

Formation informatique cybercriminalité : Virus, arnaques et piratages informatiques, risques et solutions pour nos entreprises | Denis JACOPINI

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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT fr</p>	 <p>RGPD CYBER LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
	<p>Formation informatique cybercriminalité : Virus, arnaques et piratages informatiques, risques et solutions pour nos entreprises</p>				

Le contexte de l'internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos comportements au quotidien.

Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des attitudes responsables seront les clés permettant d'enrayer le phénomène. Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours...) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un ordiphone (smartphone), d'une tablette, d'un ordinateur portable. La sécurité informatique est aussi une priorité pour la bonne marche des systèmes industriels (création et fourniture d'électricité, distribution d'eau...). Une attaque informatique sur un système de commande industriel peut causer la perte de contrôle, l'arrêt ou la dégradation des installations.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'entreprise.

Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses et faciles à mettre en oeuvre dans l'entreprise.

Suivez cette formation :

- **si vous êtes chefs d'entreprises, responsables d'agences, président d'associations, que vous soyez indépendant ;**
- **si vous souhaitez sensibiliser vos salariés, seul maillon faible sur lequel votre service informatique (probablement peu pédagogue) ne peut rien faire ;**
- **si vous souhaitez mettre en place une charte informatique et vous souhaitez qu'elle soit mieux comprise et mieux acceptée par vos salariés ;**
- **si vous souhaitez vous mettre en conformité avec la CNIL, cette formation est le premier pas vers une compréhension des risques informatiques.**

Plus d'information sur les formations que nous proposons :

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

[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"]

Escroqueries aux Faux Ordres de Virements Internationaux (FOVI)

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



Escroqueries
aux Faux
Ordres de
Virements
Internationaux
(FOVI)

La Direction Zonale de la Sécurité Intérieure à Bordeaux vous informe d'une évolution dans le mode opératoire pour les Faux Ordres de Virements Internationaux (FOVI).

Les escroqueries aux Faux Ordres de Virements Internationaux ont représenté un préjudice estimé à 550 millions d'euros depuis leur apparition début 2010. A ce jour, trois modes opératoires existent : le **faux président**, la **prise à distance du poste de travail** et le **changement de relevé d'identité bancaire (RIB)**.

Depuis septembre 2016, il a été observé un changement du mode opératoire relatif au changement de RIB.

Pour rappel, ce mode opératoire est utilisé dans le cadre du paiement d'un loyer ou d'une facture en instance dans la société ciblée. Dans ces deux cas, un individu se présente comme un responsable du fournisseur et contacte par téléphone, puis par mail, le service comptabilité de l'entreprise ciblée en l'informant d'un changement de domiciliation bancaire.

Afin de rassurer l'entreprise ciblée et de transmettre les nouvelles coordonnées bancaires, **les escrocs utilisent désormais le site Internet LA POSTE pour créer un compte leur permettant d'utiliser le service payant de la lettre recommandée en ligne**. Créé sous une fausse identité, ce compte leur permet de régler des envois postaux et ainsi de faire parvenir à l'entreprise ciblée un courrier matérialisé, distribué par LA POSTE et remis en main propre au destinataire, contenant les coordonnées bancaires gérées par les escrocs.

Face à cette nouvelle menace, une vigilance accrue est de mise. Nous vous encourageons à diffuser ce message auprès des personnes concernées de votre société.

Flash Ingérence n°22 (mars 2016) relatif aux Faux Ordres de Virements Internationaux (FOVI)

...[lire la suite]

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

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

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

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

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

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

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

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

Original de l'article mis en page : Alerte #Cybersécurité : Escroquerie aux Faux Ordres de Virements Internationaux (FOVI) | Pôle Numérique CCI Bordeaux Gironde

Est-ce utile de former les salariés à la sécurité informatique ? | Denis JACOPINI

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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
	<p>Est-ce utile de former les salariés à la sécurité informatique ?</p>				

L'avènement du big data et de la mobilité modifient en profondeur l'utilisation des outils informatiques. Le chef d'entreprise doit donc adapter ses méthodes de management, pour éviter les débordements.

Le bon usage des outils est aujourd'hui un sujet de grande importance au sein des entreprises. Si bien que les dirigeants doivent adapter leurs techniques managériales.

Une simple clé USB branchée sur son ordinateur de bureau ou une pièce jointe malveillante ouverte sans précaution peuvent s'avérer catastrophiques pour les entreprises. Au travail, l'usage des outils informatiques doit être encadré. Au dirigeant de prendre ses responsabilités et d'expliquer à ses employés que l'on n'utilise pas un ordinateur au travail comme on le ferait à la maison. Une règle primordiale pour s'assurer du bon fonctionnement et de la sécurité des données de l'entreprise.

Responsabiliser les employés

« Au-delà de la formation des salariés, je préfère la notion de responsabilisation, nuance Philippe Soullier, dirigeant chez Valtus. Il y a un degré de confiance à donner. Chez nous par exemple, je ne vois aucun souci à ce qu'un employé consulte son mail personnel ou son compte Facebook. C'est un fait, nous sommes dans une époque où se développe une certaine confusion entre le temps de travail et la vie personnelle. Mais à partir du moment où le travail est correctement effectué, je n'y vois pas d'inconvénient. »

Les salariés disposent d'un certain degré de liberté, mais des limites sont fixées. « Sur la navigation, nous fermons évidemment l'accès à certains sites internet. Nos services informatiques bloquent par exemple la consultation des sites à caractère pornographique ». Outre cet exemple évident, la confiance joue à plein. « Nous disons aux salariés: 'c'est votre outil de travail, prenez-en soin !' », assure Philippe Soullier. Une stratégie managériale confortée par le fait que les salariés ne sortent pas de l'école: « Ils ne sont pas forcément technophiles et prennent moins de risques avec leurs outils professionnels que la 'génération Facebook' », admet Philippe Soullier.

Inciter à la prudence

Du côté de l'Anssi, l'Agence nationale de sécurité informatique, on aimerait voir se développer des « chartes de bonne conduite » dans les petites structures. « Ce travail commence par le haut de la chaîne. Les dirigeants doivent se montrer eux-mêmes irréprochables, sinon le message ne passe pas. Un dirigeant doit accepter de s'entendre dire non par un administrateur, précise Vincent Strubel, sous-directeur expertise au sein de l'agence. Il faut rester simple, pragmatique. On explique par exemple que l'on ne doit pas importer sa musique ou ses photos sur l'ordinateur de travail, que l'on ne réutilise pas constamment les mêmes mots de passe et qu'il ne faut surtout pas cliquer sur un lien quelque peu douteux. » Attention aussi aux connexions wifi dans les cafés lorsque la mobilité est de mise dans l'entreprise. « Il faut faire preuve de prudence dans toutes les situations », insiste-t-il.

La question du bon usage des outils informatiques est intimement liée aux enjeux de sécurité. Toujours chez Valtus: « Nos employés travaillent avec des entreprises. Ils reviennent chez nous en possession de données potentiellement sensibles. Ils doivent absolument comprendre que ce n'est pas parce que l'on peut en discuter au bureau que nos échanges ont un caractère public », raconte Philippe Soullier.

L'utilisation des adresses e-mail personnelles, le contenu même des messages doivent donc être maniés avec vigilance. Une précaution appuyée par Jan Villeminot, employé au service informatique de l'entreprise Intersec: « Les pirates informatiques savent parfaitement que la première faille d'une entreprise, c'est l'humain ».

[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.lexpress.fr/high-tech/securite-informatique-dirigeants-formez-vos-salaries_1660968.html

La cybercriminalité, un vrai risque pour les administrations | Denis JACOPINI





La cybercriminalité, un vrai risque pour les administrations

Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages.

Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les collectivités.

Par exemple, les données les plus sensibles (fichiers administrés ou membres, contrats, projets en cours...) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un ordiphone (smartphone), d'une tablette, d'un ordinateur portable...

La sécurité informatique est aussi une priorité pour la bonne marche des systèmes informatiques. Une attaque informatique sur un système peut causer la perte de contrôle, l'arrêt ou la dégradation des installations.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de service et de l'image de la victime.

Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses et faciles à mettre en oeuvre dans votre collectivité.

[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 : Denis JACOPINI

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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LE NET EXPERT fr</p>	 <p>RGPD CYBER LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
<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.





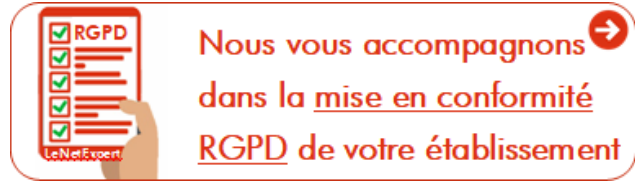
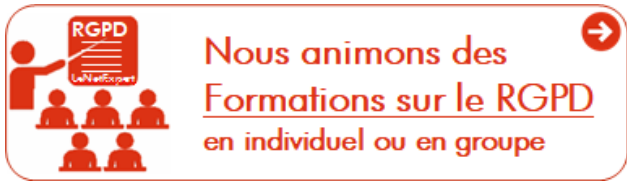
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

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 \(Délégués à la Protection des Données\)](#)

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

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