

Six conseils pour éviter d'être victimes de phishing



Six conseils pour éviter d'être victimes de phishing

Le phishing (e-mails frauduleux se faisant passer pour des marques de commerce ou de service avec l'intention de tromper le destinataire) est l'une des attaques les plus anciennes, mais aussi des plus rentable pour les cybercriminels.

Sur la base de « plus des gens le reçoivent, meilleure est la probabilité que quelqu'un tombe dans le piège » ces campagnes frauduleuses dont le seul but est le vol de données personnelles et financières, ont beaucoup évolué dans les dernières années. Et, en plus, **au cours du premier trimestre de 2016 les cas de spam avec des pièces jointes malveillantes, ils n'ont pas cessé d'augmenter.**

Il y a quelques années, il était facile de distinguer ces e-mails entrant dans la boîte de réception car ils avaient des fautes d'orthographe, des conceptions plutôt anciens... qui nous fassent au moins nous méfier. D'autres viennent directement comme spam, ou comme un courrier indésirable. Mais maintenant, **ils ont évolué.** Bon nombre de ces campagnes utilisent des courriels parfaitement conçus: avec le logo, les couleurs et l'apparence de la marque qui sont en train de supplanter.

Mais le fait que, heureusement, ils ne donnent pas des coups au dictionnaire, signifie que ces emails sont beaucoup plus difficiles à détecter comme frauduleux. Cependant, **il y a un certain nombre de précautions que nous pouvons prendre pour éviter de devenir une victime de ces e-mails malveillants.** Check Point propose ces conseils que nous devons mettre en pratique pour les détecter au début, ou presque:

1. **Surveillez les e-mails qui viennent de marques célèbres.** Le site OpenPhish rassemble les marques les plus utilisées par les cybercriminels pour mener à bien leurs attaques de phishing. **Parmi eux, Apple, Google et Paypal figurent dans le top dix des plus touchés par ce type de campagne.** Les raisons sont évidentes: ils sont extrêmement populaires, il est donc plus susceptible de réussir à usurper l'identité des victimes potentielles.
2. **Vérifiez l'expéditeur du message. Les emails officiels sont toujours envoyés avec le domaine de la marque, par exemple @paypal.com.** Les cybercriminels peuvent mettre le nom de marque, mais ils ne peuvent jamais utiliser le domaine réel.
3. **Fautes d'orthographe.** Nous venons de dire que les cybercriminelles ont beaucoup amélioré en ce sens mais **ils restent toujours quelques erreurs de basse,** souvent en raison de mauvaises traductions.
4. **Hyperliens.** Les liens qui sont envoyés par le biais de ces e-mails sont clairement frauduleux. Une fois que vous y accédez normalement **ils conduisent à des formes où ils volent les données.** Donc, lorsque vous accédez à un site Web qui n'a pas le protocole HTTPS, vous devenez une victime.
5. « **Cher utilisateur** ». Il faut tenir en compte que **les entreprises traitent leurs clients par leur nom et prénom** mais les cybercriminels envoient des e-mails en masse, impersonnelles.
6. **Urgence.** Dans de nombreux e-mails de ce type, **il y a généralement un sentiment d'urgence pour donner nos données personnelles:** le compte est fermé, vous perdrez de l'argent, votre colis sera envoyé sont des exemples.
7. **Attention aux pièces jointes.** Des entreprises n'envoient jamais des pièces jointes dans leurs e-mails. **Évitez d'ouvrir ces documents,** sauf si vous êtes très sûr de l'expéditeur.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Quelques conseils pour surfer un peu plus tranquille sur Internet

✕	Quelques conseils pour surfer un peu plus tranquille sur Internet
---	---

Quelques conseils de bon sens pour se protéger au mieux des attaques liées à l'utilisation d'Internet.

Des mises à jour régulières et automatiques

L'un des meilleurs moyens de se prémunir des risques de piratage, est de **maintenir son matériel informatique et ses logiciels à jour** avec les derniers correctifs de sécurité et les dernières mises à jour.

Par ce biais, le risque d'intrusion est minimisé. Il est donc très important de **configurer son ordinateur** pour que le système d'exploitation se mette **régulièrement et automatiquement à jour**.

Une bonne configuration matérielle et des logiciels adaptés

Les **niveaux de sécurité** de l'ordinateur doivent être **réglés au plus haut** pour minimiser les risques d'intrusions. Les **paramètres des navigateurs** et des **logiciels de messageries** électroniques peuvent aussi être configurés avec des niveaux de sécurité élevés.

L'utilisation d'un **anti-virus à jour** et d'un **pare-feu (firewall)** assureront un niveau de protection minimum pour surfer sur la toile. Le **firewall** permet de filtrer les données échangées entre votre ordinateur et le réseau. Il peut être réglé de manière à bloquer ou autoriser certaines connexions.

Utiliser un bon mot de passe

Les mots de passe sont une **protection incontournable** pour sécuriser l'ordinateur et ses données ainsi que tous les accès au service sur Internet.

Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Lire nos conseils pour choisir un bon mot de passe .

Se méfier des courriers électroniques non-sollicités et leurs pièces jointes

A la réception d'un mail dont l'**expéditeur est inconnu**, un seul mot d'ordre : **prudence !**

Les courriers électroniques peuvent être accompagnés de **liens menant vers des sites frauduleux** (voir l'article sur le *phishing*) ou de **pièces jointes piégées**. **Un simple clic sur une image suffit pour installer à votre insu un logiciel ou code malveillant** (cheval de Troie) sur votre ordinateur. La pièce jointe piégée peut être : une page html, une image JPG, GIF, un document word, open office, un PDF ou autre.

Pour se protéger de ce type d'attaque, la règle est simple : **ne jamais ouvrir une pièce jointe dont l'expéditeur est soit inconnu, soit d'une confiance relative**.

En cas de doute, une recherche sur internet permet de trouver les arnaques répertoriées.

Que faire si j'ai déjà cliqué sur la pièce jointe?

Déconnectez-vous d'internet et **passez votre ordinateur à l'analyse anti-virus** (à jour) pour détecter l'installation éventuelle d'un logiciel malveillant.

Pour tout renseignement ou pour signaler une tentative d'escroquerie :



Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Conseils de prévention sur

Comment bien se protéger contre les Cyberattaques ?

	Comment bien se protéger contre les Cyberattaques ?
---	--

On l'a encore vu récemment, aucun système informatique n'est à l'abri d'une faille...

Et en matière de cybercriminalité, les exemples nous montrent que l'attaque semble toujours avoir un coup d'avance sur la défense. L'enjeu, pour les institutions et les entreprises, est d'anticiper et de se préparer à ces situations de crise en développant, en amont, une stratégie à-même de minorer au maximum leurs conséquences.

Demande de rançons, fraudes externes, défiguration de sites web, vols ou fuites d'informations, cyber-espionnage économique ou industriel..., en 2016 huit entreprises françaises sur dix ont été victimes de cybercriminels, contre six en 2015. La tendance n'est malheureusement pas à l'amélioration et l'actualité récente regorge d'exemples frappants : le logiciel malveillant WannaCry qui vient de frapper plus de 300 000 ordinateurs dans 150 pays avec les conséquences désastreuses que l'on connaît, l'attaque du virus Adylkuzz qui ralentit les systèmes informatiques, le vol de la copie numérique du dernier opus de la saga « Pirates des Caraïbes » quelques jours avant sa sortie mondiale..., les exemples de cyberattaques ne cessent de défrayer la chronique.

Pour bien se protéger contre les Cyberattaque, nous vous conseillons de suivre les étapes suivantes :

1. Faire ou faire faire un état des lieux des menaces et vulnérabilités risquant de mettre en danger votre système informatique ;
2. Faire ou faire faire un état des lieux des failles aussi bien techniques qu'humaines ;
3. Mettre en place les mesures de sécurité adaptées à vos priorités et aux moyens que vous souhaitez consacrer ;
4. Assurer une surveillance des mesures de sécurité et s'assurer de leur bon fonctionnement et de leur adaptation au fil de vos évolutions aussi bien techniques que stratégiques.

- Vous souhaitez faire un point sur l'exposition de votre entreprise aux risques cyber ?
- Vous souhaitez sensibiliser votre personnel aux différentes arnaques avant qu'il ne soit trop tard ?
- Vous recherchez une structure en mesure de mettre en place une surveillance de votre réseau, de votre installation, de vos ordinateurs ?

Contactez-vous

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Cyberattaque, comment faire pour limiter les risques ?*

Comment bien choisir ses mots de passe ?

✖	Comment bien choisir ses mots de passe ?
---	--

Les mots de passe sont une protection incontournable pour sécuriser l'ordinateur et ses données ainsi que tous les accès aux services sur Internet. Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Qu'est ce qu'un bon mot de passe ?

Un bon de passe est constitué d'au moins **12 caractères** dont :

- des lettres majuscules
- des lettres minuscules
- des chiffres
- des caractères spéciaux

Un mot de passe est d'autant plus faible qu'il est court. L'utilisation d'un alphabet réduit ou de mot issu du dictionnaire le rend très vulnérable.

Les mots du dictionnaire ne doivent pas être utilisés.

Aussi à proscrire, les mots en relation avec soi, qui seront facilement devinables : nom du chien, dates de naissances...

Réseaux sociaux, adresses mail, accès au banque en ligne, au Trésor public, factures en ligne.

Les accès sécurisés se sont multipliés sur internet.

Au risque de voir tous ses comptes faire l'objet d'utilisation frauduleuse, il est impératif de **ne pas utiliser le même mot de passe** pour des accès différents.

Alors, choisir un mot de passe pour chaque utilisation peut vite devenir un vrai casse-tête.

Comment choisir et retenir un bon mot de passe ?

Pour créer un bon mot de passe, il existe plusieurs méthodes :

La méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour créer une phrase facilement mémorisable.

Exemple : « j'ai acheté huit cd pour cent euros ce après-midi » donnera : ght8CD%E7am

La méthode des premières lettres

Utiliser les premières lettres d'une phrase en variant majuscules, minuscules et caractères spéciaux.

Exemple : « un tiens vaut mieux que deux tu l'auras » donnera : lTvmQ2tl'@

Diversifier facilement les mots de passe

Opter pour une politique personnelle avec, par exemple, un préfixe pour chaque type d'activité. Comme BANQUE-MonMotDePassz pour la banque, IMP-MonMotDePasse pour les impôts.

Quelque chose de très facile à mémoriser qui complexifie votre mot de passe et, surtout, vous permet de le diversifier.

Diminuer les imprudences

Pour finir, il est utile de rappeler de **ne pas stocker ses mots de passe à proximité de son ordinateur** si il est accessible par d'autres personnes. L'écriture sur le

post-it déposé sous le clavier est à proscrire par exemple, de même que le stockage dans un fichier de la machine.

En règle général, les logiciels proposent de **retenir les mots de passe**, c'est très **tentant mais imprudent**. Si votre ordinateur fait l'objet d'un piratage ou d'une panne,

les mots de passe seront accessibles par le pirate ou perdus.

Que faire en cas de piratage ?

Il est recommandé de préserver les traces liées à l'activité du compte.

Ces éléments seront nécessaires en cas de dépôt de plainte au commissariat de Police ou à la Gendarmerie.

Exemple

Compte email piraté

Vos contacts ont reçu des messages suspects envoyés de votre adresse.

Contactez-les pour qu'ils conservent ces messages.

Ils contiennent des informations précieuses pour l'enquêteur qui traitera votre dépôt de plainte.

Récupérez l'accès à votre compte afin de changer le mot de passe et re-sécurisez l'accès à votre compte.

Changer de mots de passe régulièrement

Cette dernière règle est contraignante mais assurera un niveau supérieur de sécurité pour vos activités sur Internet.

Un **bon mot de passe doit être renouvelé plusieurs fois par an** et toujours en utilisant les méthodes décrites ci-dessus.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs aux **risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Comment choisir ses mots de passe ? / Cybercrime / Dossiers / Actualités – Police nationale – Ministère de l'Intérieur

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de

**passé » (à condition que...) |
Denis JACOPINI**

x	Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) Denis JACOPINI
---	---

Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « *ilfaitbeaudanstoutelafrancesaufdanslebassinparisien* » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « *p8)J#&=89pE* », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que **la phrase choisie comme mot de passe ne soit pas une phrase connue de tous**, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essayent de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « *Sur le pont d'Avignon, on y danse on y danse...* ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « *jevaispromenermonchienTITIdansle93* ».

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. Dès lors, **plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.**

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui verrouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien verrouiller son ordinateur, etc...

Article original de Denis JACOPINI et Atlantico

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) | Atlantico.fr

**Victime d'une arnaque sur
Internet ? Faites-nous part
de votre témoignage**

x	Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage
---	--

**Vous êtes victime d'une arnaque ou d'un piratage sur Internet ?
Votre témoignage nous permettra peut-être de vous aider.**

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice. Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

- une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes)
;
- un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
- Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante :)
- Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

Contactez moi

Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.



Réagissez à cet article

Comment éviter de se faire avoir par des e-mails de phishing

<p> Phone security Ervins Strauhmanis via Flickr CC License by</p>	<p>Comment éviter de se faire avoir par des e-mails de phishing</p>
---	---

Toujours, toujours être sur ses gardes.

Ça n'arrive qu'aux autres, à ceux qui ne font pas attention, qui n'y connaissent rien, qui font n'importe quoi sur internet. Jusqu'au jour où ça nous arrive à nous. Ça, c'est se faire avoir par du phishing (du hameçonnage, en français), cette technique qui consiste à vous envoyer un e-e-mail en se faisant passer pour quelqu'un dans le seul but de vous faire cliquer sur un lien, et vous faire rentrer identifiants et mots de passe dans une nouvelle page vous les demandant.

À l'été 2014, on avait ainsi découvert que de nombreuses stars américaines s'étaient ainsi fait voler leur identifiant iCloud de cette façon, permettant aux pirates de collecter leurs photos privées, dont certaines ont ensuite fini par être partagées sur des forums. Même chose avec le piratage de l'adresse e-e-mail de John Podesta, l'ancien chef de campagne d'Hillary Clinton, lors de la dernière présidentielle américaine.

Le phishing marche, souligne ainsi Wired, qui explique que 100.000 nouvelles attaques ont lieu chaque jour, et que quelques milliers réussissent. En septembre 2016, une étude allemande montrait qu'un étudiant interrogé sur deux pouvait se faire avoir par le message d'un inconnu. Alors pour éviter de se faire avoir, le magazine américain propose trois solutions.

1. Tout d'abord, **toujours réfléchir avant de cliquer**. *«Si quelque chose a l'air bizarre, c'est que ça l'est probablement»,* et *«vous devriez toujours être réticents à l'idée de télécharger les pièces jointes et de cliquer sur les liens, peu importe s'ils ont l'air innocent, ou la personne qui les a envoyés»*. En clair, toujours regarder l'origine de l'e-e-mail, et si quelque chose semble louche, ne pensez même pas à télécharger ou cliquer sur quoi que ce soit.

2. Ensuite, **scruter la source**. L'étape basique mais qu'on oublie si souvent. Pour être sûr que ce e-mail provient bien de Google, Yahoo!, ou de votre banque, vous devriez vraiment vérifier l'adresse qui vient de vous l'envoyer. Cela veut dire regarder dans l'URL de l'adresse si rien n'a l'air louche, ou si des caractères n'ont pas été remplacés par d'autres pour vous tromper (sur cette image par exemple, l'émetteur a ajouté un deuxième «l» à «paypal»). Si l'adresse e-e-mail est bien la bonne, mais que le test semble bizarre, vérifiez que c'est bien la bonne personne qui vient de vous l'envoyer, en tentant de la joindre par un autre canal.

3. Enfin, **préparer ses arrières**. En clair, faites comme si vous alliez vous faire avoir un jour ou un autre, et assurez-vous de limiter déjà les dégâts. *«Cela veut dire prendre des précautions de cybersécurité standards, comme mettre en place une authentification à plusieurs facteurs (on vous a fait un tuto ici), utiliser un gestionnaire de mots de passe ou un autre système pour créer des mots de passe unique et aléatoires, et sauvegardez vos données.»*

Parce qu'au fond, le vrai e-mailon faible dans toutes ces histoires se trouve entre la chaise et le clavier.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Comment éviter de se faire avoir par des e-mails de*

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI

x	Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits
---	---

Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.

Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant... Les accès gratuits pullulent et se généralisent.

Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit » assure-t-il. « Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants... »

Des sniffeurs de données

Il exagère ? Non. « L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés ! » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter. » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi ».

Conseils

Alors quels conseils ? « Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites. » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.

Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Android.

Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]



Réagissez à cet article

Original de l'article mis en page : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Comment détecter e-mail malveillant

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

x	x	x	x	x	x
---	---	---	---	---	---

Notre métier en RGPD et en CYBER : Auditer, Expertiser,
Accompagner, Former et Informer

x	x	x	x	x	x
---	---	---	---	---	---

**Comment détecter e-mail
malveillant**

Via votre messagerie ou votre boîte mail, certaines personnes malintentionnées tentent de mettre la main sur vos données personnelles en utilisant des techniques d'hameçonnage (phishing) ou d'escroquerie de type fraude 419 (scam) ! Ces techniques d'attaque évoluent constamment. Les conseils suivants vous aideront à déterminer si un message est légitime ou non.

Comment repérer une arnaque reçue dans votre messagerie ou votre boîte mail ?

• Est-ce que le message/courriel vous est réellement destiné ?

1. Généralement, les messages malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés.

2. Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un courriel malveillant.

• **Attention aux expéditeurs inconnus** : soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.

• **Soyez attentif au niveau de langage du courriel** : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration ...).

• **Vérifiez les liens dans le courriel** : avant de cliquer sur les éventuels liens, laissez votre souris dessus*. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.* *A noter : cette manipulation est impossible à effectuer depuis un écran de smartphone.*

• **Méfiez vous des demandes étranges** : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.

• **L'adresse de messagerie source n'est pas un critère fiable** : une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami – par exemple pour récupérer l'accès à son compte – contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !

Comment réagir ?

Si vous avez un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime :

- N'ouvrez surtout pas les pièces jointes et ne répondez pas;
- Si l'escroquerie que vous souhaitez signaler vous est parvenue par un spam (pourriel), rendez-vous sur www.signal-spam.fr;
- Supprimez le message puis videz la corbeille;
- S'il s'agit de votre compte de messagerie professionnel : transférez-le au service informatique et au responsable de la sécurité des systèmes d'information de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

Comment s'en prémunir ?

• Utilisez un logiciel de filtre anti-pourriel ou activez l'option d'avertissement contre le filoutage présent sur la plupart des navigateurs.

• Installez un anti-virus et mettez-le à jour.

• Désactivez le volet de prévisualisation des messages.

• Lisez vos messages en mode de texte brut.

Si vous êtes victime d'une escroquerie en ligne ?

Signalez les escroqueries auprès du site www.internet-signalement.gouv.fr, la plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements. Pour s'informer sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : contacter Info Escroqueries au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile) – Du lundi au vendredi de 9h à 18h

Rendez-vous sur cybermalveillance.gouv.fr, la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Que vous soyez un particulier, une entreprise ou une administration, retrouvez :

- des conseils / vidéos pour sensibiliser votre entourage professionnel ou personnel,
- des services de proximité en cas de dommages causés par une attaque informatique.

...[lire la suite]

Réagissez à cet article

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)

Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !
Commandez sur Fnac.fr

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la

Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur [Fnac.fr](https://www.fnac.fr)

Source : *Phishing : détecter un message malveillant* | CNIL

Piratage de votre boîte mail, quelles peuvent être les conséquences sur votre vie personnelle



Votre boîte mail est souvent la clé qui permet d'accéder ou de vous inscrire aux services en ligne. Raison de plus pour la sécuriser au maximum !



Pour votre boîte mail : un mot de passe solide

Vous devez utiliser un mot de passe propre et unique pour vous connecter à votre webmail et surtout ne pas l'utiliser pour un autre compte.

Pourquoi c'est important ?

Utiliser le même mot de passe pour votre compte de messagerie et votre compte de réseau social est une pratique risquée. Si votre fournisseur de réseau social est victime d'une fuite de données comprenant vos moyens d'authentification, une personne mal intentionnée pourrait les utiliser pour non seulement accéder à votre compte de réseau social mais aussi pour accéder à votre messagerie.

De plus, une fois l'accès à votre messagerie obtenu, il deviendra possible de voir la liste des messages d'inscriptions à vos comptes sur différents sites (si vous ne les avez pas supprimés de votre boîte). Il sera ainsi possible de connaître certains de vos identifiants de compte et d'utiliser la fonction d'oubli de mots de passe pour en prendre le contrôle.

Cette absence de sécurité ou l'utilisation d'un mot de passe faible vous expose à des risques :

- Usurpation de votre boîte mail pour piéger votre liste de contacts ;
- Ajout d'une redirection de mail (souvent indétectable après la compromission d'une boîte mail) : vos emails continuent de fuiter malgré tout changement de mot de passe ultérieur...
- Connexion du pirate à vos sites et applications tierces ;
- Utilisation de vos coordonnées bancaires pour payer ;
- Usurpation d'identité grâce aux données collectées dans votre boîte mail ;
- Demande de rançon suite à des données compromettantes retrouvées dans votre boîte mail ;
- ...

[CONSEIL] – En parallèle d'un bon mot de passe :

- Il est déconseillé d'utiliser sa boîte mail en tant qu'espace de stockage, notamment pour les données qui peuvent vous paraître sensibles et notamment, les bulletins de paie, les justificatifs d'identité envoyés qui peuvent notamment contenir votre adresse postale personnelle, ou les mots de passe échangés en clair. Attention également aux photos qui permettent de vous ré-identifier sur des sites de réseaux sociaux et donnent la possibilité à une personne malveillante de se créer une fausse identité.
- Il convient de supprimer les emails reçus, envoyés ou enregistrés en tant que brouillon qui paraissent avoir une importance particulière ou de chiffrer les documents que vous mettez en pièce jointe.
- Enfin pour protéger votre identité, il est recommandé d'utiliser une boîte mail sous pseudonyme pour l'inscription à des services que vous jugez intrusifs, ou particulièrement sensibles (site de jeux concours, site de rencontre ...).

L'initiative

havebeenpwned est un site conçu par Troy Int, informaticien indépendant. Il recense tous les mails compromis à l'occasion de fuite de données massive. L'utilisateur n'a qu'à entrer son email pour savoir s'il figure dans une base de données piratée et si ses mots de passes sont potentiellement entre les mains de personnes malveillantes.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous accompagner dans vos démarches de mise en conformité avec la réglementation Européenne relative à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus

d'informations

sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article