

Un technique d'attaque informatique très répandue : Le « Watering Hole » | Denis JACOPINI

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



Un technique d'attaque informatique très répandue : Le « Watering Hole »

Les motivations des attaquants sont diverses. Les plus répandues sont le gain financier, la gloire personnelle, la malveillance ou encore l'espionnage. Quelle que soit la finalité de l'attaque, cette dernière passe le plus souvent par la compromission d'un système. Pour parvenir à leur fin, les attaquants disposent d'un large arsenal comprenant le contournement des mécanismes de sécurité, l'accès physique à la machine ou encore l'exploitation de vulnérabilités. Au sein de cet arsenal, l'exploitation de vulnérabilités constitue sans aucun doute le principal vecteur d'intrusion. Les méthodes d'infection employées peuvent alors prendre différentes formes : • Infection par média amovible (CD, USB, cartes SD, ...)

- Infection par e-mail (pièce jointe ou un lien malicieux notamment)
- Infection via le réseau interne (fichiers partagés)
- Infection par visite d'un site Web

Le « Watering Hole » fait partie de la dernière catégorie : « Infection par site Web », autrement appelé « Drive-By Download ». Cette dernière repose sur le principe suivant :

1. Création ou compromission d'un site Web par l'attaquant (accès à l'interface d'administration, compromission des régies publicitaires pour injecter du code au sein des publicités affichées, découverte d'une vulnérabilité de type XSS...)
2. Dépôt du malware sur le site (Ex : code JavaScript obfusqué s'exécutant au chargement de la page, iframe contenant un ActiveX ou un applet Java malicieux hébergé sur un autre site, ...)
3. Compromission de la machine cliente. La victime est incitée à se rendre ou redirigée de manière automatique sur le site Web hébergeant le malware. Son navigateur exécute le code malicieux et un malware est installé à son insu sur son poste de travail ou son Smartphone, très souvent de manière transparente. L'attaquant dispose alors d'un accès partiel ou complet sur l'appareil infecté.

Simple attaque de type « Drive-by Download » ?

La subtilité de cette attaque réside dans le choix des sites Web initialement compromis (cf étape 1). En effet, en fonction de la cible, le choix est principalement réalisé en fonction de la localité de l'entité ciblée ou en lien avec son métier.

Plusieurs cas concrets récents peuvent être cités en exemple :

- Professionnel : (politique/religieux/syndical...) Dans le cas d'Apple, de Microsoft ou de Facebook en février dernier, le site Web compromis était un site Web consacré au développement sur iPhone (iphoneDevSDK), site susceptible d'être visité par les développeurs des trois sociétés. La population cible peut également être plus restreinte comme l'illustre la compromission du site « <http://www.rferl.org> (Radio Free Europe Radio Liberty) ».
- Géographique : En Septembre 2012 lors de l'attaque VOHO[1], les cybercriminels avaient compromis un site gouvernemental local au Maryland, celui d'une banque régionale dans le Massachusetts afin de compromettre les machines de populations spécifiques résidant ou travaillant dans les localités ciblées.
- Et pourquoi pas Personnel : Il est tout à fait possible de voir le site du club de sport ou de musique où les enfants de la victime sont inscrits, être compromis...

Pourquoi utiliser cette méthode plutôt qu'une autre ?

En comparaison de l'envoi de phishing par exemple, cette méthode présente de nombreux avantages pour les attaquants : watering hole – scalable

Scalable :

Elle permet de couvrir un grand nombre de victimes « facilement ». Le « Drive-By Download » est largement utilisé dans le domaine de la #cybercriminalité permettant de compromettre un très grand nombre de machines rapidement ;

L'exploitation de vulnérabilités Java ou Adobe Flash récentes, peuvent permettre de contourner les mécanismes de cloisonnement au sein des navigateurs Web et ainsi de couvrir de nombreux systèmes d'exploitation et navigateurs Web vulnérables différents

Efficace :

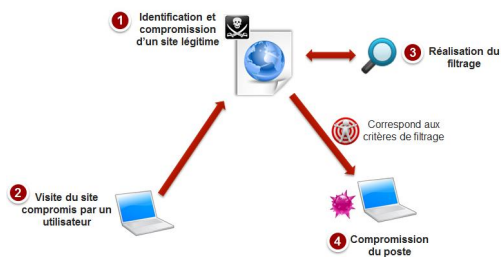
Couplée avec l'exploitation d'une vulnérabilité de type « 0-day », le taux d'infection peut être très élevé. Le rapport sur la campagne « VOHO »[2] publié par RSA et portant sur des attaques par « Watering Hole » recensait 32 160 machines infectées appartenant à 731 organisations pour un taux d'infection de 12%.

Discret :

Aucune action de l'utilisateur n'est nécessaire si ce n'est d'aller visiter ses sites Web habituels. L'absence de signaux rend également l'identification de la source de l'infection difficile. Enfin, la possibilité de filtrer les postes infectés (classe IP, langue du navigateur, localité ...) permet de restreindre les dommages collatéraux et donc de limiter la visibilité de l'attaque.

Cette méthode présente cependant un certain nombre d'inconvénients :

- Potentiellement, une phase de reconnaissance, consistant à identifier sur quels sites se rendent les futures victimes
- Une phase de compromission de sites légitimes est nécessaire : les attaquants peuvent cependant identifier les sites vulnérables via des scans automatisés.
- Les attaquants doivent réaliser une analyse post-infection afin de déterminer, pour chaque poste compromis, quel type de profil a été infecté et si le profil correspond à la cible (société, fonction, ...)



A noter que le filtrage effectué afin de réduire le périmètre des postes compromis émerge également au sein des attaques par phishing.

Quels sont les mécanismes de défense ?

Face à ce type de menace, il n'existe pas de solution « miracle ». Il convient donc d'appliquer des bonnes pratiques afin de limiter les risques d'infection et d'être réactif en cas de compromission :

1. [Mise à jour du parc] – On constate que les vulnérabilités exploitées sont le plus souvent liées aux technologies Java ou à Adobe Flash. A minima, il convient de maintenir à jour le parc applicatif. Cependant, cette mesure peut ne pas être suffisante (cas des 0-day). Nous recommandons donc de les désinstaller lorsqu'ils ne sont pas nécessaires.
2. [Filtrage Web] – Mettre à jour régulièrement et au besoin manuellement les sites connus comme hébergeant des malwares au sein des listes noires des équipements de filtrage Web (nécessite de disposer d'un service de veille). De manière plus radicale, il est envisageable d'imposer la navigation Web pour des populations sensibles depuis des postes séparés du reste du réseau de l'entreprise.
3. [Durcissement des postes] – Des mécanismes de contournement peuvent également être mis en place. Pour Java par exemple, il est possible de configurer le niveau de sécurité sur « high » de manière à n'exécuter les applets non signés qu'après validation manuelle de l'utilisateur. Des mesures similaires peuvent être appliquées sur le plug-in Flash. Il est aussi possible de pousser des plugins comme « NoScript » afin d'interdire l'exécution de code JavaScript, Flash, Java ...

Conclusion

La compromission par « Watering Hole » partage les mêmes objectifs que par « spear-phishing » et la même méthode d'infection que les attaques par « Drive-by download ».

Cette combinaison est ainsi surtout utilisée pour des attaques cherchant à s'introduire au sein d'une organisation, quel que soient les postes compromis.

Avec le temps et grâce aux campagnes de sensibilisations, les utilisateurs et en particulier les populations VIP sont de plus en plus précautionneuses quant à l'ouverture des pièces jointes aux courriels. Les attaques par « Spear-phishing » sont ainsi complétées par des attaques de type « Watering-Hole » qui ne nécessitent aucune action de la part de la victime si ce n'est de visiter ses sites Web habituels...

Réagissez à cet article

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

Denis JACOPINI Marie Nocenti (Plon) ISBN :
2259264220



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site

Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : <http://www.lexsi-leblog.fr/cert/watering-hole-et-cybercriminalite.html>

Pourquoi ne pas partager l'avertissement mettant en garde contre le pirate Jayden K. Smith ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Pourquoi ne pas partager l'avertissement mettant en garde contre le pirate Jayden K. Smith ?				

Depuis le début du mois de juillet, un hoax (canular) circule sur Facebook. Il a été traduit de l'anglais et te met en garde contre un hacker nommé Jayden K. Smith. Pas de panique, c'est une mise en garde totalement fausse. Alors ignore le message, n'accepte rien et surtout, ne le repartage pas! C'est un peu soûlant.

« S'il te plaît dis à tous tes contacts de ta liste messenger de ne pas accepter la demande d'amitié de Jayden K. Smith. C'est un hacker et a un système connecté à votre compte facebook. Si un de tes contacts l'accepte, tu seras aussi piraté, aussi assures toi que tous tes contacts le sachent. Merci. Retransmis tel que reçu. Gardes ton doigt appuyé sur le message. En bas, au milieu il sera dit transmettre. Appuyer dessus et cliquer sur les noms qui sont sur ta liste et cela leur sera envoyé. »

Voilà le message que vous avez peut-être reçu ce matin via Messenger. Il s'agit d'une nouvelle chaîne totalement infondée, comme l'ont fait remarquer certains médias outre-Atlantique. Le message est juste une traduction d'un texte en anglais qui est devenu viral un peu partout dans le monde la semaine dernière...[lire la suite]

L'avis de notre Expert Denis JACOPINI

Même s'il nous paraît difficile de pirater un compte Facebook par une simple lecture ou une demande d'ami, nous recommandons de ne pas partager ce message et de simplement le supprimer ou l'ignorer.

Ces canulars peuvent aussi bien prendre la forme d'un faux virus, d'une chaîne de solidarité (comme ici), d'un gain hypothétique, d'une pétition ou d'une fausse information destinée à influencer l'opinion publique.

Vous pouvez aisément comprendre que les intérêts ne sont pas tous dans un but de vous arnaquer ou vous soutirer de l'argent. Certains auteurs de ces chaînes recherchent la fierté d'avoir leur message qui fait le tour de la planète, d'autres de saturer les réseaux avec des messages inutiles mais les plus dangereux sont ceux qui vous demandent de cliquer ou de partager.

Même si je suis certains que vous êtes vigilants lorsqu'on vous demande de télécharger ou d'exécuter un programme, vous l'êtes certainement bien moins lorsque vous partagez un message à vos amis. L'expéditeur peut du coup disposer et utiliser de manière malveillante des informations sur eux.

Réagissez à cet article

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

Denis JACOPINI Marie Nocenti (Plon) ISBN :
2259264220



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site

Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : *Ne partage pas cet avertissement qui te met en garde contre le pirate Jayden K. Smith, c'est un hoax*

La CNIL a-t-elle une copie des fichiers qui lui sont déclarés ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	La CNIL a-t-elle une copie des fichiers qui lui sont déclarés ?				

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations [ici](https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd) : <https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd> Nous l'avons toutefois laissée accessible non pas

par nostalgie mais à titre d'information.

La CNIL a-t-elle une copie des fichiers qui lui sont déclarés ?

Non, la CNIL ne détient pas le contenu des fichiers qui lui sont déclarés. En revanche, la CNIL dispose de la liste des fichiers qui lui sont déclarés par les organismes qui les mettent en oeuvre. Ainsi, elle connaît leur existence et leurs principales caractéristiques (nom du responsable, finalité du fichier, type de données traitées, catégories de destinataires, service auprès duquel exercer ses droits).

Cette liste des fichiers déclarés est aussi appelée le « fichier des fichiers ».

Remarque :

Depuis le 25 mai 2018, il n'est plus nécessaire de réaliser de formalités préalables auprès de la CNIL pour les traitements de Données à Caractères Personnel non sensibles. Cependant, une formalité est toujours nécessaire si vous manipulez des Données à Caractères Personnel sensibles.

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.



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)

Réagissez à cet article

Source :
<https://cnil.epticahosting.com/selfcnil/site/template.do?id=498&back=true>

Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

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



Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

« Mes documents » est un terme générique. C'est encore une fois la mention « Personnel » qui permet de protéger un dossier ou un fichier. L'employeur ne peut donc pas en faire état, au risque d'avoir à payer des dommages et intérêts à son salarié. »

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.



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)

Réagissez à cet article

Source : *Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord*

Comment réagir en cas de chantage à la webcam ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Comment réagir en cas de chantage à la webcam ?				

L'arnaque à la webcam touche chaque année des milliers de victimes. Cette série de conseils vous aidera à adopter les bonnes pratiques si vous devez faire face à ce type de chantage.

A quoi ressemble un cas typique de chantage à la webcam ?
La victime se rend sur un site de rencontre puis entame la conversation avec une jeune femme ou un jeune homme au physique attrayant. Après lui avoir posé quelques questions sur sa vie privée, cette personne l'invite à approfondir les échanges via une conversation vidéo plus intime. Quelque temps plus tard, un courriel ou un message Facebook apprendra à la victime que cette rencontre a été enregistrée. Le cyber-escroc menace de diffuser la vidéo de cet échange sur le compte Facebook d'un proche ou sur un site de partage de vidéos si la victime ne lui remet pas la somme de 200 euros sous 24h/48h.

Quel réflexe adopter ?

- 1. Ne répondez surtout pas à un cyber-escroc**
Soyez parfaitement hermétique à toute tentative de chantage : ne communiquez aucune donnée personnelle, ne versez surtout pas d'argent quelle que soit la somme demandée.
- 2. Verrouillez immédiatement vos comptes sociaux**
Paramétrez vos comptes sociaux professionnellement et vos comptes Facebook de manière à ce que le malfaiteur n'associe pas votre nom à une liste d'amis / de contacts. Ne rendez accessible votre profil Facebook qu'àuprès de vos amis de confiance. Enfin, ne publiez rien de personnel sur votre mur. Des personnes mal intentionnées peuvent détourner ces informations à d'autres fins. Notre page Facebook délivre quelques conseils pour bien paramétrer vos comptes.
- 3. Alertez les autorités via la plateforme du Ministère de l'Intérieur**
 - Effectuez des captures d'écran justifiant votre situation (messages reçus, contenus à effacer...). Voir la fiche pratique
 - Signalez directement l'escroquerie sur la plateforme www.internet-signalement.gouv.fr
 - Appelez le service Info Escroqueries au 8833 62 62 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile ; Du lundi au vendredi de 9h à 18h)
- 4. Parlez-en à une personne de confiance**
La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. Il est conseillé d'en parler avec une personne de confiance. ☑ Vous êtes mineur ? Des télé-conseillers sont gratuitement à votre écoute au 0800 200 800 de 9h à 19h en semaine. Voir le site Net écoute
- 5. Informez vos amis de l'escroquerie**
Veillez à informer discrètement les personnes susceptibles d'être sollicitées par le cyber-escroc en mentionnant brièvement que vous êtes victime d'une escroquerie en ligne et qu'il ne faut ni ouvrir, ni partager, ni répondre à une éventuelle sollicitation provenant d'un inconnu.
- 6. Effectuez régulièrement des recherches à votre nom**
Vous pouvez par exemple programmer une alerte à votre nom qui vous enverra un message sur votre messagerie électronique dès qu'un contenu associé à votre nom est mis en ligne. Certains services existent ici ou là.

Si la vidéo a été diffusée –

- 7. Demandez systématiquement au site de dépublier le contenu gênant**
Exemple : si la vidéo a été mise en ligne sur YouTube : demandez à YouTube de supprimer cette vidéo. Si le site ne répond pas à votre demande sous deux mois, adressez vous à la CNIL en suivant la procédure de notre formulaire de plainte en ligne.
- 8. En parallèle, demandez au moteur de recherche de déréférencer le contenu en cause**
Depuis un récent arrêt de la cour de justice européenne, les internautes peuvent saisir les moteurs de recherche d'une demande de déréférencement d'un contenu associé à leurs nom et prénom. Le droit au déréférencement ☑
- 9. D'autres solutions existent**
Vous pouvez créer rapidement des contenus valorisants associés à votre nom et donc bien référencés. Il peut s'agir d'un blog consacré à une passion ou d'une page de curation de contenus (outil qui permet de sélectionner, éditer et partager des pages/liens web sur un sujet précis). Attention à ne pas communiquer d'éléments personnels.
- 10. Faire appel à une agence spécialisée**
Certains cas peuvent nécessiter l'intervention d'une agence spécialisée dans l'effacement de contenus gênants. Soyez néanmoins vigilant sur les compétences vantées dans l'annonce. N'hésitez pas à vous rendre sur des forums pour vous renseigner sur la réputation de ces agences.

Réagissez à cet article

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

Denis JACOPINI Marie Nocenti (Plon) ISBN :
2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaqes 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'arnaqes 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'arnaqes Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

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

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

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

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

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

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

Original de l'article remis en page : Réagir en cas de chantage à la webcam | CNIL

10 règles d'or pour se rendre visible sur les réseaux sociaux | Denis JACOPINI

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



10 règles
d'or pour se
rendre
visible sur
les réseaux
sociaux

[Redacted]

[Redacted]

[Redacted]

Pour promouvoir votre nouvelle activité, votre nouveau produit ou travailler votre image, les réseaux sociaux représentent une solution efficace. Mais comment les rendre encore plus performants en jouant sur votre visibilité ?

Assurez votre présence

Votre présence sur les réseaux sociaux pertinents reste indissociable d'une vie professionnelle réussie. À savoir, les plus courants sont Facebook, Twitter, LinkedIn, Viadeo et Google+.

Soignez votre marque

Il ne suffit pas uniquement de s'inscrire, tenez toujours à jour votre profil afin qu'il reflète bien votre identité et image de marque. Qui dit soigner sa marque, dit soigner son e-réputation et son identité numérique. Maîtriser son e-réputation est souvent difficile, mais continuer à véhiculer une bonne image de soi sur les réseaux sociaux garantit un bon écho sur le web.

Ciblez vos « amis »

Comme toute forme de publicité, les réseaux sociaux facilitent la création d'un carnet d'adresses à travers des recherches par mot-clé. Avec eux, trouver des groupes qui traitent de votre thématique ou des influenceurs, devient plus facile. Les rassembler dans votre cercle constitue un avantage et reste une bonne tactique pour monter en puissance sur les réseaux sociaux.

Demandez des recommandations

Demander une recommandation venant d'un client satisfait n'est pas une honte. Les réseaux sociaux offrent cette possibilité-là et représente une opportunité à saisir pour rester influent. De même, si vous êtes satisfait d'un service d'un de vos fournisseurs, faites-le savoir sur ses réseaux. Cela jouera également en votre faveur.

Soyez dynamique

Publiez une actualité et rajoutez-y quelques avis, participez à un hub, créez un événement et invitez votre entourage à y participer... Non seulement, vous animerez votre page, mais vous créerez à coup sûr du « buzz » autour de vous, favorable pour augmenter votre visibilité.

Utilisez des mots-clés

Pour chacune de vos publications, choisissez un ou quelques mots-clés pertinents. Un hashtag permet, lors d'une recherche, de trouver rapidement des personnes parlant du même sujet. Son utilisation vous mettra en relation avec ces personnes.

Humanisez votre présence

Être actif sur les réseaux sociaux est une chose, mais savoir cibler les informations à diffuser en est une autre. La présence sur ces réseaux est chronophage et demande de la patience, à l'instar du réseau physique. Triez les informations à partager de manière à viser vos cibles, et surtout parlez de ce qu'ils attendent de vous.

Soyez réactif

Une question qui se pose, des commentaires qui pourraient vous concerner, un message à votre intention ou des avis défavorables sur votre entreprise ? Réagissez dans la minute qui suit la publication. Vous gagnerez ainsi en présence, mais aussi en visibilité.

Gérez votre temps

Consacrez chaque jour, un petit créneau pour « écouter » les autres. Cela peut se manifester par l'envoi d'un message privé, ou par un petit commentaire sur leur page, ou un partage de leur publication. Montrez-leur que vous êtes attentif à leur égard.

Choisissez le bon moment

Prenez le temps d'analyser les heures où les visites sont nombreuses (par le nombre de publications par exemple) et choisissez ce moment-là pour poster vos articles et commentaires. Cela ne sert à rien de communiquer tard le soir ou tôt le matin ! Privilégiez plutôt le milieu de la matinée.

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

- **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition*

l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



[Contactez-nous](#)



Denis JACOPINI et Julien COURBET vont parler du livre « CYBERARNAQUES S'informer pour mieux se protéger » ce jeudi sur C8 dans l'émission « C'est que de la télé! »

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

x

x

x

x

x

x


x

Denis JACOPINI et Julien COURBET vont parler du livre « CYBERARNAQUES S'informer pour mieux se protéger » ce jeudi sur C8 dans l'émission « C'est que de la télé! »

Internet et les réseaux sociaux ont envahi notre quotidien, pour le meilleur mais aussi pour le pire... Qui n'a jamais reçu de propositions commerciales pour de célèbres marques de luxe à prix cassés, un email d'appel au secours d'un ami en vacances à l'autre bout du monde ayant besoin d'argent ou un mot des impôts informant qu'une somme substantielle reste à rembourser contre la communication de coordonnées bancaires ? La Toile est devenue en quelques années le champ d'action privilégié d'escrocs en tout genre à l'affût de notre manque de vigilance. Leur force ? Notre ignorance des dangers du Net et notre « naïveté » face aux offres trop alléchantes qui nous assaillent.

« Puisse cet ouvrage avoir de nombreux lecteurs ! Il ne devrait pas plaire aux arnaqueurs, car il est un réquisitoire contre leur perfidie et, sans aucun doute, une entrave à leur chiffre d'affaire. »

Général d'armée (2S) Watin- Augouard

Denis JACOPIN et Julien COURBET en parlent en parle ce jeudi sur C8 dans l'émission « C'est que de la télé! ». <https://www.mycanal.fr/chaines/c8>

Plutôt qu'un inventaire, Denis Jacopini, avec la collaboration de Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en éviterez les conséquences parfois dramatiques... et coûteuses.

Un livre indispensable pour « surfer » en toute tranquillité !

Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier.

Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques. Marie Nocenti est romancière.

Réagissez à cet article

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

Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



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

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

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

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

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

Commandez sur Fnac.fr

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

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

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

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

Source : *Cyberarnaques S'informer pour mieux se protéger – broché – Denis Jacopini, MARIE NOCENTI – Achat Livre – Achat & prix | fnac*

Votre image est en ligne : comment demander son retrait ? | Denis JACOPINI

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



vous informe...

Votre image est en ligne : comment demander son retrait ?

Vous constatez qu'une photo/vidéo de vous est diffusée sur internet sans votre consentement ? La CNIL vous explique comment exercer vos droits.

Une personne qui conteste la diffusion de son image sur un site web peut s'adresser soit au responsable de site en application du droit d'opposition prévu par la loi informatique et libertés, soit au juge en s'appuyant sur les principes du droit à l'image (obligation de recueil du consentement).

Deux procédures existent : l'une dans le cas où vous souhaitez que le gestionnaire des droits de l'image supprime votre image, l'autre dans le cas où vous souhaitez demander au site de dépublier votre photo/vidéo. Vous pouvez effectuer ces demandes en parallèle.

« DEMANDER AU PHOTOGRAPHE LE RETRAIT D'UNE PHOTO AU NOM DU DROIT A L'IMAGE »

Situation type : « J'ai donné mon accord pour être pris en photo et ne souhaite plus voir ma photo en ligne aujourd'hui »

Il faut bien dissocier la protection des données personnelles – champ qui relève de la loi informatique et libertés – du « droit à l'image », qui est en fait le droit à la vie privée prévu dans le code pénal **.

Le « droit à l'image » permet à toute personne de faire respecter son droit à la vie privée. Un internaute pourra par exemple refuser que son image ne soit reproduite ou diffusée sur n'importe quel support sans son autorisation expresse.

Étape 1 – Assurez vous que cette photo permet de vous identifier

Étape 2 – Assurez vous que vous n'avez à aucun moment consenti à cette prise de vue

Le fait d'autoriser l'exploitation de votre image restreint votre capacité de contester sa diffusion ou sa réutilisation sauf si les termes de l'accord écrit ne correspondent pas au cadre prévu par la loi.

Forme de l'accord écrit : ce « contrat » passé entre le photographe/vidéaste est le plus souvent un engagement écrit daté et signé de votre part et qui vous demande votre consentement à être photographié/filmé et votre autorisation à ce que votre image soit diffusée et ce , dans un cadre bien précis : quels supports seront diffusés les photos ? Quels sont les objectifs de cette diffusion ? Sur quelle durée porte cette autorisation ? Pour en savoir plus ...

A noter : dans le cas d'images prises dans les lieux publics, seule l'autorisation des personnes qui sont isolées et reconnaissables est nécessaire.

Votre enfant est mineur ? Soyez particulièrement vigilants à ce que le photographe vous demande une autorisation écrite parentale. Quelques modèles sont téléchargeables depuis le site eduscol.education.fr

Étape 3 (Facultative) – Contactez l'auteur de la diffusion

Dans le cas d'une initiative d'un particulier, il peut s'agir du photographe à l'origine de la photo ou de la personne qui a publié votre image. Dans un contexte plus professionnel (clip musical, spot publicitaire ...) il peut s'agir de l'organisme qui utilise ces images à des fins de communication.

Si le photographe/vidéaste refuse de dépublier/flouter votre image, vous avez la possibilité de saisir le juge civil*/pénal** afin qu'il prononce des sanctions à l'encontre de l'auteur de la diffusion litigieuse. Vous disposez d'un délai de 3 ans à partir de la diffusion de l'image.

Les sanctions prévues en cas de non-respect

* Sur le fondement de l'article 9 du code civil, « Chacun a droit au respect de sa vie privée »

** L'article 226-1 du code pénal punit d'un an d'emprisonnement et 45 000 € d'amende le fait de porter atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Par ailleurs, l'article 226-8 du code pénal punit d'un an d'emprisonnement et de 15 000€ d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.

« JE SOUHAITE DEMANDER AU SITE DE DÉPUBLIER MA PHOTO »

Situation type « Je n'ai pas donné mon accord pour être pris en photo », « J'ai donné mon accord pour me faire photographier mais pas pour une diffusion en ligne... ».

Étape 1 – Assurez vous que cette photo permet de vous identifier ...

Dès lors qu'elle se rapporte à une personne identifiée ou identifiable, l'image d'une personne est une donnée à caractère personnel. Pour vous appuyer sur les droits prévus par la loi « informatique et libertés » vous devez prouver que l'on vous reconnaît.

Étape 2 – contactez le responsable du site sur lequel est publiée l'image

Écrire au site/réseau social/service en ligne pour lui demander de dépublier l'image. « Conformément à l'article 38 de la loi informatique et libertés, je souhaite m'opposer à ce que cette image – qui constitue une donnée personnelle – fasse l'objet d'un traitement pour le(s) motif(s) suivant(s) (...) »

Il est important d'indiquer les motifs légitimes de votre demande d'opposition. Votre courrier doit être signé et vous devez préciser l'adresse à laquelle doit parvenir la réponse de l'organisme.

Joindre un justificatif d'identité. Votre demande doit – en principe – être accompagnée de la photocopie d'un titre d'identité comportant votre signature. Attention, le responsable du fichier ne doit pas vous demander des pièces justificatives disproportionnées par rapport à votre demande.

Remarque : Le droit d'opposition est un droit personnel ! Vous ne pouvez en aucun cas exercer ce droit au nom d'une autre personne sauf les cas de représentation de mineurs ou de majeurs protégés.

Étape 3 (facultative) – Si la réponse n'est pas satisfaisante

Si aucune réponse satisfaisante n'a été formulée par le site sous deux mois, contactez la CNIL, via son formulaire de plainte en ligne, en n'oubliant pas de joindre une copie des démarches effectuées auprès du site.

Vous avez également la possibilité de saisir une juridiction.

Situations particulières

Usage domestique. La loi « informatique et libertés » ne s'applique pas pour l'exercice d'activités purement personnelles ou domestiques. Par exemple, la photographie d'un parent ou d'un ami prise depuis un smartphone puis diffusée à un nombre limité de correspondants sur un site dont l'accès est restreint, ne rentre pas dans le champ de compétence de la CNIL.

Usage artistique. La publication de photographies de personnes identifiables aux seules fins d'expression artistique n'est pas soumise aux principales dispositions de la loi informatique et libertés.

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.



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)

Réagissez à cet article

Source :
<http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/votre-image-est-en-ligne-comment-demander-son-retrait>

TCP Stealth : Un nouveau logiciel pour se protéger des cybercriminels | Denis JACOPINI

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





#TCP Stealth : Un nouveau logiciel pour se protéger des cybercriminels

Les balayeurs de ports sont des programmes qui parcourent le web en recherchant les ports ouverts, donc vulnérables, sur un serveur de réseau. Dans le cadre des récentes révélations de cyber-espionnage massif, un tel logiciel aurait été utilisé. Une équipe de l'Université technique de Munich (TUM, Bavière) a développé un logiciel de défense contre ce type d'attaques.

Baptisé « TCP Stealth », ce programme peut empêcher la détection des systèmes sur le net lors d'attaques par balayage de ports, ainsi que la prise de contrôle massive de ces systèmes. Ce logiciel, gratuit, nécessite tout de même certaines connaissances en informatique et systèmes pour être utilisé. Un usage plus large nécessitera encore une phase de développement. Cet outil peut venir en complément des pare-feux, antivirus et réseaux privés virtuels qui ne protègent que partiellement face à de telles attaques.

La connexion d'un utilisateur à un serveur se fait à travers un protocole de transport fiable (TCP). Afin d'accéder au service souhaité par l'utilisateur, sa machine envoie une demande au serveur. La réponse du serveur contient parfois des données susceptibles d'être utilisées pour mener des attaques. Le logiciel développé se fonde sur le principe suivant : un nombre est partagé uniquement entre la machine d'un utilisateur et le serveur. Sur la base de ce numéro, un code secret est généré puis transmis de manière invisible au serveur lors de la mise en connexion. Si le code reçu par le serveur n'est pas correct, le système ne répond pas et ne transmet donc pas d'informations au possible pirate.

De tels moyens de défense sont déjà connus, mais le logiciel développé est présenté par les chercheurs comme un outil de protection plus fiable, car il gère également une variante de cette attaque. Il est ici question d'attaques générées lors de l'échange de données entre l'utilisateur et le serveur, mais cette fois-ci dans le cas où la connexion est déjà établie. Les données envoyées par l'utilisateur au serveur peuvent être, à ce stade, encore interceptées et modifiées. Afin d'empêcher cette attaque et suivant le même principe que précédemment, un code secret intégré au flux de données est également envoyé au serveur. Le serveur reconnaîtra alors si le contenu est conforme à l'original.

Le logiciel est disponible au téléchargement à l'adresse suivante :
<https://gnunet.org/knock>.

Les personnes intéressées peuvent également participer à son développement.

Christian Grothoff, chercheur à la TUM, faculté d'architecture des réseaux et services

email : knock@gnunet.org

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)



Sources : « TUM-Forscher entwickeln Abwehrsystem gegen Cyberangriffe », dépêche idw, communiqué de presse de la TUM – 15/08/2014- <http://idw-online.de/pages/en/news599759>

Rédacteurs :

Aurélien Filiali, aurelien.filiali@diplomatie.gouv.fr –
<http://www.science-allemande.fr>

Références

: <http://www.bulletins-electroniques.com/actualites/76579.htm>

Wifi gratuit: Attention à vos données personnelles !

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



Wifi gratuit: Attention à vos données personnelles !

Les utilisateurs de réseaux de wifi du monde entier ne sont pas à l'abri du danger. D'après une enquête réalisée par Norton by Symantec, la grande majorité des internautes de l'Hexagone adoptent des comportements dangereux pour leur sécurité comme pour leur confidentialité.

Les Français parmi les mauvais élèves

Un sondage a été réalisé par Norton by Symantec sur un échantillon de 1 000 personnes environ dans chacun des 15 pays supervisés, dont la France et les Etats-Unis. L'enquête a tenté de mettre en avant les dangers d'une **connexion à des réseaux de wifi gratuit**. Il a été révélé que les internautes prennent de très gros risques pour leur sécurité et leur confidentialité par le biais du troc connexion-information. Ce dernier se manifeste sous plusieurs formes : adresse email à fournir, coordonnées, géolocalisation à accepter ou encore publicité à voir. Selon l'étude, la quasi-totalité des internautes de l'Hexagone (87%) ne cesse de multiplier les comportements dangereux pour leur sécurité comme pour leur confidentialité.

Les comportements dangereux des mobinautes

L'étude a mis en avant le comportement des internautes du monde entier. Ainsi, 43% des sondés sont impatients de se connecter à peine installés au restaurant, au café, à l'hôtel, dans un magasin ou même chez un ami. Plus encore, l'envie est si pressante que 25% avouent avoir déjà tenté de se connecter sans la permission du propriétaire du réseau. Les 7% ont déjà tenté de pirater ou deviner le mot de passe (7%), rapporte *LCI*. Pour avoir une bonne **connexion**, 55% des personnes enquêtées accepteraient de fournir n'importe quelle information...[lire la suite]

Réagissez à cet article

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

Denis JACOPINI Marie Nocenti (Plon) ISBN :
2259264220



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site

Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source :
<http://www.linfo.re/magazine/high-tech/722259-wifi-gratuit-halte-a-vos-donnees-personnelles> »>Wifi gratuit: attention à vos données personnelles! – LINFO.re – Magazine, High-Tech