A+ A-

Comment assurer votre sécurité numérique ?

Par Bercy Infos < https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous> , le 17/10/2022 - Droits et protection sur internet

De nombreuses démarches quotidiennes (achats, réservations, déclarations administratives, etc.) s'effectuent en ligne sur ordinateur, tablette ou téléphone mobile, via les sites internet, messageries et réseaux sociaux. Si dans la plupart des cas ces outils numériques vous facilitent la vie, leur usage peut être détourné par des personnes mal intentionnées afin de pirater vos données. Découvrez nos conseils pour assurer votre sécurité numérique.

Sécurisez votre terminal informatique : mise à jour, verrouillage et sauvegarde

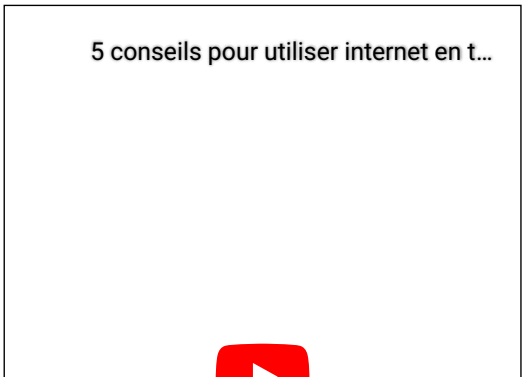
Disposer d'un équipement informatique efficace et mis à jour régulièrement est la première étape importante pour vous protéger d'éventuelles cyberattaques.

Nos conseils :

- **Mettez à jour régulièrement vos équipements** : téléphone portable, tablette, ordinateur portable, etc. Il est important également d'en respecter les conditions d'utilisation et de ne pas y installer de logiciels non autorisés.
- **Utilisez un anti-virus et un pare-feu** : et veillez également à les mettre à jour régulièrement.
- **Sécurisez votre accès au wifi** : configurez votre wifi personnel, a minima avec une clé WEP et idéalement avec une clé WPA 2 qui est plus sécurisée. Pour basculer vers cette dernière, saisissez « 192.168.1.1 » sur la barre d'adresse de votre navigateur Internet ou accédez directement aux paramètres de votre wifi depuis votre compte personnel en ligne auprès de votre fournisseur d'accès. Plus généralement, ne vous connectez pas sur un wifi non sécurisé.
- **Verrouillez l'accès à votre profil utilisateur :** par un code ou mot de passe, afin de protéger vos documents.
- **Sauvegardez régulièrement vos fichiers**.

Nos cinq conseils pour utiliser internet en toute sécurité

Bercy infos vous livre, en vidéo, cinq conseils pour garantir votre sécurité numérique lorsque vous utilisez internet :



Sécurisez vos achats en ligne

Avoir en tête quelques bons réflexes et quelques bonnes pratiques lorsque vous réalisez vos achats en ligne, peut vous éviter de nombreux risques de piratage.

Nos conseils :

- **Il est vivement recommandé de faire vos achats sur un site web disposant d'une sécurité « https »** : en effet, il existe deux types de sites internet. Ceux dont l'adresse commence par « http:// » et ceux dont l'adresse commence par « https:// ». Évitez de faire vos achats sur les sites en « http:// » et ne créez par un compte sur un site lorsque l'url commence par « http:// » car les informations (mot de passe, informations personnelles, informations bancaires ...) peuvent être interceptées par des tiers (attention, cette condition est nécessaire, mais pas suffisante).
- **Ne partagez jamais des informations personnelles (mot de passe, informations bancaires)** : aucun site fiable ne vous demande ce type d'informations.
- **Consultez régulièrement votre compte bancaire en ligne :** afin de vérifier qu'aucune transaction douteuse n'a été réalisée**.**

Sécurisez vos mots de passe

Comptes mail, sites d'e-commerce, services administratifs...de nombreux sites demandent de créer un compte et de le protéger avec un mot de passe et de nombreux internautes utilisent le même mot de passe sur tous les sites afin de ne pas l'oublier. Attention ! Cette pratique est risquée et peut permettre à des pirates d'avoir accès à toutes vos informations pour utiliser votre identité, ou votre compte bancaire.

Nos conseils :

- **Variez les mots de passe et réservez chacun à un usage unique** : la règle d'or est : « **1 compte = 1 mot de passe dédié** ».
- **Utilisez, si nécessaire, des logiciels** qui aident à la gestion des mots de passe.
- **Créez des mots de passe qui remplissent toutes les conditions de sécurité** : à ce titre, vous pouvez consulter nos conseils dédiés sur comment créer un mot de passe sécurisé et simple à retenir.

Les bonnes pratiques pour sécuriser vos mots de passe

Profitez des conseils du **Haut fonctionnaire de défense et de sécurité (HFDS) du ministère de l'Économie** pour sécuriser vos mots de passe :

Utilisez votre messagerie de façon sécurisée

La messagerie électronique permet de communiquer facilement entre particuliers ou avec différents organismes. L'adresse électronique peut être utilisée pour créer un compte auprès d'un site marchand et recevoir des factures et des messages promotionnels. Mais, c'est également par le biais des courriers électroniques que des personnes malveillantes peuvent récupérer des informations confidentielles (codes d'accès, informations bancaires, etc). **Un courriel n'est pas anodin !**

Nos conseils :

- **Lisez attentivement** les informations contenues dans les courriels : interrogez-vous sur la pertinence et la crédibilité du contenu, sur l'identité de l'expéditeur et son langage, etc.
- **Si un courriel vous semble douteux, ne cliquez pas sur les pièces jointes ou sur les liens qu'il contient** : dans tous les cas méfiez-vous des extensions de pièces jointes qui paraissent douteuses (exemples : pif ; .com ; .bat ; .exe ; .vbs ; .lnk...), et qui peuvent contenir des codes malveillants.
- **Ne vous fiez pas aux éléments graphiques des courriels** : en effet de nombreux courriels frauduleux utilisent les logos et chartes graphiques des administrations ou entreprises les plus connues. Voir figurer des logos qui paraissent officiels ne veut pas nécessairement dire qu'il s'agit d'un courriel officiel.

Méfiez-vous des faux sites administratifs

Méfiez-vous des faux sites administratifs. En effet de nombreuses arnaques font tout pour tromper le consommateur et prendre l'apparence d'un site officiel. Généralement ces sites sont souvent des sites commerciaux qui proposent de réaliser pour vous des démarches administratives (demande d'extrait d'acte de naissance, consultation de points sur le permis de conduire, etc.) moyennant rémunération alors que les sites officiels de l'administration proposent les mêmes prestations gratuitement. Si ces types de services peuvent être légaux, soyez vigilant sur les services qu'ils proposent.

Nos conseils :

- **Sachez reconnaitre les faux sites** : les sites officiels de l'administration française se terminent par « .gouv.fr » ou « .fr » et jamais par « .gouv.org » ou « .gouv.com ».
- **Consultez le site service-public.fr** : pour être redirigé vers le site adéquat en fonction de la demande.
- **Ne vous fiez pas aux premiers résultats des moteurs de recherche** : car ils ne correspondent pas toujours aux sites officiels.
- **Vérifiez l'identité du site et ses mentions légales** avant de réaliser le moindre paiement.

Soyez également attentif à vos opérations bancaires !

Faux sites internet de banques, mails frauduleux envoyés soi-disant par votre conseiller bancaire, comptes bancaires piratés...les fraudes aux opérations bancaires sont également répandues.

Et même si les banques ont des systèmes de protection qu'elles renforcent sans cesse, en tant que client de la banque, votre rôle est essentiel pour utiliser vos moyens de paiement et vos services bancaires à distance de manière sécurisée.

Pour connaitre les bons réflexes, consultez le **guide de la Fédération bancaire française sur le site lesclesdelabanque.com < https://www.lesclesdelabanque.com/Web/Cdb/Particuliers/Content.nsf/DocumentsByIDWeb/6WNHMA/$File/Guide-HS-fraudes-remboursement.pdf?v=1666008259>**

Communiquez sur les réseaux sociaux avec précaution

Les réseaux sociaux sont des lieux d'échanges. Mais soyez prudents sur ce que vous communiquez. Les informations diffusées sur la toile s'effacent difficilement. **Donc restez vigilants ! Ne contribuez pas à votre propre piratage.**

Nos conseils :

Assurez de l'identité du demandeur d'informations : à l'instar du **phishing** (hameçonnage), des demandes d'informations personnelles peuvent se faire via les réseaux sociaux, par des interlocuteurs qui peuvent évoquer des situations d'urgence, des demandes de confirmation, etc. Dans ce contexte, il est important de s'assurer de l'identité réelle de son interlocuteur et d'obtenir des informations pour juger de sa vraisemblance et de sa réalité.

En cas d'incident, contactez cybermalveillance.gouv.fr < http://cybermalveillance.gouv.fr>

Nos conseils :

- Si vous êtes victime d'un incident de cybersécuité, connectez-vous sur le site cybermalveillance.gouv.fr < https://www.cybermalveillance.gouv.fr> qui permet d'établir un diagnostic précis de votre situation ainsi qu'une mise en relation avec des spécialistes et organismes compétents proches de chez vous. Le site propose aussi des outils et des publications dispensant de nombreux conseils pratiques.
- Il est possible également de signaler un contenu illicite sur le site internet-signalement.gouv.fr < https://www.internet-signalement.gouv.fr> .

Ces contenus peuvent aussi vous intéresser

Usurpation d'identité, comment s'en protéger ?
Comment se prémunir contre le phishing ?
Dix règles pour vous protéger contre les risques de piratage de votre ordinateur
Achats en ligne : comment vérifier la fiabilité d'un site ?
Comment créer un mot de passe sécurisé et simple à retenir ?
Attention aux faux courriels et appels qui se font passer pour l'administration

En savoir plus sur la cyber sécurité

Sur le portail du HFDS Bercy
Sur le site de l'AFNIC < https://www.afnic.fr/>
Sur le site de la CNIL < https://www.cnil.fr/>

En cas d'incident

Plateforme **cybermalveillance.gouv.fr < https://www.cybermalveillance.gouv.fr/>**

Thématiques : Droits et protection sur internet

Ce sujet vous intéresse ? Chaque mardi avec la lettre Bercy infos Particuliers, ne manquez aucune info pratique sur vos droits et obligations en matière de fiscalité, épargne, consommation ...

exemple : nom.prenom@domaine.com Je m'al

Je consens à ce que mon adresse email soit utilisée afin de recev
de Bercy infos. Consulter notre politique de confidentiali

Partager la page