

Les 10 mesures essentielles pour assurer votre sécurité numérique

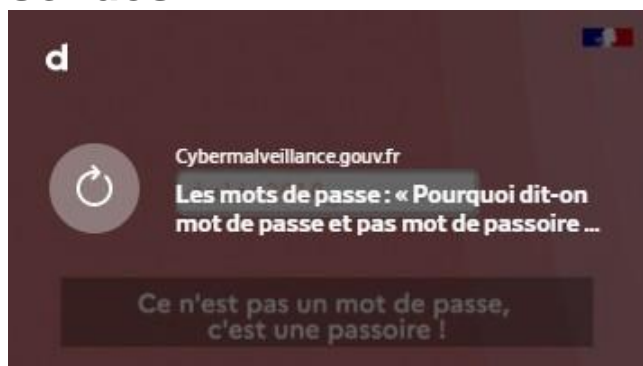
1. [1. PROTÉGEZ VOS ACCÈS AVEC DES MOTS DE PASSE SOLIDES](#)
2. [2. SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT](#)
3. [3. APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS](#)
4. [4. UTILISEZ UN ANTIVIRUS](#)
5. [5. TÉLÉCHARGEZ VOS APPLICATIONS UNIQUEMENT SUR LES SITES OFFICIELS](#)
6. [6. MÉFIEZ-VOUS DES MESSAGES INATTENDUS](#)
7. [7. VÉRIFIEZ LES SITES SUR LESQUELS VOUS FAITES DES ACHATS](#)
8. [8. MAÎTRISEZ VOS RÉSEAUX SOCIAUX](#)
9. [9. SÉPAREZ VOS USAGES PERSONNELS ET PROFESSIONNELS](#)
10. [10. SÉCURITÉ NUMÉRIQUE : ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS](#)

AUTRES FICHES

[Les mots de passe](#), [Les sauvegardes](#), [Les mises à jour](#),

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés... Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques. Comment se protéger au mieux face à ces risques ? Voici 10 bonnes pratiques essentielles à adopter pour assurer votre sécurité numérique.

1. Protégez vos accès avec des mots de passe solides



<https://dai.ly/x7txg0c>

« Pourquoi dit-on mot de passe et pas mot de passoire ? » – Vidéo réalisée en partenariat avec le groupe [France Télévisions](#)

Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est souvent due à des mots de passe trop simples ou réutilisés. Au moindre doute, ou même régulièrement en prévention, changez-les. Utilisez un gestionnaire de mots de passe et activez la double authentification chaque fois que c'est possible pour renforcer votre sécurité ([Voir notre fiche sur les mots de passe](#)).

2. Sécurité numérique : sauvegardez vos données régulièrement



<https://dai.ly/x7txg0b>

« Comment gommer les accidents numériques ? » – Vidéo réalisée en partenariat avec le groupe [France Télévisions](#)

En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages...). Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée ([Voir notre fiche sur les sauvegardes](#)).

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



<https://dai.ly/x7txg0d>

« Comment mettre en échec le piratage ? » – Vidéo réalisée en partenariat avec le groupe [France Télévisions](#)

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner ([Voir notre fiche sur les mises à jour](#)).

4. Utilisez un antivirus



<https://dai.ly/x7np0en>

« Comment sécuriser mes appareils pour qu'ils ne soient pas attaqués par des virus ? » – « La minute Info » réalisée en partenariat avec l'[INC](#).

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.

5. Téléchargez vos applications uniquement sur les sites officiels



<https://dai.ly/x7nwhoa>

« Applications : faut-il accepter toutes les autorisations pour pouvoir les utiliser ? » – « La minute Info » réalisée en partenariat avec l'[INC](#).

N'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater vos équipements. De même, évitez les sites

Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux) qui pourraient également installer un virus sur vos matériels.

6. Sécurité numérique : méfiez-vous des messages inattendus

Mots de passe, sauvegardes, mises à jour.



Les 3 réflexes essentiels
pour votre sécurité numérique.



<https://dai.ly/x7txg0e>

« Comment pêcher un numéro de carte bancaire ? » – Vidéo réalisée en partenariat avec le groupe [France Télévisions](#)

En cas de réception d'un message inattendu ou alarmiste par messagerie (*courriel*), SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par [hameçonnage](#) (*phishing*) visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce-jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.

7. Vérifiez les sites sur lesquels vous faites des achats



<https://dai.ly/x7mzzn4>

« Sécuriser ses achats sur Internet : les bonnes pratiques ! » – Consomag réalisé en partenariat avec l'[INC](#).

Si le commerce en ligne facilite les achats et offre l'opportunité de faire de bonnes affaires, il existe malheureusement de nombreux sites de vente douteux, voire malveillants. Avant d'acheter sur Internet, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site officiel, la crédibilité de l'offre et consultez les avis. Sans cette vérification, vous prenez le risque de vous faire [dérober votre numéro de carte bancaire](#) et de ne jamais recevoir votre commande, voire de recevoir une contrefaçon ou un produit dangereux.

8. Maîtrisez vos réseaux sociaux



<https://dai.ly/x7n00db>

« Comment utiliser les réseaux sociaux en toute sécurité ? » – Consomag réalisé en partenariat avec l'[INC](#).

Les réseaux sociaux sont de formidables outils de communication et d'information collaboratifs. Ils contiennent toutefois souvent de nombreuses informations personnelles qui ne doivent pas tomber dans de mauvaises mains. Sécurisez l'accès à vos réseaux sociaux avec un mot de passe solide et unique, définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire, ne relayez pas d'informations non vérifiées (*fake news*). ([Voir notre fiche sur les réseaux sociaux](#)).

9. Séparez vos usages personnels et professionnels

Avec l'accroissement des usages numériques, la frontière entre utilisation personnelle et professionnelle est souvent ténue. Ces utilisations peuvent même parfois s'imbriquer. Matériels, messageries, « cloud » ... Il est important de séparer vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise, ou inversement, que la compromission de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles. ([Voir notre fiche sur les usages personnels et professionnels](#)).

10. Sécurité numérique : évitez les réseaux WiFi publics ou inconnus



<https://dai.ly/x7nwhg7>

« WiFi public : comment empêcher le vol de mes données ? » – « La minute Info » réalisée en partenariat avec l'[INC](#).

En mobilité, privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) aux réseaux WiFi publics. Ces réseaux WiFi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire...). Si vous n'avez d'autre choix que d'utiliser un WiFi public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).