



Published on *Force Ouvrière Territoriaux* (<https://foterritoriaux.org>)

[Accueil](#) > [Printer-friendly PDF](#) > Sécurité des données : attention au piratage (intégralité de l'article ICI)

Sécurité des données : attention au piratage (intégralité de l'article ICI)

Rançongiciels, vols de mots de passe, faux sites Internet, phishing? Il existe moult moyens pour les pirates de s'emparer de vos données. Se protéger est donc nécessaire

Le phishing ou hameçonnage consiste à faire croire à la victime qu'elle communique avec un tiers de confiance dans le but de lui soutirer des informations (numéro de carte bancaire, mot de passe?)

Pour se protéger : si vous réglez un achat, vérifiez que vous le faites sur un site web sécurisé dont l'adresse commence par « https ». Si un courriel vous semble douteux (par défaut tous doivent l'être, y compris ceux de vos proches?), ne cliquez pas sur les pièces jointes ou sur les liens qu'il contient ! Ne communiquez jamais votre mot de passe. Vérifiez que votre antivirus est à jour pour maximiser la protection de votre ordinateur contre les programmes malveillants.

Gare aux sites non sécurisés

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus. L'objectif du pirate est de chiffrer les données informatiques puis de demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Pour se protéger : tout d'abord effectuez des sauvegardes régulières de vos données et, là encore, n'ouvrez pas les messages dont la provenance ou la forme est douteuse, a fortiori les fichiers exécutables (par exemple : vacances-photos.exe).

Le vol de mot de passe consiste à utiliser des logiciels destinés à tenter un maximum de combinaisons possibles dans le but de trouver les mots de passe des utilisateurs. Le vol de mot de passe peut également se faire en multipliant les essais d'après des informations obtenues, par exemple, sur les réseaux sociaux. Pour se protéger : il ne faut pas utiliser comme mot de passe le nom de vos enfants, de vos mascottes ou d'autres éléments susceptibles de figurer dans vos réseaux sociaux. Construisez des mots de passe compliqués avec des lettres, des majuscules et des caractères spéciaux? N'utilisez pas le même mot de passe partout ! L'usage d'un antivirus et antispyware, régulièrement à jour, peut être utile.

Les logiciels malveillants sont des programmes développés dans le seul but de nuire à un système informatique. Ils peuvent être cachés dans des logiciels de téléchargement gratuits ou dans une clé USB. Pour se protéger : n'installez que des logiciels provenant de sources fiables et méfiez-vous particulièrement de ceux proposés à titre gratuit.

Des faux sites (boutiques en ligne, sites web administratifs?) peuvent être des copies parfaites de l'original. Leur but : récupérer vos données de paiement ou mots de passe. Encore une fois, ne saisissez pas vos données de paiement ou mots de passe sur des sites web non sécurisés, c'est-à-dire ne commençant pas par « https ».

Attention également aux connexions wifi ouvertes dans les lieux publics. Certains de ces réseaux sont piégés et destinés à voler vos informations.

Pour se protéger : vérifiez l'originalité du réseau et au besoin demandez confirmation à l'un des responsables du réseau ouvert (bibliothécaire, responsable du café?). Si vous devez créer un mot de passe dédié, n'utilisez pas le mot de passe d'un de vos comptes. Ne vous connectez jamais à des sites web bancaires ou importants (boîte de

réception, documents personnels stockés en ligne?) via l'un de ces réseaux. N'achetez jamais en ligne via ces derniers non plus, attendez d'être sur un réseau fiable pour le faire. Enfin, n'installez jamais de mise à jour prétendument obligatoire à partir de l'un de ces réseaux.

6 janvier 2020

AFOC

Date:

Mardi, 7 Janvier, 2020

Rubrique:

- [Afoc](#) ^[1]



Fédération FORCE OUVRIERE
des Personnels des Services Publics
et des Services de Santé
153,155, rue de Rome 75017 PARIS
Tél. 01 44 01 06 00

- [Contact](#)
- [Infos légales](#)
- [Politique de confidentialité](#)

Source URL: <https://foterritoriaux.org/securite-des-donnees-attention-au-piratage-integralite-de-larticle-ici>

..

Links

[1] <https://foterritoriaux.org/confederation-international/afoc>