Union Fédérale des Consommateurs Que Choisir 43
29 Bd Chantemesse, 43000 AIGUILHE
☎ 04 71 02 29 45
Courriel : *ufc.quechoisir43@orange.fr*

Cybersécurité : comment protéger son matériel informatique et ses données personnelles ?

POURQUOI ET COMMENT GERER MES MOTS DE PASSE,

Les mots de passe sont les clés d'accès… à vos messageries, vos profils réseaux sociaux, votre compte bancaire, aux sites de ventes en ligne… Ils sont personnels, confidentiels et indispensables. Plus votre mot de passe est complexe, plus il est difficile de le deviner. Les personnes malveillantes s'attaquent principalement à des comptes faciles à pirater.

Un mot de passe solide est composé de caractères variés :

- ☞ chiffres,
- ☞ lettres,
- ☞ majuscules,
- ☞ minuscules,
- ☞ caractères spéciaux
- ☞ et a une longueur minimum (8 caractères minimum).

C'est le couplage de ces éléments qui rend un mot de passe difficile à trouver.

Lorsque vous utilisez le même mot de passe sur l'ensemble de vos comptes, vous facilitez le travail du pirate puisqu'il lui suffira de trouver votre mot de passe pour se connecter à tous les comptes sur lesquels vous l'utilisez. Il est donc important d'utiliser des mots de passe différents pour tous vos comptes.

Vous pouvez utiliser un gestionnaire de mots de passe pour ne pas avoir à tous les mémoriser.

Ces logiciels, disponibles en version gratuite ou payante, vous permettent de stocker vos mots de passe de façon simple et sécurisée. Certains d'entre eux vous suggèrent d'ailleurs des mots de passe quasiment impossible à trouver. Soyez tout de même vigilant avant d'en choisir un : privilégiez notamment le téléchargement depuis le site officiel de l'application et vérifiez les avis des utilisateurs.

Autres règles élémentaires à respecter : ne jamais communiquer votre mot de passe à un tiers et prendre l'habitude de les changer régulièrement pour renforcer votre sécurité.

Vous trouverez sur le site Cybermalveillance.gouv.fr des conseils complémentaires pour bien gérer vos mots de passe.

Union Fédérale des Consommateurs Que Choisir 43
29 Bd Chantemesse, 43000 AIGUILHE
☎ 04 71 02 29 45
Courriel : *ufc.quechoisir43@orange.fr*

Cybersécurité : comment protéger son matériel informatique et ses données personnelles ?

ESCROQUERIE SUR INTERNET : COMMENT NE PAS SE FAIRE AVOIR ?

Qui n'a jamais reçu dans sa boîte mail ou par SMS, des offres alléchantes indiquant que vous avez gagné une somme d'argent ou que les services des impôts, de la CAF ou de l'assurance-maladie vous doivent un trop perçu ou encore qu'un colis vous attend à la Poste ?

Cette pratique s'appelle le phishing. Le principe du phishing est de vous voler OU de récupérer vos données personnelles sur internet. Des pirates informatiques tentent, en prenant l'identité d'un interlocuteur avec lequel vous avez l'habitude de communiquer, de vous demander des données personnelles : vos numéros de code, votre numéro de carte bancaire… dans l'unique but de vous les voler.

Surfer sur Internet sans être vigilant, c'est comme traverser une rue sans regarder : ça peut faire très mal.

Sur Internet, il faut aussi acquérir les bons gestes réflexes : ne répondez jamais à un courriel qui vous demande vos coordonnées bancaires, identifiant ou mot de passe. Votre banque ou toute autre institution de confiance ne vous les demandera jamais par mel. En cas de doute, contactez directement l'organisme concerné et ce, sans utiliser le lien ou le numéro de téléphone proposé dans le mel et qui peuvent être piégés.

Pour prévenir tout risque d'escroqueries :

- ne jamais communiquer d'informations sensibles par messagerie ou téléphone,
- vérifier l'adresse du site qui s'affiche dans votre navigateur et en cas de doute, contacter l'organisme concerné,
- utiliser des mots de passe complexes et différents sur tous les sites,
- activer la double authentification pour sécuriser vos accès,
- signaler les mails douteux à Signal-spam.fr

Si vous êtes victime d'une escroquerie, déposez plainte au commissariat ou à la gendarmerie la plus proche avec tous les renseignements utiles en votre possession.

Pour être conseillé, vous pouvez appeler Info Escroquerie au 0 805 805 817 ou signaler un contenu illicite sur le site internet-signalement.gouv.fr.

Pour plus d'informations visitez le site Cybermalveillance.gouv.fr

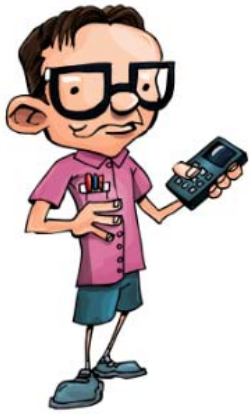
Union Fédérale des Consommateurs Que Choisir 43
29 Bd Chantemesse, 43000 AIGUILHE
☎ 04 71 02 29 45
Courriel : *ufc.quechoisir43@orange.fr*

Cybersécurité : comment protéger son matériel informatique et ses données personnelles ?

POURQUOI FAUT-IL SÉCURISER SON TÉLÉPHONE MOBILE ?

La capacité de stockage des appareils mobiles ne cesse d'augmenter, et le nombre de fonctionnalités disponibles est parfois supérieur à celui des ordinateurs.

Vous stockez sur votre smartphone ou sur votre tablette une multitude d'informations et de données personnelles, voire intimes : mots de passe, contacts, photos privées, fichiers confidentiels, accès à votre boite email, vos comptes de réseaux sociaux, votre compte en banque. Bien que vous ayez certainement le réflexe de sécuriser votre ordinateur, vous attachez souvent moins d'importance à la sécurisation de vos appareils mobiles.



Si vous n'avez pas sécurisé votre smartphone ou votre tablette, faites le immédiatement pour vous préserver des risques en cas de vol ou de perte de votre appareil. En effet, vous vous exposez non seulement à une intrusion dans votre vie privée mais aussi potentiellement à un piratage de vos comptes, et ainsi à toute une série de désagréments, comme par exemple un chantage avec une demande de rançon pour récupérer vos données.

Pour sécuriser votre téléphone mobile :

- ☞ commencez par mettre un code de déverrouillage complexe pour éviter que n'importe qui puisse accéder à votre appareil,
- ☞ acceptez de faire les mises à jour, elles protègent votre appareil en cas de faille de sécurité,
- ☞ faites aussi régulièrement des sauvegardes de vos données.

Si vous téléchargez des applications, faites le uniquement depuis des plateformes officielles (**Apple Store, Play Store, Windows Phone Apps**) et consultez les avis des autres utilisateurs avant d'installer l'application. Les applications provenant de plateformes officielles sont moins susceptibles de contenir un programme malveillant tel qu'un virus.

Vous trouverez sur le site Cybermalveillance.gouv.fr des informations et conseils complémentaires pour sécuriser au mieux votre téléphone.