Préférences systèmes"
- Puis rendez-vous dans **"Sécurité et confidentialité"** > Onglet "**Firevault**" > Cliquer sur le bouton "**Activer Firevault**"

Lorsqu'il est activé, votre mot de passe de connexion est utilisé pour crypter le disque dur, et tous les nouveaux fichiers créés sont automatiquement cryptés lorsqu'ils sont enregistrés sur votre disque.

Pour aller plus loin

Sauvegarde des données numériques.
cybermalveillance.gouv.fr,
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/sauvegarde-des-donnees-numeriques

Photos, fichiers, messages… : comment protéger ses données numériques grâce aux sauvegardes ?
cybermalveillance.gouv.fr, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/sauvegarde-des-donnees-numeriques