Sécurité informatique

Source : https://www.cybermalveillance.gouv.fr/

Son but : Garder accès à ses biens

- Ses sous
- Ses données numériques
- Son matériel
  - Ordinateur
  - Téléphone

Les risques

- Perte
- Maladresse
- Malveillance

Protégez vos accès avec des mots de passe solides

Mot de passoire

Réseaux sociaux

☞ Cliquer sur la miniature pour voir la vidéo

Protégez vos accès avec des mots de passe solides

La tentation est forte de n'utiliser qu'un ou deux mots de passe souvent faciles à retenir (et donc à deviner) pour l'ensemble de nos comptes.

LES RISQUES

En cas de vol d'un de vos mots de passe, tous les services pour lesquels vous l'utilisez pourraient être piratés. En d'autres termes, vous vous exposeriez alors à une **prise de contrôle de l'ensemble de vos comptes** par un individu malveillant qui pourrait vous dérober des informations personnelles pour en faire un usage frauduleux : **usurpation d'identité, achats ou virements en votre nom, revente de vos données…**

Protégez vos accès avec des mots de passe solides

LES CONSEILS

Pour réduire les risques et éviter un piratage de vos différents comptes en ligne, nous vous recommandons d'utiliser des mots de passe suffisamment longs, **complexes et différents** pour accéder à chacun de vos équipements et services. Au moindre doute, ou même par prévention, n'hésitez pas à **en changer et à activer la double authentification** chaque fois que possible pour renforcer votre sécurité.

Enfin, utilisez un **gestionnaire de mots de passe** pour les stocker de manière sécurisée.

KEEPASS PC et téléphone

Sauvegardez vos données régulièrement

☞ Cliquer sur la miniature pour voir la vidéo

Sauvegardez vos données régulièrement

LES RISQUES

Les appareils numériques (ordinateur, téléphone portable, tablette…) sont soumis à des risques qui peuvent entraîner une perte, parfois irréversible, de vos données. Ces situations sont plus nombreuses que vous ne l'imaginez : il peut s'agir **d'un piratage, d'une panne, d'un vol ou d'une perte, voire de la destruction de votre appareil…** La sauvegarde est alors souvent le seul moyen de retrouver vos données.

Sauvegardez vos données régulièrement

LES CONSEILS

Afin de prévenir de tels risques, Cybermalveillance.gouv.fr vous recommande fortement 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, DVD ou disque dur externe), que vous débranchez une fois la sauvegarde effectuée, pour éviter qu'elle ne soit détruite également en cas de piratage ou d'infection de votre appareil par un virus. Il existe par ailleurs des **services en ligne (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.

Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées

☞ Cliquer sur la miniature pour voir la vidéo

Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées

LES RISQUES

Les appareils numériques et les logiciels que nous utilisons au quotidien sont **exposés à des failles de sécurité**. Ces failles peuvent être utilisées par des cybercriminels comme une **porte d'entrée pour s'introduire dans nos équipements, pour en prendre le contrôle ou bien encore dérober des informations personnelles ou confidentielles** afin d'en faire un usage frauduleux (usurpation d'identité, espionnage, fraude bancaire…). Face à ces risques, les éditeurs et les fabricants proposent régulièrement des mises à jour de sécurité (patch en anglais) qui corrigent ces failles.

Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées

LES CONSEILS

Cybermalveillance.gouv.fr vous recommande **d'accepter les mises à jour de sécurité sur tous vos appareils** (ordinateurs, tablettes, téléphones mobiles, objets connectés…) dès qu'elles sont proposées pour corriger ces failles et ainsi vous protéger. Nous vous conseillons également de **vérifier régulièrement dans les paramètres de vos équipements et logiciels que les mises à jour sont bien appliquées** et d'activer l'option de téléchargement et d'installation automatique des mises à jour, si le logiciel le permet. Enfin, veillez à **télécharger les mises à jour uniquement depuis les sites officiels**, sinon, vous risqueriez de télécharger également un virus.

Vérifiez les sites sur lesquels vous faites des achats

☞ Cliquer sur la miniature pour voir la vidéo

Vérifiez les sites sur lesquels vous faites des achats

LES RISQUES

Les criminels redoublent d'imagination et de savoir-faire pour essayer de vous abuser : messages hameçonnage (phishing) par SMS, mail ou téléphone, fausses annonces promotionnelles (bon de réduction, cadeaux…), faux sites de commerce en ligne ou créés pour les circonstances (fête des mères ou des pères…), faux sites « officiels », faux transporteurs, fausses confirmations de commandes… L'objectif : **vous voler vos données personnelles ou bancaires**, vous inciter à acheter un bien que vous ne recevrez jamais, à rappeler des numéros surtaxés ou à vous abonner à des services payants à votre insu.

Vérifiez les sites sur lesquels vous faites des achats

LES CONSEILS

Choisissez de préférence un site d'achat français ou de l'Union Européenne : la réglementation européenne qui s'applique à tous ces sites en cas de litige vous protégera. Nous vous invitons également **à vérifier la notoriété et l'adresse des sites sur lesquels vous allez faire vos achats** : si c'est votre premier achat sur un site Internet, n'hésitez pas à taper son nom sur un moteur de recherche et à consulter les avis pour vous éviter des déconvenues. De plus, vérifiez bien l'adresse car un seul caractère dans le nom du site peut différer du site officiel. Et lorsque les offres sont trop alléchantes, nous vous conseillons de comparer le prix du produit recherché sur différents sites Internet pour vous assurer du caractère crédible de la vente. Enfin, **privilégiez les moyens de paiement les plus sécurisés** (Paylib, e-Carte Bleue…).

Vérifiez les sites sur lesquels vous faites des achats

APPUI SANTE 28

Point de vigilance

- **Qui envoie le mail :**
  exemple : ameli5273@gmail.com
- **En survolant un lien on peut voir, au bas du navigateur, l'adresse réelle du lien**
  exemple : http://ameli.tm
- **Les fautes d'orthographe**
- **Le caractère urgent et impérieux**

Vérifiez les sites sur lesquels vous faites des achats

APPUI SANTE 28

Si vous avez un doute sur l'authenticité d'un message

Consultez le site de l'organisme sans passer par le lien du message d'alerte.

En entreprise, alertez le support informatique ou la personne référente au sein de l'entreprise

Vérifiez les sites sur lesquels vous faites des achats

Comment réagir

- **Faites opposition immédiatement (en cas d'arnaque bancaire)**
- **Changez vos mots de passe divulgués/compromis**
- **Déposez plainte**
- **Signalez-le sur les sites spécialisés :**

  Signal-spam.fr

  Phishing-initiative.fr

  Info Escroqueries : 0 805 805 817 (gratuit)

Les rançongiciels

Comment réagir

- **Débranchez la machine d'Internet et du réseau local**
- **En entreprise, alertez le support informatique ou la personne référente au sein de l'entreprise**
- **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.html

Maîtrisez vos réseaux sociaux

☞ Cliquer sur la miniature pour voir la vidéo

Maîtrisez vos réseaux sociaux

LES RISQUES

Les réseaux sociaux n'échappent pas aux activités malveillantes : escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation… Les techniques frauduleuses ne manquent pas. **Certaines malveillances ciblent expressément les enfants et les adolescents sur les réseaux sociaux** : les jeux morbides ou dangereux déguisés en challenges, jeu-concours frauduleux, messages privés à caractère pornographique ou incitant à la prostitution…

Maîtrisez vos réseaux sociaux

LES CONSEILS

Pour utiliser les réseaux sociaux en toute sécurité et protéger l'accès à vos comptes, nous vous recommandons d'utiliser à la fois **des mots de passe robustes et systématiquement différents pour chaque service** mais aussi d'**activer la double authentification** lorsque cela est possible. Par ailleurs, nous vous recommandons de **vérifier régulièrement les paramètres de confidentialité de vos comptes** pour définir les options de visibilité de vos publications. Enfin, ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire et bien sûr, **faites attention à qui vous parlez sur les réseaux**.

Séparez vos usages personnels et professionnels

APPUI SANTE 28

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

Évitez les réseaux WiFi publics ou inconnus

☞ Cliquer sur la miniature pour voir la vidéo

Évitez les réseaux WiFi publics ou inconnus

LES RISQUES

S'ils sont pratiques et faciles d'accès, les réseaux wi-fi publics peuvent se révéler dangereux et constituer une véritable aubaine pour les pirates informatiques.

En effet, **les réseaux Wi-Fi publics ne sont pas toujours sécurisés et peuvent être contrôlés ou usurpés par des cybercriminels**. Des pirates pourraient ainsi capturer vos informations personnelles : mots de passe, numéro de carte bancaire par exemple, pour les utiliser à des fins frauduleuses.

Évitez les réseaux WiFi publics ou inconnus

LES CONSEILS

En dehors de votre domicile, **nous vous suggérons de privilégier la connexion de votre abonnement téléphonique** (3G, 4G ou 5G) aux réseaux Wi-Fi publics. Si vous ne pouvez faire autrement, nous vous conseillons de vérifier scrupuleusement le nom du réseau proposé et celui affiché sur votre appareil et de **ne jamais y réaliser d'opérations sensibles** (paiement par CB, consultation de compte bancaire, renseignement d'informations confidentielles…).

Ne branchez pas de clé USB trouvée

Les risques vont de la contamination du PC à sa mort

On peut vacciner sa clé USB : réduire les risques de contamination grâce à un script.

Sécurisation des smatphones

- Téléchargez les applications uniquement sur plateforme reconnue (playstore ou appstore)
- Vérifiez les droits demandés par l'application
- Gardez précieusement le code IMEI de son smartphone pour le bloquer par l'opérateur en cas de vol.

Information pratique :

IMEI est consultable par appel téléphonique au *#06#

Sécurisez la mobilité avec le matériel professionnel

Gardez le matériel avec soi ou sous clé.

Sur les ordinateurs :

- Pas de post-it de mot de passe
- Vérifiez déconnexion compte Google
- N’enregistrez pas les identifiants et mots de passe
- Effacez l’historique de navigation avant mobilité

Cookies

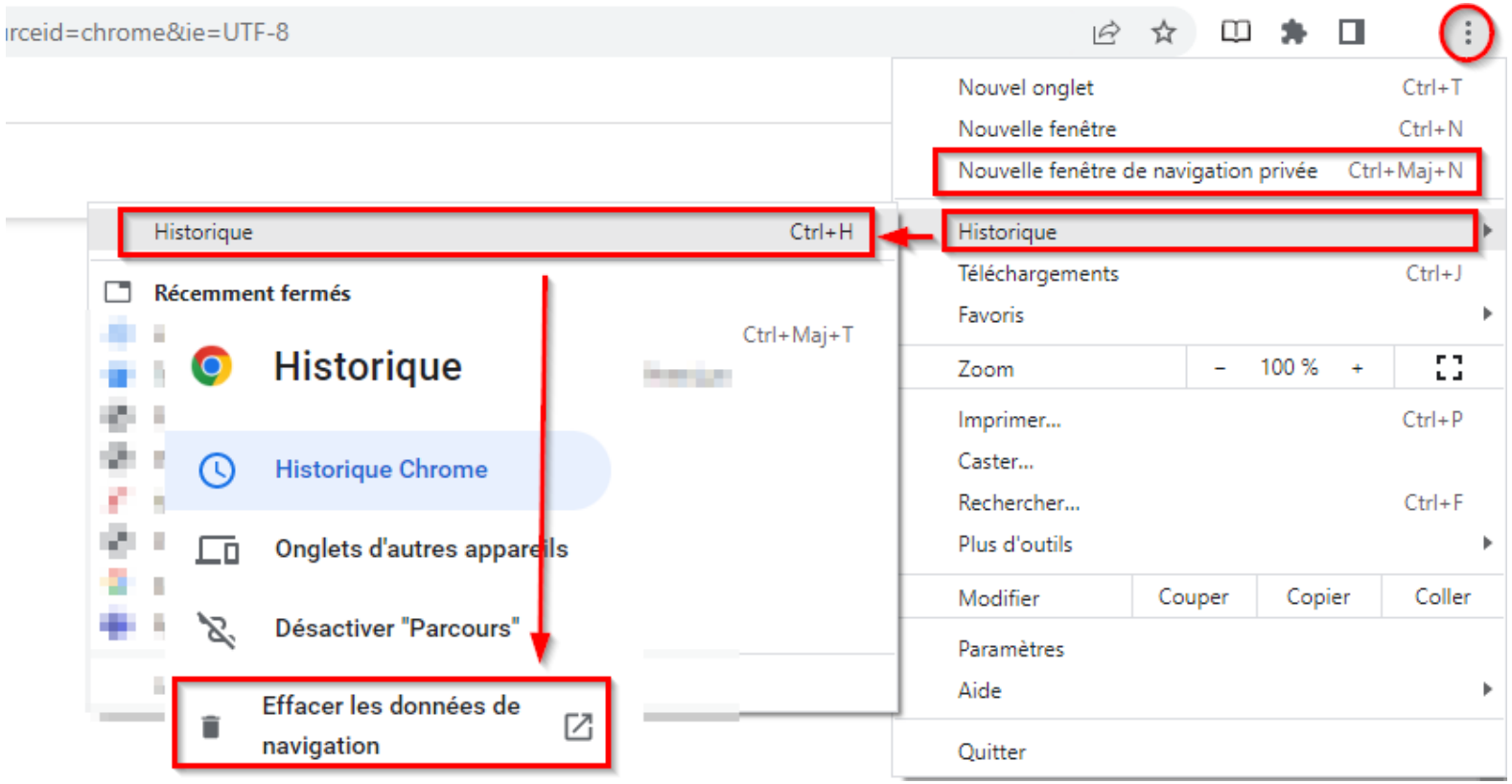
- Vous consultez une page avec cookies
- Le site crée un petit fichier texte sur votre ordinateur
  ex : PHPSESSID=q7c6efuci0uioeq95qn13nbtnq
- La consultation d'une autre page va consulter ce fichier et adapter son contenu pour des raisons :
  - fonctionnelles (ex : est-ce que je suis bien connecté)
  - commerciale (ex : envoi de publicités ciblées)
- Les cookies ne sont pas nocifs mais c'est ce qui en est fait qui peut être dérangeant.

Bonne pratique vis-à-vis des cookies

- Avoir un esprit critique sur le site consulté :
  - SPHERE ne va pas nous envoyer des pub. => c’est ok pour les cookies
  - AMAZON va nous bombarder de pub => on refuse le maximum

Bonne pratique vis-à-vis des cookies et autres traceurs

- Firefox préserve d'avantage la vie privée des utilisateurs
- La navigation privée efface les cookies à la fermeture de la fenêtre.
- La suppression de l'historique



Quizz

J’ai un mot de passe très sécurisé. Je peux donc l’utiliser sur tous mes comptes et services.

Vrai

Faux

Quizz

J’ai un mot de passe très sécurisé. Je peux donc l’utiliser sur tous mes comptes et services.

Vrai

Faux

C’est Faux :
Il vaut mieux utiliser un mot de passe différent et complexe pour chaque accès ou service. En effet, en cas de perte ou de vol d’un de vos mots de passe, vous limitez les risques d’accès frauduleux au seul compte lié à ce mot de passe.

Quizz

Il est inutile de déposer plainte pour un message d’hameçonnage auquel j'ai répondu.

Vrai

Faux

Quizz

Il est inutile de déposer plainte pour un message d’hameçonnage auquel j'ai répondu.

Vrai

Faux

C’est Faux :
Si vous avez malencontreusement communiqué des informations sensibles, comme votre numéro de carte bancaire, déposez plainte au commissariat de police ou à la gendarmerie la plus proche. Les cybercriminels pourraient, en effet, en faire un usage frauduleux. Pour être conseillé en cas d’hameçonnage, contactez le service Info Escroqueries au 0805 805 817 (appel gratuit).

Quizz

Pour sauvegarder mon téléphone, je dois utiliser, de préférence, une application payante.

Vrai

Faux

Quizz

Pour sauvegarder mon téléphone, je dois utiliser, de préférence une application payante.

Vrai

Faux

C’est Faux :
Je peux utiliser un espace cloud gratuit (iCloud, OneDrive ou Google drive) ou transférer directement du téléphone à l’ordinateur par le câble d’alimentation.

LES RÉSEAUX SOCIAUX EN BD

APPUI SANTE 28

FAITES ATTENTION À QUI VOUS PARLEZ

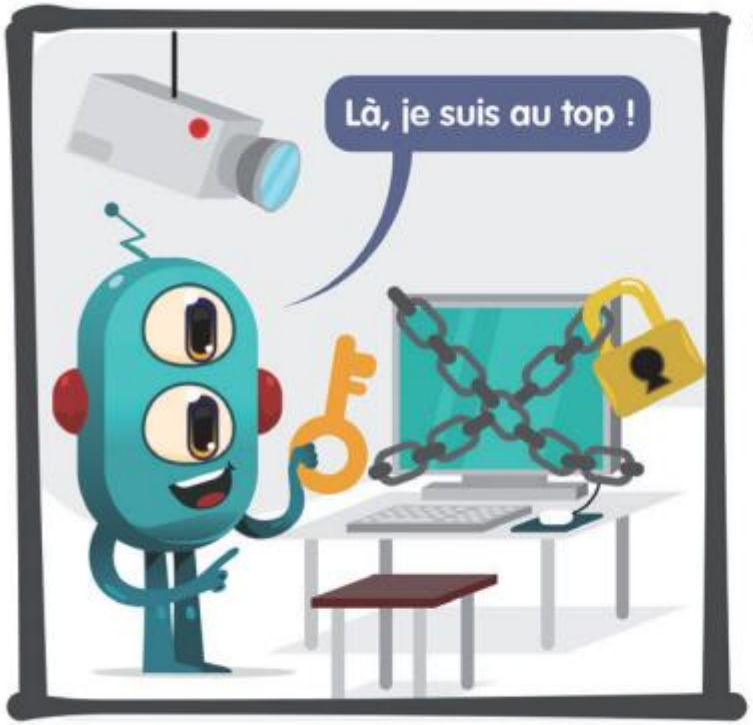
Connaissez-vous l'identité réelle de vos interlocuteurs ?

À leur insu, même vos contacts peuvent vous partager des contenus malveillants.

Méfiez-vous de certaines offres alléchantes, qui peuvent cacher des arnaques

LES RÉSEAUX SOCIAUX EN BD

PROTÉGEZ L'ACCÈS À VOS COMPTES



Pas besoin d'être dans l'excès pour protéger l'accès à vos comptes...

Un conseil : utilisez des mots de passe uniques, différents et robustes.

Lorsque votre service le permet, activez également la double authentification.

LES RÉSEAUX SOCIAUX EN BD

APPUI SANTE 28

MAÎTRISEZ VOS PUBLICATIONS

Avant de publier vos messages, pensez à l'utilisation qui pourrait en être faite.

Ne diffusez pas d'informations personnelles ou sensibles, même à un cercle restreint.

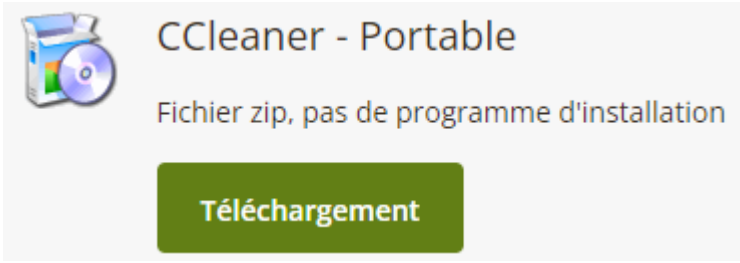
Comme Super Discret, faites attention à ce que vous postez sur les réseaux !

Si mon PC perso rame….

- Désinstallez les logiciels inutiles

- Nettoyez vos historique d’usage

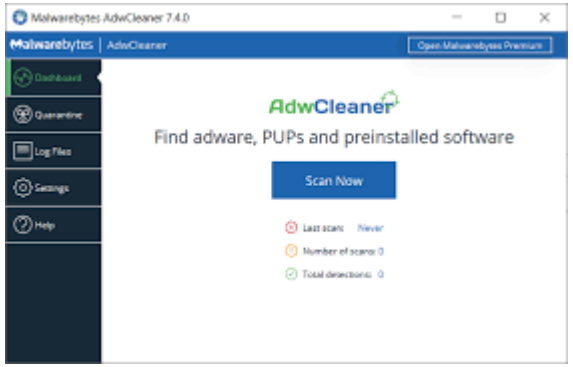
  https://www.ccleaner.com/fr-fr/ccleaner/builds
  Je conseille la version portable
  Tuto : https://youtu.be/-ATpmSOVtLY



- Nettoyez les programmes malveillants

  https://downloads.malwarebytes.com/file/adwcleaner

  Tuto : https://youtu.be/FGgideje-OY



Récupérer des fichiers effacés

Lorsqu'un fichier est effacé, il peut être, parfois, récupéré simplement en installant le logiciel recuva :

https://www.ccleaner.com/recuva/download/standard

Un tuto :
https://youtu.be/wy5_WO8B4s0

Nous vous souhaitons un bon usage de l’informatique en toute sécurité