Les règles pour vous prémunir contre le piratage de vos données personnelles

On vous promet monts et merveilles, des placements à forte rentabilité... mais ces placements proposés sur internet sont toujours très risqués. Avec l'Autorité des marchés financiers, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) surveille ces sites de près.

De nombreuses démarches quotidiennes (achats, réservations, déclarations administratives, etc.) sont désormais réalisables en ligne et s'effectuent 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, 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'adresses 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.

Quelle sécurité pour votre navigateur 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 faire 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 2 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 pas 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

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.

SECURITE NUMERIQUE

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.

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

Nos conseils :

Si vous êtes victime d'un incident de cybersécurité, connectez-vous sur le site 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.

Vous pensez être anonyme sur le web ? Que personne ne trouvera votre mot de passe ? Que votre code wifi vous protège amplement ? Faux ! Si vous souhaitez vous protéger contre les risques de piratage de vos données, voici quelques conseils à suivre !

Créez des mots de passe sécurisés

Utilisez des mots de passe de qualité, sans quoi vous risquez de faciliter l'accès à vos données personnelles. Privilégiez les mots de passe longs, comprenant des majuscules et des minuscules, des chiffres, et des caractères spéciaux. Par exemple : ***Wejd*25ipO%Ram.***
Nombre de pirates disposent en effet de logiciels leur permettant de générer toutes les combinaisons du dictionnaire, voire des formules plus complexes. Des mots de passe tels que « chocolat », votre date d'anniversaire ou le nom de votre mascotte sont donc à proscrire.
Changez votre mot de passe régulièrement et choisissez-en un différent pour chacun de vos comptes. En effet, une fois qu'un hacker (cyberpirate) a trouvé l'un de vos mots de passes, il va essayer d'accéder à vos autres comptes avec celui-ci. Si vous avez reçu un nouveau mot de passe par courriel, n'oubliez pas de vous débarrasser de ce message.

Mettez votre système d'exploitation à jour

Votre système d'exploitation (navigateur, antivirus, bureautique, pare-feu personnel, etc.) doit être à jour.
Les agresseurs profitent en effet des logiciels non mis à jour afin d'utiliser les failles non corrigées par votre système pour s'y introduire. C'est la raison pour laquelle la mise à jour de vos outils est essentielle.

Portez attention à votre clé wifi !

Il existe plusieurs types de clés wifi. La clé WEP est la plus courante, car elle reste habituellement le choix par défaut des fournisseurs d'accès. Mais c'est également la moins sécurisée. Les clés WEP peuvent être décryptées par des pirates en quelques minutes, contre une quinzaine d'heures pour une clé WPA 2.

Pour basculer vers cette dernière, saisissez « 192.168.1.1 » sur la barre d'adresses de votre navigateur internet ou accédez directement aux paramètres de votre wifi depuis votre compte personnel en ligne auprès de votre fournisseur d'accès.

Sauvegardez vos données

Ce conseil ne vous protègera pas d'une attaque malveillante mais pourra au moins en réduire les conséquences. En effet, l'une des meilleures façons de se prémunir contre les pertes de données suite à une attaque, est tout simplement de les sauvegarder assez régulièrement.
Vous pourrez ainsi retrouver vos fichiers si vous ne parvenez plus à y accéder sur votre ordinateur. Un disque dur externe ou une clé USB (que vous débrancherez une fois l'opération de sauvegarde terminée) feront très bien l'affaire.

Méfiez-vous des liens

Ne cliquez pas trop vite sur les liens, même ceux qui vous paraissent familiers. Une des attaques les plus classiques vise à tromper l'internaute en l'incitant à cliquer sur des liens figurant dans un e-mail ou une page web. Ce lien peut-être malveillant.
En cas de doute, abstenez-vous et préférez écrire vous-même l'adresse voulue dans la barre d'adresses de votre navigateur.

Soyez vigilant concernant les pièces jointes dans les courriels

Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles peuvent contenir des codes malveillants. Faites particulièrement attention à celles dont les extensions se terminent par.pif ;.com ;.bat ;.exe ;.vbs ;.lnk : recevez-vous ce type de pièces jointes habituellement ? Par exemple : photosvacances.pif

Ne naviguez pas sur le web depuis votre compte administrateur

L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur. Préférez l'utilisation d'un compte utilisateur, qui vous permet également de naviguer sur le web sans entraves.

Utilisez un antivirus ou un pare-feu

Aucun ordinateur n'est imprenable, mais ne facilitez pas la tâche aux hackers. Mieux vous serez protégé, plus rude et dissuasive sera la tâche pour les personnes malveillantes. En informatique, le pare-feu permet de limiter un certain nombre de connexions entrantes et sortantes. Si malgré tout, le pirate trouve une faille dans votre ordinateur, un antivirus peut l'empêcher de nuire.

Soyez attentif à ce que vous écrivez sur le web !

Il est très important de contrôler la diffusion d'informations personnelles.
Internet est loin d'être ce lieu d'anonymat qu'on imagine.
Évitez de fournir vos coordonnées ou d'autres données sensibles dans les forums, sur des sites n'offrant pas toutes les garanties requises ou même sur les réseaux sociaux.
Un conseil : le symbole https :// au début de l'adresse web et l'image d'un petit cadenas est gage de site web certifié et sécurisé, mais dans le doute, mieux vaut s'abstenir.

Méfiez-vous de tous les expéditeurs, même ceux que vous connaissez

L'envoi de liens malveillants peut-être indépendant de la volonté de leurs expéditeurs, même de ceux que vous connaissez ! Si un correspondant avec lequel vous échangez régulièrement vous adresse par exemple un message dans une langue étrangère, ou que sa manière de s'exprimer est différente, n'ouvrez pas les pièces jointes contenues dans son message et ne cliquez pas sur les liens qui y figurent. En cas de doute, passez-lui un coup de fil !