A

A

Sécurité de vos données : qu'est-ce que l'attaque par hameçonnage ciblé (spearphishing) ?

LECTURE : 3 MINUTES

Par **Bercy Infos** , le 15/09/2023 - **Sécurité numérique**

Entreprises, vous connaissez peut-être le hameçonnage ou « phishing », en anglais, mais connaissez-vous le hameçonnage ciblé ou « spearphishing » ? Cette méthode de piratage consiste à usurper l'identité d'un de vos contacts pour vous piéger. Le point sur cette pratique et nos conseils pour ne pas vous faire piéger.

Qu'est-ce que le spearphishing ?

L'**Agence nationale de la sécurité des systèmes d'information (ANSSI)** définit le **hameçonnage ciblé** ou ***spearphishing*** comme une **méthode de piratage** qui « repose généralement sur une **usurpation de l'identité** de l'expéditeur, et procède par **ingénierie sociale** forte afin de lier l'**objet du co** le **corps du message** à l'**activité de la personne** ou de l'**organisation ciblée** ».

En d'autres termes, contrairement aux classiques tentatives de **hameçonnage (ou *phishing*)** <https://www.economie.gouv.fr/particuliers/phishing-hameconnage-filoutage>, le pirate tente de se faire passer pour une personne, une société ou un établissement avec lequel vous avez l'habitude de travailler pour vous faire baisser votre garde et vous pousser à **ouvrir une pièce jointe corrompue** ou un **lien vers un site Web malveillant**.

Quels sont les risques si mon ordinateur est infecté ?

> Une fois le premier poste de travail contaminé, l'attaquant prend secrètement le contrôle de ce poste (phase d'infiltration) pour tenter d'obtenir les droits d'administrateur et renforcer son assise sur l'ensemble du réseau de votre entreprise (phase dite « escalade des privilèges »). Le but étant d'**accéder aux informations convoitées**.

Pour agir sans se faire détecter, **l'usurpateur profite des périodes de moindre surveillance du système** : la nuit ou durant les vacances, par exemple.

L'**ANSSI** rappelle que le pirate peut également s'infiltrer d'une manière « **progressive plus insidieuse** », en veillant à effacer derrière lui toute trace d'activité malveillante.

Quelles précautions prendre pour éviter les attaques par hameçonnage ciblé ?

Afin de protéger votre entreprise d'une attaque par hameçonnage ciblé, **respectez ces quelques conseils et sensibilisez vos salariés à ces pratiques** :

- **Mettez votre système à jour**. Des mises à jour importantes sur d'éventuelles failles de sécurité peuvent en effet être installées par votre système d'exploitation.
- **Méfiez-vous des extensions de pièces jointes qui semblent douteuses** et **peuvent contenir des codes malveillants** (exemples : .pif ; .com ; .bat ; .exe ; .vbs ; .lnk, etc.).
- **Utilisez un compte utilisateur plutôt qu'administrateur**. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser des actions ou accéder à des fichiers cachés de votre ordinateur. Préférez l'utilisation d'un compte utilisateur, qui vous permet également d'effectuer vos tâches quotidiennes sans entrave.
- **Portez une attention toute particulière aux liens sur lesquels vous cliquez**. Une lettre ou caractère en trop ou en moins peut vous conduire vers un tout autre site web. Privilégiez la saisie des URL directement sur la barre d'adresses ainsi que les liens commençant par « https ».
- **Utilisez un antivirus ou un pare-feu**. En informatique, le pare-feu permet de limiter un certain nombre de connexions entrantes et sortantes. Si malgré tout, le pirate trouve une faille dans votre ordinateur, un antivirus peut l'empêcher de nuire.
- **Utilisez le filtre contre le filoutage du navigateur Internet**. La plupart des navigateurs existants proposent une fonctionnalité d'avertissement contre le filoutage. Ces fonctions aident à maintenir votre vigilance.
- **Utilisez un logiciel de filtre anti-pourriel** ou **les fonctionnalités de classement automatique en tant que spam < https://www.economie.gouv.fr/entreprises/comment-lutter-contre-spams> de votre boîte de réception** : même si ces filtrages ne sont pas exhaustifs, ils permettent de réduire le nombre de ces courriels.

Ces contenus peuvent aussi vous intéresser

- Entreprises, faites attention aux tentatives d'escroqueries ! < https://www.economie.gouv.fr/entreprises/attention-tentatives-escroqueries-fraude-arnaques>
- Sécurité de vos données : comment vous protéger des méthodes de piratage ? < https://www.economie.gouv.fr/entreprises/m[illegible]des-piratage>
- Comment lutter contre les spams ? < https[illegible]onomie.gouv.fr/entreprises/comment-lutter-contre-spams>
- Entreprises : comment protéger vos donné[illegible]es lors de déplacements à l'étranger ? < https://www.economie.gouv.fr/entreprises/pr[illegible]ion-donnees-a-l-etranger>

En savoir plus sur le hameçonnage ciblé

<

- Attaque par hameçonnage ciblé (spearphishing) *sur le site de l'ANSSI*

<

- Attention aux arnaques ! *sur le site impots.gouv.fr*

<

- Sécurité informatique : soyez vigilants ! *sur le site impots.gouv.fr*

<

- Guide de prévention contre les arnaques de la Task-Force nationale de lutte contre les arnaques [PDF – 1 232 Ko]

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.