Guide des bonnes pratiques à adopter face aux risques numériques

Guide des bonnes pratiques à adopter face aux risques numériques

Issu des premiers constats réalisés par les référents de l'ANSSI en région, le guide d'élaboration en 8 points clés d'une charte d'utilisation des moyens informatiques et des outils numériques est une première réponse apportée aux PME et ETI.

Ce nouveau guide constitue le point de départ indispensable pour la mise en place ou de la réactualisation des bonnes pratiques à adopter face aux risques numériques.
S'il s'adresse avant tout aux PME et ETI, ce guide ne manquera pas également d'intéresser l'ensemble des organisations invariablement soumises aux mêmes problématiques.

PDF
Charte d'utilisation des moyens informatiques et des outils numériques
734.06 Ko

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 d'expertises, d'audits, de formations et de sensibilisation 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

---

Réagissez à cet article

Source : *Charte d'utilisation des moyens informatiques et des*

outils numériques – Le guide indispensable pour les PME et ETI | Agence nationale de la sécurité des systèmes d'information

---

Victime de piratage ? Les bons réflexes à avoir

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Victime de piratage ? Les bons réflexes à avoir				

Sur Internet, nul n'est à l'abri d'une action malveillante ou de messages non sollicités. Les éléments suivants vous aideront à avoir les bons réflexes.

VOUS ETES UN PARTICULIER, TPE/PME OU UNE COLLECTIVITÉS TERRITORIALES ?

Désormais, vous pouvez contacter le dispositif d'assistance aux victimes d'actes de cybermalveillance : cybermalveillance.gouv.fr Cette plateforme est le résultat d'un programme gouvernemental assumant un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française. Vous êtes un particulier, une entreprise ou une collectivité territoriale et vous pensez être victime d'un acte de cybermalveillance ?

La plateforme en ligne du dispositif est là pour vous mettre en relation avec les spécialistes et organismes compétents proches de chez vous ; : cybermalveillance.gouv.fr

Pour information, Nous sommes inscrits au programme cybermalveillance.gouv.fr

Ce dispositif est animé par le groupement d'intérêt public (GIP) Action contre la cybermalveillance (ACYMA) et porté par une démarche interministérielle.

VOUS SOUHAITEZ PORTER PLAINTE ?

Rapprochez du commissariat ou de la brigade de Gendarmerie les plus proches du lieu de l'infraction. Facilitez le travail de l'agent de Police ou de Gendarmerie auprès de qui vous déposerez plainte.

• **Victime de VIRUS – CRYPTOVIRUS – LOGICIEL ESPION** : Portez plainte pour l'infraction suivante : Atteintes aux Systèmes de Traitement Automatisé de Données (S.T.A.D.) sanctionnées par les articles L.323-1 et suivants du Code pénal ;

• **UTILISATION ILLICITE DE VOS DONNÉES PERSONNELLES** : Vous devez saisir la CNIL sur les motifs d'atteintes aux droits de la personne liés aux fichiers ou traitement informatiques (art. 226-16 à 226-24 du Code pénal / Loi 78-17 du 6 janvier 1978 dite « informatique et liberté » modifiée par la loi 2004-801 du 6 aout 2004) ;

• **USURPATION D'IDENTITÉ** : Portez plainte sur ce motif en apportant les preuves (captures d'écran, e-mails, mieux encore un constat d'huissier) ;

• **MENACES** : Déposez plainte sur le motif d'atteintes aux personnes en apportant toutes les preuves (les témoignages ou attestations sont très souvent insuffisants) ;

• **PHISHING / FAUSSE LOTERIE / UTILISATON FRAUDULEUSE DE CB** : Déposez plainte pour Escroquerie ; Une plateforme téléphonique spécialisée existe : « Info-escroqueries » : 0811 02 02 17

• **ATTEINTE AUX MINEURS** : Déposez plainte sur le fondement de l'article 227-23 du Code pénal ;

QUE DEVIENDRA MA PLAINTE EN CAS D'ATTAQUE POUR RANSOMWARE (CRYPTO-VIRUS) ?

Depuis la loi du 03 juin 2016, la section F1 spécialisée cyber du parquet de Paris jouit d'une compétence nationale concurrente. Une circulaire du Ministère de la Justice du 10 mai 2017 ordonne aux parquets locaux de se dessaisir systématiquement au profit du parquet de Paris en cas de plainte pour ransomware.

La politique du parquet de Paris est de systématiquement saisir:

– la DCPJ (OCLCTIC) pour les victimes en zone police

– la DGGN (SCRC/C3N) pour les victimes en zone gendarmerie

En bref:

-la plainte peut être déposée n'importe où, mais prioritairement auprès de l'unité de police/gendarmerie territorialement compétente et avec laquelle la victime a l'habitude de traiter pour tout type d'infraction

– une fois déposée, la plainte sera transmise par l'unité de police/gendarmerie au parquet local, qui la transmettra immédiatement au parquet de Paris, qui saisira pour enquête la DCPJ (OCLCTIC) ou la DGGN (SCRC/C3N) en fonction de la zone de la victime

NB: La mission de la DCPJ (OCLCTIC) et de la DGGN (SCRC/C3N) est de conduire les enquêtes judiciaires pour identifier et interpeller les auteurs. Notre mission n'est en aucun cas de faire de la remédiation et de la gestion de crise SSI. Cette mission de remédiation / gestion de crise SSI est de la compétence:

– pour les OIV (opérateurs d'infrastructures vitales) et les administrations: ANSSI

– pour les entreprises non OIV: de leur propre compétence (elles peuvent faire appel à des prestataires privés en SSI)

VOUS RECEVEZ DES MESSAGES NON SOLLICITÉS ?

Utilisez Signal-Spam

VOUS SOUHAITEZ SIGNALER UN CONTENU ILLICITE ?

Utilisez le portail officiel de signalements de contenus illicites

VOUS AVEZ DES SOUPÇON D'ATTAQUE INFORMATIQUE ?

Consultez la note d'information *Les bons réflexes en cas d'intrusion sur un système d'information* sur le site du CERT-FR

La Police et la Gendarmerie nationale ont toutes deux mis en place un réseau territorial d'enquêteurs spécialisés en cybercriminalité répartis par zones de compétence. Les Investigateurs en CyberCriminalité (ICC/Police) et les N-TECH (Gendarmerie) sont présents dans les services territoriaux de vos régions.

Si vous êtes victime d'infractions mentionnées ci-dessus, vous pouvez directement déposer plainte auprès de leurs services ou bien adresser un courrier au Procureur de la République près le Tribunal de Grande Instance compétent.

Pour information, en fonction du type d'infraction, des services sont spécialisés dans le traitement judiciaire de la cybercriminalité :

SOUS-DIRECTION DE LUTTE CONTRE LA CYBERCRIMINALITÉ (SDLC)

Service interministériel qui dépend de la Direction Centrale de la Police Judiciaire (DCPJ)

Cette Sous-Direction reprend les missions traditionnelles de l'Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC) auxquelles doit être ajoutée une plateforme de signalement et d'orientation technique et judiciaire.

Infractions traitées : piratages, fraudes aux moyens de paiement, téléphonie et escroqueries sur Internet.

Contact :

SDLC/OCLCTIC

101, rue des 3 Fontanots

92 000 Nanterre

Site Internet

Services de signalements en ligne de contenus illégaux sur l'Internet

Plateforme téléphonique « Info-escroqueries » : 0811 02 02 17

BRIGADE D'ENQUÊTE SUR LES FRAUDES AUX TECHNOLOGIES DE L'INFORMATION (BEFTI)

Paris et petite couronne – Particuliers & PME

La BEFTI dépend de la Direction Régionale de la Police Judiciaire de Paris (DRPJ-PARIS).

Composée de groupes d'enquêtes spécialisés et d'un centre d'assistances techniques, cette brigade est compétente pour les investigations relatives aux actes de piratage sur Paris et ses trois départements limitrophes (92, 93 et 94).

Contact :

BEFTI

122-126 rue du Château des Rentiers

75 013 Paris

Site Internet

CENTRE DE LUTTE CONTRE LES CRIMINALITÉS NUMÉRIQUES (C3N) DU SERVICE CENTRAL DU RENSEIGNEMENT CRIMINEL (SCRC) DE LA GENDARMERIE NATIONALE

France – Particuliers & organismes

Ce centre dépend du Pôle judiciaire de la Gendarmerie nationale.

Service à compétence judiciaire nationale, il regroupe l'ensemble des unités du PJGN qui traitent directement de questions (formation, veille et recherche, investigation, expertise) en rapport avec la criminalité et les analyses numériques (Département Informatique-Electronique de l'IRCGN). Il assure également l'animation et la coordination au niveau national de l'ensemble des enquêtes menées par le réseau gendarmerie des enquêteurs numériques.

Domaine de compétence: atteintes aux STAD, infractions visant les personnes et les biens.

Contact :

SCRC/C3N

5, Boulevard de l'Hautil – TSA 36810

95037 CERGY PONTOISE CEDEX

contact : cyber[at]gendarmerie.interieur.gouv.fr

DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE (DGSI)

France – État, secteurs protégés, OIV

La DGSI dépend du Ministère de l'Intérieur.

Créée en mai 2014 à la suite de la DCRI (Direction Centrale du Renseignement Intérieur), cette direction générale en poursuit les missions de protection des intérêts fondamentaux de la Nation.

Infractions traitées : actes de piratage ciblant les réseaux d'État, les établissements composés de Zones à Régime Restrictif et les Opérateurs d'Importance Vitale.

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 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 : *En cas d’incident | Agence nationale de la sécurité des systèmes d’information*

Cyberarnaques S’informer pour mieux se protéger – Denis Jacopini, Marie Nocenti | fnac

	Cyberarnaques S’informer pour mieux se protéger

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.

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.
Commandez CYBERARNAQUES sur le site de la FNAC (disponible à partir du 29/03/2018)

Réagissez à cet article

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

GDPR compliance: Request for costing estimate

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

GDPR compliance: Request for costing estimate

You seem to express an interest in the GDPR (perhaps a little by obligation) and you want to tell us about a project. We thank you for your confidence.
Intervening on Data Protection missions since 2012, after having identified different types of expectations, we have adapted our offers so that they best meet your needs.
Thus, we can assist you in bringing your structure into compliance in several ways : :
1. Are you looking for autonomy ?
We can assist you to learn the essentials of European regulations relating to the Protection of Personal Data and the necessary to understand and start a compliance. Once the training is completed, you are independent but can always count on our support either in the form of personalized training, or in the form of personalized support;
At the end of this training, we will give you a certificate proving the implementation of a process to bring your establishment into compliance with the GDPR (General Data Protection Regulations). For information, we are referenced to the CNIL.
2. Do you want to be accompanied for the implementation of compliance ?
We carry out for you the audit which will highlight the points to be improved. At the end of this stage you can, if you wish, achieve compliance or let us proceed with the improvements that you have validated;
At the end of this audit, we will give you a report proving the implementation of corrections as part of your process to bring your establishment into compliance with the GDPR (General Data Protection Regulations).
3. Do you want to entrust all of your compliance?
In a perfectly complementary way with your IT service provider and possibly with your legal department, we can take care of the entire process of bringing your establishment into compliance with the GDPR (General Data Protection Regulation) and the various regulations relating to the protection of Personal Data.
From the audit to the follow-up, you can count on our technical and educational expertise so that your establishment is supported externally.
In order to send you a personalized proposal adapted both to the needs of your structure, in accordance with your strategy and your priorities, we would like you to answer these few questions :

We guarantee extreme confidentiality on the information communicated. Persons authorized to consult this information are subject to professional secrecy.

Do not hesitate to communicate as many details as possible, this will allow us to better understand your expectations.

Your First Name / NAME (required)

Your Organization / Company (required)

Your email address (required)

A telephone number (will not be used for commercial prospecting)

You can write us a message directly in the free text area. However, if you want us to establish precise costing for you, we will need the information below.

In order to better understand your request and establish a quote, please provide us with the information requested below and click on the "Send entered informations" button at the bottom of this page for us to receive it. You will receive an answer quickly.

YOUR ACTIVITY

Details about your activity :
Are you subject to professional secrecy? OYes⊕NoOI don't know
Does your activity depend on regulations? OYes⊕NoOI don't know
If "Yes", which one or which ones?

YOUR COMPUTER SYSTEM

Can you describe the composition of your computer system. We would like, in the form of an enumeration, to know the equipment which has any access to personal data with for each device ALL the software (s) used and their function (s) .
Examples :
- 1 WEB server with website to publicize my activity;
- 1 desktop computer with billing software to bill my clients;
- 2 laptops including:
> 1 with email software to correspond with clients and prospects + word processing for correspondence + billing software to bill my clients ...
> 1 with email software to correspond with customers and prospects + accounting software to do the accounting for my company ;
- 1 smartphone with email software to correspond with customers and prospects.

Do you have one or more websites? OYes⊕NoOI don't know
What is (are) this (thoses) website (s)?
Do you have data in the Cloud? OYes⊕NoOI don't know
Which cloud providers do you use?

YOUR PERSONAL DATA PROCESSING

If you have already established it, could you provide us with the list of processing of personal data (even if it is incomplete)?

SIZING YOUR BUSINESS

Number of employees in your structure : 0
How many of these employees use computer equipment ? 0
Number of departments or departments ** in your structure (example: Commercial service, technical service ...) : 0
Please list the services or departments ** of your structure:

SERVICE PROVIDERS & SUBCONTRACTORS

Do you work with sub-contractors? OYes⊕NoOI don't know
Please list these subcontractors :
Do you work with service providers who work on your premises or in your agencies (even remotely) ? OYes⊕NoOI don't know
Please list these providers :
How many IT companies do you work with ? 0
Please list these IT companies indicating the products or services for which they operate and possibly their country of establishment :

YOUR SITUATION TOWARDS THE GDPR

Does your establishment exchange data with foreign countries ? OYes⊕NoOI don't know
If "Yes", with which country(ies)?
Have you already been made aware of the GDPR ? OYes⊕NoOI don't know
Have people using IT equipment already been made aware of the GDPR ? OYes⊕NoOI don't know
If you or your employees have not been made aware of the GDPR, would you like to undergo training ? OYes⊕NoOI don't know

YOUR WORKPLACE

The analysis of the data processing conditions in your professional premises or your professional premises is part of the compliance process.
Do you have several offices, agencies etc. legally dependent on your establishment ? OYes⊕No
If "Yes", how much ? 0
In which city (ies) (and country if not in France) do you or your employees work ?

TYPE OF SUPPORT DESIRED

We can support you in different ways.
A) We can teach you to become autonomous (training) ;
B) We can support you at the start and then help you become independent (support, audit + training) ;
C) We can choose to entrust us with the entire process of compliance (support) ;
D) We can accompany you in a personalized way (thank you to detail your expectations).
What type of support do you want from us (A / B / C / D + details) ?

END OF QUESTIONNAIRE

If you wish, you can send us additional information such as:
- Emergency of your project;
- Any additional information that you deem useful to allow us to better understand your project.

Send entered informations

Les informations recueillies sont enregistrées dans la messagerie électronique et le système informatique de LeNetExpert pour les traitements correspondant à la gestion de vos demandes et la proposition de services correspondant à votre demande. Le lieu de traitement de stockage et de sauvegarde se situe en France et auprès d'établissements respectant le bouclier de protection des données UE-États-Unis (en anglais : EU-US Privacy Shield). Elles sont conservées 3 ans après notre dernier échange et sont destinées aux services internes. Une démarche de mise en conformité a été entamée en interne depuis 2010 et jusqu'à ce jour par des formations régulières, l'identification des traitements, la réalisation d'un registre des traitements, une analyse de risques sur nos traitements manipulant des données sensibles ou des « données à caractère hautement personnel » pour lesquels leur violation pourrait avoir de graves conséquences dans la vie quotidienne des personnes concernées et un suivi semestriel. Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit RGPD (Règlement Général sur la Protection des Données), à la loi n°78-17 dite «Informatique et Libertés» du 6 janvier 1978 et à la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant Le Net Expert, Monsieur le Délégué à la Protection des Données – 1 les Magnolias – 84300 CAVAILLON par Recommandé avec accusé de réception. Enfin, sur le fondement des articles 131-13, 222-17, 222-18, 222-18-1, 322-12, 322-13, R-621-1, R-621-2, R-623-1, R-624-3, R-624-4, R 631-1 et R634-1 du code Pénal et l'article 29 de la loi du 29 juillet 1881 sur la liberté de la presse, votre adresse IP horodatée est également collectée.

Sauf indication contraire ou information publique, nous nous engageons à la plus totale discrétion et la plus grande confidentialité concernant les informations que vous nous communiquez.

** = for example, commercial service, technical service, educational service, administrative and financial service ...

Δ

or send an email to rgpd[at]lenetexpert.fr

Denis JACOPINI is our Expert who will accompany you in your compliance with the GDPR.

Let me introduce myself: Denis JACOPINI. I am an expert in sworn IT and specialized in GDPR (protection of Personal Data) and in cybercrime. Consultant since 1996 and trainer since 1998, I have experience since 2012 in compliance with the regulations relating to the Protection of Personal Data. First technical training, CNIL Correspondent (CIL: Data Protection Correspondent) then recently Data Protection Officer (DPO n ° 15845), as a compliance practitioner and trainer, I support you in all your procedures for compliance with the GDPR.

« My goal is to provide all my experience to bring your establishment into compliance with the GDPR. »

Quelques conseils pour surfer un peu plus tranquille sur Internet

	Quelques conseils pour surfer un peu plus tranquille sur Internet

Quelques conseils de bon sens pour se protéger au mieux des attaques liées à l'utilisation d'Internet.

Des mises à jour régulières et automatiques

L'un des meilleurs moyens de se prémunir des risques de piratage, est de **maintenir son matériel informatique et ses logiciels à jour** avec les derniers correctifs de sécurité et les dernières mises à jour.

Par ce biais, le risque d'intrusion est minimisé. Il est donc très important de **configurer son ordinateur** pour que le système d'exploitation se mette **régulièrement et automatiquement à jour.**

Une bonne configuration matérielle et des logiciels adaptés

Les **niveaux de sécurité** de l'ordinateur doivent être **réglés au plus haut** pour minimiser les risques d'intrusions. Les **paramètres des navigateurs** et des **logiciels de messageries** électroniques peuvent aussi être configurés avec des niveaux de sécurité élevés.

L'utilisation d'un **anti-virus à jour** et d'un **pare-feu** (*firewall*) assureront un niveau de protection minimum pour surfer sur la toile. Le*firewall* permet de filtrer les données échangées entre votre ordinateur et le réseau. Il peut être réglé de manière à bloquer ou autoriser certaines connexions.

Utiliser un bon mot de passe

Les mots de passe sont une **protection incontournable** pour sécuriser l'ordinateur et ses données ainsi que tous les accès au service sur Internet.

Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Lire nos conseils pour choisir un bon mot de passe .

Se méfier des courriers électroniques non-sollicités et leurs pièces jointes

A la réception d'un mail dont l'**expéditeur est inconnu**, un seul mot d'ordre : **prudence** !

Les courriers électroniques peuvent être accompagnés de **liens menant vers des sites frauduleux** (voir l'article sur le *phishing*) ou de **pièces jointes piégées**. **Un simple clic sur une image suffit pour installer à votre insu un logiciel ou code malveillant**(cheval de Troie) sur votre ordinateur. La pièce jointe piégée peut être : une page html, une image JPG, GIF, un document word, open office, un PDF ou autre.

Pour se protéger de ce type d'attaque, la règle est simple : **ne jamais ouvrir une pièce jointe dont l'expéditeur est soit inconnu, soit d'une confiance relative.**

En cas de doute, une recherche sur internet permet de trouver les arnaques répertoriées.

Que faire si j'ai déjà cliqué sur la pièce jointe?

Déconnectez-vous d'internet et **passez votre ordinateur à l'analyse anti-virus** (à jour) pour détecter l'installation éventuelle d'un logiciel malveillant.

Pour tout renseignement ou pour signaler une tentative d'escroquerie :

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Conseils de prévention sur

Comment bien se protéger contre les Cyberattaques ?

Comment bien se protéger contre les Cyberattaques ?

On l’a encore vu récemment, aucun système informatique n’est à l’abri d’une faille…

Et en matière de cybercriminalité, les exemples nous montrent que l’attaque semble toujours avoir un coup d’avance sur la défense. L’enjeu, pour les institutions et les entreprises, est d’anticiper et de se préparer à ces situations de crise en développant, en amont, une stratégie à-même de minorer au maximum leurs conséquences.

Demande de rançons, fraudes externes, défiguration de sites web, vols ou fuites d’informations, cyber-espionnage économique ou industriel…, en 2016 huit entreprises françaises sur dix ont été victimes de cybercriminels, contre six en 2015. La tendance n’est malheureusement pas à l’amélioration et l’actualité récente regorge d’exemples frappants : le logiciel malveillant WannaCry qui vient de frapper plus de 300 000 ordinateurs dans 150 pays avec les conséquences désastreuses que l’on connait, l’attaque du virus Adylkuzz qui ralentit les systèmes informatiques, le vol de la copie numérique du dernier opus de la saga « Pirates des Caraïbes » quelques jours avant sa sortie mondiale…, les exemples de cyberattaques ne cessent de défrayer la chronique.

Pour bien se protéger contre les Cyberattaque, nous vous conseillons de suivre les étapes suivantes :

1. Faire ou faire faire un état des lieux des menaces et vulnérabilités risquant de mettre en danger votre système informatique ;
2. Faire ou faire faire un état des lieux des failles aussi bien techniques qu’humaines ;
3. Mettre en place les mesures de sécurité adaptées à vos priorités et aux moyens que vous souhaitez consacrer ;
4. Assurer une surveillance des mesures de sécurité et s’assurer de leur bon fonctionnement et de leur adaptation au fil de vos évolutions aussi bien techniques que stratégiques.

• Vous souhaitez faire un point sur l’exposition de votre entreprise aux risques cyber ?
• Vous souhaitez sensibiliser votre personnel aux différentes arnaques avant qu’il ne soit trop tard ?
• Vous rechercher une structure en mesure de mettre en place une surveillance de votre réseau, de votre installation, de vos ordinateurs ?

Contactez-vous

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 d’expertises, d’audits, de formations et de sensibilisation 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

---

Réagissez à cet article

Source : *Cyberattaque, comment faire pour limiter les risques ?*

Comment bien choisir ses mots de passe ?

	Comment bien choisir ses mots de passe ?

Les mots de passe sont une protection incontournable pour sécuriser l'ordinateur et ses données ainsi que tous les accès aux services sur Internet. Mais encore faut-il en choisir un bon.Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Qu'est ce qu'un bon mot de passe ?

Un bon de passe est constitué d'au moins **12 caractères** dont :

• des lettres majuscules
• des lettres minuscules
• des chiffres
• des caractères spéciaux

Un mot de passe est d'autant plus faible qu'il est court. L'utilisation d'un alphabet réduit ou de mot issu du dictionnaire le rend très vulnérable.
Les mots du dictionnaire ne doivent pas être utilisés.
Aussi à proscrire, les mots en relation avec soi, qui seront facilement devinables : nom du chien, dates de naissances…
Réseaux sociaux, adresses mail, accès au banque en ligne, au Trésor public, factures en ligne.
Les accès sécurisés se sont multipliés sur internet.
Au risque de voir tous ses comptes faire l'objet d'utilisation frauduleuse, il est impératif de **ne pas utiliser le même mot de passe**pour des accès différents.
Alors, choisir un mot de passe pour chaque utilisation peut vite devenir un vrai casse-tête.

Comment choisir et retenir un bon mot de passe ?

Pour créer un bon mot de passe, il existe plusieurs méthodes :

La méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour créer une phrase facilement mémorisable.
Exemple : « j'ai acheté huit cd pour cent euros ce après-midi» donnera : ght8CD%E7am

La méthode des premières lettres

Utiliser les premières lettres d'une phrase en variant majuscules, minuscules et caractères spéciaux.
Exemple : « un tiens vaut mieux que deux tu l'auras » donnera : 1TvmQ2tl'@

Diversifier facilement les mots de passe

Opter pour une politique personnelle avec, par exemple, un préfixe pour chaque type d'activité. Comme BANQUE-MonMotDePassz pour la banque, IMP-MonMotDePasse pour les impôts. Quelque chose de très facile à mémoriser qui complexifie votre mot de passe et, surtout, vous permet de le diversifier.

Diminuer les imprudences

Pour finir, il est utile de rappeler de **ne pas stocker ses mots de passe à proximité de son ordinateur** si il est accessible par d'autres personnes. L'écriture sur le post-it déposé sous le clavier est à proscrire par exemple, de même que le stockage dans un fichier de la machine.
En règle général, les logiciels proposent de **retenir les mots de passe**, c'est très **tentant mais imprudent**. Si votre ordinateur fait l'objet d'un piratage ou d'une panne, les mots de passe seront accessibles par le pirate ou perdus.

Que faire en cas de piratage ?

Il est recommandé de préserver les traces liées à l'activité du compte.
Ces éléments seront nécessaires en cas de dépôt de plainte au commissariat de Police ou à la Gendarmerie.
Exemple
Compte email piraté
Vos contacts ont reçu des messages suspects envoyés de votre adresse.
Contactez-les pour qu'ils conservent ces messages.
Ils contiennent des informations précieuses pour l'enquêteur qui traitera votre dépôt de plainte.
Récupérez l'accès à votre compte afin de changer le mot de passe et re-sécurisez l'accès à votre compte.

Changer de mots de passe régulièrement

Cette dernière règle est contraignante mais assurera un niveau supérieur de sécurité pour vos activités sur Internet.
Un **bon mot de passe doit être renouvelé plusieurs fois par an** et toujours en utilisant les méthodes décrites ci-dessus.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Comment choisir ses mots de passe ? / Cybercrime / Dossiers / Actualités – Police nationale – Ministère de l'Intérieur

---

Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur

professionnel à votre employeur ?

Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur professionnel à votre employeur ?

Ne pas effacer ses données personnelles sur son ordinateur de fonction est-il dommageable (risque d'accès à nos données personnelles, vol d'identité ou accès frauduleux etc…)? Si oui, pourquoi ?

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :
• Accéder à vos documents et découvrir les informations qui peuvent soit être professionnelles et être utilisées contre vous, soit personnelles permettant à un voyou de les utiliser contre vous soit en vous demandant de l'argent contre son silence ou pour avoir la paix ;
• Accéder aux identifiants et mots de passe des comptes internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes facebook, twitter, dropbox… ;
• Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement déposer des commentaires ou envoyer des e-mails en utilisant votre identité. Même si l'article 226-4 du code pénal complété par la loi LOPPSI du 14 mars 2011 d'un article 226-4-1, l'usurpation d'identité numérique est un délit puni de deux ans d'emprisonnement et de 20 000 euros d'amende, il sera fastidieux d'une part pour vous, de prouver que vous n'êtes pas le véritable auteur des faits reprochés, et difficile pour les enquêteurs de retrouver le véritable auteur des faits.

Ne pas effacer ses données personnelles sur l'ordinateur que l'on rend, donne, vend, c'est laisser l'opportunité à un inconnu de fouiller dans vos papier, violer votre intimité et cambrioler votre vie.
Pire ! vous connaissez bien le donataire de votre matériel et vous savez qu'il n'y a aucun risque qu'il ait des intentions répréhensibles. Mais êtes vous certain qu'il sera aussi prudent que vous avec son matériel ?
Êtes-vous prêt à prendre des risques s'il perdait ce matériel ?
Dormiriez-vous tranquille si vous imaginiez que votre ancien ordinateur est actuellement sous l'emprise d'un pirate informatique prêt à tout pour tricher, voler et violer en utilisant votre identité ?

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : 5 applications pour effacer des données de façon sécurisée — ZDNet

Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d’expéditeurs inconnus ?

	Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d’expéditeurs inconnus ?

Selon une enquête de la FAU (University of Erlangen-Nuremberg), près de la moitié des utilisateurs cliqueraient sur des liens d'expéditeurs inconnus (environ 56% d'utilisateurs de boite mails et 40% d'utilisateurs de Facebook), tout en étant parfaitement conscient des risques de virus ou d'autres infections.
Le site d'information Français Pure Player Atlantico à interrogé à ce sujet Denis JACOPINI, Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles

Atlantico :
Pourquoi donc, selon vous, le font-ils malgré tout ? Qu'est-ce qui rend un mail d'un inconnu si attirant, quitte à nous faire baisser notre garde ?

Denis JACOPINI :
Ça-vous est très probablement déjà arrivé de recevoir un e-mail provenant d'un expéditeur anonyme ou inconnu.
Avez-vous résisté à cliquer pour en savoir plus ? Quels dangers se cachent derrière ces sollicitations inhabituelles ? Comment les pirates informatiques peuvent se servir de nos comportements incontrôlables ?

Aujourd'hui encore, on peut comparer le courrier électronique au courrier postal.
Cependant, si l'utilisation du courrier postal est en constante diminution (-22% entre 2009 et 2014), l'usage des messages électroniques par logiciel de messagerie ou par messagerie instantanée a lui par contre largement augmenté.
Parmi les messages reçus, il y a très probablement des réponses attendues, des informations souhaitées, des messages de personnes ou d'organismes connus nous envoyant une information ou souhaitant de nos nouvelles et quelques autres messages que nous recevons avec plaisir de personnes connues et puis il y a tout le reste, les messages non attendus, non désirés qui s'appellent des spams.
En 2015, malgré les filtres mis en place par les fournisseurs de systèmes de messagerie, il y avait tout de même encore un peu plus de 50% de messages non désirés.
Parmi ces pourriels (poubelle + e-mail) se cachent de nombreux message ayant des objectifs malveillant à votre égard. Les risques les plus répandus sont les incitations au téléchargement d'une pièce jointe, au clic sur un lien renvoyant vers un site Internet piégé ou vous proposer d'échanger dans le but de faire « copain copain » et ensuite vous arnaquer.

La solution : ne pas cliquer sur un e-mail ou un message provenant d'un inconnu, de la même manière qu'on apprend aux enfants de ne pas parler à un inconnu…Pourtant, des millions de personnes en France se font piéger chaque année. Pourquoi ?

A mon avis, les techniques d'Ingenierie sociale sont à la base de ces correspondances. L'ingénierie sociale est une pratique qu exploite les failles humaines et sociales. L'attaquant va utiliser de nombreuses techniques dans le but d'abuser de la confiance, de l'ignorance ou de la crédulité des personnes ciblées.
Imaginez, vous recevez un message ressemblant à ça :
« Objet : changements dans le document 01.08.16
Expéditeur : Prénom et Nom d'une personne inconnue
Bonjour,
Nous avons fait tous les changements necessaires dans le document.
Malheureusement, je ne comprends pas la cause pour la quelle vous ne recevez pas les fichier jointes.
J'ai essaye de remettre les fichier jointes dans le e-mail. »
…
Dans cet exemple, on ne connaît pas la personne, on ne connaît pas le contenu du document, mais la personne sous-entend un nouvel envoi qui peut laisser penser à une ultime tentative. Le document donne l'impression d'être important, le ton est professionnel, il n'y pas trop de faute d'orthographe… Difficile de résister au clic pour savoir ce qui se cache dans ce mystérieux document.

Un autre exemple d'e-mail ou similaire souvent reçu :
« Objet : Commande – CD2533
Expéditeur : Prénom et Nom d'une personne inconnue
Madame, Monsieur,
Nous vous remercions pour votre nouvelle « Commande – CD2533".
Nous revenons vers vous au plus vite pour les delais
Meilleures salutations,
VEDISCOM SECURITE »

En fait, bien évidemment pour ce message aussi, la pièce jointe contient un virus et si le virus est récent et s'il est bien codé, il sera indétectable par tous les filtres chargés de la sécurité informatique de votre patrimoine immatériel.
Auriez-vous cliqué ? Auriez-vous fais partie des dizaines ou centaines de milliers de personnes qui auraient pu se faire piéger ?

Un autre exemple : Vous recevez sur facebook un message venant à première vue d'un inconnu mais l'expéditeur a un prénom que vous connaissez (par exemple Marie, le prénom le plus porté en France en 2016). Serait-ce la « Marie » dont vous ne connaissez pas le nom de famille, rencontrée par hasard lors d'un forum ou d'une soirée qui vous aurait retrouvé sur Facebook ?
Dans le doute vous l'acceptez comme amie pour en savoir plus et engager pourquoi pas la conversation…
C'est un autre moyen utilisé par les pirates informatiques pour rentrer dans votre cercle d'amis et probablement tenter des actes illicites que je ne détaillerai pas ici.

Vous rappelez-vous avoir accepté une demande de mise en contact provenant d'un inconnu sur Facebook ? Peut-être que vous ne connaissiez pas les risques, mais qu'est-ce qui vous a poussé à répondre à un inconnu ? La politesse ? La curiosité ?

A mon avis, le principal levier utilisé pour pousser les gens à cliquer sur les emails pour en voir l'objet, cliquer sur les pièces jointes pour en voir le contenu ou cliquer sur les liens pour découvrir la suite, est une des nombreuses failles humaine : la curiosité.

Cette curiosité peut nous faire faire des choses complètement irresponsables, car on connaît les dangers des pièces jointes ou des liens dans les e-mails. Malgré cela, si notre curiosité est éveillée, il sera difficile de résister au clic censé la satisfaire.

Il est clair que la curiosité positive est nécessaire, mais dans notre monde numérique où les escrocs et pirates oeuvrent en masse le plus souvent en toute discrétion et en toute impunité, la pollution des moyens de communication numériques grand public est telle que le niveau de prudence doit être augmenté au point de ne plus laisser de place au hasard. Le jeu vaut-il vraiment la chandelle face aux graves conséquences que peut engendrer un simple clic mal placé ?

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : One in two users click on links from unknown senders › FAU.EU

Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?

Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de trace sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé (effacer l'historique de ses comptes mails et personnelles, formatage complet, logiciel d'aide à la suppression etc…) ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage.
Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :
• Des programmes ajoutés ;
• Nos e-mails ;
• Nos traces de navigation ;
• Nos fichiers téléchargés ;
• Divers identifiants et mots de passe ;
• Les fichiers temporaires

Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes ajoutés
Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :
• soit par le raccourcis de désinstallation que le programme a créé ;
• s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
• Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (gratuit).

Concernant les e-mails
Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :
• fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
• fichiers dans « » »% »'AppDataLocalMicrosoftWindows Live Mail » pour le logiciel « Windows Live Mail » ;
• les fichiers contenus dans ' » »% »'APPDATA%ThunderbirdProfiles » pour le programme Mozilla Thunderbird
• le dossier contenu dans « ..Local SettingsApplication DataIMIdentities » pour le programme Incredimail.

Concernant nos traces de navigation
En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».

Concernant les fichiers téléchargés
En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Concernant divers identifiants et mots de passe
Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».
Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans vote ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires
En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).
En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Pour finir
Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore »…

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : 5 applications pour effacer des données de façon sécurisée – ZDNet