Mai 2017

CYBERSÉCURITÉ

ce qu'il faut savoir pour se protéger

unapl FORMATION

FONDS INTERPROFESSIONNEL DE FORMATION DES PROFESSIONNELS LIBÉRAUX

AU PLUS PRÈS DES PROFESSIONNELS

L'arrivée de la nouvelle économie numérique dans le champ des professions libérales apparaît autant comme une opportunité, en facilitant notamment le travail collaboratif, que comme un facteur de risques menant à la déréglementation accrue et à l'ubérisation. Dans le même temps, le paysage législatif et réglementaire reste mouvant, imposant de nouvelles normes d'exercice. Enfin, la croissance économique très ralentie, impose aux professionnels de se challenger en permanence pour conserver leurs marchés et en développer de nouveaux. Ce contexte impose, plus que jamais, aux professions libérales de faire preuve d'agilité et d'adaptation. La formation professionnelle continue apparaît ainsi la ressource à privilégier pour s'adapter sans retard à ces multiples évolutions.

Depuis plus de 23 ans, le **FIF PL** accompagne les professionnels libéraux dans leur démarche de formation professionnelle continue. Créé à l'initiative de l'UNAPL et animé par les professionnels, via leurs organisations membres de cette confédération, le **FIF PL** réajuste en permanence ses critères de prise en charge afin de répondre, de façon précise et en temps réel, aux besoins des professionnels.

Ainsi, afin de répondre à l'attente du plus grand nombre, le **FIF PL** a développé la prise en charge de formations propres à chaque profession, qu'elles soient de longue durée ou plus courtes, qu'elles soient présentielles ou à distance en E-learning. Au-delà, il contribue notamment à l'installation et la reprise d'entreprises, aux bilans de compétences, aux VAE et aux formations de conversion. En 2015, quelque 130 000 professionnels libéraux ont ainsi été pris en charge par le **FIF PL**, ce qui représente 2,7 millions d'heures de formation continue. Ces chiffres attestent de la bonne adéquation des dispositifs de prises en charge au regard des besoins des professionnels.

L'objectif permanent du **FIF PL** est de rester concrètement au plus près des attentes des professionnels. Les adaptations sont constantes. Ainsi, pour faciliter le dépôt des demandes de prise en charge et leur suivi, mais aussi pour accélérer le temps de traitement, le **FIF PL** a totalement dématérialisé des procédures. Celles-ci se font désormais en ligne en quelques clics et sans aucun papier. C'est rapide, simple et efficace.

Je vous invite à visiter notre site : **www.fifpl.fr**, afin de découvrir nos prises en charge et de déposer votre demande en quelques clics. Le FIP PL est l'outil des professionnels libéraux géré par vos organisations professionnelles.

Philippe DENRY
Président du FIF PL

PRISES EN CHARGE 2016 SUR FONDS SPÉCIFIQUES

Dans la limite des fonds disponibles de ces fonds spécifiques, hors budget annuel des professions.

Formation de longue durée	Prise en charge plafonnée à **70%** du coût réel de la formation, limitée à : ▶ **2 000 €** par professionnel pour **les formations prioritaires** ▶ **1 000 €** par professionnel pour **les formations non prioritaires** • *Limitée à une prise en charge tous les 3 ans.* • *100 heures de formation minimum.* • *Thèmes de formation entrant dans les critères de prise en charge 2016 de la profession concernée.*
VAE *(Validation des Acquis d'Expérience)* + diplôme qualifiant interne à une profession	Forfait de **1 000 €** par an et par professionnel
Bilan de compétences	Forfait de **1 500 €** par professionnel *Limité à une prise en charge tous les 3 ans.*
Formation de conversion	Prise en charge plafonnée à **2 000 €**, limitée à **200 €** par jour et par professionnel • *Limitée à une prise en charge tous les 3 ans.* • *Le professionnel libéral doit joindre obligatoirement un courrier de motivation à sa demande de prise en charge.*
Participation à un jury d'examen ou de VAE	Prise en charge plafonnée à **200 €** par jour, limitée à **4 jours** par an et professionnel
Aide à l'installation et à la création ou reprise d'entreprise	Prise en charge plafonnée à **200 €** par jour, limitée à **5 jours** par an et par professionnel • *Formations dispensées par les ORIFF PL dans le cadre de dossiers collectifs.* • *Fourniture d'un justificatif d'inscription à l'INSEE mentionnant le numéro Siret et le code NAF du participant.* • *Dans le cas où le demandeur de prise en charge n'est pas encore installé en libéral, ce dernier doit fournir une attestation sur l'honneur stipulant qu'il suit cette formation en vue d'une future activité libérale.*

www.fifpl.fr

104 rue de Miromesnil 75384 Paris Cedex 08 - Tél. 01 55 80 50 00 - Fax 01 55 80 50 29

unapl

Sommaire

- Edito 4
- Cybercriminalité, attention danger ! 5
- Un enjeu pour les professions libérales 6
- Cybersécurité législation / Quand l'Europe fait sa loi 11
- Cybersécurité bonnes pratiques / Ce qu'il faut faire et pas faire 14

FICHE SÉCURITÉ

- Les indices pour vérifier l'authenticité d'un e-mail 20
- Process en cas d'incident 21
- 10 points clés pour éviter une cyberattaque : rappel des précautions 22

EDITO

Dans notre exercice professionnel, l'informatique et le numérique sont omniprésents.

Parmi les nouveaux risques auxquels les professionnels libéraux sont confrontés, celui des failles de sécurité dans leurs dispositifs informatiques n'est pas moindre. Il aura fallu l'attaque massive et mondiale de hackers qui ont répandu un virus affectant les données de plusieurs entreprises pour qu'une prise de conscience s'opère.

Plus que tout autre, les professionnels libéraux ont la responsabilité des données personnelles et très sensibles de leurs patients ou clients. Ils doivent protéger les secrets dont ils sont les dépositaires.

Ce guide pratique, qui ne prétend pas à l'exhaustivité, a pour but de vous aider à comprendre les enjeux de la cybersécurité pour vous-même et votre activité.

Si vous souhaitez aller plus loin, sachez que l'UNAPL organise des formations sur ce sujet.

Ainsi l'UNAPL est aux côtés des professions libérales.

Dr Michel CHASSANG,
Président de l'UNAPL

Cybercriminalité, attention danger !

Dans une société de plus en plus numérisée et virale, la cybersécurité est devenue un enjeu majeur. Et pas uniquement pour les grandes entreprises. Les TPE-PME et donc les professions libérales sont concernées et dans le collimateur des hackers dans la mesure où leurs données informatiques représentent une valeur marchande et économique.

La chose n'a rien d'anecdotique et impacte tous les professionnels à des degrés divers. L'Union européenne ne s'y est pas trompée en édictant, en mai 2016, un Règlement général européen sur la protection des données personnelles, lequel devra être effectif dans tous les pays membres de l'UE à partir du 25 mai 2018. Outre cette législation coercitive, il importe d'adopter les comportements adéquats et de mettre en place de véritables politiques de gestion des données. C'est tout le sens du « Guide des bonnes pratiques de l'informatique » édité notamment par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et dont les douze recommandations qu'il contient constituent un corpus incontournable

Un enjeu pour les professions libérales

La cybercriminalité est en hausse en France. Elle ne touche pas seulement les grandes entreprises. Elle concerne également les petites sociétés et les professions libérales. Rançonnage, détournements de fonds, atteinte au secret professionnel : les risques sont nombreux.

Depuis deux ans, la cybercriminalité augmente en France de façon inquiétante. Selon le rapport annuel de la société américaine de sécurité informatique Symantec, en 2015, l'Hexagone faisait son retour dans le top dix des pays où la cybercriminalité est la plus active. Une hausse due au nombre de rançongiciels (ransomwares en anglais) comptabilisés cette année-là : plus de 391 000 attaques en France, soit 2,6 fois plus qu'un an plus tôt ! En 2016, le bilan n'est pas plus brillant.

« La fraude explose en France », tel est le titre du rapport du cabinet de conseil PwC sur la cybercriminalité en 2016. Ainsi, 68 % des entreprises françaises ont été victimes d'une fraude au cours des vingt-quatre derniers mois contre 55 % au Royaume-Uni et en Espagne et 38 % aux États-Unis. En outre, la cybercriminalité représente plus de la moitié des fraudes rapportées par les entreprises françaises. Ce qui représente une croissance de +25 % entre 2014 et 2016. *« Le nombre d'incidents de cybercriminalité a augmenté de plus de 50 % au cours des douze derniers mois, les organisations françaises étant victimes en moyenne d'environ vingt-et-un incidents de cybercriminalité par jour »,* précise le rapport. Des attaques qui ont évidemment un coût : selon l'enquête de PwC, *« les pertes financières liées aux incidents de cybersécurité se seraient élevées à 3,7 milliards de dollars en France en 2015, en augmentation de 28 % par rapport à 2014 ».* La cybercriminalité ne touche pas uniquement les grandes entreprises. Toujours selon PwC, le taux de fraude pour les entreprises de moins de 100 employés s'élève à 43 % alors qu'il n'atteint que 22 % en Europe de l'Ouest. Et les professions libérales ne sont pas à l'abri.

Jean-Yves CANNESSON
Président de la commission
Sécurité-Citoyenneté-
Défense de l'UNAPL

« Les professions libérales ne sont évidemment pas épargnées par les cyberattaques, lesquelles sont susceptibles de revêtir plusieurs modalités.
Outre le préjudice qu'elles causent aux entreprises libérales, elles mettent en péril l'une des obligations essentielles des professionnels : le secret professionnel et le secret médical. Il est donc essentiel de se prémunir contre cette forme de délinquance et de ne surtout pas attendre d'en être victime pour prendre le problème à bras le corps, sachant que la valeur de ces données informatiques est multiple. Elles peuvent en effet faire l'objet d'une demande de rançon mais aussi d'une revente à un tiers ou encore, d'une exploitation à divers titres. »

Rançon et usurpation d'identité

L'exemple le plus médiatisé est celui du piratage de données médicales d'un laboratoire de biologie médicale français. Le 16 mars 2015, Rex Mundi, un groupe de pirates informatiques, a ainsi diffusé sur Internet les données de plus de 15 000 patients, volées à ce laboratoire de biologie médicale français. Pour ne pas divulguer plus d'informations, les pirates réclamaient 20 000 euros. Ils n'en étaient pas à leur coup d'essai, puisqu'ils ont rançonné une douzaine de sociétés de divers secteurs d'activité. Les attaques par rançongiciel font partie des cybercrimes. Les rançongiciels sont des programmes informatiques malveillants diffusés par un mail qui contient des pièces jointes ou des liens piégés. Il peut s'agir d'un mail demandant le règlement rapide d'une facture. En un clic, le logiciel malveillant est téléchargé sur l'ordinateur et commence à chiffrer toutes les données contenues dans l'ordinateur : fichiers, photos, vidéos etc. Cryptés, les documents ne sont plus accessibles et un message s'affiche alors pour réclamer le versement d'une rançon en échange de la clé de déchiffrement.

Autre cybercrime : l'hameçonnage ou phishing. Cette technique vise à usurper une identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel. Le cybercriminel se fait passer pour un tiers de confiance (banques, administrations, fournisseurs d'accès à Internet…) et diffuse un mail frauduleux pouvant contenir une pièce jointe piégée. Le mail invite les destinataires à mettre à jour leurs informations personnelles, souvent bancaires, en cliquant sur un lien les redirigeant sur un faux site internet permettant au cybercriminel de récupérer les données et de les utiliser. Généralement, le mail est adressé à un grand nombre de contacts afin d'augmenter les *« chances »* que plus d'un destinataire suive les instructions.

ATTENTION AUSSI AUX FRAUDES !

Outre la cybercriminalité, les entreprises et les professionnels libéraux peuvent être victimes de fraudes pratiquées via Internet : vol de sommes directement sur les comptes bancaires grâce à la reconstitution du mot de passe par un outil informatique, désactivation de l'antivirus pour avoir accès aux fichiers du professionnel ou utilisation frauduleuse de l'accès wifi pour des attaques informatiques de sites Internet. Les entreprises peuvent aussi être victimes d'espionnage, d'atteinte à l'image ou de sabotage informatique. ***« Pour mieux appréhender ces problématiques, l'ANSSI a identifié douze recommandations, souvent des réflexes simples, à destination des non-spécialistes : choisir avec soin ses mots de passe, mettre à jour ses logiciels etc. »,*** **souligne Cyrille Tesser.**

Violation du secret professionnel

Le vol de données ne représente pas seulement un risque financier pour l'entreprise ou le professionnel libéral. Les professions libérales réglementées sont en effet soumises au secret professionnel ou, pour les professions de santé, au secret médical. Le secret professionnel est à la fois une obligation qui pèse sur le professionnel, notamment les juristes, et un droit pour ses clients. Ainsi, tous les échanges entre un avocat et son client, qu'il s'agisse de conseil ou de défense, sont soumis au secret professionnel. Et ceci englobe les supports immatériels : mails mais aussi échanges pécuniaires comme des virements. Or, un avocat est responsable de la violation du secret professionnel et peut encourir des sanctions disciplinaires et pénales.

Il en est de même pour le secret médical. Les données à caractère personnel relatives à la santé des personnes sont des données sensibles, qu'elles soient recueillies ou produites à l'occasion d'activités de prévention, de diagnostic ou de soins. Les biologistes, les médecins ou encore les pharmaciens sont par conséquent responsables des données des patients qui relèvent du secret médical. Dans ce cas aussi, s'il y a violation, les professionnels de santé encourent des sanctions disciplinaires et pénales.

Serge CARRIGOU
Président de la commission Numérique de l'UNAPL

« Avec la numérisation de leur exercice, les professionnels libéraux se sont penchés sur la pérennisation et la sauvegarde des données mais n'ont pas toujours conscience des problèmes de cybercriminalité. Ils prennent parfois des risques d'une utilisation frauduleuse »

UN ATELIER SUR LA CYBERSÉCURITÉ À PARIS LE 30 NOVEMBRE

Le 30 novembre, en prélude au congrès national des professions libérales qui se tiendra le lendemain au Palais Brongniart, la Commission Sécurité-Citoyenneté-Défense de l'UNAPL organise un atelier sur la cyber sécurité. Cet atelier se déroulera de 13h00 à 17h00 au siège de la Garde Républicaine à Paris. Il rassemblera des experts de Agence Nationale pour la Sécurité des Systèmes d'Information et du ministère de l'Intérieur. Retenez cette date dès à présent sur vos agendas.

Une prise de conscience progressive

Pour autant, les professionnels libéraux ne prennent pas toujours la mesure des menaces cybercriminelles qui peuvent peser sur eux. *« Avec la numérisation de leur exercice, les professionnels libéraux se sont penchés sur la pérennisation et la sauvegarde des données mais n'ont pas toujours conscience des problèmes de cybercriminalité. Ils prennent parfois des risques d'une utilisation frauduleuse »,* estime Serge Garrigou, Président de la commission Numérique de l'UNAPL. Selon Cyrille Tesser, référent de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en Île-de-France, *« les problématiques rencontrées par les petites et les moyennes entreprises pour la sécurité de leurs systèmes d'information sont nombreuses : protection des fichiers clientèle, des données personnelles et du savoir-faire technologique, sécurité des systèmes de production… Or, les TPE et les PME sont confrontées, chaque jour, à de nouveaux risques menaçant leur intégrité, leur image et leur compétitivité : vol de données, escroqueries financières, sabotage de sites d'e-commerce. »*

Les professionnels libéraux commencent néanmoins à prendre la mesure des problèmes liés à la circulation des données avec la mise en place de plates-formes de prestations. *« La maîtrise des données leur échappe et cela les inquiète,* commente Serge Garrigou. *Dans le même temps, la maîtrise, la sécurisation et la sauvegarde des données représentent des*

Cybersécurité législation Quand l'Europe fait sa loi

Le Règlement général européen sur la protection des données personnelles a été voté il y a un an et publié le 4 mai 2016 au Journal Officiel de l'Union européenne. Il entrera en vigueur à compter du 25 mai 2018 dans tous les pays membres de l'Union européenne. Il s'appliquera à toute structure qui collecte, traite et stocke des données personnelles dont l'utilisation peut permettre, directement ou indirectement, d'identifier une personne. Nombre d'entreprises libérales sont donc concernées. Quitte à devoir revisiter leur système d'information et leurs usages d'Internet pour être dans les clous.

La nature même des données personnelles et la convoitise malintentionnée qu'elles peuvent susciter justifient que les entités concernées (sociétés, associations, administrations, collectivités locales et syndicats) prennent des mesures pour se prémunir des cyberattaques. Le législateur européen envisage d'ailleurs la notion de données personnelles au sens large puisqu'elles ont également trait aux informations sur les salariés, les clients etc. En somme, *« toute donnée concernant une personne physique identifiée ou identifiable (personne concernée) ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à une ou plusieurs caractéristiques spécifiques d'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne ».* Ce qui comprend notamment les adresses de courrier électronique, les adresses IP ou encore les posts sur les réseaux sociaux.

Outre le traditionnel consentement des personnes concernées pour ce qui est du recueil et de l'usage de ces données, les entreprises ont le devoir de veiller à leur préservation (non-destruction ou altération) ainsi qu'à leur non-diffusion à des destinataires entre les mains desquels elles n'ont pas vocation à tomber. Autrement dit, à prendre toutes les mesures pour parer d'éventuelles cyberattaques. Et, en cas d'infraction, hors de question d'adopter la politique de l'autruche. Elles ont alors l'obligation d'en faire état dans les plus brefs délais (72 heures) à l'autorité nationale compétente, en l'occurrence à la Commission nationale de l'informatique et des libertés (Cnil) en France, mais aussi aux personnes auxquelles se réfèrent lesdites données, a fortiori si l'acte délictueux risque de leur porter préjudice.

Les entreprises soumises à une obligation de moyens

Dans tous les cas, les entreprises sont soumises à une obligation de moyens. Elles doivent être en mesure de justifier n'importe quand auprès des tutelles, notamment en produisant des documents justificatifs, les dispositifs qu'elles ont mis en œuvre pour se prémunir des hackers et garantir la protection des données. De même, l'externalisation hors des frontières de l'Union européenne de ces dernières est-elle soumise au respect de règles, en particulier, à la tenue d'un registre consignant les données qui quittent le ressort territorial de l'UE et sous quelle forme. Et ce, afin d'assurer un niveau de protection égal à celui en vigueur à l'intérieur de l'Union. Enfin, les professionnels libéraux sont tenus de choisir des partenaires agréés lorsqu'ils souhaitent leur déléguer le stockage ou le traitement de leurs bases de données. Quitte à les auditer préalablement dans la mesure où il leur sera ensuite impossible de se défausser totalement sur eux et de s'exonérer de toute responsabilité en cas de cyberinfraction. Autre moyen de s'exposer a minima aux détournements de données : ne conserver que celles dont on a besoin et détruire définitivement celles qui ne sont de plus aucune utilité.

En théorie, les structures, à l'image des entreprises et des cabinets libéraux, dont le cœur de métier n'est pas le traitement de données, ne sont pas tenues de désigner un Délégué à la protection des données chargé de veiller à leur sécurité. En revanche, les dirigeants de sociétés qui gèrent une base de données ont tout intérêt, soit en nommant un salarié, soit en s'en chargeant eux-mêmes, à être en mesure de se prévaloir, vis-à-vis des pouvoirs publics, d'une personne référente en la matière.

LA PEUR DU GENDARME

Les sanctions financières encourues en cas de non-respect des dispositions européennes se veulent dissuasives. Elles sont en effet susceptibles d'atteindre jusqu'à 4 % du chiffre d'affaires annuel mondial ou 20 millions d'euros. Sans compter que ce sera à l'entreprise de prendre en charge l'indemnisation des personnes ayant subi un préjudice matériel et moral dû(s) à un manquement à ses obligations.

On l'aura compris, la question de la cybersécurité et de la gestion des risques afférents n'ont rien d'accessoire ni de secondaire pour les entreprises libérales amenées à collecter et à traiter des données personnelles. Il s'agit, pour elles, d'être proactives et surtout pas d'attendre et de voir en cas de survenue d'un problème. La sécurité informatique doit faire l'objet d'une politique minutieuse arrêtée en amont, mêlant prévention et gestion des cyberattaques. Un impératif qui est l'affaire de tous, dirigeants et salariés, lesquels sont pour priés, pour cela, de suivre les formations adéquates.

Des formations en région avec l'UNAPL sur la cybersécurité

Dans le cadre des Rendez-vous des professions libérales, l'UNAPL organise dans les régions des réunions de formation et d'information sur la cybersécurité et comment se protéger de la cybercriminalité. L'une d'entre elles a eu lieu le 6 avril à Amiens, à l'initiative de l'UNAPL Picardie.

UNE AFFAIRE D'ÉTAT

A l'heure où le cyberterrorisme est un mode opératoire de plus en plus prégnant, la France entend protéger ses secteurs économiques vitaux. Dans cette optique, 249 Opérateurs d'importance vitale (OIV) ont été désignés. Il s'agit de grandes entreprises mais aussi d'organismes publics ou parapublics officiant dans douze domaines (eau, l'alimentation, santé, télécommunications, énergie etc.) en lien avec la sécurité nationale. Tous ces acteurs devront mettre en œuvre des mesures de protection renforcée en matière informatique. Les premiers arrêtés en ce sens, recensant leurs obligations, sont entrés en vigueur l'année dernière. Ils détaillent les règles organisationnelles et techniques pour sécuriser l'accès et la gestion des systèmes d'information les plus convoités, lesquels doivent être expressément identifiés selon une procédure que les textes énoncent. Idem en ce qui concerne la notification des incidents de sécurité et des contrôles réguliers à mettre en place.

A ce jour, les entreprises libérales ne sont bien sûr pas (encore) concernées par un tel dispositif. Néanmoins, on peut s'attendre à ce que ce type de réglementation soit, à l'image de celles sur la sécurité incendie, progressivement étendu à tous les acteurs économiques, y compris les plus petits.

Cybersécurité bonnes pratiques Ce qu'il faut faire et pas faire

Le « Guide des bonnes pratiques de l'informatique », édité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), recense les écueils à éviter en matière de cybersécurité. Des recommandations qui valent pour les TPE et PME libérales quelle qu'en soit la nature.

Depuis deux ans, la cybercriminalité augmente en France de façon inquiétante. Selon le rapport annuel de la société américaine de sécurité informatique Symantec, en 2015, l'Hexagone faisait son retour dans le top dix des pays où la cybercriminalité est la plus active. Une hausse due au nombre de rançongiciels (ransomwares en anglais)

1 / Choisir avec soin ses mots de passe

Les mots de passe doivent être difficiles à retrouver à l'aide d'outils automatisés ou à deviner. Pour cela, ils doivent comporter douze caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec l'utilisateur (nom, date de naissance…) et ne figurant pas dans le dictionnaire.

Au sein de l'entreprise, il convient de :

- déterminer des règles de choix et de dimensionnement (longueur) des mots de passe et de… les faire respecter ;
- modifier toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs…) ;
- ne pas conserver les mots de passe dans des fichiers ou sur des post-it ;
- sensibiliser les collaborateurs au fait qu'ils ne doivent pas préenregistrer leurs mots de passe dans les navigateurs

2 / Mettre à jour régulièrement ses logiciels

Dans chaque système d'exploitation (Android, IOS, Windows,...), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent des mises à jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les hackers exploitent ces vulnérabilités pour mener à bien leurs attaques.

Il faut donc :

- définir et faire appliquer par l'équipe une politique de mises à jour régulières ;
- configurer les logiciels de la société ou du cabinet pour que les mises à jour de sécurité s'installent automatiquement et, à défaut, de télécharger les correctifs de sécurité disponibles ;
- utiliser exclusivement les sites Internet officiels des éditeurs.

3 / Bien connaître ses utilisateurs et ses prestataires

Lors de l'utilisation quotidienne de son ordinateur, on ne se sert que du compte utilisateur. Le compte administrateur, lui, n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité...).

Les systèmes d'exploitation récents permettent d'intervenir facilement sur le fonctionnement global d'une machine sans changer de compte. Le mot de passe administrateur est simplement demandé pour effectuer les manipulations désirées. Le compte administrateur permet d'effectuer d'importantes modifications sur votre ordinateur.

Au sein de l'entreprise, il est impératif de :

- réserver l'utilisation du compte administrateur au service informatique si celui-ci existe, sinon d'en protéger l'accès en n'ouvrant pour les employés que des comptes utilisateur ;
- identifier les différents utilisateurs du système et les droits qui leur sont accordés.
- supprimer les comptes anonymes et génériques (stagiaire, presse etc.), chaque utilisateur devant être identifié nommément afin de pouvoir relier une action sur le système à un utilisateur ;
- encadrer par des procédures les arrivées et les départs de personnels pour s'assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et qu'ils sont révoqués lors du départ de la personne.

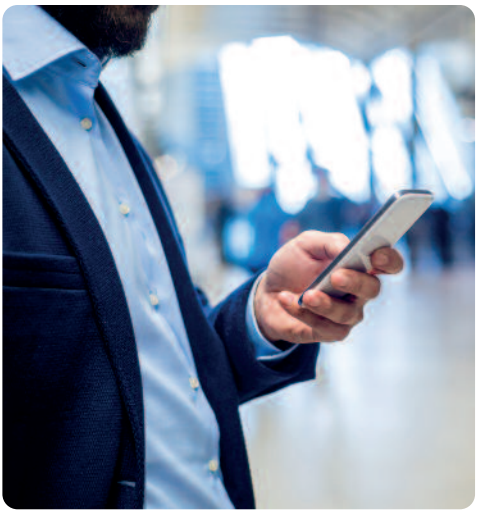
4 / Effectuer des sauvegardes régulières

Pour sauvegarder ses données, on peut utiliser des supports externes (disque dur externe réservé exclusivement à cet usage…) que l'on range ensuite dans un lieu éloigné de l'ordinateur, de préférence à l'extérieur du siège social pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur.

5 / Sécuriser l'accès Wi-Fi de votre entreprise

Un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour effectuer des opérations malveillantes. C'est pourquoi l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre professionnel : une installation filaire est plus sécurisée et plus performante. Si le Wi-Fi est le seul moyen possible d'accéder à Internet, il convient de sécuriser l'ensemble en configurant la borne d'accès à Internet, notamment en modifiant la clé de connexion par défaut par une clé (mot de passe) de plus de douze caractères de types différents.

6 / Être aussi prudent avec son ordiphone (Smartphone) ou sa tablette qu'avec son ordinateur



Les ordiphones (Smartphones) sont très peu sécurisés. Il est donc indispensable :

- n'installer que les applications nécessaires et vérifier à quelles données elles peuvent avoir accès avant de les télécharger ;
- en plus du code PIN qui protège la carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l'accès au terminal et le configurer pour qu'il se verrouille automatiquement ;
- effectuer des sauvegardes régulières des contenus sur un support externe ;
- ne pas préenregistrer les mots de passe.

7 / Protéger ses données lors de ses déplacements

Voyager avec des appareils nomades fait peser des menaces sur des informations sensibles en cas de vol ou de perte. Il convient donc de n'utiliser que du matériel dédié à la mission et ne contenant que les données nécessaires ou encore d'éviter de connecter ses équipements à des postes qui ne sont pas de confiance. Autre précaution, ne jamais utiliser les clés USB offertes lors des déplacements car elles sont susceptibles de contenir des programmes malveillants.

8 / Être prudent lors de l'utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent un rôle central dans les attaques informatiques. Des précautions sont donc à prendre :

- vérifier la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité ;
- ne pas ouvrir les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents ;
- si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer, l'adresse complète du site s'affichera dans la barre d'état du navigateur, ce qui permet d'en vérifier la cohérence ;
- ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles car il s'agit d'attaques par hameçonnage ;
- ne pas ouvrir ni relayer de messages de types alerte virale etc. ;
- désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir.

9 / Télécharger ses programmes sur les sites officiels des éditeurs

Télécharger du contenu numérique sur des sites Internet dont l'origine n'est pas assurée c'est prendre le risque d'enregistrer sur son ordinateur des programmes ne pouvant être mis à jour et qui, le plus souvent, contiennent des virus ou des chevaux de Troie.

Dans ce contexte, il est recommandé de :

- télécharger les programmes sur les sites de leurs éditeurs ou d'autres sites de confiance ;
- décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
- réfléchir avant de cliquer sur des liens sponsorisés ;
- désactiver l'ouverture automatique des documents téléchargés et de lancer une analyse antivirus avant de les ouvrir.

10 / Être vigilant lors d'un paiement sur Internet

Avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications :

- contrôler la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet ;
- s'assurer que la mention « https:// » apparaît au début de l'adresse du site Internet.
- de vérifier l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe ;
- privilégier la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ;
- ne jamais transmettre jamais le code confidentiel de sa carte bancaire.

11 / Séparer les usages personnels des usages professionnels

Il est recommandé de :

- ne pas faire suivre ses messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
- ne pas héberger des données professionnelles sur des équipements personnels ou sur des moyens personnels de stockage en ligne ;
- éviter de connecter des supports amovibles personnels aux ordinateurs de la structure professionnelle.

12 / Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Les données qu'on laisse sur Internet nous échappent instantanément. D'où la plus grande prudence dans la diffusion d'informations personnelles sur Internet. Par exemple, en décochant les cases qui autoriseraient le site à conserver ou à partager ses données ou en utilisant plusieurs adresses électroniques dédiées à ses différentes activités (sérieuses ou autres) sur Internet.

FICHE SÉCURITÉ

Sources ANSSI : www.ssi.gouv.fr/en-cas-dincident/ ▪ ATIXNET : www.atixnet.fr

Les indices pour vérifier l'authenticité d'un e-mail

INOPINÉ : vous n'avez aucune raison de recevoir un message de cet expéditeur

URGENT : une deuxième demande de paiement, un ami en détresse : les messages de phishing vous demandent souvent d'agir immédiatement.

FAUTES D'ORTHOGRAPHE : vérifiez l'adresse e-mail de l'expéditeur. En général, elle contient des fautes d'orthographe, mais ce n'est pas toujours le cas. En somme, restez vigilant !

IMAGE : vérifiez la qualité de l'image. Si le visuel ou le logo est dégradé ou erroné, ne répondez pas et ne cliquez sur aucun lien.

TITRE DE CIVILITÉ VAGUE : le titre de salutation est très général et ne mentionne pas votre nom ? En l'occurrence, il peut s'agir d'un message falsifié.

MÉTHODE DE PAIEMENT : les messages de phishing demandent souvent d'utiliser des modes de paiement inhabituels.

FICHE SÉCURITÉ

Sources ANSSI : www.ssi.gouv.fr/en-cas-dincident/ ▪ ATIXNET : www.atixnet.fr

Process en cas d'incident

Vous n'avez pas eu le temps de mettre en œuvre les règles décrites dans ce guide ou les attaquants ont réussi à les contourner. Ne cédez pas à la panique, et ayez les bons réflexes.

- **En cas de comportement inhabituel de votre ordinateur,** vous pouvez soupçonner une intrusion (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation…)
- **Déconnectez la machine du réseau / désactivez le Wi-Fi,** pour stopper l'attaque. En revanche, maintenez là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque
- **Prévenez votre service informatique**, au téléphone ou de vive voix, car l'intrus peut être capable de lire les courriels. Prenez également contact avec un prestataire informatique qui vous aidera dans la restauration de votre système ainsi que dans l'analyse de l'attaque
- **Faites faire une copie physique du disque**
- **Faites rechercher les traces disponibles liées à la compromission**. Un équipement n'étant jamais isolé dans un système d'information, des traces de sa compromission doivent exister dans d'autres équipements sur le réseau (pare-feu, routeurs, outils de détection d'intrusion, etc.)
- **Déposez une plainte** auprès de la brigade de gendarmerie ou du service de police judiciaire compétent pour le siège de la société, de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Paris et petite couronne), ou de la Direction générale de la sécurité intérieure.
- **Après l'incident : réinstallez complètement le système d'exploitation** à partir d'une version saine, supprimez tous les services inutiles, restaurez les données d'après une copie de sauvegarde non compromise, et changez tous les mots de passe du système d'information

A noter : *En cas d'infection, le support informatique sera obligé de reformater le contenu de votre disque dur. Cette opération pourrait entraîner une perte irréversible de vos données dans le cas où vous n'auriez pas sauvegardé vos données.*

FICHE SÉCURITÉ

Sources ANSSI : www.ssi.gouv.fr/en-cas-dincident/ ▪ ATIXNET : www.atixnet.fr

10 points clés pour éviter une cyberattaque : rappel des précautions

FAIRE DES SAUVEGARDES

Effectuez régulièrement une copie de secours (ou back-up) des données et informations importantes. Conservez ce back-up dans un endroit sûr et veillez à ce qu'il soit toujours déconnecté du réseau. Gardez également sur un ordinateur qui n'est pas connecté au réseau ou sur papier les informations utiles, telles que les adresses e-mail et numéros de téléphone importants, ou encore les informations sur votre fournisseur d'accès à Internet.

METTRE À JOUR LES LOGICIELS ET LES ANTIVIRUS DE VOTRE ORDINATEUR

Vous pouvez configurer votre ordinateur pour que le système d'exploitation procède automatiquement et régulièrement à une mise à jour de tous vos logiciels avec les derniers correctifs de sécurité. Effectuez des sauvegardes régulières de votre système afin de pouvoir le restaurer. Mettez à jour régulièrement vos logiciels et téléchargez les programmes uniquement sur les sites officiels des éditeurs.

PROTÉGER VOTRE SMARTPHONE AVEC UN ANTIVIRUS, SURTOUT SI VOUS LE SYNCHRONISEZ AVEC VOTRE ORDINATEUR

ÊTRE VIGILANT AVEC LES EXPÉDITEURS VOS EMAILS

Vérifier la cohérence entre l'expéditeur présumé et le contenu du message. En cas de doute sur l'émetteur : N'ouvrez pas la pièce jointe, ne cliquez pas sur les liens web. Attention : ce n'est pas parce que l'adresse de l'expéditeur est connue qu'elle n'est pas usurpée. Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles.

UTILISER DES MOTS DE PASSE FORTS ET VARIÉS

Idéalement votre mot de passe doit être de 12 caractères minimum. Il doit comprendre des caractères de type différent (ma-juscules, minuscules, chiffres, caractères spéciaux), ne pas être en lien avec vos informations personnelles (noms, dates de naissance,...) et ne pas être utilisé pour différents accès.

ÊTRE VIGILANT LES PAIEMENTS EN LIGNE

Vérifiez que le site de paiement a bien un accès https. Préférez les méthodes de paiement impliquant la réception d'un code de confirmation par sms. Ne répondez jamais à un email vous demandant de renvoyer vos informations bancaires.

PROTÉGER LES INFORMATIONS DES POSTES DE TRAVAIL EN ENTREPRISE

Naviguez jamais sur internet sur la session administrateur. Sécurisez l'accès wi-fi de l'entreprise et désactivez-le lorsqu'il n'est pas utilisé. Eteignez les ordinateurs pendant les périodes d'inactivité, nuits, week-end, vacances.
Lors de vos déplacements : désactivez les fonctions wi-fi ou bluethooth, ne laissez pas vos appareils sans surveillance dans votre hôtel par exemple. Signalez la perte ou le vol d'un matériel informatique appartenant à l'entreprise.

CARTOGRAPHIER ET SURVEILLER L'ENSEMBLE DE L'INFRASTRUCTURE ET DES RÉSEAUX

SÉPARER LES USAGES PERSONNELS DES USAGES PROFESSIONNELS

unapl
UNION NATIONALE
DES PROFESSIONS LIBÉRALES

Union Nationale des Professions Libérales
46 boulevard de la Tour-Maubourg - 75 343 PARIS cedex 07
T. 01 44 11 31 50 / F. 01 44 11 31 51
email : unapl@unapl.fr

www.unapl.fr

Sylvie Fontlupt Communication _ Crédit photos : IStock©