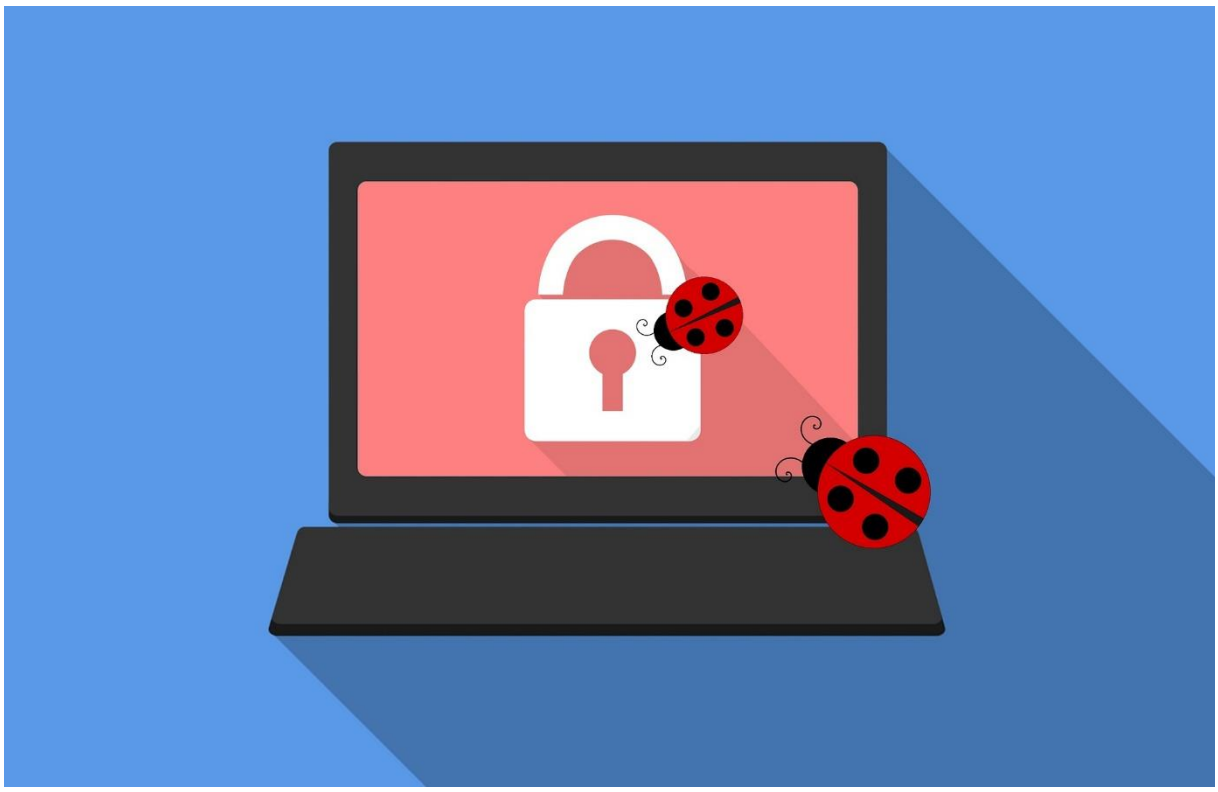
Sécurité en ligne



ATHANOR
CENTRE CULTUREL

Ville de
Guérande

www.mediatheque.ville-guerande.fr

Logiciels malveillants

Un **logiciel malveillant** est un logiciel qui s'installe sur votre ordinateur à votre insu et en perturbe le fonctionnement normal. Il s'agit d'une grande famille qui regroupe de nombreuses catégories :

- Les **rançongiciels** prennent en otage les données stockées sur votre ordinateur en réclamant une rançon,
- Les **chevaux de Troie** rentrent dans votre ordinateur par des moyens détournés, notamment les pièces jointes infectées,
- Les **logiciels espions** vont transmettre les informations que vous saisissez sur votre ordinateur aux malfaiteurs,
- Les **logiciels indésirables,** moins nocifs, mais qui peuvent remplacer certaines fonctions de votre ordinateur sans votre accord et ralentir son fonctionnement.

Un **logiciel antivirus** surveille les allées et venues sur votre ordinateur et compare les fichiers en transit à une base de registre de logiciels malveillants. Lorsqu'un fichier est identifié comme une menace, l'antivirus va mettre celui-ci en quarantaine et l'empêcher de nuire.

Cyril Brosset, *UFC-Que Choisir*, **« Comment choisir son antivirus ? »**, https://www.quechoisir.org/guide-d-achat-antivirus-n11017/#peut-on-faire-confiance-aux-antivirus-gratuits

Depuis Windows 10, le système d'exploitation Windows intègre un logiciel antivirus, **Windows Defender**, d'une qualité similaire à la concurrence. Il reste possible de le remplacer par un autre antivirus. La plupart des entreprises développant des logiciels antivirus proposent une version gratuite de leur produit, qui proposent une protection équivalente, quelques services supplémentaires en moins. **AdwCleaner** est un logiciel utilitaire qui permet de réaliser une analyse de sécurité ponctuelle de son ordinateur.

Pour vous protéger des logiciels malveillants :

- Suivez les **mises à jour** de votre système d'exploitation, de votre antivirus et de votre navigateur web,
- N'ouvrez pas les **pièces jointes** de messages suspects ou venant d'expéditeurs inconnus,
- Téléchargez les logiciels **uniquement depuis leur site officiel** et évitez les versions piratées ou redistribuées,
- Réalisez une **sauvegarde** de vos données sur un support de stockage distinct,
- **Ne cédez pas aux menaces ou pressions**, qu'il s'agisse de rançons ou d'achats.

Il n'est pas nécessaire d'installer un logiciel antivirus sur votre tablette ou smartphone : les systèmes d'exploitation **iOS** et **Android** ont des architectures différentes de Windows, qui sont plus axées sur la sécurité. L'installation d'applications depuis les magasins officiels, l'App Store et le Play Store, permettent également de filtrer les logiciels malveillants. Il reste néanmoins important de rester vigilant et de ne pas cliquer sur n'importe quoi.

Hameçonnage

L'**hameçonnage**, ou **phishing**, est une technique visant à soutirer des informations personnelles en se faisant passer pour un interlocuteur de confiance : entreprise,

magasin, organisme public… Un mail vous avertit d'une urgence (promotion choc, problème de sécurité grave, irrégularité à corriger) et vous renvoie vers un formulaire à compléter. Les données renseignées sont ensuite exploitées à votre insu.

Un minimum de circonspection permet de défaire les tentatives d'hameçonnage, qui misent sur le sentiment d'urgence. Prenez le temps de vérifier si :

Votre mot de passe peut être compromis par une tentative d'hameçonnage. Il est préférable de ne pas utiliser le même mot de passe sur plusieurs sites, afin d'éviter qu'une erreur ne mette en danger l'ensemble de vos comptes.

De nombreux sites web et l'ensemble des banques proposent aujourd'hui des systèmes d'**authentification double facteur** ou **double authentification**. Lors d'une connexion ou d'une transaction, vous devrez valider toute transaction en ligne par le biais d'une application mobile ou avec un code reçu par SMS. Ce dispositif rend l'utilisation des données personnelles volées beaucoup plus difficile, mais n'exclut pas de changer de mot de passe en cas de tentative d'hameçonnage réussie.

Être victime d'un mail frauduleux n'est ni une honte ni une fatalité. En cas d'hameçonnage, faites immédiatement opposition à votre carte bancaire, changez votre mot de passe sur le site web hameçonné et tous les autres sites où vous l'utilisez. Conservez les preuves et portez plainte en commissariat de police. Vous pouvez également vous rendre en agence bancaire pour demander le remboursement d'un paiement non autorisé, soumis à l'approbation de la banque.

Fuites de données

Sites web et services en ligne collectent des données personnelles, à l'inscription et à l'utilisation : adresse mail, mot de passe, statistiques d'utilisation, informations enregistrées… Ces informations sont stockées dans des **bases de données**, des entrepôts d'informations normalement protégées contre les intrusions.

Néanmoins, certaines entreprises peuvent être plus ou moins diligentes quant à la protection de leurs bases de données. Il peut arriver que ces bases soient pénétrées par

des malfaiteurs, qui collectent l'ensemble des données pour les employer à des fins illicites ou les revendre à d'autres malfaiteurs : il s'agit là d'une **fuite de données**.

Troy Hunt, ***haveibeenpwnd***, https://haveibeenpwned.com/

Une fuite de données est plus ou moins grave selon le site ou service affecté. Dans la plupart des cas, l'adresse mail des clients ou utilisateurs est utilisée dans des campagnes de spam et d'hameçonnage. Le site web anglophone **haveibeenpwnd.com** vous permet de savoir si votre adresse mail a été compromise par une fuite de données.

Afin de réduire l'impact potentiel d'une fuite de données, **ne communiquez que le strict nécessaire** aux divers sites web et services en ligne, ne communiquez pas de documents importants de manière inconsidérée, et n'enregistrez pas vos coordonnées de carte bancaire lors d'achats en ligne.

Pour aller plus loin

GIP Acyma, *cybermalveillance.gouv.fr*, **« Virus informatique, que faire ? »**, 2021, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/virus-informatiques

GIP Acyma, *cybermalveillance.gouv.fr*, **« Que faire en cas de phishing ou hameçonnage ? »**, 2020, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

GIP Acyma, *cybermalveillance.gouv.fr*, **« Comment réagir en cas de fuite ou violation de données personnelles ? »**, 2022, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-fuite-de-donnees-personnelles

GIP Acyma, *cybermalveillance.gouv.fr*, **« Comment sécuriser ses achats sur Internet ? »**, 2023, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-securiser-ses-achats-sur-internet

Date de dernière mise à jour : avril 2023