PIRATAGE DE VOS DONNEES : COMMENT VOUS PROTEGER ?

Solutions DECIDEUR

FCC
Comptez sur nous !

PIRATAGE DE VOS DONNEES : COMMENT VOUS PROTEGER ?

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.

SOMMAIRE

LE PHISHING

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**. 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 ?

Vous pouvez rappeler à vos employés **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. 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.
3. **Ne communiquez jamais votre mot de passe.** Aucun site web fiable ne vous le demandera.
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 phishing ciblé. Restez vigilant et vérifiez les paramètres des comptes de votre entreprise.

LE RANÇONGICIEL

Les rançongiciels, ou ransomware en anglais, **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 ?

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

1. **Effectuez des sauvegardes régulières de vos données**
   C'est le meilleur moyen de couper l'herbe sous le pied aux pirates souhaitant prendre vos données en otage ! Déplacez physiquement la sauvegarde de votre réseau (hors réseau), placez-la en lieu sûr et veillez à ce qu'elle fonctionne !

2. **N'ouvrez pas les messages dont la provenance ou la forme est douteuse** Ne vous laissez pas tromper par un simple logo ! Pire, le hacker peut avoir récupéré certaines de vos données préalablement (les noms de vos clients par exemple) et créer des adresses de messagerie ressemblant à un détail près à celle de vos interlocuteurs habituels.
   Restez donc très vigilants ! Certains messages paraissent tout à fait authentiques.
   Apprenez à identifier les courriels piégés (ou autres formes de récupération de vos données) sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).
   Vous avez un doute ? Contactez le messager par un autre biais.

LE RANÇONGICIEL

3. Apprenez à identifier les extensions douteuses des fichiers

Vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute se finit par un autre type d'extension ? Ne l'ouvrez surtout pas !

Voici quelques exemples d'extensions douteuses : .pif, .com, .bat ; .exe, .vbs, .lnk, ... Attention à l'ouverture de pièces jointes de type .scr ou .cab. Comme le rappelle l'Agence nationale de la sécurité des systèmes d'information (ANSSI), il s'agit des extensions de compression des campagnes CTB-Locker sévissant chez les particuliers, les PME ou les mairies.

4. Mettez à jour vos principaux outils

On ne vous le dira jamais assez : traitement de texte, lecteur PDF, navigateur mais aussi antivirus... Si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée.

Cette règle évitera en effet la propagation des rançongiciels via les vulnérabilités des applications. Considérez que, d'une manière générale, les systèmes d'exploitation en fin de vie, qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes.

5. Utilisez un compte « utilisateur » plutôt qu'un compte « administrateur »

Évitez de naviguer depuis un compte administrateur. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur. Préférez l'utilisation d'un compte utilisateur. Cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.

LE VOL DE MOT DE PASSE

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 ?

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 :**

1. **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.

2. **Construisez des mots de passe compliqués :** utilisez des lettres, des majuscules et des caractères spéciaux.

3. **N'utilisez pas le même mot de passe partout.**

4. **Enfin, pensez à changer régulièrement votre mot de passe.**

LES LOGICIELS MALVEILLANTS

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 ?

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

1. **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.

2. **Ne connectez pas une clé USB trouvée par hasard,** elle est peut être piégée. 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.**

LE FAUX RÉSEAU WIFI

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 ?

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 :**

1. **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.).

2. **Si vous devez créer un mot de passe dédié**, n'utilisez pas le mot de passe d'un de vos comptes existants.

3. **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.

4. **N'installez jamais de mise à jour soi-disant obligatoire à partir de l'un de ces réseaux.**

UN VPN, UN ATOUT SÉCURITÉ POUR VOTRE ENTREPRISE

Un VPN (Virtual Private Network) est **un réseau privé virtuel** : il s'agit d'un tunnel permettant de créer un lien direct entre des ordinateurs distants, de manière sécurisée et isolée du reste du trafic.

En cryptant vos données et en modifiant votre localisation, le **VPN** permet de sécuriser les connexions Internet au sein de votre entreprise en :

1. **Sécurisant vos échanges de données :** les données échangées entre collaborateurs circulent uniquement via le tunnel sécurisé et crypté, sans contact avec le reste du web. Le risque d'interception est donc limité.

2. **Cryptant vos données sensibles :** lors des déplacements professionnels, les connexions à des réseaux tiers peuvent représenter un risque. Grâce à un VPN, vous pouvez naviguer en toute sécurité car l'ensemble des données transmises sont chiffrées.

3. **Garantissant votre confidentialité :** l'historique des navigations web est habituellement traçable grâce à l'adresse IP. Avec un VPN, vous disposez d'une nouvelle adresse IP, empêchant les tiers d'avoir accès à vos informations confidentielles (historique, localisation, etc.).

Mieux vous informer,
nous rapprocher de vous
& encore mieux
vous conseiller.
Nos équipes
restent à votre écoute.

FCC
Comptez sur nous !

AUDECIA
EXPERTS COMPTABLES
COMMISSAIRES AUX COMPTES