

# Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

<input type="checkbox"/>	<b>Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques</b>
--------------------------	---

---

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

## 1. CHOISISSEZ AVEC SOIN VOS MOTS DE PASSE

Entrer un mot de passe permettant de s'authentifier pour accéder à son ordinateur, sa tablette ou son téléphone portable est un geste quotidien de sécurité.

Choisir un mot de passe difficile à deviner par une tierce personne ou par du piratage informatique est ainsi un rempart efficace pour protéger ses données personnelles contre les intrusions frauduleuses.

### Comment bien choisir son mot de passe ?

Définissez des mots de passe composés d'au moins 12 caractères

- mélangeant majuscules, minuscules, chiffres et caractères spéciaux
- n'ayant aucun lien avec vous comme votre nom, date ou lieu de naissance
- ne formant pas de mots figurant dans le dictionnaire

### Comment faire en pratique ?

Pour cela 2 méthodes simples :

- la méthode phonétique : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CDn€7am
- la méthode des premières lettres : « Un tiens vaut mieux que deux tu l'auras » : ltvnQ2tl'A

### Quelques recommandations supplémentaires

- n'utilisez pas le même mot de passe pour tout, notamment pour accéder à votre banque en ligne et votre messagerie personnelle ou professionnelle
- méfiez-vous des logiciels qui vous proposent de stocker vos mots de passe

## 2. ENTRETIENEZ RÉGULIÈREMENT VOS APPAREILS NUMÉRIQUES

### En mettant à jour régulièrement les logiciels de vos appareils numériques

Dans chaque système d'exploitation (Android, MacOS, Linux, Windows,...), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité.

Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations longtemps encore après leur découverte ou même leur correction. Il donc **nécessaire de procéder aux mises à jour régulières des logiciels.**

#### Comment faire ?

- configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible
- ou téléchargez les correctifs de sécurité disponibles en utilisant pour cela exclusivement les sites Internet officiels des éditeurs
- en effectuant couramment des sauvegardes

## 3. Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple) permet de disposer de ses données après un dysfonctionnement ou une panne d'ordinateur

#### Comment faire ?

- utilisez des supports externes tels qu'un disque dur externe, un CD ou un DVD enregistrable pour enregistrer et sauvegarder vos données.

## 4. PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES ET DE VOTRE IDENTITÉ NUMÉRIQUE

Les données que vous laissez sur Internet vous échappent instantanément.

Des personnes malveillantes récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité et de conduire des activités d'espionnage industriel.

**Une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet.**

Voici quelques recommandations générales :

- soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir : ne transmettez que les informations strictement nécessaires et pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données, par exemple avec des partenaires commerciaux
- ne donnez accès qu'à un minimum d'informations personnelles sur les réseaux sociaux
- utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle...) et une adresse destinée aux autres services en ligne (forums, jeux concours...)

## 5. PROTÉGEZ VOS DONNÉES LORS DE VOS DÉPLACEMENTS

L'emploi d'ordinateurs portables, d'ordiphones (*smartphones*) ou de tablettes facilite le quotidien lors des déplacements professionnels. Pourtant, voyager avec ces appareils nomades peut mettre en péril des informations sensibles sur l'entreprise ou vous travaillez.

### Précautions à prendre avant de partir en mission

- utilisez le matériel dédié à la mission prêté par votre entreprise (ordinateur, clefs USB, téléphone)
- sauvegardez aussi vos données sur un support amovible pour les retrouver en cas de perte
- si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur
- apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport

### Pendant la mission

- gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel)
- si vous êtes contraint de vous séparer de votre téléphone, retirez la carte SIM et la batterie
- en cas d'inspection ou de saisie de votre matériel par des autorités étrangères, informez votre organisation
- n'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance
- évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présentation

## 6. SÉCURISEZ VOTRE WI-FI

Si l'utilisation du Wi-Fi est une pratique attractive, elle permet, lorsque le point d'accès n'est pas sécurisé, à des personnes malintentionnées d'intercepter vos données et d'utiliser votre connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes.

C'est pour cette raison que l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise.

**Le Wi-Fi, solution pratique et peu coûteuse, peut cependant être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre box. Pour ce faire, n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès.**

Quelques recommandations générales :

- modifiez le nom d'utilisateur et le mot de passe par défaut (généralement « admin » et « 0000 ») de votre page de configuration accessible via votre navigateur Internet
- vérifiez que votre box dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version précédente WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes)
- modifiez la clé de connexion par défaut avec une clé (mot de passe) de plus de 20 caractères de types différents (cf. Choisissez des mots de passe robustes)
- ne divulguez votre clé de connexion qu'à des tiers de confiance et changez-la régulièrement
- activez et configurez les fonctions pare-feu / routeur.
- désactivez le Wi-Fi de votre borne d'accès lorsqu'il n'est pas utilisé

## 7. SÉPAREZ VOS USAGES PERSONNELS DES USAGES PROFESSIONNELS

Monsieur Paul, directeur commercial, rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Monsieur Paul. Des informations sensibles ont été volées puis revendues à la concurrence.

**Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone,...) personnels et professionnels.**

**Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :**

- ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles
- ne stockez pas de données professionnelles sur vos équipements communicants personnels

**En savoir plus sur le AVEC ou BYOD :**

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle est cependant très problématique pour la sécurité des données personnelles et professionnelles (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).

De la même façon, il faut éviter de connecter des supports amovibles personnels (clés USB, disques durs externes) aux ordinateurs de l'entreprise.

## 8. SOYEZ AUSSI PRUDENT AVEC VOTRE ORDIPHONE (SMARTPHONE) OU VOTRE TABLETTE QU'AVEC VOTRE ORDINATEUR

Alexandre possède un ordiphone. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, les éditeurs peuvent accéder à tous les SMS présents sur son téléphone.

**Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires d'hygiène informatique :**

- n'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement : il faut éviter de les installer
- en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et configurez votre téléphone pour qu'il se verrouille automatiquement
- effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les retrouver en cas de panne de votre ordinateur ou ordiphone

## 9. SOYEZ PRUDENT LORSQUE VOUS OUVREZ VOS MESSAGES ÉLECTRONIQUES

Suite à la réception d'un courriel semblant provenir d'un de ses amis, Madame Michel a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Madame Michel le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

**Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,...).**

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- l'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoyez habituellement vos contacts
- si un lien ou plusieurs figurent dans un courriel, vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire)
- n'ouvrez pas et ne retapez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

## 10. SOYEZ VIGILANT LORS D'UN PAIEMENT SUR INTERNET

Lorsque vous réalisez des achats en ligne, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants, directement sur votre ordinateur.

**Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :**

- contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs)
- assurez-vous que la mention « https:// » apparaît au début de l'adresse du site Internet
- vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple

Si possible, lors d'un achat en ligne, privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.

De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire.

## 11. TÉLÉCHARGEZ LES PROGRAMMES, LOGICIELS SUR LES SITES OFFICIELS DES ÉDITEURS

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui le plus souvent contiennent des virus ou des chevaux de Troie. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

- C'est la raison pour laquelle il est vivement recommandé de télécharger vos programmes sur les sites officiels des éditeurs
- Enfin, désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir, afin de vérifier qu'ils ne sont pas infectés par un quelconque virus ou spyware.



Réagissez à cet article

# Comment sécuriser Firefox efficacement en quelques clics de souris ?

 Comment sécuriser Firefox  
efficacement en quelques  
clics de souris ?

---

**Vous utilisez Firefox est vous souhaitez que cet excellent navigateur soit encore plus sécurisé lors de vos surfs sur Internet ? Voici quelques astuces qui supprimeront la géolocalisation, le profilage de Google ou encore que vos données offline disparaissent du regard d'espions locaux.**

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.

Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande `about:config`. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne `security.tls.version`. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne `geo.enabled` pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaissent pas la dernière page que vous avez pu visiter, cherchez la ligne `network.http.sendRefererHeader` et mettez la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne `browser.safebrowsing.malware.enabled`.

Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne `browser.safebrowsing.provider.google.lists` et effacez la valeur proposée.

Pour finir, vos données peuvent être encore accessibles en « offline », en mode hors connexion. Cherchez les lignes `offline-apps.allow_by_default` et `offline-apps.quota.warn`. La première valeur est à passer en False, la seconde valeur en 0.

Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.

Article original de Damien Bancal



Réagissez à cet article

Original de l'article mis en page : Sécuriser Firefox efficacement en quelques clics de souris – Data Security BreachData Security Breach

---

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

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

---

**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

---

# Compte Facebook piraté : Quelles sont les bons réflexes à avoir ? | Denis JACOPINI

21



**Il arrive parfois de se faire pirater son compte Facebook. Soit parce qu'on a oublié de se déconnecter du site sur un ordinateur public, soit parce qu'on s'est fait voler d'une manière ou d'une autre son mot de passe. Il arrive aussi que des personnes se fassent passer pour vous et ouvrent un profil à votre nom avec vos informations et photos personnelles.**

Dans ces cas de piratage ou d'usurpation d'identité, il importe de réagir rapidement pour empêcher toute possibilité de nuisance.

**Première chose à faire : signaler le compte piraté ou usurpé à Facebook.**

#### Si votre compte a été piraté



Signaler un compte piraté

Si vous pensez que votre compte a été piraté ou infecté par un virus, cliquez sur le bouton Mon compte a été piraté ci-dessous. Nous vous aiderons à vous reconnecter afin d'en reprendre le contrôle.

Mon compte a été piraté Annuler

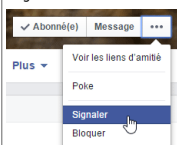
Rendez-vous sur la page Signaler un compte piraté.

Indiquez l'identifiant de votre compte puis suivez les instructions. Vous serez notamment amené à taper votre ancien mot de passe et Facebook vous posera quelques questions pour vérifier votre identité.


Dans le pire des cas, vous pourrez faire appel à contacts de confiance pour récupérer votre compte.

#### Si votre identité (ou celle d'une autre personne) a été usurpée

Rendez-vous sur la page du profil suspicieux et cliquez sur le bouton contenant 3 petits points, juste en dessous de la photo de couverture. Sélectionnez Signaler.



Dans la fenêtre qui s'affiche alors, sélectionnez l'option Signaler ce compte et cliquez sur Continuer.



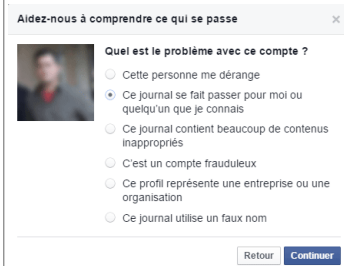
Aidez-nous à comprendre ce qui se passe

Que voulez-vous faire ?

- Signaler du contenu partagé par Gauthier
- Signaler ce compte
- Obtenir de l'aide pour un autre problème

Continuer

Dans l'écran suivant, sélectionnez ensuite l'option Ce journal se fait passer pour quelqu'un que je connais.



Aidez-nous à comprendre ce qui se passe

Quel est le problème avec ce compte ?

- Cette personne me dérange
- Ce journal se fait passer pour moi ou quelqu'un que je connais
- Ce journal contient beaucoup de contenus inappropriés
- C'est un compte frauduleux
- Ce profil représente une entreprise ou une organisation
- Ce journal utilise un faux nom

Retour Continuer

Vous êtes amené ensuite à préciser votre cas.



Aidez-nous à comprendre ce qui se passe

Qui prétendent-ils être ?

- Moi
- Une personne que je connais
- Une célébrité

Retour Continuer

**Si il s'agit de votre propre identité,** sélectionnez l'option Moi. Vous pouvez alors demander à fermer le compte.

**Si l'identité de quelqu'un d'autre a été usurpée,** sélectionnez l'option Une personne que je connais ou éventuellement Une célébrité.

Cliquez sur Continuer pour valider et suivez les instructions.

#### Aller plus loin et porter plainte

Si vous estimez qu'il y a préjudice, vous pouvez aller porter plainte au Commissariat de police ou à la Gendarmerie de votre lieu d'habitation. N'hésitez pas à faire des captures d'écran pour nourrir votre dossier.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

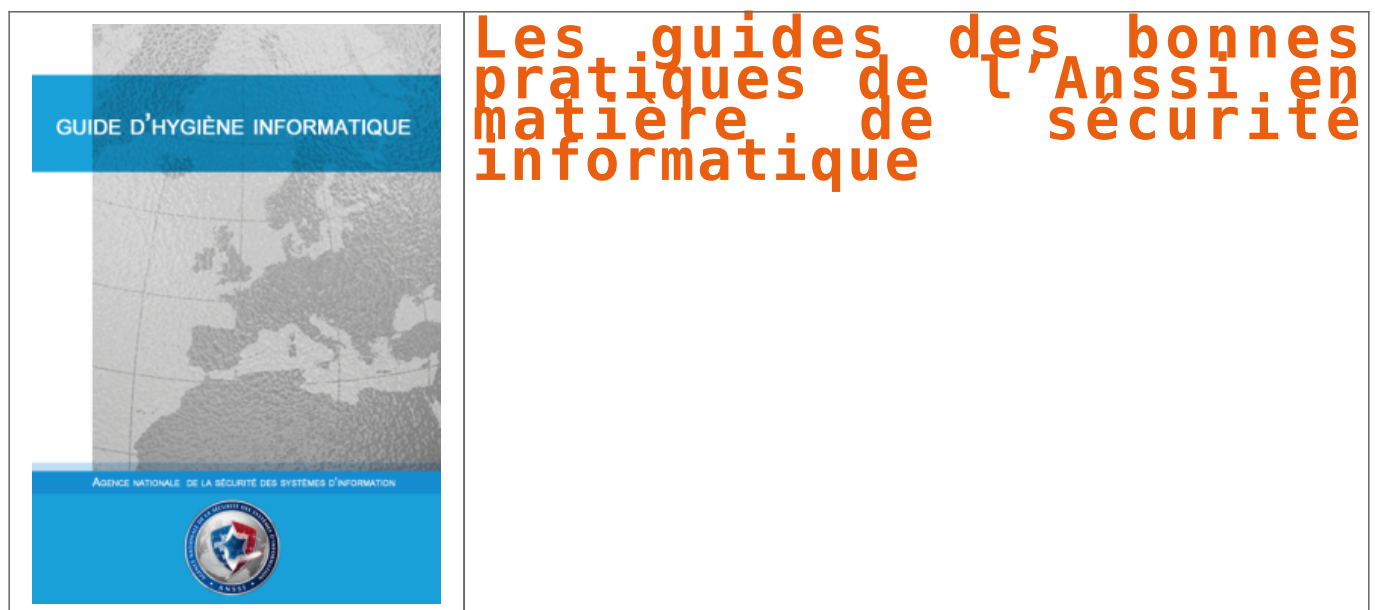
Cliquez et laissez-nous un commentaire...

Source : <http://www.aussitot.fr/facebook/signaler-compte-pirate-usurpation-identite-facebook.html>



---

# Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



**Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.**

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

#### LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique... comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

---

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

---

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>

---

# Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI

Votre responsabilité  
engagée en cas de piratage  
de vos données

---

**Si vous vous faites pirater votre ordinateur ou votre téléphone, votre responsabilité pourrait bien être engagée vis-à-vis des données que ce support numérique renferme.**

Imaginez que vous disposiez de différents appareils numériques informatiques renfermant une multitude de données, dont des données d'amis, de prospects, de clients, de fournisseurs (tout ce qu'il y a de plus normal), et tout à coup, à cause d'un Malware (Méchangiciel selon D. JACOPINI), un pirate informatique en prend possession de ces données, les utilise ou pire, les diffuse sur la toile. Que risquez-vous ?

En tant que particulier victime, pas grand chose, sauf s'il est prouvé que votre négligence est volontaire et l'intention de nuire retenue.

Par contre, en tant que professionnel, en plus d'être victime du piratage (intrusion causée par une faille, un virus, un crypto virus, un bot, un spyware), et d'avoir à assumer les conséquences techniques d'un tel acte illicite pourtant pénalement sanctionné notamment au travers de la loi godfrain du 5 janvier 1988 (première loi française réprimant les actes de criminalité informatique et de piratage), vous risquez bien de vous prendre une seconde claque vis à vis de la loi Informatique et Libertés du 6 janvier 1978.

En effet, Les entreprises, les sociétés, tous ceux exerçant une activité professionnelle réglementée ou non, les associations, les institutions, administrations et les collectivités, sont tenues de respecter la loi Informatique et Libertés du 6 janvier 1978 et notamment la sécurité des données selon les termes de son Article n°34 :

*Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.*

*De plus, les sanctions jusqu'alors limitées à 5 ans d'emprisonnement et 300 000 euros d'amendes vont à partir du 25 mai 2018, par la mise en application du RGPD (Règlement Général sur la Protection des Données) être portées à 20 millions d'euros et 4% du chiffre d'affaire mondial.*

#### **Partons d'un cas concret.**

*La société Cochamboptnalds voit son système informatique piraté. Des investigations sont menées et le pirate informatique arrêté.*

*Vis à vis de la loi Godfrain du 5 janvier 1988, le voyou risque jusqu'à 2 ans de prison et 20 000 euros d'amende. Or ce dernier, après avoir découvert que la société Cochamboptnalds n'était pas en règle avec la CNIL la dénonce auprès de cette dernière.*

*Le responsable de traitement, généralement le chef d'entreprise risquera, lui, 5 ans de prison et 300 000 euros d'amende, une peine bien supérieure à son voleur.*

*Est-ce bien normal ?*

*Non, mais pourtant c'est comme ça et ça peut être le cas de toutes les entreprises, administrations et administrations françaises en cas de piratage de leurs ordinateurs, téléphones, boîtes e-mail...*

#### **Autre cas concret**

*Monsieur Roudoudou-Maxitout voit son téléphone portable mal protégé et exposé aux virus et aux pirates. Un jour il apprend par un ami que les contacts de son téléphone se sont fait pirater. Il se déplace à la Police ou à la Gendarmerie, dépose une plainte mais le voleur n'est jamais retrouvé. Qui est responsable de cette fuite d'informations ?*

*La première chose à savoir, c'est si ce téléphone est professionnel ou personnel. S'il est professionnel, référez vous au cas contrés précédent. Si par contre le téléphone portable est personnel, vis à vis de la loi Informatique et Libertés, les particuliers ne sont pour l'instant pas concernés par l'obligation de sécurisation des données.*

*Ainsi, si la faute volontaire du propriétaire de l'appareil n'est pas retenue, le seul responsable de cette fuite de données sera et restera l'auteur du piratage.*

---

*Denis JACOPINI est Expert Informatique et aussi **formateur en Protection des données personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).*

*Nous pouvons vous animer des **actions de sensibilisation ou de formation** à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.*

*Plus d'informations sur*

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

*Denis JACOPINI*



**Réagissez à cet article**

Original de l'article mis en page : **Informatique et Libertés : suis-je concerné ? | CNIL**

---

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

 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

---

# 5 règles d'or pour les utilisateurs des réseaux

# sociaux | Denis JACOPINI

 5 règles d'or pour les utilisateurs des réseaux sociaux

---

Le nombre total d'individus dans le monde est de 7,4 milliards. Fin 2015, Facebook a atteint les 1,59 millions d'utilisateurs. Avec une augmentation annuelle de 17%, le géant des réseaux sociaux est tout simplement trop important pour être ignoré. Ceci étant dit, c'est aussi vrai pour beaucoup d'autres réseaux sociaux.

Les 310 millions d'utilisateurs actifs par mois sur Twitter postent 347 222 fois en moyenne. Plusieurs d'entre eux tweetent plus d'une centaine de fois par jour, et nombreux sont ceux à tweeter une fois par jour. Plus de 40 millions de photos ont été partagées sur Instagram depuis son lancement, et plus de 80 millions de photos y sont publiées chaque jour.

Ceci représente une énorme quantité de données : certaines importantes, d'autres intéressantes ou encore inutiles. Les réseaux sociaux, avec leurs propres tendances et leurs propres lois, fonctionnent comme une extension du monde réel, qui a un énorme impact sur nos vies hors-ligne. Dans cet article, nous vous dévoilons quelques règles simples que chaque utilisateur de réseaux sociaux devrait garder en tête.

### 1. N'alimentez pas les trolls

Les trolls sur Internet sont des provocateurs qui se joignent à des conversations dans le but d'agacer les autres utilisateurs pour le « fun ». On peut trouver des trolls n'importe où : sur les forums, les chats, et autres plateformes de communication en ligne. Les forums des nouveaux médias sont connus pour la participation élevée de trolls. D'ailleurs, il y en a plein sur les réseaux sociaux.

Comment devez-vous parler aux trolls ? D'aucune façon ! Ignorez-les. Plusieurs personnes se font prendre au piège et engagent alors des débats houleux en essayant d'expliquer leur point de vue et passent une grande partie de leur temps et de leur énergie en vain. Quelqu'un a toujours tort sur Internet. Ne perdez pas votre temps et votre énergie pour des trolls.

View image on Twitter



Si vous n'avez pas de chance, vous pourriez tomber sur un troll en quête de revanche, en spammant votre e-mail, ou même en essayant de ruiner votre vie. Par exemple, un couple américain a perdu du temps, de l'argent, leur travail et même détruit leur mariage en étant les victimes de cyberintimidation, se traduisant par des canulars téléphoniques (swatting) et autres formes d'harcèlement hors-ligne.

### 2. Ne postez pas ou ne partagez pas de contenu illégal

Les Emirats Arabes Unis et la Nouvelle Zélande disposent de lois qui punissent sévèrement les trolls et la cyberintimidation avec des sanctions allant de 35 000\$ à la prison.

Toutefois, vous pouvez écoper d'une amende ou même être confronté à des conséquences bien plus graves pour avoir posté, partagé du contenu ou toutes autres actions relatives dans bon nombre de pays. Par exemple, deux hommes ont été condamnés à quatre ans de prison après avoir créé une page Facebook qui encourageait une révolte. Un homme au Bangladesh a été envoyé en prison pour avoir plaisanté sur son souhait de voir le premier ministre mort. Par conséquent, mieux vaut être au courant des lois de chaque pays et de s'en souvenir au moment de publier ou partager sur Facebook ou Twitter.

### 3. Ne partagez pas des arnaques

Les fraudeurs piègent souvent les victimes avec des histoires choquantes telles que des bébés mourants, des chiots qui se noient, ou d'anciens combattants. De tels articles font le tour des réseaux sociaux en criant à l'aide. En réalité, ils sont déployés dans le but de voler de l'argent, de diffuser des malwares et des méthodes d'hameçonnage.

View image on Twitter



Follow



CityNews Toronto

@CityNews

Consumers warned about online scam involving free puppies<http://ow.ly/YAgcm>

3:14 AM – 22 Feb 2016

\*

\*

2020 Retweets

\*

99 likes

De tels articles génèrent beaucoup de partages, mais la majorité d'entre eux sont des arnaques. De vrais appels au secours proviennent en général de votre famille, amis, et amis de vos amis. Ayez toujours en tête que ce sont les pages officielles des entreprises qui mettent en place ce type d'aide et non pas des individus inconnus.

C'est la raison pour laquelle il vaut mieux rester vigilant et vérifier chaque article avant de cliquer sur « aimer » ou « partager ». Pas envie de tous les contrôler un par un ? Ne prenez donc pas de risques pour vous et vos amis.

### 4. Pensez aux réactions des lecteurs

Vous avez probablement des collègues, des supérieurs et des clients parmi vos connections Facebook ou Instagram. Lorsque vous postulez pour un emploi, il est très probable par exemple que les ressources humaines jettent un coup d'œil à votre profil sur les réseaux sociaux. Prenez en compte ce que vous voulez leur montrer, et plus important encore, ce que vous ne voulez pas.

Vous devez aussi réfléchir prudemment à ce que vous publiez sur les pages d'autres utilisateurs et sur des comptes publics tels que des entreprises ou des universités. Par exemple, en 2013, un homme originaire de Pennsylvanie a été renvoyé pour avoir « complimenté » une étudiante en ligne. Son commentaire n'avait rien de sexuel ou d'inapproprié, mais de toute évidence la mère de la jeune fille n'avait pas apprécié. Un an auparavant, une professeure de Moses Lake, Washington, avait été virée parce qu'une femme qu'elle n'avait jamais rencontrée s'était plainte d'un de ces articles. Il s'agit de quelques exemples parmi tant d'autres qui prouvent qu'il vaut mieux garder ses photos personnelles et ses articles pour des amis sûrs.

Si vous avez besoin d'aide pour dissimuler vos articles privés des regards indiscrets, vous pouvez retrouver nos articles sur les paramètres de confidentialité de Facebook, Twitter, Instagram, LinkedIn, et Tumblr.

View image on Twitter



Follow



Kaspersky Lab

@kaspersky

Check your Facebook privacy settings NOW <https://kas.pr/3Wpw>

8:13 PM – 26 Oct 2015

\*

\*

2525 Retweets

\*

1313 likes

### 5. Ne dévoilez pas vos données publiques

De nombreux réseaux sociaux proposent d'« enregistrer » la géolocalisation lorsque vous prenez une photo, postez du contenu ou montrez les lieux que vous avez visités. Si vous êtes intéressé par un événement, le réseau social peut en informer vos amis au cas où ils voudraient vous accompagner.

Par défaut, tout le monde peut accéder à vos données, et les cybercriminels ont mille et une méthodes de s'en servir, ça peut aller de s'introduire dans votre maison jusqu'à voler votre identité numérique. C'est la raison pour laquelle nous vous recommandons vivement de dissimuler ce type des données à des personnes inconnues, à l'aide des paramètres de confidentialité de Facebook.

C'est aussi une bonne occasion pour que vous n'ajoutiez pas n'importe qui aveuglément : les gens envoient des demandes d'amis qui peuvent s'avérer être des bots, des trolls ou même des hackers. Même si Facebook vous informe que vous avez des dizaines d'amis en commun, n'acceptez pas de demandes si vous n'êtes pas certain que ce soit des connaissances sûres.

Article original de John Snow



Réagissez à cet article



Original de l'article mis en page : 5 règles d'or pour les utilisateurs des réseaux sociaux | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

---

## **Attaques informatiques : Comment s'en protéger ?**

 <b>Attaques informatiques : Comment s'en protéger ?</b>
---

---

**Les cyberattaques se faisant de plus en plus nombreuses et sévères, les entreprises doivent apprendre à s'en protéger. Pour cela, les directions juridiques et de l'informatique peuvent s'appuyer sur l'expertise de la police judiciaire et des experts en data protection.**

Tous les quinze jours en moyenne, une attaque sévère – où des données sont exfiltrées – est découverte. Face à ce constat, le tribunal de commerce de Paris a réuni quatre tables rondes d'experts de la sécurité informatique, des représentants de la police judiciaire et des experts-comptables fin juin pour examiner les solutions de protection dont disposent les entreprises. Julien Robert, directeur de la sécurité chez SFR, résume les trois facteurs agissant sur la sécurité : les utilisateurs, car ce sont eux qui choisissent les données qu'ils utilisent et partagent, les fournisseurs d'accès et l'encadrement d'un data center externe fortement conseillé.

#### **Prévention**

« *Il est difficile d'agir lorsque l'attaque a déjà eu lieu* », précise Sylvie Sanchis, chef de la Becti (1) de la police judiciaire de Paris. Le moyen le plus efficace dont disposent les entreprises pour se protéger est donc la prévention. Il faut avant tout investir dans la sécurité informatique. Si certaines sociétés sont réticentes en raison du coût, il est important de rappeler qu'il sera toujours moindre que celui engendré par une attaque.

Tous les salariés doivent par ailleurs être formés car certaines intrusions sont rendues possibles par leur comportement, sans qu'ils en soient conscients, notamment par leur exposition sur Internet.

#### **Les modes opératoires**

Les modes opératoires d'exfiltration des données se diversifient et se sophistiquent au fil des années. Certains se veulent discrets afin que l'entreprise ne prenne connaissance de l'attaque que très tardivement, d'autres relèvent du chantage ou de la demande de rançon.

L'attaque peut venir d'un mail qui, à son ouverture, téléchargera un virus sur l'ordinateur de l'employé. Les données peuvent également être extraites grâce au social engineering, pratique qui exploite les failles humaines et sociales de la cible, utilisant notamment la crédulité de cette dernière pour parvenir à ses fins (arnaque au patron). Quant aux ransomwares, il s'agit de logiciels malveillants permettant de rançonner l'entreprise pour qu'elle récupère ses données. Dans ce cas, Anne Souvira, chargée de mission aux questions liées à la cybercriminalité au cabinet du préfet de police de Paris, précise que « *même si l'entreprise paye, il est très rare de récupérer toutes les données.* » Si elle peut être tentée de payer la rançon sans prévenir les autorités compétentes pour une somme modique, il n'y a aucune garantie de récupérer les données et les traces de l'attaque seront perdues. D'autres techniques de chantage sont utilisées, comme lorsque l'on se voit menacer d'une divulgation des vulnérabilités du système.

#### **L'importance de porter plainte**

La réaction à adopter, la plus rapide possible, fait partie de la sécurité informatique : « *C'est un travail de réflexion en amont qui permettra d'adopter la bonne stratégie* », selon Cirył Piat, lieutenant-colonel de la gendarmerie nationale. Suite à une cyber-attaque, la plupart des entreprises sont réticentes à porter plainte, par peur d'une mauvaise réputation ou par scepticisme vis-à-vis de la réelle utilité de cette procédure. Alice Cherif, chef de la section « cybercriminalité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments d'investigation qui permettront de remonter au cybercriminel. « *Toute autre alternative est bien moins efficace et fait perdre un temps précieux à l'entreprise ainsi que des éléments d'investigation.* »

#### **L'utilité du cloud**

L'une des façons de sécuriser ses données est de les confier à un tiers spécialiste qui les stockera en ligne sur un cloud. « *Il s'agit d'un système complexe connecté sur Internet, où les données sont stockées sur des disques durs physiques situés dans des salles d'hébergement, les fameux data centers* », explique Julien Levrard, chef de projet sécurité chez OVH. Le cloud rend l'accès plus difficile aux malfaiteurs d'autant qu'ils ignorent la localisation de la donnée. Vigilance et prévention : les maîtres mots en matière de cybercriminalité.

Article original de Emilie Smelten

(1) Brigade d'enquête sur les fraudes aux technologies de de l'information



Réagissez à cet article

**Original de l'article mis en page : Cybercriminalité : comment se protéger ? – Magazine Decideurs**

---

# Bonnes pratiques face à une tentative de cyber-extorsion

## | Denis JACOPINI



Bonnes pratiques face à une tentative de cyber-extorsion

---

## Bonnes pratiques face à une tentative de cyber-extorsion

### 1. Typologie des différents cas de cyber-extorsion

Le type le plus répandu de cyber-extorsion est l'attaque par crypto-ransomware. Ce dernier est une forme de malware qui chiffre les fichiers présents sur la machine infectée. Une rançon est par la suite demandée afin d'obtenir la clef qui permet de déchiffrer les données compromises. Ces attaques touchent autant les particuliers que les acteurs du monde professionnel. Il existe cependant deux autres types de cyber-extorsion auxquels doivent faire face les sociétés.

Le premier cas est celui du chantage faisant suite à un vol de données internes. L'exemple le plus marquant de ces derniers mois est celui du groupe Rex Mundi : ce dernier dérobe des informations sensibles/confidentielles – comme une base clientèle – puis demande une rançon à sa victime sous peine de divulguer son butin et par conséquent de rendre public l'acte de piratage; ce qui peut être fortement compromettant pour la société ciblée comme pour sa clientèle. De nombreuses entreprises comme Dexia, Xperthis, Voo ou encore Labio ont été victimes des chantages du groupe Rex Mundi.

La deuxième pratique est celle du DDoS contre rançon, spécialité des pirates d'Armada Collective. Le modus operandi est simple et efficace : la cible reçoit un email l'invitant à payer une rançon en Bitcoin afin de ne pas se voir infliger une puissante attaque DDoS qui rendrait son site web indisponible à ses utilisateurs. La plupart des victimes sont des sociétés de taille intermédiaire dont le modèle économique est basé sur le principe de la vente en ligne – produits ou services – comme le fournisseur suisse de services de messagerie ProtonMail en novembre 2015.

### 2. Bonnes pratiques à mettre en place

En amont de la tentative de cyber-extorsion

Un ensemble de bonnes pratiques permet d'éviter qu'une attaque par ransomware se finalise par une demande de rançon.

Il convient de mettre en place une stratégie de sauvegarde – et de restauration – régulière des données. Ces back-ups doivent être séparés du réseau traditionnel des utilisateurs afin d'éviter d'être chiffrés en cas de déploiement d'un crypto-ransomware. Dans ce cas de figure, le système pourra être restauré sans avoir besoin de payer la rançon exigée.

La propagation d'un malware peut également être évitée par l'installation d'outils/solutions de cybersécurité notamment au niveau du client, du webmail et du système d'exploitation (antivirus). Ceci doit obligatoirement être couplé à une mise à jour régulière du système d'exploitation et de l'ensemble des logiciels installés sur le parc informatique.

L'être humain étant toujours le principal maillon faible de la chaîne, il est primordial de sensibiliser les collaborateurs afin qu'ils adoptent des comportements non-risqués. Par exemple : ne pas cliquer sur les liens et ne pas ouvrir les pièces-jointes provenant d'expéditeurs inconnus, ne jamais renseigner ses coordonnées personnelles ou bancaires à des opérateurs d'apparence légitimes (banques, fournisseurs d'accès Internet, services des impôts, etc.).

Ces bonnes pratiques s'appliquent également dans le cas d'un chantage faisant suite à un vol de données internes. Ces dernières sont en général dérobées via l'envoi dans un premier temps d'un spam contenant une pièce jointe malicieuse ou une URL redirigeant vers un site web compromis. Une fois le système d'information compromis, un malware est déployé afin de voler les informations ciblées.

La menace provient également de l'intérieur : un employé mal intentionné peut aussi mettre en place une tentative de cyber-extorsion en menaçant de divulguer des informations sensibles/confidentielles. Ainsi, il est important de gérer les accès par une hiérarchisation des droits et un cloisonnement.

### Pendant la tentative de cyber-extorsion

Lors d'un chantage faisant suite à un vol de données internes, il est important de se renseigner sur la véracité des informations qui ont été dérobées. Certains groupes de pirates se spécialisent dans des tentatives de cyber-extorsion basées sur de fausses informations et abusent de la crédulité de leurs victimes. Il en va de même concernant l'origine du corbeau : de nombreux usurpateurs imitent le style du groupe Armada Collective et envoient massivement des emails de chantage à des TPE/PME. Ces dernières cèdent fréquemment à ces attaques qui ne sont pourtant que des canulars.

Il est vivement recommandé de ne jamais payer une rançon car le paiement ne constitue pas une garantie. De nombreuses victimes sont amenées à payer une somme bien plus conséquente que la rançon initialement demandée. Il n'est pas rare de constater que les échanges débutent de manière très cordiale afin de mettre la cible en confiance. Si cette dernière cède au premier chantage, l'attaquant n'hésite pas à profiter de sa faiblesse afin de lui soutirer le plus d'argent possible. Il abuse de techniques basées sur l'ingénierie sociale afin d'augmenter ses profits. Ainsi, l'escroc gentil n'existe pas et le paiement de la rançon ne fait que l'encourager dans sa démarche frauduleuse.

De nombreuses victimes refusent de porter plainte et cela pour plusieurs raisons. Elles estiment à tort que c'est une perte de temps et refusent également de communiquer sur les résultats et conséquences d'une attaque qui ne feraient que nuire à leur image auprès des clients, fournisseurs ou partenaires. Pourtant cette mauvaise stratégie ne fait que renforcer le sentiment d'impunité des attaquants, les confortent dans le choix de leurs modes opératoires et leur permet de continuer leurs actions malveillantes. Il est ainsi vital de porter plainte lors de chaque tentative de cyber-extorsion. L'aide de personnes qualifiées permet de faciliter ce genre de démarches.

En cas d'attaque avérée, il est essentiel pour la victime de s'appuyer sur un panel de professionnels habitués à gérer ce type de situation. La mise en place d'une politique de sauvegarde ou bien la restauration d'un parc informatique n'est pas à la portée de toutes les TPE/PME. Il est nécessaire de faire appel à des prestataires spécialisés dans la réalisation de ces opérations complexes.

Par ailleurs, en cas de publication de la part de l'attaquant de données sensibles/confidentielles, il convient de mettre en place un plan de gestion de crise. La communication est un élément central dans ce cas de figure et nécessite l'aide de spécialistes.

Article original de Adrien Petit



Réagissez à cet article

Original de l'article mis en page : Bonnes pratiques face à une tentative de cyber-extorsion [Par Adrien Petit, CEIS] | Observatoire FIC