

Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité | Denis JACOPINI

	Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité
---	--

Pour information, Denis JACOPINI propose depuis quelques mois deux nouveaux sujets de formation à destination des chefs d'entreprise, de leurs salariés mais aussi des administrations et de leurs agents :

- **La cybercriminalité, un vrai risque pour les chefs d'entreprises- Mettre son entreprise en conformité avec la CNIL, secrets et mode d'emploi**
- **Cybercriminalité, sécurité informatique et CNIL, bonnes pratiques et cadre juridique**
- **La cybercriminalité, un vrai risque pour administrations**

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84


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 sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Règlement européen sur la protection des données : Evolution du cadre juridique

	Règlement européen sur la protection des données : Evolution du cadre juridique
---	---

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne le 4 mai 2016 et entré en application le 25 mai 2018. L'adoption de ce texte permet à l'Europe de s'adapter aux nouvelles réalités du numérique.

Un cadre juridique unifié pour l'ensemble de l'UE

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

Un champ d'application étendu

• Le critère du ciblage

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

• La responsabilité des sous-traitants

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le projet de règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

Un guichet unique : le « one stop shop »

Les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements transnationaux.

Une coopération renforcée entre autorités pour les traitements transnationaux

Toutefois, dès lors qu'un traitement sera transnational – donc qu'il concernera les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernées seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G29.

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ».

Que le CEPD soit ou non saisi, l'autorité « chef de file » portera la décision ainsi partagée par ses homologues. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».

• **Par exemple**, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'État. Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

source : CNIL



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur



Etapes à suivre
si vous comptez
rendre votre
ordinateur
professionnel à
votre employeur

Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction (sauvegarder des fichiers importants et personnelles (contacts importants, copier des fichiers et tout ce qui nous concerne (photo, pdf, CV etc..)) sur un disque dur ou un système de Cloud etc..) ?

L'ordinateur professionnel qui vous a été mis à disposition était probablement en état de marche. A moins d'avoir des circonstances ou des consignes particulières, vous devrez donc rendre cet appareil au moins dans l'état initial.

1. En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tel que les fichiers clients. On pourrait bien vous reprocher d'en avoir conservé une copie et de l'utiliser contre votre ancien employeur.
2. Identifiez les données ayant un caractère confidentiel et qui nécessiteront une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hashage.
3. Identifiez les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre...
4. Identifiez les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits enfants...)
5. Identifiez les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ça soit au bureau à la maison, en déplacement ou en vacances.

Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifiez les fonctions de « Sauvegarde », « Enregistrer sous » ou d' »Export ». Vous pourrez alors choisir le support adapté.

Enfin, en fonction des critères de sécurité choisis, vous pourrez sauvegarder sur des supports adaptée soit :

- à la confidentialité (tout support numérique en utilisant un logiciel de cryptage ou de hashage tel de Truecrypt, Veracrypt, ou AxCrypt...);
- à l'intégrité (multiplier le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à n'absolument pas perdre) ;
- à la longévité en utilisant des supports avec une durée de vie adapté à vos attentes. Sachez qu'à ce jour, il est difficile de garantir la lecture d'une informations numérique au delà de plusieurs dizaines d'années (en raison de l'altération des supports avec le temps, mais aussi de l'évolution des versions, des formations et des logiciels). Qui peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
- à la disponibilité sur plusieurs plateformes et sur plusieurs lieux, comme le proposent les solutions cloud qui sont éclos il y a quelques dizaines d'années seulement ;
- à la quantité (car vous devez rapidement stocker pour ensuite trier et choisir un support adapté) en choisissant par exemple un disque dur USB externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

Les risques

Les clés USB sont des outils permettant de conserver une copie facilement accessible et aisément transportable. 100% des clés USB tomberont un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.

Idem pour les disques durs. 100% des disques durs tomberont un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettront plus facilement de récupérer leur contenu en cas de panne.

Les supports de type lecteurs ZIP, lecteur JAZ, lecteurs magnéto-optiques, lecteurs de bandes etc. sont de plus en plus rares. Conserver des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginez un instant jour ou vous souhaitez y accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vies de vos données numériques entre les mains du bon coin...

Voilà, en fonction de tous ces critères et à partir de ces conseils, il ne vous reste plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Comparatif

Disque dur : Quelques Go à quelques To – Bon marché Rapide mais fragile

Clé USB : Quelques Go – Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.

Cloud : Quelques Mo à quelques To – Accessible de n'importe où mais aussi par tous ceux qui ont le mot de passe (risqué) – Dépend du fonctionnement et de la rapidité d'Internet – Les services de cloud gratuits peuvent s'arrêter du jour au lendemain et vous perdrez tout.

Disques optiques (CD, DVD, Magnéto Optique) : Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (pérennité des lecteurs de disques) jusqu'à quand ?

Supports spéciaux (ZIP/Jazz/QIC/DAT/DLT/DOS/SDLT) : Supports fragiles, lecteurs trop rares pour garantir une lecture au delà de 5 ans.

Denis JACOPINI anime des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux CyberRisques.

Il est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant a une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

<http://www.lenetexpert.fr/contact>

<https://twitter.com/lenetexpert>

<https://www.linkedin.com/in/lenetexpert>

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, pièges, fraudes, attaques Internet...) et judiciaires (investigation téléphones, disques durs, e-mails, contenus, échantillonnage de données...);

- Expertises de systèmes de vote électronique ;

- Formations et conférences en cybercriminalité ;

- Formation de C.I.L. (Correspondants Informatique et Liberté) ;

- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Supprimer vos données personnelles avant de donner ou recycler un ordi – FrancoisCharron.com

Huit lois en dix ans pour encadrer le Web français | Denis JACOPINI



Huit lois en dix ans pour encadrer le Web français

<p>Le Net Expert</p> <p>Le Net Expert est une entreprise spécialisée dans la conception, la mise en œuvre et la maintenance de solutions informatiques. Elle propose des services de conseil, de développement, de maintenance et de support technique. Elle est agréée par le Ministère de l'Intérieur et dispose d'une certification ISO 9001.</p> <p>Le Net Expert</p> <p>Le Net Expert est une entreprise spécialisée dans la conception, la mise en œuvre et la maintenance de solutions informatiques. Elle propose des services de conseil, de développement, de maintenance et de support technique. Elle est agréée par le Ministère de l'Intérieur et dispose d'une certification ISO 9001.</p> <p>Le Net Expert</p> <p>Le Net Expert est une entreprise spécialisée dans la conception, la mise en œuvre et la maintenance de solutions informatiques. Elle propose des services de conseil, de développement, de maintenance et de support technique. Elle est agréée par le Ministère de l'Intérieur et dispose d'une certification ISO 9001.</p>	<p>Le Net Expert</p> <p>Le Net Expert est une entreprise spécialisée dans la conception, la mise en œuvre et la maintenance de solutions informatiques. Elle propose des services de conseil, de développement, de maintenance et de support technique. Elle est agréée par le Ministère de l'Intérieur et dispose d'une certification ISO 9001.</p> <p>Le Net Expert</p> <p>Le Net Expert est une entreprise spécialisée dans la conception, la mise en œuvre et la maintenance de solutions informatiques. Elle propose des services de conseil, de développement, de maintenance et de support technique. Elle est agréée par le Ministère de l'Intérieur et dispose d'une certification ISO 9001.</p> <p>Le Net Expert</p> <p>Le Net Expert est une entreprise spécialisée dans la conception, la mise en œuvre et la maintenance de solutions informatiques. Elle propose des services de conseil, de développement, de maintenance et de support technique. Elle est agréée par le Ministère de l'Intérieur et dispose d'une certification ISO 9001.</p>
---	---

52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois

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

LE NET EXPERT
AUDITS & EXPERTISES

LE NET EXPERT
EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES

LE NET EXPERT
MISES EN CONFORMITÉ

LE NET EXPERT
SPY DETECTION
Services de détection de logiciels espions

LE NET EXPERT
FORMATIONS

LE NET EXPERT
ARNAQUES & PIRATAGES

Denis JACOPINI

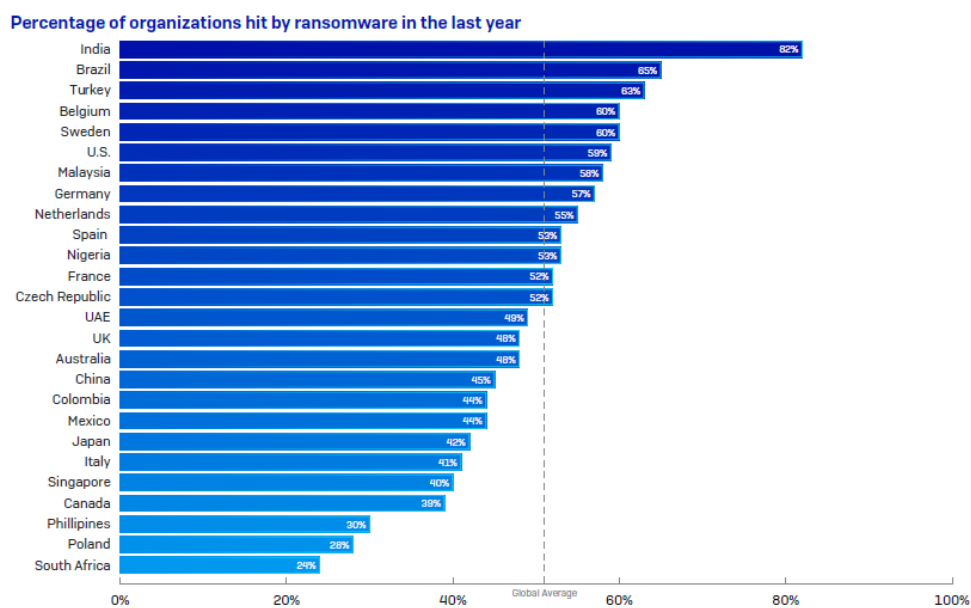
vous informe

SPAM : GARE AUX ARNAQUES !

vous informe

52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois

En France, 52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois. Elles étaient 48 % en 2019. Le coût moyen d'une attaque par rançongiciel est de 420 000 euros en dehors de la rançon exigée. Ce montant prend en compte les temps d'arrêt, la perte de chiffre d'affaires et les coûts opérationnels. En cas de paiement de la rançon, cette somme double.



LA CLÉ DE CHIFFREMENT N'EST PAS UNE SOLUTION MIRACLE

« Les entreprises se sentent parfois sous pression pour payer la rançon afin d'éviter les temps d'arrêt préjudiciables. À première vue, effectuer le paiement de la rançon semble être une manière efficace de restaurer les données, mais ce n'est qu'illusoire (...) En effet, une simple clé de chiffrement n'est pas un remède miracle et il faut souvent bien plus pour restaurer les données », a expliqué Chester

Wisniewski, Principal Research Scientist chez Sophos.

En France, plus de la moitié (61%) des responsables IT interrogés déclarent avoir pu restaurer leurs données à partir de sauvegardes sans payer la rançon. Dans 2 % de cas, le paiement de la rançon n'a pas permis de restaurer les données. À l'échelle mondiale, ce chiffre s'élève à 5 % pour les organisations du secteur public.

...[lire la suite]

Commentaire de notre Expert : Denis JACOPINI

La demande de rançon est la résultante dans la quasi totalité des cas de l'ouverture d'une pièce jointe à e-mail piégé ou le clic sur un lien aboutissant sur un site Internet piégé.

Les conséquences

Il n'est plus à rappeler qu'être victime d'un ransomware entraînent un arrêt de l'outil informatique, une perte de productivité et une dégradation de la réputation auprès des clients et partenaires.

Les solutions

Nous le répéterons jamais assez, les seuls moyens d'empêcher ce type de situation sont l'utilisations d'outils de filtrage et la sensibilisation. N'hésitez pas à nous contacter pour l'organisation de sessions de sensibilisation auprès de vos équipes pour leur apprendre à détecter e-mails et sites Internet malveillants, en quasi totalité à l'origine des rançongiciels dans les systèmes informatiques.

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

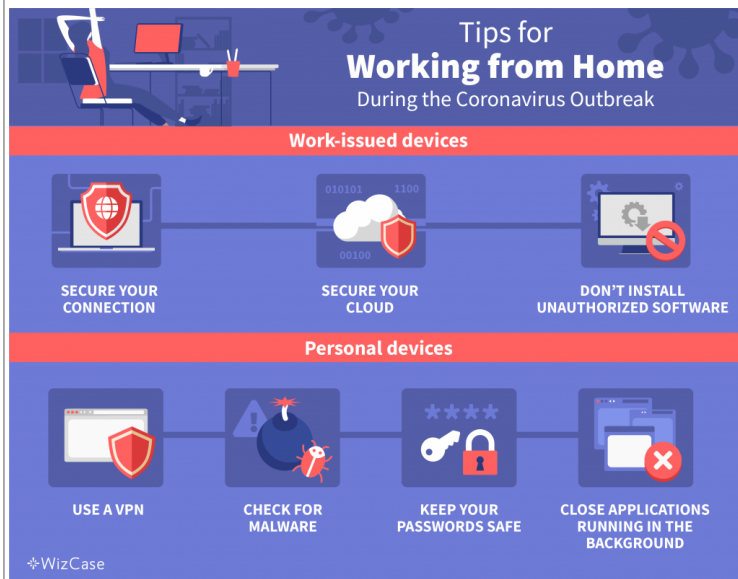
Source : Etude : Payer la rançon multiplie par deux le coût total d'un ransomware

Pour ceux qui continuent le travail à domicile, respectez les cybergestes barrière

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
					
 VOUS INFORME		<p>Pour ceux qui continuent le travail à domicile, respectez les cybergestes barrière</p>			

Alors que la pandémie mondiale continue à se propager parmi les populations, plusieurs pays ont fermé leurs frontières et suggéraient aux entreprises de recourir au travail à distance. Même si les risques de contagion sont quasiment inexistantes, d'autres précautions et des cybergestes barrière sont à respecter.

Restez en sécurité



Comme vous ne savez peut-être pas dans quelle mesure votre environnement de travail assure la sécurité de vos informations, vous risquez de devenir une cible facile pour les hackers une fois que vous serez en confinement ou que vous travaillez à domicile.

Appareils & Équipements de travail

Si vous utilisez un ordinateur de bureau ou un appareil mobile fourni par l'entreprise, il est fort probable que vous soyez déjà muni de quelques éléments de base pour vous protéger. En tant que propriétaire ou dirigeant d'entreprise, vous devrez également vous assurer que les mesures suivantes soient en place pour votre équipe.

1. Sécurisez votre connexion

Si vous n'êtes pas encore installé, demandez à votre responsable informatique de vous fournir un VPN. Il vous aidera à sécuriser votre activité professionnelle. Le wifi public – que vous utilisiez un hotspot local ou que vous partagiez un réseau avec votre voisin – est plus vulnérable que votre propre réseau privé, mais un VPN vous protégera des menaces sur les deux.

2. Sécurisez votre Cloud

Disposer d'une solution de sécurité premium pour le Cloud (CASB) permet de limiter l'accès à vos données dans le Cloud aux seuls membres autorisés de l'équipe.

3. N'installez pas de logiciels non autorisés

Si vous avez apporté votre ordinateur portable de travail à la maison, n'installez aucun logiciel qui ne soit pas lié au travail et n'utilisez pas de clés USB sans être sûr de ce qu'elles contiennent.

Appareils personnels

Mélanger le travail et le plaisir ? Dans certains cas, vous n'avez pas vraiment le choix.

1. Vérifier la présence des malwares

Vérifiez que votre logiciel antivirus est à jour et recherchez tout logiciel malveillant sur votre ordinateur ou votre téléphone portable personnel.

2. Protéger les mots de passe

Utiliser un gestionnaire de mots de passe pour se tenir au courant des meilleures pratiques d'utilisation des différents mots de passe sur le web.

3. Utiliser un VPN

Comme nous l'avons déjà mentionné, un VPN conservera vos informations cryptées pendant toute la durée du confinement – et vous aurez en plus la possibilité d'accéder à l'ensemble de la bibliothèque Netflix dans le monde entier une fois votre journée de travail terminée.

4. Fermer les applications fonctionnant en arrière-plan

N'utilisez pas de logiciels ou d'applications qui ne sont pas en rapport avec le travail, y compris en les laissant s'exécuter en arrière-plan. Évitez également de télécharger de nouvelles applications qui ne sont pas liées au travail pendant cette période.

5. Ne pas enregistrer vos données sans autorisation

Lorsque vous travaillez sur votre ordinateur personnel, évitez de sauvegarder vos données professionnelles, à l'exception de ce qui est absolument nécessaire pour travailler.

6. Garder les choses séparées

Si vous utilisez un ordinateur partagé, créez un espace de travail séparé. Créez un nouvel utilisateur pour l'ordinateur, si possible. Sinon, créez une nouvelle session de navigation avec vos informations spécifiques au travail et pour le travail uniquement – et n'oubliez pas de vous déconnecter à chaque fois !

[L'article complet de l'auteur Chase Williams]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *5 idées pour travailler à domicile pendant l'épidémie de coronavirus*

« Vous avez été en contact avec une personne testée positive au Covid-19 » : Attention aux arnaques sur les smartphones



	<p>« Vous avez été en contact avec une personne testée positive au Covid-19 » : Attention aux arnaques sur les smartphones</p>
---	--

MÉFIEZ-VOUS ! – La crise sanitaire liée à la pandémie est perçue comme une opportunité par les pirates informatiques qui jouent sur les craintes et les angoisses des citoyens pour les piéger. Attention donc si vous recevez des messages liés au Covid-19 sur votre téléphone.

A l'approche de la levée du confinement, profitant de l'inquiétude qui règne au sein de la population, les pirates informatiques agissent, multipliant fraudes et arnaques sur le web, notamment à travers la pratique de l'hameçonnage (ou « phishing » en anglais), particulièrement lucrative. Pour rappel, cette technique consiste à « piéger » une personne en le poussant à cliquer sur un lien dans le but d'installer un logiciel malveillant sur son appareil ou de collecter ses informations personnelles. ...[lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : « Vous avez été en contact avec une personne testée positive au Covid-19 » : attention aux arnaques sur les smartphones | LCI

Le prestataire informatique responsable en cas de perte de données par un cryptovirus

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI vous informe		Le prestataire informatique responsable en cas de perte de données par un cryptovirus			

Un arrêt de la Cour d'Appel de Paris, dans un litige entre un prestataire de maintenance et son client, vient rappeler qu'un virus ou un ransomware ne constituent pas un cas de force majeure permettant d'exonérer qui que ce soit de ses obligations.

Le litige est né en 2016 mais la Cour d'Appel de Paris vient de le juger après une décision de première instance du tribunal de commerce en janvier 2018. Si l'affaire est assez complexe et avec de nombreuses ramifications sur la responsabilité et les manquements de chaque partie, un point particulier mérite d'être relevé. En l'occurrence, un crypto-virus a rendu inexploitable les sauvegardes et les données de l'entreprise cliente, problème de plus en plus fréquent de nos jours. Le prestataire a voulu faire considérer ce fait comme une circonstance de force majeure l'exonérant de sa responsabilité. La Cour d'Appel vient rappeler qu'un virus n'est aucunement un cas de force majeure (Cour d'appel de Paris, Pôle 5 – chambre 11, 7 février 2020, affaire n° 18/03616, non-publié)...[lire la suite]

Commentaire de notre Expert : Denis JACOPINI

Il est évident qu'à partir du moment où un prestataire informatique vend un service de sauvegarde et assure d'une quelconque manière sa maintenance, il devient responsable de la réalisation de cette prestation, quelles qu'en soient les conditions excepté dans des situations appelés cas de force majeure.

En droit, les conditions de la force majeure évoluent au gré de la jurisprudence et de la doctrine. Traditionnellement, l'événement doit être « imprévisible, irrésistible et extérieur » pour constituer un cas de force majeure. Cette conception classique est cependant remise en cause (Wikipédia).

Dans la vraie vie, la situation dans laquelle s'est produit la perte de données doit être vue d'un peu plus près. Il n'y a pas à mon avis un cas de figure mais des cas de figure et les situations doivent être étudiées au cas par cas (chers avocats, je suis à votre disposition).

Certes, il est vrai, que le cryptovirus puisse être considéré comme imprévisible et extérieur, mais l'article 1218 du Code Civil précise :

« Il y a force majeure en matière contractuelle lorsqu'un événement échappant au contrôle du débiteur, qui ne pouvait être raisonnablement prévu lors de la conclusion du contrat et dont les effets ne peuvent être évités par des mesures appropriées, empêche l'exécution de son obligation par le débiteur »

C'est là que la balance du mauvais côté pour le prestataire informatique. Depuis 1989, date du premier cryptovirus (PC Cyborg) et pour être un peu plus gentil, depuis 2017, année durant laquelle le nombre de cas de rançongiciels a explosé de plusieurs centaines de pourcents, les cryptovirus sont prévisibles et les effets peuvent être évités par des mesures appropriées.

Ainsi, mesdames et messieurs les prestataires informatiques, mesdames et messieurs les chefs d'entreprises, je ne peux que vous recommander de faire auditer techniquement et juridiquement vos services de sauvegarde afin d'en analyser les risques résiduels car seule une analyse de risques permettra non seulement d'avoir une visibilité technique complète de votre services, mais vous pourrez également adapter vos contrats au résultat de cette dernière et convenir avec vos clients de l'existence ou non de cas pour lesquels la panne de votre système de sauvegarde sera « éligible » au cas de force majeure.

Intéressé par la réalisation d'un tel audit ?

N'hésitez pas à me contacter.

Denis JACOPINI (Expert informatique près les tribunaux diplômé en Cybercriminalité, Gestion des risques et Investigation Numérique)

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Justice : Un virus n'est pas un cas de force majeure*
– *Le Monde Informatique*

Une faille informatique concernant un milliard d'appareils connectés en Wi-Fi découverte !





D'après les chercheurs à l'origine de cette découverte, la vulnérabilité se trouverait dans les puces Wi-Fi fabriquées par Cypress Semiconductor et Broadcom. Parmi les appareils touchés, nous retrouvons les iPhone, iPad, Mac, ou les enceintes Echo d'Amazon, la Kindle, les appareils Android, ou encore le Raspberry Pi 3. D'après la société Eset, la faille affecterait principalement les puces WLAN FullMAC de Cypress et Broadcom. Pour information, les chercheurs ont nommé cette faille Kr00k.

Les chercheurs de l'Eset précisent que : *"cette faille de sécurité est gigantesque puisqu'un hacker peut déchiffrer des données qui ont été transmises par un point d'accès Wi-Fi vulnérable, sur près d'un milliard d'appareils"*. En réalité, **Kr00k exploite une faiblesse** qui se produit lorsque les appareils sans fil se dissocient d'un point d'accès sans fil. Plutôt que de chiffrer les données avec une clé pré-définie et utilisée lors de la connexion, les appareils vulnérables **utilisent une clé composée de zéros**, ce qui rend le déchiffrement très facile...[lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

[Les 10 conseils pour ne pas se faire «hacker» pendant l'été](#)
[Les meilleurs conseils pour choisir vos mots de passe](#)

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Un milliard d'appareils connectés en Wi-Fi touchés par une faille*

Des pirates informatiques profitent du coronavirus pour vous piéger et vous infecter avec un virus

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES	 LE NET EXPERT MISES EN CONFORMITÉ	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI EXPERT INFORMATIQUE ASSERMENTÉ SPÉCIALISÉ EN CYBERCRIMINALITÉ vous informe		Des pirates informatiques profitent du coronavirus pour vous piéger et vous infecter avec un virus			

Les courriels – qui circulent principalement en Asie pour le moment – prétendent contenir de l’information légitime au sujet du coronavirus.

Le destinataire est invité à cliquer sur une pièce jointe pour obtenir plus d’information. Ceux qui tombent dans le piège permettent involontairement aux pirates d’avoir accès à leurs documents personnels.

IBM dit qu’on s’attend à «voir circuler davantage de courriels malveillants inspirés par le coronavirus dans le futur, alors que l’infection se propagera. Cela se produira probablement aussi dans d’autres langues».

Les pirates informatiques exploitent régulièrement l’actualité et les craintes de la population pour sévir. «Une telle stratégie permet de berner plus de victimes pour qu’elles cliquent des liens malveillants ou ouvrent des fichiers malveillants, accroissant ultimement l’efficacité de la campagne malveillante», peut-on lire dans le rapport...[lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

[Les 10 conseils pour ne pas se faire «hacker» pendant l’été](#)

[Les meilleurs conseils pour choisir vos mots de passe](#)

[Victime d’un piratage informatique, quelles sont les bonnes pratiques ?](#)

[Victime d’usurpation d’identité sur facebook, tweeter ? Portez plainte mais d’après quel article de loi ?](#)

[Attaques informatiques : comment les repérer ?](#)

[block id="24760" title="Pied de page BAS"]

Source : *Des pirates informatiques profitent du coronavirus pour répandre un logiciel malveillant | HuffPost Québec*