A

A

Sécurité de vos données : comment vous protéger des méthodes de piratage ?

<

LECTURE : 6 MINUTES

Par **Bercy Infos** , le 06/09/2023 - **Sécurité numérique**

Phishing, rançongiciels, vols de mots de passe, logiciels malveillants, faux sites Internet, faux réseaux Wi-Fi, etc., 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

L'hameçonnage ou *phishing*

Qu'est-ce que l'hameçonnage ou *phishing* ?

L'hameçonnage, ou *phishing* en anglais, 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, etc.). 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, voici **quatre pratiques à respecter** :

1. 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).

2. **Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles** (ex : mot de passe, code confidentiel et numéro de carte bancaire). Aucun site web fiable ne vous le demandera.
3. 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.
4. **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 hameçonnage ciblé. Restez vigilant et vérifiez les paramètres des comptes de votre entreprise.

Le rançongiciel

Qu'est-ce qu'un rançongiciel ?

Les rançongiciels , ou *ransomware* en anglais, sont des **programmes informatiques malveillants** de plus en plus répandus. Il s'agit de mettre l'ordinateur ou le système d'information de la victime hors d'état de fonctionner de manière réversible en chiffrant les données.

Avec quel objectif ? **Demander au propriétaire d'[illegible]yer de l'argent en échange de la clé qui permettra de les déchiffrer**.

Comment vous protéger contre un rançongici[illegible]

En tant qu'entreprise, appliquez les conseils suivants :

- **effectuez des sauvegardes régulières** de vos données,
- **maintenez à jour** vos logiciels et systèmes,
- **utiliser et maintenez à jour** les logiciels antivirus,
- **cloisonnez** le système d'information,
- **limitez les droits** des utilisateurs et les autorisations des applications,
- **maitrisez** les accès Internet,
- **mettez en œuvre une supervision** des incidents de sécurité informatique,
- **évaluez l'opportunité de souscrire** à une assurance cyber,
- **mettez en œuvre un plan** de réponse aux cyberattaques,
- **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.
- **sensibilisez** vos collaborateurs.

Plus sur le rançongiciel et comment s'en protéger

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 **cinq réflexes à s'approprier** :

- **Utilisez un mot de passe anonyme**

Ainsi, 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**

Les mots de passe doivent être longs, complexes avec majuscules, minuscules, chiffres et caractères spéciaux (*% ! etc). Ils peuvent prendre la forme d'une phrase de passe. Plus longue qu'un mot de passe et plus facile à retenir, elle augmentera considérablement la robustesse des accès. Faire appel à un coffre-fort de mots de passe est également une solution recommandée.

- **N'utilisez pas le même mot de passe partout**

Recycler un mot de passe sur plusieurs sites ou [illegible]tions peut s'avérer très dangereux ! Certains sites sont faciles à pirater et des données personnelles pourraient être r[illegible]

Il est donc conseillé d'utiliser un mot de passe unique pour chaque compte, en particulier pour les comptes les plus sensibles : adresses mails et usages professionnels.

- **Pensez à changer régulièrement votre mot de passe**

De nombreuses cyberattaques réussissent à atteindre leur cible en se basant sur un mot de passe par défaut, toujours très simple, qui n'a pas été changé. Il est recommandé de changer ses mots de passe par défaut dès que possible.

- **Ne communiquez pas vos mots de passe**

Transmettre un mot de passe à des collègues ou l'inscrire sur un post-it crée un risque important qu'il soit intercepté par un attaquant. Il est conseillé de ne jamais partager ses mots de passe.

Vous souhaitez tester la solidité d'un mot de passe ?

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) vous le propose depuis **son site Internet** .

Vous pouvez également **en générer un** grâce à la Commission nationale de l'informatique et des libertés (CNIL)

Les logiciels malveillants

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

Le logiciel malveillant, ou *malware* en anglais, 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 Wi-Fi

Un faux réseau Wi-Fi, qu'est-ce que c'est

Dans un lieu public, **à l'étranger < https://www.economie.gouv.fr/entreprises/protection-donnees-a-l-etranger>** , à domicile, ou même en entreprise, une multitude de **connexions Wi-Fi 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 Wi-Fi ?

Avec l'essor du télétravail, notamment, beaucoup d'employés se connectent désormais à des réseaux Wi-Fi dans le cadre de leur activité professionnelle. Afin de se prémunir des faux réseaux Wi-Fi, 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 sur 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**.

<

En savoir plus

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, à savoir, **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 ? < https://www.economie.gouv.fr/particuliers/phishing-hameconnage-filoutage>
- Comme se prémunir contre les rançongiciels ? < https://www.economie.gouv.fr/entreprises/rancongiciels-ransomware-protection>
- Comment créer un mot de passe sécurisé et simple à retenir ? < https://www.economie.gouv.fr/particuliers/creer-mot-passe-securise>
- Comment lutter contre les spams ? < https://www.economie.gouv.fr/entreprises/comment-lutter-contre-spams>
- Entreprises : comment protéger vos données sensibles lors de déplacements à l'étranger ? < https://www.economie.gouv.fr/entreprises/protection-donnees-a-l-etranger>

En savoir plus sur les méthodes de piratage

- La cybersécurité pour les TPE/PME en dou ns < https://www.economie.gouv.fr/files/files/2(uidetpepme.pdf?v=1666168542> [PDF - 571,5 Ko] <
- Attaques par rançongiciels, tous concernés : comment les anticiper et réagir en cas d'incident [PDF – 962 Ko] <
- Guide des bonnes pratiques de l'informatique [PDF – 853 Ko] <
- Recommandations de sécurité relatives aux réseaux Wi-Fi [PDF – 861 Ko] <
- Catalogue des guides et notes techniques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) [PDF - 2,71 Mo]

Thématiques : Sécurité numérique

Ce sujet vous intéresse ? Chaque jeudi avec la lettre Bercy infos Entreprises, recevez les toutes les dernières actus fiscales, comptables RH et financières… utiles à la gestion de votre activité.