

# 5 conseils pour combattre le piratage informatique



5 conseils pour combattre le piratage informatique

---

Pour beaucoup d'entre nous, acheter en ligne est devenu une habitude sans laquelle nous pouvons pas vivre. Les achats online simplifient notre quotidien car ils nous permettent de acheter des voyages, des vêtements, des cadeaux et aussi de faire nos courses alimentaires sans bouger ! Internet à changé notre système de vie et, aujourd'hui, presque tout peut s'acheter sur Internet.

Oui, il est beaucoup plus simple et confortable mais, au moment de payer, les doutes aflorent : **comment garantir la sécurité d'une transaction pour pouvoir faire nos achats avoir la mouche à l'oreille ?** Voici 5 conseils donnés pour le cabinet de sécurité ESET pour se prémunir contre les risques de piratage en ligne.

### **Vérifiez l'URL du site internet**

Lorsque vous effectuez un paiement en ligne, l'URL doit impérativement commencer par « https:// ». Cela signifie que le site Internet est sécurisé. De plus, **votre navigateur vous indiquera, au moyen d'un symbole en forme de cadenas, que la sécurité entre votre ordinateur et le site est bien établie.** Doc, si vous n'êtes pas complètement sûrs du site dont vous êtes en train de mettre vos coordonnées, il vaut mieux faire demi-tour.

### **Faites vos achats que sur votre ordinateur personnel**

À priori évident, **il ne faut pas profiter d'un réseau WiFi ouvert pour faire des achats et, non plus, sur un ordinateur que ne soit pas le vôtre.** Il est important de rappeler que quand vous faites ce type d'activité, vous apprêtez à transmettre des données sensibles, telles que votre numéro de carte bleue ou votre adresse personnelle.

**Il est dès lors déconseillé d'utiliser un ordinateur public,** ou même l'ordinateur d'un ami car vous ne connaissez pas si l'appareil est bien protégé. Il suffirait alors qu'un logiciel malveillant soit installé sur la machine pour que vos données privées soient récupérées par des cybercriminels.

### **Privilégiez les réseaux privés**

On vient de le dire: les réseaux publics doivent, par essence, être faciles d'accès : c'est pourquoi ils sont le plus souvent dépourvus de toute protection. **Si vous pouvez y accéder, un cybercriminel peut le faire aussi.** On comprend donc facilement pourquoi il vaut mieux ne pas utiliser ce type de réseau pour effectuer un achat en ligne. **Un hacker pourrait facilement accéder à votre ordinateur et à ce que vous y faites,** et donc dérober sans difficulté votre numéro de carte bleue et autres données sensibles.

### **Évitez d'enregistrer vos données en ligne**

Avec le développement d'intérêt et les services de pub sur la toile. De plus en plus de sites Internet vous proposent d'enregistrer vos coordonnées, numéro de carte bleue compris, afin que vous n'ayez pas à les saisir à nouveau à chaque achat.

C'est vrai que, si vous êtes des fous des achats en ligne, celle-ci est une fonctionnalité très pratique – surtout sur les sites sur lesquels vous achetez souvent, mais attention : **si vous permettez au site Web de se rappeler de vos coordonnées, l'accès à votre compte doit absolument être protégé par un mot de passe fort** pour éviter que ces données soient facilement récupérables par les cybercriminels. Voici quelques conseils pour créer un mot de passe efficace.

### **Utilisez un navigateur sécurisé**

Même si le site sur lequel vous vous apprêtez à payer vous paraît fiable et que vous utilisez un réseau sécurisé, il se peut que des pirates informatiques parviennent à contourner les sécurités pour voler votre numéro de carte bleue. **L'idéal est donc d'utiliser un navigateur sécurisé,** comme celui inclut dans la solution **ESET Internet Security.** Grâce à cet outil, **vos données sont cryptées directement entre le clavier et le navigateur,** ce qui empêche toute possibilité de récupération de vos données bancaires.

---

Notre métier : Nous réalisons des audits sécurité, nous vous apprenons comment vous protéger des pirates informatiques et vous aidons à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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 conseils pour combattre le piratage en ligne – Globb Security FR

---

**Toujours sous Windows XP ?  
Vous êtes une menace pour la  
société**

	<b>Toujours sous Windows XP ? Vous êtes une menace pour la société</b>
---	--

---

**Windows XP ne bénéficie plus de correctif de sécurité depuis 2014 et représente par conséquent un risque. Les utilisateurs ont donc une responsabilité. Et si vous êtes un professionnel de l'IT avec des capacités de décision en entreprise, vous devriez être licencié pour maintenir l'usage d'XP.**

La réaction à mon dernier article – « Pourquoi Windows doit mourir pour la troisième fois » – était considérable. Des centaines de milliers de personnes ont lu cet article, et nous avons eu des discussions très spirituelles, en effet.

Un tas d'entre vous l'a déclaré sans ambages : vous ne souhaitez pas mettre à niveau Windows XP. Vous êtes fâchés que Microsoft vous ait fait passer de XP à 7 et de 7 à 10. Vous êtes en colère de devoir en permanence mettre à jour le logiciel.

Une poignée d'entre vous a même suggéré de s'en prendre physiquement aux développeurs qui codent le logiciel vers lequel vous refusez de migrer...[lire la suite]

---

## **NOTRE MÉTIER :**

- **FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO**
- **EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES**
- **AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT**
  - **MISE EN CONFORMITE RGPD / FORMATION DPO**

**FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO :** En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

**EXPERTISES TECHNIQUES :** Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

**COLLECTE & RECHERCHE DE PREUVES :** Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

**AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT :** Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD :** Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

**Besoin d'un Expert ? contactez-nous**

### **NOS FORMATIONS**

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>  
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Toujours sous Windows XP ? Vous êtes une menace pour la société – ZDNet*

---

# Formation pour DPO externe mutualisé et Délégués à la protection des données externalisé

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



Depuis 2012, nous accompagnons des établissements dans leur mise en conformité avec la réglementation sur les Données à Caractère Personnel.



Formation RGPD  
pour DPO externe  
mutualisé et  
Délégués à la  
protection des  
données  
externalisé

---

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

**Formation pour DPO externe ou Délégué à la protection des données externalisé : « J'accompagne mes clients dans leur mise en conformité avec le RGPD » : 3 jours + 1 jour d'accompagnement personnalisé (C'est le moment ou jamais de vendre des services « RGPD »)**

Si votre objectif est avant tout de développer l'activité de mise en conformité avec le RGPD afin de vendre cette prestation auprès de vos clients, cette formation est faite sur-mesure pour vous en vous apportant l'ensemble des mesures et des cas qu'il est nécessaire de maîtriser pour que vos clients soient mis sur le chemin de la mise en conformité. Vous êtes une société d'Informatique, un cabinet d'avocat, un cabinet d'expertise comptable, un consultant et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation se passe sur 3 jours en groupe plus une journée supplémentaire en individuel pour superviser la mise en place du RGPD dans votre établissement ou chez un de vos clients (frais liés au déplacement dans cet établissement en sus). Suivez LA formation qui vous apportera la plus grande autonomie dans la mise en conformité de tout notre catalogue.

Consultez les prochaines dates d'animation autour de chez vous ?



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel), consultant depuis 1996 et formateur depuis 1998. J'ai 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi aisé d'expliquer le côté pragmatique et la démarche de mise en conformité avec le RGPD.

**« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »**

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

**Vous souhaitez avoir des informations sur :**

- La formation « Comprendre le RGPD » : 1 jour
- La formation « Je veux devenir Délégué à la Protection des Données » 2 jours
- La formation « Je mets en conformité mon établissement » 3+1 jours
- La formation « Mise en conformité RGPD sur mesure »
- un accompagnement personnalisé au RGPD

**Vous souhaitez réserver une ou plusieurs place(s) à la formation :**

Formation pour TPE/PME : « **Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.

Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.

N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : « **Je veux devenir le Délégué à la Protection des Données de mon établissement** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.

Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.

N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : « **J'accompagne mes clients dans leur mise en conformité avec le RGPD** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.

Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.

N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte sera remboursé en intégralité dans les 5 jours (Les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

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 : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

---

# Pendant les vacances continuez à protéger vos données personnelles

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"/>	<b>Pendant les vacances, continuez à protéger vos données personnelles</b>				



**Pendant les vacances, continuez à protéger vos données personnelles**

---

Les utilisateurs sont de plus en plus concernés par le sort de leurs données. Potentiellement victimes, ils doivent prendre plus de temps pour consulter les pages de politique de confidentialité. Qu'en est-il de ces utilisateurs finaux ? Sont-ils acteurs de la sécurité en ligne de leurs données ? Il n'est pas inutile de rappeler certains points.

- **Les dangers du Wi-fi public**

Lorsque vous rejoignez un réseau Wi-Fi public ouvert à votre café préféré, vous pouvez obtenir plus qu'un expresso. Vous pourriez potentiellement être victime d'un vol d'informations. En outre, un pirate peut avoir créé un faux réseau Wi-Fi qui semble réel (avec un nom similaire par exemple). L'utilisation d'un VPN est donc fortement recommandée.

- **Les dangers des applications**

Les applications sur votre smartphone peuvent vous espionner. Soyez très prudent lorsque vous sélectionnez des applications. Jetez un œil aux fonctionnalités dictées par le développeur. Maximisez les paramètres de confidentialité autant que possible.

- **Les dangers des médias sociaux**

Évitez les quiz Facebook qui peuvent relever toutes vos données (Cambridge Analytica). Minimisez les informations que vous partagez sur les réseaux sociaux. N'acceptez pas les demandes de personnes que vous ne connaissez pas.

Tout le monde peut prétendre être quelqu'un d'autre en ligne – prenez des mesures supplémentaires pour assurer votre sécurité et celle de votre famille. En conclusion, n'hésitez pas à vous référer à des conseils, guides, vidéos de la part des professionnels du secteur et autres associations, sans oublier le site de la CNIL et ses guides qui fournissent de bons conseils et recommandations.

[Lire l'article complet sur [LaTrinune.fr](http://LaTrinune.fr)]

---

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](#)



Source : *Vous attendez tout du RGPD pour protéger vos données en ligne. Pas si vite !*

# Comment retrouver l'auteur d'un e-mail ou d'un post ? | Denis JACOPINI

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



Denis JACOPINI



Comment retrouver l'auteur d'un e-mail ou d'un post ?

**Victime d'usurpation d'identité, d'insultes ou de propos diffamatoires, vous désirez retrouver l'auteur d'un e-mail ou d'un post sur un forum ou sur un réseau social ? Les conseils de Denis JACOPINI, expert informatique assermenté.**

## **1. RETROUVER L'AUTEUR D'UN EMAIL**

### **1.1 Les envois d'e-mail**

Tout comme un courrier postal sans système de sécurité tel le Recommandé avec Accusé de Réception, l'envoi d'un e-mail ne garanti pas sa réception par le destinataire désiré.

Il devient ainsi aisé de contester la réception d'un e-mail et quand bien même il a été prouvé qu'un email a été reçu et lu, rien ne peut attester qu'il a bien été consulté par la bonne personne. Pour parer à ses failles, il existe des solutions rarement utilisées d'envoi sécurisés par des tiers de confiance pouvant attester la récupération d'un e-mail par une personne identifiée et des procédés de cryptages/décryptages permettant de rendre consultable l'email par le détenteur d'une clé unique.

Sachez que la notion d'accusé de réception n'est pas universelle et dépendant de la compatibilité éventuelle être les logiciels de messagerie de l'expéditeur et du destinataire.

En conclusion, après l'envoi d'un e-mail qui n'utilise pas de procédé de traçabilité, il n'y a pas d'outil permet de confirmer la lecture de l'e-mail par une personne précise. Les outils de traçabilité standards communément rencontrés dans les solutions d'e-mailing, utilisent généralement une petite image spécifique, invisible stockée sur un serveur qui, une fois affichée sur le logiciel de messagerie du destinataire, horodate et mémorise l'adresse IP de l'accès et les paramètres du destinataire ayant affiché l'image.

### **1.2 La réception d'emails**

Lorsque le destinataire d'un e-mail prend connaissance de son message, il est mis en forme par son logiciel de messagerie électronique. Les e-mails peuvent être reçus au format « texte » ou au format « html » avec des mises en forme esthétiquement intéressantes et peuvent contenir ou non une ou plusieurs pièces jointes.

Cependant, chaque e-mail reçu répond à un format spécifique

Un courrier électronique est composé de deux parties : les entêtes et le corps du message, séparés par une ligne vide. Les entêtes stockent les informations contextuelles : qui envoie le message, à qui, avec quel objet, ou encore à quelle date. Le corps du message est quant à lui encodé sous forme de texte, ou de parties multiples (par exemple un texte et des images).

Exemple d'entête d'un message ayant comme seul texte affiché pour le destinataire :

Objet : Bonjour !

Message :

Bonjour David,

Tiens-moi au courant pour la réunion.

Thomas

L'entête contiendra :

Received: from 31.121.118.45 (EHLO serveur.fr)

by mta1007.mail.ukl.yahoo.com with SMTP; Fri, 21 Sep 2012 21:31:16 +0000

Received: by serveur.fr (Postfix, from userid 106)

id 3DF2F15A0CD; Fri, 21 Sep 2012 23:31:16 +0200 (CEST)

From: "Thomas"

To: david@yahoo.fr

Subject: Bonjour !

Date: Fri, 21 Sep 2012 23:31:16 +0200

MIME-Version: 1.0

Content-Transfer-Encoding: 8bit

Content-Type: text/plain; charset=iso-8859-1

X-Mailer: Mozilla Thunderbird

Message-Id:

Bonjour David,

Tiens-moi au courant pour la réunion.

Thomas

L'analyse de l'entête nous permet d'avoir la date et l'heure d'envoi (attention aux indications de fuseau horaire), l'adresse IP et le nom de domaine du serveur expéditeur, l'ID de l'e-mail sur le serveur expéditeur

#### **Remarque :**

Un échange d'e-mails (minimum envoi + réponse) permettra plus facilement d'apporter la preuve de que le destinataire a bien reçu le message électronique puisqu'il y répond...

A la suite d'une usurpation d'identité, d'une arnaque, d'un dénigrement, d'injures, de médisance ou de propos diffamatoires, vous pouvez souhaiter retrouver l'expéditeur d'un e-mail :

A) Constat éventuel par Procès Verbal d'Huissier de l'e-mail ;

B) Analyse des éventuels échanges d'e-mails

C) Analyse par un Expert Informatique de l'entête de l'email afin d'extraire la date, l'heure, l'adresse IP et le nom de domaine du serveur d'expédition de l'e-mail ;

D) Rechercher le propriétaire d'une adresse IP avec l'outil [www.ripe.net](http://www.ripe.net) ou <http://network-tools.com> ;

E) Plages d'adresses IP attribuées par opérateurs sur la page <http://www.nirsoft.net/countryip/fr.html> ;

F) Contact éventuel des fournisseur d'accès à Internet pour retrouver l'abonné à Internet à partir de l'adresse IP (ordonnance d'un Juge).

## **2. RETROUVER L'AUTEUR D'UN POST SUR UN FORUM**

A la suite d'une arnaque, d'un dénigrement, d'injures, de médisance ou de propos diffamatoires, vous pouvez chercher des traces de l'auteur dans des forums ou réseaux sociaux. Vous aurez alors des traces de ses posts, souvent bien insuffisants pour remonter jusqu'à l'auteur malveillant.

Pourtant, quelques pistes peuvent être exploitées :

A) Constat éventuel par Procès Verbal d'Huissier du post avec horodatage.

B) L'auteur peut utiliser des éléments permettant de retrouver son identité (par exemple, son pseudo est peut-être utilisé sur plusieurs sites et l'identification peut être tentée par recoupement d'informations...)

C) Rechercher d'autres traces du pseudo dans d'autres sites (Social Mention, Samepoint, Mention.net, Alerti, Youseemii.fr, Webmii, Sprout social, eCaim.com, zen-reputation) ;

D) L'analyse de données Exif permet d'avoir des renseignements supplémentaires (par exemple : ExifViewer) ;

E) Si une demande de retrait par voie amiable des informations par l'auteur n'aboutit pas, vous avez la possibilité de signaler un acte d'injure ou de diffamation sur le site Internet du ministère de l'Intérieur : <http://www.internet-sigalement.gouv.fr> ou saisir une juridiction de proximité (<https://www.service-public.fr/particuliers/vosdroits/F1785>) ;

F) Comme pour un contenu dans un moteur de recherche, on peut essayer d'utiliser le Flooding pour envoyer le post dans des pages de résultat lointaines.

Bien évidemment cette liste de conseils pas exhaustive et n'attend que vos avis et commentaires pour l'enrichir

---

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](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](http://Fnac.fr)

Etude et publication de Denis JACOPINI

LIENS SOURCES

Utilisation des moteurs de recherche en France

<http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/>

Taux de clic en fonction de la position dans les résultats

<http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fonction-des-positions-dans-google/544>

---

# Tout ce que vous ne savez pas sur les clés USB | Denis JACOPINI

	<b>Tout ce que vous ne savez pas sur les clés USB</b>
---	---

---

La majorité des personnes savent très bien que la clé USB est un support de stockage amovible, c'est ce qui leur fait penser qu'une clé USB permet uniquement de stocker des fichiers à partir de tout système disposant de prises USB ou de transférer des données entre ordinateur. Or la clé USB peut être utilisée de plusieurs manière différentes.



Aujourd'hui, je vais vous montrer qu'il existe d'autres fonctions plus intéressante qu'on peut les utiliser à l'aide d'une simple clé USB.

### **1. Transformer votre clé USB à une barrette mémoire RAM**

Une clé USB peut être utiliser pour améliorer les performances de votre ordinateur et augmenter la vitesse de son fonctionnement. L'astuce consiste à utiliser une clé USB pour augmenter la mémoire de votre ordinateur et booster ses performances à l'aide de logiciel eBoostr. Pour en savoir plus, je vous invite à lire cet article: l'utilisation de clé USB en tant que barrette.

### **2. Sécuriser votre PC avec une clé USB**

On peut aussi utiliser une clé USB pour sécuriser son PC. L'utilitaire Rohos Logon Key fera en sorte que votre ordinateur s'ouvrira automatiquement au moment où vous insérerez la clé USB et se verrouillera lorsque vous la retirerez. Vous pourrez donc quitter votre ordinateur en toute sérénité. Pour en savoir plus, je vous invite à lire l'article suivant: la sécurité de votre pc avec une clé USB

### **3. Création d'une clé USB rootkit**

Une autre fonction qu'on peut l'utiliser avec une clé USB, c'est la récupération des mots de passe d'un ordinateur. La clé USB s'exécute automatiquement et récupère la plupart des mots de passe stockés sur votre ordinateur. Il est vraiment très utile surtout quand on perd les mots de passe. Pour en savoir les étapes pour créer une clé USB rootkit, je vous invite à lire cet article: création d'une clé USB rootkit.

### **4. Injecter une backdoor dans une machine Windows avec une clé USB**

On peut aussi utiliser une clé USB pour accéder à votre PC à distance depuis n'importe quelle machine. Pour créer votre USB backdoor suivez les étapes de notre article: injection d'une backdoor dans une machine Windows avec une clé USB.

### **5. Emporter dans une clé USB vos logiciels préférés sans avoir besoin de les installer**

Enfin, une autre fonction qui pourrait vous intéresser: c'est d'utiliser des logiciels stockés sur votre clé USB sans avoir besoin de les installer. Pour cela, il faut installer le programme gratuit **PortableApps** .

Il devient alors très facile d'ajouter vos logiciels préférés au lanceur d'applications portable « PortableApps ». Un outil principalement destiné aux développeurs qui enrichit et complète la suite logicielle référence en la matière. Le logiciel Open Source PortableApps propose déjà un panel très large d'applications portables : Firefox, LibreOffice, Google Chrome, Skype ou encore Dropbox. Ce lanceur vous permet d'utiliser les logiciels stockés sur la clé USB depuis un autre PC sans avoir à les installer.

Comme nous l'avons vu précédemment, une clé USB peut servir à autre chose qu'à stocker des données. Elle possède d'autres avantages. Si vous avez d'autres fonctions d'une clé USB, n'hésitez pas de les partager avec nous dans un commentaire . ☐

Article original de Ahmed



Réagissez à cet article

Original de l'article mis en page : Tout ce que vous ne savez pas sur les clés USB | FunInformatique

---

# Fraude sur Internet : comment éviter les pièges | Denis JACOPINI

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



**Fraude sur Internet : comment éviter les pièges**

**Les fraudes sur Internet sont de plus en plus fréquentes. Apprenez à éviter les pièges tendus par ces pirates qui se font passer pour EDF, la Caf ou encore l'Assurance maladie.**

Si vous bénéficiez d'une aide de la Caf, êtes client EDF ou assuré social, il est possible que vous soyez victimes d'arnaques sur Internet appelées phishing.

Des pirates envoient des e-mails frauduleux pour récupérer vos données personnelles, vous soutirer de l'argent, voire usurper votre identité.

#### **En quoi consiste le phishing ?**

Le phishing (ou hameçonnage) est une fraude pratiquée par des pirates informatiques. Ils envoient en masse et de manière aléatoire de faux e-mails en prenant l'identité de grandes sociétés ou organismes.

Leur objectif : recueillir vos données personnelles afin de vous escroquer. Ils peuvent tenter de récupérer :

- les données d'accès à votre espace personnel ;
- le numéro de votre carte bancaire, votre RIB ;
- votre adresse postale...

Le plus souvent, les messages frauduleux vous informent d'un retard de paiement, d'un remboursement, ou proposent de mettre à jour vos informations personnelles.

Ne cliquez pas sur les liens présents dans ces e-mails car ils peuvent contenir des virus et rediriger vers des sites non sécurisés.

#### **Comment identifier une tentative de phishing ?**

EDF, la Caf et l'Assurance maladie ne demandent jamais de coordonnées bancaires par e-mail (numéro de compte, numéro de carte bancaire, cryptogramme).

Ces données sont strictement confidentielles et sont uniquement requises dans votre espace personnel pour le paiement d'une éventuelle facture par carte bancaire ou par prélèvement automatique.

Afin de ne pas être victime d'une arnaque sur Internet, il est conseillé de regarder :

- l'adresse du site Internet dans la barre de navigation : sécurisée, elle commence toujours par « https » (et non pas « http ») ;
- l'adresse Internet de votre espace personnel. Elle est aussi sécurisée et commence par « https » ;
- l'exactitude de vos informations dans l'espace personnel (numéro de facture EDF, par exemple qui n'est certainement pas le même que celui qui apparaît sur votre véritable facture) ;
- l'orthographe et la syntaxe des messages que vous recevez. Les messages frauduleux comportent souvent des fautes de français.

#### **Comment se protéger des arnaques sur Internet ?**

Si vous avez des doutes concernant l'origine d'un e-mail, il est recommandé de :

- ne pas y répondre ;
- ne pas fournir les données qui vous sont demandées ;
- ne pas cliquer sur les liens ou les boutons présents dans l'e-mail, ne pas ouvrir ses pièces-jointes ;
- signaler le message frauduleux en le transmettant aux adresses suivantes :
  - pour EDF : [message-frauduleux@edf.fr](mailto:message-frauduleux@edf.fr) ;
  - pour la CAF : [www.phishing-initiative.com](http://www.phishing-initiative.com) ;
  - pour l'Assurance maladie : plateforme Pharos ;
- mettre à jour le système de sécurité de votre ordinateur ou de votre smartphone ;
- éviter de consulter des pages Internet contenant vos données confidentielles depuis des ordinateurs installés dans des lieux publics.

#### **Que faire si vous êtes victime d'une fraude sur Internet ?**

Si vous avez cliqué involontairement sur le lien d'un e-mail frauduleux ou si vous avez fourni des informations confidentielles, suivez ces étapes :

- contactez immédiatement votre établissement bancaire et faites opposition ;
- modifiez votre mot de passe directement dans votre espace personnel. Si vous ne parvenez plus à vous connecter, demandez un nouveau mot de passe par e-mail ;
- mettez à jour votre antivirus et procédez à une analyse de votre ordinateur ;
- vérifiez que votre pare-feu est bien activé ;
- sélectionnez l'e-mail frauduleux dans votre boîte de réception et signalez-le comme « indésirable ».

**Le phishing, même une seule tentative, est un délit pénal contre lequel vous pouvez porter plainte au commissariat ou à la gendarmerie la plus proche.**

Pour cela, munissez-vous de tout document permettant d'en identifier l'auteur (copie des e-mails, adresse e-mail ou postale, référence du transfert d'argent effectué...).

---

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](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.dossierfamilial.com/fraude-sur-internet-comment-eviter-les-pieges-20905.html>  
Auteur : Ysabelle Silly

---

# 10 bonnes pratiques pour des soldes sur Internet en sécurité

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"/>	<b>10 bonnes pratiques pour des soldes sur Internet en sécurité</b>				

---

**Pour réaliser vos achats en ligne en toute sécurité, ESET vous donne des conseils pour éviter de se faire pirater sa carte bancaire.**

– **Faites attention aux sites Internet que vous ne connaissez pas.** Au moindre doute, n'effectuez pas vos achats, car il peut s'agir d'un faux site Internet qui tente de récupérer les informations de votre carte bancaire.

– **Préparez-vous aux attaques par phishing.** Elles se diffusent massivement par e-mail lors des soldes, car c'est à cette période que les internautes passent le plus de temps sur les sites Internet de vente en ligne. ESET a réalisé une courte vidéo pour vous expliquer comment éviter le phishing par e-mail.

– **Utilisez des méthodes de paiement sécurisé.** Vérifiez que l'URL mentionne HTTPS. Effectuez toujours vos paiements sur des sites Internet chiffrés.

– **Attention aux annonces sur Facebook.** Les plateformes des réseaux sociaux abondent de fausses annonces et sites Internet proposant des offres intéressantes. Évitez également de partager les détails de votre carte bancaire par message : vous ne pouvez pas vérifier l'identité des personnes qui ont accès au compte et qui recevront ces informations.

– **Effectuez toujours vos achats sur des appareils sécurisés et évitez de vous connecter à un Wi-Fi public.** Ce genre d'arnaque, appelé Man-in-the-Middle (MiTM) est très répandu. En 10 minutes, le pirate peut voler toutes les informations vous concernant.

– **Utilisez des mots de passe forts ou un gestionnaire de mots de passe.** Plusieurs études ont montré que les utilisateurs ayant plus de 20 comptes en ligne et étant actifs sur Internet sont plus susceptibles de réutiliser les mêmes mots de passe pour plusieurs accès. Selon le rapport de recherche et de stratégie Javelin, cette méthode augmente de 37% le risque de voir ses comptes compromis. Aussi, les experts ESET recommandent d'utiliser des mots de passe forts mélangeant des minuscules et des majuscules à des symboles et chiffres. Les gestionnaires de mots de passe peuvent être utilisés pour ne pas avoir à les apprendre par cœur. Retrouvez les erreurs les plus courantes lors de l'utilisation d'un mot de passe en cliquant [ici](#).

– **Soyez prudent avec votre smartphone.** Le nombre de cybermenaces sur cette plateforme a considérablement augmenté. Pour commencer, faites vos achats uniquement via des applications certifiées et supprimez les applications dont vous ne vous servez pas. Pensez à désactiver le Wi-Fi lorsque vous faites votre shopping dans un lieu public, privilégiez les données cellulaires, ceci permettra d'empêcher les cybercriminels de vous diriger vers un faux Wi-Fi afin de voler vos informations bancaires.

– **Utilisez une e-carte bleue.** Non seulement elle est déconnectée de vos comptes bancaires et est également assurée contre les fraudes.

– **Respectez les règles de sécurité de base.** Cela peut paraître évident, mais avant de faire vos achats, assurez-vous d'être correctement protégé : installez une solution de sécurité efficace et mise à jour. Optez pour une solution qui offre une navigation sécurisée pour les transactions bancaires. Enfin, ajoutez des mots de passe à votre écran de verrouillage ou un code PIN à votre smartphone.

– **Évitez de réaliser vos achats sur différents appareils (1 à 2 maximum).** Plus vous entrerez les informations de votre carte de crédit sur des appareils différents (PC, tablette, smartphone...), plus vous multipliez le risque d'être victime d'une fraude.

---

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](http://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](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)

Article original de ESET

---

## **Piratage massif sur Twitter :**

# voici comment protéger votre compte (et le récupérer en cas de besoin) | Denis JACOPINI

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

x

x

x

x

x

x

x

**Piratage massif sur Twitter : voici comment protéger votre compte (et le récupérer en cas de besoin)**

**Pas moins de 32 millions d'identifiants Twitter seraient actuellement mis en vente en ligne à la suite d'un piratage massif : des adresses e-mails, des identifiants et des mots de passe, dérobés directement sur les navigateurs des internautes. Voici nos astuces pour mieux protéger votre compte, et le récupérer en cas de piratage.**



Le réseau social américain s'est empressé de rassurer ses utilisateurs après les révélations par le site LeakedSource de la mise en vente en ligne de plus de 32 millions d'identifiants Twitter dérobés par des hackers. A la différence de MySpace, victime d'une fuite de données identique en mai dernier, Twitter n'a pas été directement infiltré par les pirates.

D'après LeakedSource, les données dérobées – des adresses e-mail, des identifiants, et des mots de passe – l'ont été directement sur les navigateurs des victimes grâce à des malwares. Evidemment, le risque zéro n'existe pas, néanmoins, des solutions simples peuvent contribuer à compliquer un peu plus l'action de ces hackers malintentionnés. Voici comment procéder.

#### **► Optez pour le bon mot de passe**

Bien qu'on rechigne souvent à le faire, de peur de l'oublier, le choix du mot de passe est une étape cruciale pour s'assurer un niveau de protection suffisant. Utilisez autant que possible chiffres, lettres, minuscules, capitales et symboles.

La Commission nationale de l'informatique et des libertés (Cnil) recommande d'utiliser un moyen mnémotechnique : par exemple, la phrase « un Utilisateur d'Internet averti en vaut deux » correspond au mot de passe « 1Ud'Iaev2 ».

#### **► Ajoutez votre numéro de téléphone**

En associant un numéro de téléphone à votre compte, vous pourrez profiter de fonctionnalités de sécurité telles que la vérification de connexion (grâce à la réception d'un SMS). Pour ce faire, il suffit de se rendre dans le menu, en haut droite, en cliquant sur votre image de profil. Puis, allez dans la section « Mobile ».

#### **► Comment savoir que votre compte a été piraté**

Toujours dans le menu « Réglages », cette fois, rendez-vous dans la section « Vos données Twitter ». Vous pourrez ainsi consulter l'historique des connexions, ainsi que les appareils qui s'y sont connectés. Si, comme dans l'exemple ci-dessous, vous constatez une anomalie (dans notre cas, une connexion depuis le Mexique), cela signifie que votre compte Twitter est compromis.



#### **► Que faire quand son compte est hacké**

Le diagnostic classique : vous n'arrivez plus à vous connecter et votre compte se met à tweeter tout seul ou vos amis reçoivent du spam en message privé. Si vous pouvez accéder à votre compte, changez votre mot de passe immédiatement. Twitter propose une réinitialisation du mot de passe en entrant votre email ou bien votre numéro de téléphone (mais pour cela, il faut l'avoir associé comme expliqué plus haut).

Enfin, si aucune de ces solutions ne marche, vous pouvez demander l'assistance de Twitter. Pour terminer, n'oubliez pas de révoquer l'autorisation de toutes les apps utilisant Twitter. Pour ce faire, allez dans « Réglages », puis dans « Applications ».

Article original de MATTHIEU DELACHARLERY



---

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](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](http://Fnac.fr)

Original de l'article mis en page : Piratage massif sur Twitter : voici comment protéger votre compte (et le récupérer en cas de besoin) – metronews

---

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

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"/>	<b>Victime d'un piratage informatique, quelles sont les bonnes pratiques ?</b>				

**Les cas de piratages informatiques ne se comptent plus depuis bien longtemps. Cependant, si vous vous êtes retrouvés victimes, il est urgent de mettre en pratique des règles de base.**

Les 3 axes vers lesquels votre structure devra progresser seront :

- Technique, par une amélioration des mesures de sécurité en place ;
- Juridique, par une présentation, auprès des principaux acteurs de votre structure pour une meilleure acceptation, des principales mesures de mise en conformité avec les règles françaises et européennes relatives à la protection des données personnelles ;
- Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

Face à vos besoins d'accompagnement, nos formateurs ont élaboré un parcours destinés aux équipes de direction de votre structure, à l'équipe informatique et aux utilisateurs susceptibles d'être piégés.

En vous accompagnant sur ces 3 axes et auprès de ces 3 profils, vous pourrez alors comprendre comment les pirates informatiques vous ont piégé, découvrir s'ils pourront encore vous piéger et surtout, le plus important, quelles changements mettre en place pour limiter les risques à l'avenir.

---

[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](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)