BERCY INFOS ENTREPRISES

Sécurité de vos données : les méthodes de piratage les plus courantes

par Bercy Infos, le 22/02/2019 – **Cybersécurité**

Phishing, rançongiciels, vols de mots de passe, logiciels malveillants, faux sites internet, faux réseaux wifi… Les pirates ne manquent pas d'imagination pour tenter de s'en prendre à vos données.

© Fotolia

Le phishing

Le phishing, qu'est-ce que c'est ?

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 personnelles telles que son numéro de carte bancaire ou son mot de passe

Comment vous protéger contre le phishing ?

Trois conseils pour vous protéger contre le phishing

- Si vous réglez un achat, vérifiez que vous le faites sur un site web sécurisé dont l'adresse commence par « http**s** ».
- Si un courriel vous semble douteux, ne cliquez pas sur les pièces jointes ou sur les liens qu'il contient ! Connectez-vous en saisissant l'adresse officielle dans la barre d'adresse de votre navigateur.
- Ne communiquez jamais votre mot de passe. Aucun site web fiable ne vous le redemandera !
- Vérifiez que votre antivirus est à jour pour maximiser sa protection contre les programmes malveillants.

Réseaux sociaux

Les pirates peuvent parfois se servir des informations publiques diffusées sur les réseaux sociaux pour réaliser un phishing ciblé. Restez vigilant et vérifiez les paramètres de vos comptes !

Lire aussi : Comment se prémunir contre le phishing ? | Sécurité de vos données : qu'est-ce que l'attaque par hameçonnage ciblé (spearphishing) ?

Le rançongiciel

Qu'est-ce qu'un rançongiciel ?

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Wannacrypt, Jaff, Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Comment vous protéger contre un rançongiciel ?

Trois conseils pour vous protéger contre un rançongiciel :

- Effectuez des sauvegardes régulières de vos données.
- N'ouvrez pas les messages dont la provenance ou la forme est douteuse.
- Apprenez à identifier les extensions douteuses des fichiers : si elles ne correspondent pas à ce que vous avez l'habitude d'ouvrir, ne cliquez pas ! Exemple : Vacances_photos.**exe**

Lire aussi : Cinq conseils pour se prémunir contre les « rançongiciels » (ransomware)

Le vol de mot de passe

Le vol de mot de passe, qu'est-ce que c'est ?

Le vol de mot de passe consiste à utiliser des logiciels destinés à tenter un maximum de combinaisons possibles dans le but de trouver votre mot de passe. 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.

Comment vous protéger contre un vol de mot de passe ?

Quatre conseils pour vous protéger contre le vol de mot de passe :

- N'utilisez pas le nom de vos enfants, de vos mascottes ou d'autres éléments susceptibles de figurer dans vos réseaux sociaux comme mot de passe.
- Construisez des mots de passe compliqués : utilisez des lettres, des majuscules et des caractères spéciaux.
- N'utilisez pas le même mot de passe partout !
- Procurez-vous un anti-virus et anti-spyware et mettez-le régulièrement à jour

Lire aussi : Comment créer un mot de passe sécurisé et simple à retenir ?

Les logiciels malveillants

Un logiciel malveillant, qu'est-ce que c'est ?

Il s'agit d'un programme développé dans le seul but de nuire à un système informatique. Il peut être caché dans des logiciels de téléchargement gratuits ou dans une clé USB.

Comment vous protéger contre un logiciel malveillant ?

Deux conseils pour vous protéger contre un logiciel malveillant :

- N'installez que des logiciels provenant de sources fiables ! Si un logiciel normalement payant vous est proposé à titre gratuit, redoublez de vigilance. Préférez les sources officielles !
- Ne connectez pas une clé USB trouvée par hasard, elle est peut être piégée !

Lire aussi : Comment lutter contre les spams ?

Les faux sites internet

Un faux site internet, qu'est-ce que c'est ?

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.

Comment vous protéger contre un faux site internet ?

Encore une fois, ne saisissez pas vos données de paiement ou mots de passe dans des sites web non sécurisés, c'est-à-dire ne commençant pas par « https ».

Lire aussi : Sécurité sur le web : découvrez le site web cybermalveillance.gouv.fr

Le faux réseau wifi

Un faux réseau wifi, qu'est-ce que c'est ?

Lorsque vous êtes dans un lieu public, une multitude de connexions wifi ouvertes peuvent apparaître. Méfiez-vous, certains de ces réseaux sont piégés et destinés à voler vos informations.

Comment vous protéger contre un faux réseau wifi ?

Quatre conseils pour vous protéger contre un faux réseau wifi :

- Assurez-vous de l'originalité du réseau concerné. Si possible, demandez confirmation à l'un des responsables du réseau ouvert (Exemple : le bibliothécaire, le responsable d'un 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 quelque chose en ligne via ces derniers non plus. Attendez d'être sur un réseau fiable pour ce faire.
- N'installez jamais de mise à jour soi-disant obligatoire à partir de l'un de ces réseaux.

La clé USB piégée

Une clé USB piégée, qu'est-ce que c'est ?

Si vous avez trouvé une clé USB, abstenez-vous de la connecter à votre ordinateur ! Celle-ci peut avoir été abandonnée dans le seul but de voler ou de **chiffrer vos données contre rançon.**

Comment vous protéger contre une clé USB piégée ?

En évitant tout simplement de la connecter à votre ordinateur. Rapportez-la plutôt au service des objets perdus de l'établissement dans lequel vous vous trouvez ou de votre ville.

La Hack Academy

La Hack Academy présente, avec humour, les cyber-risques auxquels s'exposent quotidiennement les internautes. Vous pourrez ainsi

Cette initiative est soutenue par l'**Agence nationale de la sécurité des systèmes d'information** (ANSSI) et le ministère de l'Intérieur.

Publié initialement le 19/05/2017

Aller plus loin

ANSSI

- Alerte, campagne de rançongiciel
- Les cinq dernières alertes du CERT-FR