HTTP/2 : une évolution importante du protocole du web, notamment pour les mobiles | Denis JACOPINI

	#HTTP/2 : une évolution importante du protocole du web, notamment pour les mobiles

Le protocole HTTP a 20 ans. On a récemment parlé de son évolution HTTP/2 avec la possibilité de chiffrer systématiquement les échanges sur le web, mais cela va bien au-delà et pourrait constituer une évolution importante, notamment pour les mobiles.

Le protocole HTTP, support historique du web avec le langage HTML, a été inventé par Tim Berners-Lee il y a maintenant 20 ans. On a récemment parlé de son évolution HTTP/2, notamment dans le contexte d'un possible chiffrement systématique des échanges entre navigateurs et serveurs, après les affaires d'écoutes illégales des communications Internet révélées par Edward Snowden. Pour autant, cette amélioration à venir de HTTP va bien au-delà et pourrait constituer une étape de progrès importante pour le web, notamment depuis les mobiles.
Vous avez peut-être lu récemment des articles sur HTTP/2, dans le contexte d'une volonté de sécurisation accrue des échanges de données sur le web. Mais comme l'explique #Mark Notthingham, responsable du groupe de travail HTTP/2 à l'IETF – #Internet Engineering Task Force – les attentes de la communauté du web vont au-delà, et les évolutions prévues sont plus larges.

Mark Notthingham, responsable du groupe de travail HTTP/2 à l'IETF

Car cela fait maintenant 20 ans que le protocole HTTP – #HyperText Transfer Protocol – a été inventé, et depuis les versions HTTP/1.0 en mai 1996 et #HTTP/1.1 en janvier 1997 il n'a plus évolué. Dans le même temps l'Internet s'est diffusé massivement dans le grand public et en entreprise, et en moins de deux décennies on est passé de connexions téléphoniques à 56 kb/s à des dizaines de Mb/s sur des liaisons DSL ou fibre optique, et la part du trafic Internet réalisés par des smartphones, tablettes et terminaux mobiles de toute sortes a explosé.
Afin de pallier les limitations de HTTP, Google a mené ses propres travaux, dévoilant #SPDY en 2012. Cette proposition visait essentiellement à réduire le temps de chargement des pages web en priorisant les contenus nécessaires à leur affichage et en multiplexant leur transfert au sein d'une seule connexion TCP. Ces travaux ont inspiré l'IETF qui a repris cette approche dans un cadre plus global d'amélioration des performances du web.
Faisons donc le point sur les axes d'évolution du protocole HTTP, en listant les principaux apports techniques de HTTP/2.

Conserver les mêmes API
La compatibilité ascendante est primordiale, compte tenu de nombre colossal de services qui ont été développées au-dessus du protocole HTTP : on ne saurait exiger des développeurs de logiciels utilisant HTTP qu'ils retouchent leur code, parfois embarqué dans des systèmes matériels, pour l'adapter. Les mêmes méthodes (GET, PUT, POST etc), les mêmes entêtes et les mêmes statuts et code d'erreur (le fameux 404 et tous les autres) seront conservés inchangés, et il suffira de remplacer une bibliothèque de fonctions HTTP/1.1 par une bibliothèque HTTP/2 pour que le logiciel qui l'utilise soit compatible.

Rendre les requêtes moins coûteuses
HTTP est un protocole coûteux en ressources réseaux, notamment parce que les entêtes de messages sont verbeux. C'est pénalisant pour l'échange de courtes informations, et ça l'est encore plus pour les mobiles : même si les débits ont été fortement accrus avec la 3G puis la 4G, tout ce qui contribue à optimiser la bande passante des réseaux mobiles et bénéfique. Pour cela, http va utiliser un mécanisme de « multiplexage » qui permettra l'échange de plusieurs messages simultanément, et non plus séquentiellement. De surcroît, les entêtes seront systématiquement compressés.

Optimiser les connexions TCP avec les serveurs
Alors qu'aujourd'hui HTTP permet d'ouvrir plusieurs connexions TCP parallèles et simultanées vers un serveur, ce qui peut créer de la congestion sur le réseau, HTTP/2 permettra de regrouper les échanges avec un même serveur au sein d'une seule et même connexion TCP. Là encore, ce sera bénéfique pour les réseaux mobiles.

Pré-remplir le cache des navigateurs
Un mécanisme de « cache pushing » permettra à un serveur d'envoyer des informations à un client pour un usage ultérieur. Ainsi il ne sera plus nécessaire à un navigateur web de demander d'abord le contenu d'une page HTML, puis les feuilles de style CSS référencées par la page : le serveur pourra envoyer le HTML et les CSS d'un seul coup, évitant un dialogue inutile entre le navigateur et le serveur. Le logiciel client pourra évidemment débrayer ce mécanisme si nécessaire.

Interrompre une connexion TCP sans la fermer
Avec HTTP, si un logiciel client envoie une requête et décide de ne plus attendre la réponse, la seule façon de préserve la bande passante est de fermer la connexion TCP. Il n'y a aucune façon de la récupérer si cela s'avère nécessaire plus tard.

Avec HTTP/2, un logiciel client pourra maintenir active une connexion TCP même s'il abandonne un échange en cours à la suite d'une action de l'utilisateur, ce qui rendra moins coûteuse en ressources réseaux une éventuelle reprise du dialogue ultérieurement.

Faciliter le chiffrement des échanges
C'est là le point qui a le plus attiré l'attention sur HTTP/2, et qui n'a peut-être pas été bien compris : la nouvelle version du protocole ne rendra pas obligatoire l'utilisation du chiffrement #TLS, sur lequel repose le chiffrement #SSL entre sites web et navigateurs. En revanche, ses performances accrues réduiront l'impact négatif du chiffrement sur la rapidité de réponse d'un site telle que la perçoivent les utilisateurs.

En rendant le chiffrement des communications plus performant, HTTP/2 pourra contribuer à rendre le web plus sûr pour ses utilisateurs, tant vis-à-vis de la cybercriminalité que d'États qui, on le voit aujourd'hui, n'hésitent pas à espionner massivement les internautes de toutes nationalités. Pour autant, au regard des moyens technologiques colossaux dont s'est dotée la NSA, il ne faudrait pas croire en une sécurité absolue d'un tel chiffrement…

Pour autant, HTTP/2 n'est pas magique
On l'a vu, HTTP/2 apporte de nombreuses évolutions positives. Mais il n'aura pas d'impact magique sur les sites web : afin d'en tirer le meilleur, les évolutions des navigateurs web, et aussi des logiciels serveurs web, devront être faites en prenant en compte différents scénarios d'usage. En effet, s'ils sont mal utilisés, des mécanismes tels que le pré-remplissage du cache du navigateur ou le maintien de sessions TCP inactives pourraient aller à l'encontre du but recherché : l'amélioration globale de la performance du web.

Et ensuite, HTTP/3 ?
HTTP existe depuis 20 ans : sa simplicité et sa versatilité ont permis l'incroyable développement du web que l'on connaît aujourd'hui. Le développement de HTTP/2 a été très compliqué, notamment parce qu'un grand nombre de matériels ont été conçus dans l'idée que HTTP ne changerait jamais. Une fois la transition de HTTP à HTTP/2 lancée, les choses seront différentes, et de futures nouvelles versions pourront être introduites plus facilement.

Parmi des évolutions déjà envisagées, certaines n'ont pas été intégrées dans HTTP/2 pour ne pas retarder encore sa sortie. Sont notamment prévus l'envoi au client de certificats TLS et d'entrées DNS. Des problèmes non encore résolus par HTTP/2 pourront l'être dans une version future, mais cela devrait être marginal, car la communauté est confiante dans HTTP/2, au vu des premiers tests de déploiement déjà réalisés. L'objectif de tous est maintenant qu'il sorte rapidement et commence à être déployé.

Les résultats des travaux de l'IETF sur les spécifications techniques de HTTP/2 sont publics. Le draft 10 (http://tools.ietf.org/html/draft-ietf-httpbis-http2-10) peut être consulté et va être discuté durant une période de 6 mois prenant fin en août 2014.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/http-2-une-evolution-importante-du-protocole-du-web-notamment-pour-les-mobiles-39798198.htm
par Pierre Col

Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)

Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.

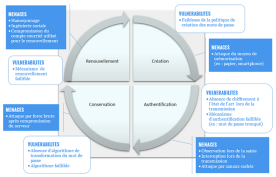
Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)

Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.

Basée sur la gestion d'un secret, l'authentification par identifiant et mot de passe est un moyen simple et peu coûteux à déployer pour contrôler un accès.
Toutefois, cette méthode d'authentification présente un niveau de sécurité faible.
Ces dernières années, de nombreuses attaques informatiques ont entrainé la compromission de bases de données entières de comptes et des mots de passe associés. Ces fuites de données ont notamment contribué à enrichir les connaissances des attaquants en matière de mots de passe. Les risques de compromission des comptes associés à cette méthode d'authentification se sont fortement accrus et imposent une vigilance particulière.

Les risques liés à la gestion des mots de passe sont multiples et reposent notamment sur :
1. la simplicité du mot de passe ;
2. l'écoute sur le réseau afin de collecter les mots de passe transmis ;
3. la conservation en clair du mot de passe ;
4. la faiblesse des modalités de renouvellement du mot de passe en cas d'oubli (cas des questions « secrètes »).

Les principaux risques identifiés au cours du cycle de vie d'un mot de passe



Il n'existe pas de définition universelle d'un bon mot de passe, mais sa complexité et sa longueur permettent de diminuer le risque de réussite d'une attaque informatique qui consisterait à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères. Lorsque la taille du mot de passe diminue, des mesures compensatoires doivent être prévues.

PHRASE2PASSE : UN OUTIL POUR ACCOMPAGNER LES UTILISATEURS

Pour aider les utilisateurs à choisir un mot de passe robuste et un moyen mnémotechnique, la CNIL a développé un outil pour générer un mot de passe à partir d'une phrase.
Le code de cet outil est disponible sous la forme d'une extension logicielle en javascript, afin que vous puissiez l'intégrer dans vos applications.
>Télécharger l'extension

Les exigences de la CNIL

1.

L'authentification par mot de passe : longueur, complexité, mesures complémentaires

Les exigences minimales de la CNIL en termes de taille et de complexité du mot de passe varient en fonction des mesures complémentaires mises en place pour fiabiliser le processus d'authentification : ainsi, si une authentification est basée exclusivement sur un mot de passe, cela implique a minima l'utilisation d'un mot de passe complexe d'au moins 12 caractères composé de majuscules de minuscules, de chiffres et de caractères spéciaux. Des mesures complémentaires à la saisie d'un mot de passe (restrictions, d'accès, collecte d'autres donnée, support détenu en propre par l'utilisateur) permettent de réduire la longueur et la complexité du mot de passe, car ces mesures permettent d'assurer un niveau de sécurité équivalent au mot de passe seul.

Le tableau ci-dessous fait état des 4 cas d'authentification par mot de passe identifiés par la CNIL dans sa recommandation

	Exemple d'utilisation	Longueur minimum	Composition du mot de passe	Mesures complémentaires
Mot de passe seul	FORUM, BLOG	12	• majuscules • minuscules • chiffres • caractères spéciaux	Conseiller l'utilisateur sur un bon mot de passe
Avec restriction d'accès (le plus répandu)	SITES DE E-COMMERCE, COMPTE D'ENTREPRISE, WEBMAIL	8	Au moins 3 des 4 types suivants : • majuscules • minuscules • chiffres • caractères spéciaux	Blocage des tentatives multiples : (exemples) • Temporisation d'accès au compte après plusieurs échecs • « Capcha » • Verrouillage du compte après 10 échecs
Avec information complémentaire	BANQUE EN LIGNE	5	Chiffres et/ou lettres	Blocage des tentatives multiples + • Information complémentaire communiquée en propre d'une taille d'au moins 7 caractères (ex : identifiant dédié au service) **ou** • Identification du terminal de l'usager (ex : adresse IP, adresse MAC…)
Avec matériel détenu par la personne	CARTE BANCAIRE OU TÉLÉPHONE	4	Chiffres	Matériel détenu en propre par la personne (ex : carte SIM, carte bancaire, certificat) + Blocage au bout de 3 tentatives échouées

Dans tous les cas,
le mot de passe ne doit pas être communiqué à l'utilisateur en clair par courrier électronique.
Ces exigences sont des règles minimales. Le contrôle d'accès peut devoir reposer sur des règles plus robustes selon les risques auxquels le système est exposé.

2.

Sécurisation de l'authentification

Quelles que soient les mesures mises en place, la fonction d'authentification doit être sûre :
• elle utilise un algorithme public réputé fort ;
• sa mise en œuvre logicielle est exempte de vulnérabilité connue.
Lorsque l'authentification n'a pas lieu en local, l'identité du serveur doit être contrôlée au moyen d'un certificat d'authentification de serveur et le canal de communication entre le serveur authentifié et le client doit être chiffré à l'aide d'une fonction de chiffrement sûre. La sécurité des clés privées doit être assurée.

3.

La conservation des mots de passe

Le mot de passe ne doit jamais être stocké en clair. Il doit être transformé au moyen d'une fonction cryptographique non-réversible et sûre, intégrant l'utilisation d'un sel ou d'une clé.
Le sel ou la clé doit être généré au moyen d'un générateur de nombre pseudo-aléatoires cryptographiquement sûr (il utilise un algorithme public réputé fort et sa mise en œuvre logicielle est exempte de vulnérabilité connue). Il ne doit pas être stocké dans le même espace de stockage que l'élément de vérification du mot de passe.

4.

Le renouvellement du mot de passe

Renouvellement périodique

Le responsable de traitement veille à imposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable, qui dépend notamment de la complexité imposée du mot de passe, des données traitées et des risques auxquels il est exposé.
La personne concernée doit être en mesure de changer elle-même son mot de passe. Dans ce cas, les règles afférentes à la création de mots de passe s'appliquent.

Renouvellement sur demande

À la demande de la personne concernée, par exemple en cas d'oubli, le responsable de traitement met en œuvre une procédure de renouvellement du mot de passe.
Si ce renouvellement nécessite l'intervention d'un administrateur, un mot de passe temporaire est attribué à la personne concernée, le changement du mot de passe attribué temporairement lui est imposé lors de sa première connexion.
Si ce renouvellement intervient de manière automatique : le mot de passe ne doit pas être transmis en clair. L'utilisateur doit être redirigé vers une interface dont la validité ne doit pas excéder 24 heures, lui permettant de saisir un nouveau mot de passe, et ne permettre qu'un seul renouvellement.
Si le renouvellement fait intervenir un ou plusieurs éléments supplémentaires (numéro de téléphone, adresse postale…) :
• ces éléments ne doivent pas être conservés dans le même espace de stockage que l'élément de vérification du mot de passe ; sinon, ils doivent être conservés sous forme chiffrée à l'aide d'un algorithme public réputé fort, et la sécurité de la clé de chiffrement doit être assurée ;
• afin de prévenir les tentatives d'usurpation s'appuyant sur le changement de ces éléments, la personne doit être immédiatement informée de leur changement.

Que faire en cas de risque de compromission du mot de passe ?

Si un responsable de traitement de données détecte une violation de données en rapport avec le mot de passe d'une personne,
• Le responsable de traitement doit notifier la personne concernée, dans un délai n'excédant pas 72 heures ;
• Il doit imposer à l'utilisateur concerné le changement de son mot de passe lors de sa prochaine connexion ;
• Il doit lui recommander de veiller à changer ses mots de passe d'autres services dans l'hypothèse où il aurait utilisé le même mot de passe pour ceux-ci.
Faites-nous par de vos remarques
Les professionnels sont invités à remonter à la CNIL les difficultés de mise en œuvre que pourrait poser l'application de cette recommandation. Cette recommandation pourra faire l'objet de révisions et de mises à jour.

Texte officiel

> Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe
…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».
• Audits Sécurité (ISO 27005) ;
• Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
• Expertises de systèmes de vote électronique ;
• Formations et conférences en cybercriminalité ;
(Autorisation de la DIRECCTE n°93 84 03041 84)
• Formation de C.I.L. (Correspondants Informatique et Libertés) ;
• Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité
Contactez-nous

Réagissez à cet article

Hotspot Shield le logiciel VPN pour Windows MacOs IOS Android Apple Samsung pour accéder de manière sécurisée à un Wifi public | Denis JACOPINI

	#Hotspot Shield le #logiciel VPN pour Windows MacOs IOS Android Apple Samsung pour accéder de manière sécurisée à un Wifi public

En période de vacances ou lors de déplacements professionnels, nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants… En juillet 2015, nous vous avions publié un article « Est-il risqué de se connecter au wifi public ? » pour vous informer des principaux risques à partager ces accès sans fil à internet avec d'autres. Cette fois, nous allons parler des solutions pour surfer sécurisé en utilisant les réseaux Wifi publics.

RAPPEL DU PRINCIPAL RISQUE

Un pirate peut se connecter tout aussi facilement que vous sur un réseau Wifi Public et espionner les données qui y transitent.
Il peut ainsi, en fonction des données qu'il récupère, accéder à toutes les informations qui sortent et qui entrent de votre ordinateur (le protocole tcp/ip n'étant pas protégé par défaut).

LA SOLUTION ?

Utiliser une connexion Wifi qui sera cryptée au moyen d'un logiciel VPN (ce ctyptage n'a aucun rapport avec les clés Wifi) .
La connexion Wifi ainsi créée étant crypté, toutes les informations qui véhiculeront (identifiants, adresses email, mots de passe, numéros de cartes bancaires…) seront illisibles pour tous les pirates qui seront connectés sur le mêle point d'accès wifi.

Vous pouvez certes partager la connexion 3G ou 4G de votre smartphone, mais l'utilisation d'un logiciel VPN est recommandé.
Un logiciel « VPN » (Virtual Private Network) est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais elle est du coup sécurisée.

Nous utilisons régulièrement un logiciel VPN #HotSpotShield. C'est un logiciel qui coûte moins de 25 euros et qui vous rendra les connections Wifi publiques sécurisées.
HotSpot Shield existe pour Windows pour protéger par un logiciel VPN les connexions Wifi des ordinateurs assemblés, Acer, Asus, IBM, Dell ;
HotSpot Shield existe aussi pour MacOs X Lion pour protéger par un logiciel VPN les connexions Wifi des ordinateurs Apple ;
HotSpot Shield existe aussi pour Android pour protéger par un logiciel VPN les connexions Wifi des smartphones Samsung, HTC, Archos, LG, Acer, Wiko, Sony, Asus, Alcatel, ZTE… ;
Enfin, HotSpot Shield existe aussi pour IOs pour protéger par un logiciel VPN les connexions Wifi des smartphones Apple.

Téléchargez et testez gratuitement HotSpot Shield

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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

RGPD et Vidéosurveillance dans les écoles : Comment éviter d’être épinglé par la CNIL

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

RGPD et Vidéosurveillance dans les écoles : Comment éviter d’être épinglé par la CNIL

Épinglée en début de semaine pour avoir surveillé ses étudiants en continu, l'école parisienne Itic veut se conformer aux exigences de la Cnil, l'autorité de protection des données personnelles.

Un établissement supérieur parisien épinglé par l'autorité de protection des données personnelles, la Cnil, pour une vidéosurveillance permanente de ses classes va se mettre en conformité avec les demandes de l'autorité. «Si on nous dit qu'il faut enlever les caméras, on le fera», a expliqué Roger Hagege, cofondateur de l'Institut des techniques informatiques et commerciales (Itic), à l'AFP. «Je veux qu'ils (la Cnil) nous expliquent à quel moment» le besoin de sécurité «s'arrête» face à la nécessité de respecter la vie privée. «Je veux connaître cette limite et je me conformerai à la limite que va nous accorder la Cnil», poursuit-il…[lire la suite]

Denis JACOPINI vous informe :

Pour sécuriser les accès et éviter les incidents, des caméras sont installées dans les établissements scolaires pour filmer les couloirs, les halls d'entrées, mais aussi la rue. Ces dispositifs doivent respecter différentes règles afin de ne pas porter atteinte à la vie privée des personnes filmées.
Quelles sont ces règles ? Quelles précautions prendre ?

Dans quel but ?

Des caméras peuvent être installées à l'intérieur d'un établissement à des fins de sécurité des biens et des personnes (lutte contre les violences entre élèves, les dégradations sur les portes ou murs, les vols, etc). Des caméras peuvent également filmer l'extérieur de l'établissement afin de renforcer la sécurité de ses abords (prévention d'actes de terrorisme).

Quelles précautions prendre lors de l'installation du dispositif ?

Les caméras peuvent filmer les accès de l'établissement (entrées et sorties) et les espaces de circulation. Il est exclu, sauf cas exceptionnels, de filmer les lieux de vie des établissements (cour de récréation, préau, salle de classe, cantine, foyer, etc.) pendant les heures d'ouverture de l'établissement : les élèves comme les enseignants et les autres personnels de l'établissement ont droit au respect de leur vie privée.
La sécurisation des biens et des personnes peut être obtenue par la mise en œuvre de moyens moins intrusifs. L'utilisation de caméras doit rester limitée et constituer un moyen complémentaire à d'autres mesures de sécurité. Seules des circonstances exceptionnelles (établissements scolaires victimes d'actes de malveillance fréquents et répétés) justifient de filmer les élèves et les enseignants en continu.
Dans une école maternelle ou élémentaire, c'est la commune qui décidera, ou non, d'installer des caméras.
La CNIL recommande aux chefs d'établissements concernés d'adopter une « charte d'utilisation de la vidéosurveillance » en impliquant l'ensemble des acteurs (administration, personnel, représentants des parents d'élèves).

Pour compléter votre article, les recommandations de la CNIL sont accessibles sur :
https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_etablissements_scolaires.pdf

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

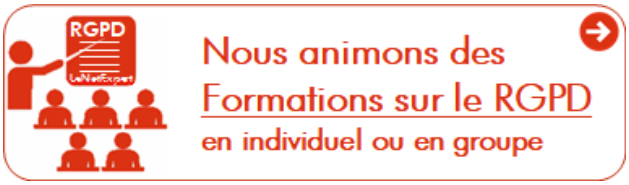
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

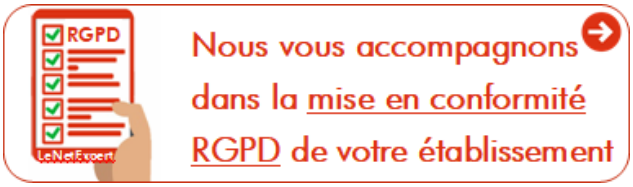
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Source : *Vidéosurveillance : l'école épinglée par la Cnil se mettra en conformité – Le Figaro Etudiant*

Denis JACOPINI interviewé par une journaliste de Ouest France | Denis JACOPINI

Est-il risqué de se connecter au wifi public ?
Nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants… Mais y a-t-il un risque à partager ces accès sans fil à internet avec d'autres ? Peut-on se faire pirater ses données ? Le point avec Denis Jacopini, expert en cybercriminalité.

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français).
Résultat, on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en sécurité informatique, nous explique pourquoi.

Denis Jacopini, créateur du site LeNetExpert.fr et correspondant Cnil (Commission nationale de l'informatique et des libertés), est aussi formateur en protection des données personnelles et en sécurité informatique. (Photo : DR)

À quoi faut-il faire attention, quand on se connecte à une borne wifi publique ou semi-publique, en ville ou dans un hôtel ?
Si possible, il faut choisir un réseau wifi où la connexion se fait avec un nom d'identifiant et un mot de passe personnalisés, différents pour chaque utilisateur. En cas d'utilisation malveillante du réseau par quelqu'un, cette identification fournit une piste, sur le plan judiciaire, pour remonter jusqu'à l'auteur. Avec les wifi qui proposent un identifiant et un mot de passe identiques pour tout le monde, on est moins protégé. Les réseaux wifi les plus dangereux sont ceux qui sont complètement ouverts, sans aucun mot de passe, où les utilisateurs sont impossibles à tracer.

Quel est le danger ? Se faire espionner ?
Tout à fait. À partir du moment où quelqu'un se trouve connecté au même point wifi que vous, il a techniquement la possibilité d'accéder aux informations qui transitent sur le réseau, il peut « voir » ce qui entre et qui sort. Les pirates utilisent pour cela des logiciels espions, appelés « sniffers », ou « renifleurs » en bon français. Ces programmes sont désormais très faciles à trouver et à télécharger sur internet. Plus ou moins sophistiqués, ils permettent de capter, trier et interpréter le « bruit » informatique qui transite par le wifi.

Le wifi public, c'est pratique, mais pas très sécurisé. (Photo : FlickR/Richard Summers)

La confidentialité de la navigation n'est donc pas garantie ?
En effet. Et pas uniquement sur les réseaux wifi, d'ailleurs. C'est ainsi depuis la création d'internet : les protocoles de communication du web ne sont pas cryptés. Mais de plus en plus de sites « sensibles » – par exemple les messageries électroniques, les banques, les boutiques en ligne, etc. – ont désormais des adresses commençant par « https » au lieu de « http ». Le « s », souvent associé avec un petit cadenas dans la barre du navigateur, signifie que les communications sont sécurisées. Quand on navigue sur internet via un wifi, il faut donc privilégier ces sites.

Le risque de se faire voler ses mots de passe, ou ses coordonnées bancaires, est donc bien réel ?
Oui, mieux vaut éviter de saisir des données confidentielles quand on navigue sur internet via un wifi public ou semi-public. On a ainsi vu des hommes d'affaires se faire voler des informations importantes, car ils utilisaient en toute confiance un wifi d'hôtel… sur lequel étaient aussi connectés des pirates !

Un café Starbucks à Londres, très apprécié pour sa connexion wifi gratuite. (Photo : Stefan Wermuth/Reuters)

Peut-on se faire abuser par une fausse borne wifi ?
Oui, c'est une raison supplémentaire de se méfier des réseaux complètement ouverts : certains pirates créent leur propre borne wifi à partir d'un simple ordinateur portable. Les passants se connectent dessus, par facilité, sans se douter qu'il ne s'agit pas du tout d'une « vraie » borne. Ensuite, la personne mal intentionnée n'a plus qu'à récupérer les informations qui transitent par le réseau qu'elle a créé… Aujourd'hui, c'est très facile de devenir pirate !

Comment se protéger ?
En s'abstenant de réaliser des opérations sensibles, comme des achats en ligne ou des opérations bancaires, sur un wifi public. Si on le peut, mieux vaut utiliser le réseau 3G ou 4G pour se connecter à internet en mobilité. Les informations qui transitent par cette voie sont beaucoup moins faciles à pirater. Il y a aussi la solution consistant à installer, sur son smartphone ou son ordinateur, ce qu'on appelle un « VPN ». C'est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais c'est beaucoup plus sûr.

Zone de wifi gratuit à New York : en France comme à l'étranger, mieux vaut se connecter sur un nom de réseau connu, éventuellement signalé via l'affichage public. (Photo : Keith Bedford/Reuters)

[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 : http://www.ouest-france.fr/leditiondusoir/data/492/reader/reader.html?t=1431534138729#!preferred/1/package/492/pub/493/page/7
Par Corinne Bourbeillon

Arnaques par courriel (scam, phishing) : la CNIL peut-elle agir ? | Denis JACOPINI

Arnaques par courriel (scam, phishing) : la CNIL peut-elle agir ?

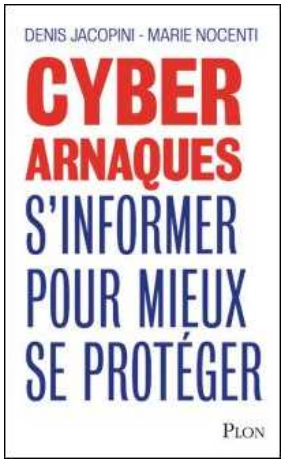
Ces procédés ne sont pas liés à la protection des données personnelles : ce sont des tentatives d'escroquerie ou d'extorsion de fonds.

Si vous en êtes victime, signalez-les sur le service PHAROS du ministère de l'Intérieur (http://www.internet-signalement.gouv.fr) et au service phishing-initiative (http://www.phishing-initiative.com) mis en place par plusieurs acteurs de l'internet.

Vous pouvez également joindre par téléphone le service Info Escroquerie de la police nationale au 0811 02 02 17 (coût d'un appel local).

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

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



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

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

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

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

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

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

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

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : *CNIL Besoin d'aide ? – Arnaques par courriel (scam, phishing) : la CNIL peut-elle agir ?*

Est-ce utile de protéger la

WebCam et le microphone de son ordinateur avec de l'adhésif ? | Denis JACOPINI

Cela peut sembler absurde, mais c'est une mesure de précaution élémentaire, probablement conseillée par la direction en charge de la sécurité de Facebook, sur tous les ordinateurs portables susceptibles d'être attaqués.

En 2013, des chercheurs en sécurité informatique de l'université John Hopkins, aux Etats-Unis, avaient démontré qu'il était possible de prendre le contrôle des webcams des Mac, ce qui est aussi chose fréquente sur les PC.
La firme Symantec avait même alerté, la même année, sur ce qu'elle désignait comme des « creepwares »,« Certaines personnes mettent un morceau d'adhésif sur la webcam de leur portable, peut-être vous-mêmes le faites. Sont-elles trop prudentes, paranoïaques, un peu étranges ? (…)
Beaucoup d'entre nous ont entendu des histoires de gens qui étaient espionnés sur leur ordinateur (…). Mais ces histoires sont-elles vraies et les précautions prises par des gens en apparence paranoïaques sont elles justifiées ? Malheureusement la réponse est oui », écrivait alors Symantec.
L'éditeur a même publié une vidéo de prévention :
Source Numerama

[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"]

Original de l'article mis en page : Pourquoi Mark Zuckerberg met du scotch sur la webcam et le micro de son Mac — Tech — Numerama

---

Combien de temps doivent être conservées les données utilisées pour le suivi du temps de travail ? | Denis JACOPINI

Combien de temps doivent être conservées les données utilisées pour le suivi du temps de travail ?

Les éléments relatifs à l'identification des salariés et les données utilisées pour le suivi du temps de travail, y compris les données relatives aux motifs des absences, ne peuvent pas être conservés plus de 5 ans après le départ des employés.

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

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=0245F4689A67B389E322EB9815FEF32B?name=Contr%C3%B4le+des+horaires+%3A+combien+de+temps+sont+conserv%C3%A9es+les+donn%C3%A9es+%3F&id=365

Quelles précautions prendre avant de fermer la messagerie professionnelle d'un employé ? | Denis JACOPINI

Quelles précautions prendre avant de fermer la messagerie professionnelle d'un employé ?

La CNIL recommande à l'employeur d'avertir l'employé de la date de fermeture de sa messagerie afin que ce dernier puisse faire le tri et transférer ses messages privés vers sa messagerie personnelle.

Une fois que l'employé a quitté l'organisme, l'employeur doit supprimer son adresse électronique nominative.
La CNIL invite les employeurs à définir, en concertation avec les représentants des personnels, des chartes d'utilisation des outils informatiques.

Réagissez à cet article

Source : *CNIL Besoin d'aide ? – Messagerie professionnelle : quelles précautions avant de fermer le compte d'un employé ?*

Quelles sont les mentions obligatoires sur un site internet ? | Denis JACOPINI

Quelles sont les #mentions obligatoires sur un site internet ?

Tous les sites internet édités à titre professionnel, qu'ils proposent des ventes en ligne ou non, doivent obligatoirement indiquer les mentions légales suivantes :

• pour un entrepreneur individuel : nom, prénom, domicile
• pour une société : raison sociale, forme juridique, adresse de l'établissement ou du siège social (et non pas une simple boîte postale), montant du capital social
• adresse de courrier électronique et numéro de téléphone
• pour une activité commerciale : numéro d'inscription au registre du commerce et des sociétés (RCS)
• pour une activité artisanale : numéro d'immatriculation au répertoire des métiers (RM)
• numéro individuel d'identification fiscale : numéro de TVA intracommunautaire
• pour une profession réglementée : référence aux règles professionnelles applicables et au titre professionnel
• nom et adresse de l'autorité ayant délivré l'autorisation d'exercer quand celle-ci est nécessaire
• nom du responsable de la publication
• coordonnées de l'hébergeur du site : nom, dénomination ou raison sociale, adresse et numéro de téléphone
• pour un site marchand, conditions générales de vente (CGV) : prix (exprimé en euros et TTC), frais et date de livraison, modalité de paiement, service après-vente, droit de rétractation, durée de l'offre, coût de la technique de communication à distance
• numéro de déclaration simplifiée Cnil, dans le cas de collecte de données sur les clients

Avant de déposer ou lire un cookie, les éditeurs de sites ou d'applications doivent :
• informer les internautes de la finalité des cookies,
• obtenir leur consentement,
• fournir aux internautes un moyen de les refuser.
La durée de validité de ce consentement est de 13 mois maximum. Certains cookies sont cependant dispensés du recueil de ce consentement.

Le manquement à l'une de ces obligations peut être sanctionné jusqu'à un an d'emprisonnement, 75 000 € d'amende pour les personnes physiques et 375 000 € pour les personnes morales.
Remarque : Depuis l'entrée en application du RGPD, Règlement Général sur la Protection des Données), vous devez également prévoir des mentions relatives à la protection des données à caractère Personnel ainsi que prévoir des précautions relatives à la demande de consentement des internautes à utiliser leurs coordonnées.
Consultez notre dossier consacré à la demande de consentement

---

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
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

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://vosdroits.service-public.fr/professionnels-entreprises/F31228.xhtml