A+ A-

Sécurité de vos données : quelles sont les méthodes de piratage les plus courantes ?

Par Bercy Infos < https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous> , le 25/01/2022 - Sécurité numérique

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 professionnelles. On fait le point sur différentes méthodes de piratage et on vous explique comment vous en protéger.

Tour d'horizon des 6 méthodes de piratage les plus courantes

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.

Le plus fréquemment, le phishing est réalisé par le biais de **faux sites internet** (boutiques en ligne, sites web administratifs…). Ils peuvent être des copies parfaites de l'original.

Dans quel but ? **Récupérer des données de paiement ou mots de passe** qui peuvent nuire à vos salariés et à votre entreprise.

Comment vous protéger contre le phishing ?

Afin de vous protéger du phishing, en tant qu'entreprise vous pouvez rappeler à vos employés **quatre pratiques à respecter** :

- Si vous réglez un achat, vérifiez que vous le faites sur un **site web sécurisé dont l'adresse commence par « https »** (attention, cette condition est nécessaire, mais pas suffisante).
- 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 demandera !
- **Vérifiez que votre antivirus est à jour** pour maximiser sa protection contre les programmes malveillants.

Pensez à vous protéger sur les 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 des comptes de votre entreprise !

Le rançongiciel

Qu'est-ce qu'un rançongiciel ?

Les rançongiciels (ou ransomware) sont des **programmes informatiques malveillants** de plus en plus répandus.

Avec quel 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 ?

En tant qu'entreprise, appliquez les conseils suivants, et relayez les à vos salariés :

- **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 !

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.

Dans quel but ? **Récupérer des données**, personnelles comme professionnelles mais aussi **usurper votre identité** ou celle de votre entreprise.

Comment vous protéger contre un vol de mot de passe ?

Là aussi, il peut être utile de rappeler les bonnes pratiques à vos salariés. Pour se prémunir du vol de mot de passe, voici **quatre réflexes à s'approprier** :

- **Utilisez un mot de passe anonyme !** Aussi, évitez d'avoir recours aux noms de vos enfants, de vos mascottes ou d'autres informations susceptibles de figurer sur vos réseaux sociaux pour composer votre 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 !**
- Enfin, pensez à **changer régulièrement votre mot de passe**.

Les logiciels malveillants

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

Le **logiciel malveillant** ou **malware** est 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.

Avec quel objectif ? **Accéder à votre réseau professionnel** pour **dérober des informations sensibles.**

Comment vous protéger contre un logiciel malveillant ?

Afin de vous protéger des logiciels malveillants, voici **deux pratiques à suivre** :

- **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 (voir le détail dans le dernier paragraphe de cet article) !

Le faux réseau wifi

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

Dans un lieu public, à domicile, ou même en entreprise, une multitude de **connexions wifi ouvertes** provenant de l'extérieur peuvent apparaître. Attention, certains de ces réseaux sont **piégés**.

Dans quel but ? **Récupérer des données sensibles** dont le vol pourra nuire à vos salariés et à votre entreprise.

Comment vous protéger contre un faux réseau wifi ?

Avec l'essor du télétravail, notamment, beaucoup d'employés se connectent désormais à des réseaux wifi dans le cadre de leur activité professionnelle. Afin de se prémunir des faux réseaux wifi, voici **quatre règles à mettre en pratique et à leur rappeler** :

- **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, etc.).
- Si vous devez créer un mot de passe dédié, **n'utilisez pas le mot de passe d'un de vos comptes existants**.
- **Ne vous connectez jamais à des sites bancaires ou sensibles** (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 ?

Lorsque l'on trouve une clé USB, il faut s'abstenir de la connecter à son ordinateur ! Celle-ci peut avoir été abandonnée dans un objectif malveillant.

Avec quel objectif ? **Voler ou chiffrer les données contre rançon.**

Comment vous protéger contre une clé USB piégée ?

Comme pour tous les autres conseils de cet article, en tant qu'entreprise il peut être utile de rappeler la règle d'or suivante à vos salariés : **évitez de la connecter à votre ordinateur** ! Rapportez-la plutôt au service des objets perdus de l'établissement dans lequel vous vous trouvez.

Ces contenus peuvent aussi vous intéresser

Comment se prémunir contre le phishing ?
Comme se prémunir contre les rançongiciels ?
Comment créer un mot de passe sécurisé et simple à retenir ?
Comment lutter contre les spams ?
Sécurité sur le web : découvrez le site web cybermalveillance.gouv.fr

En savoir plus sur les méthodes de piratage

Consultez **La cybersécurité pour les TPE/PME en douze questions** [PDF - 571,5 Ko] le guide développé par l'**Agence nationale de la sécurité des systèmes d'information (ANSSI) < https://www.ssi.gouv.fr/>** en partenariat avec la **Direction générale des entreprises (DGE) < https://www.entreprises.gouv.fr/fr>** , afin d'assurer la sécurité de votre entreprise

Thématiques : **Sécurité numérique**