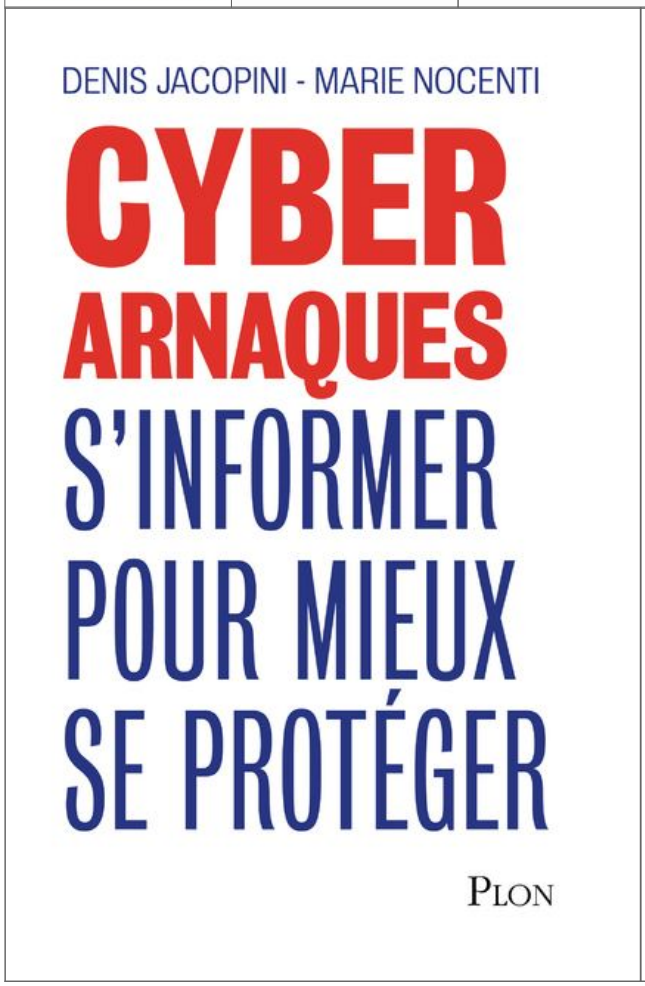
Denis JACOPINI sur Europe 1 parle de son livre « CYBERARNAQUES S'informer pour mieux se protéger » dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel WIZMAN

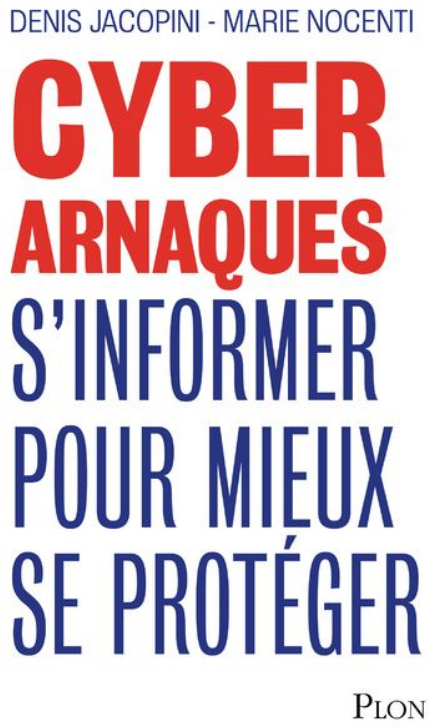


Denis JACOPINI sur Europe 1 parle de son livre « CYBERARNAQUES S'informer pour mieux se protéger » dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel WIZMAN

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.

Denis JACOPINI en parle ce jeudi 14 avril 2018 en direct sur Europe 1 dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel Wizman

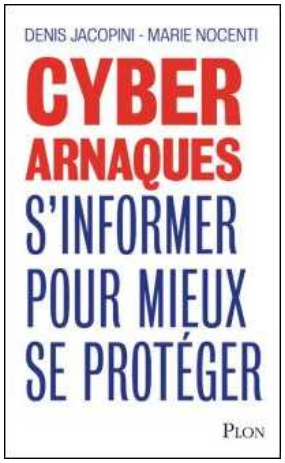
http://www.europe1.fr/emissions/bonjour-la-france



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.

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

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

Commandez sur Fnac.fr

---

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

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

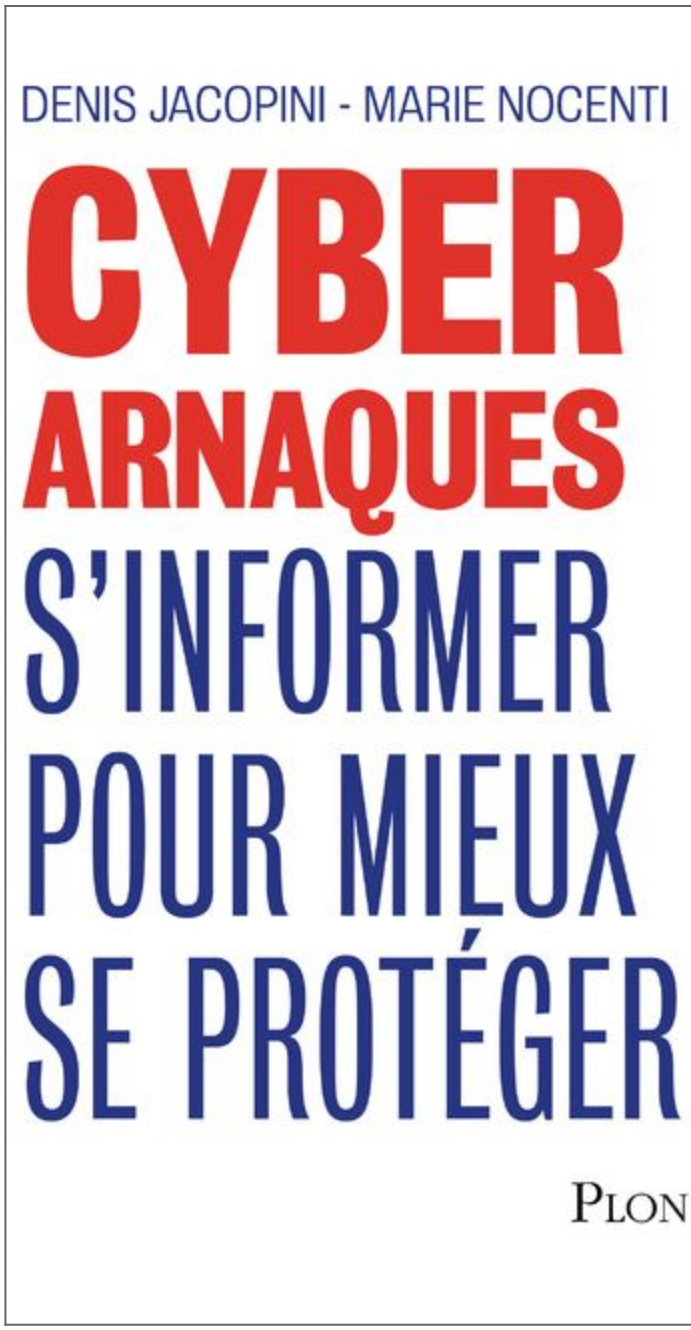
Commandez sur amazon.fr

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

Commandez sur Fnac.fr

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

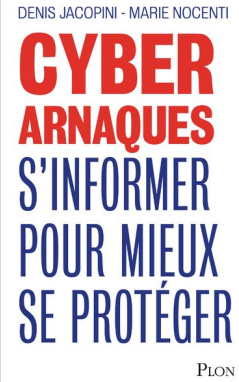
Denis JACOPINI sur Europe 1 parle de son livre « CYBERARNAQUES S'informer pour mieux se protéger » ce jeudi 12 avril 2018 en direct dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel WIZMAN



Denis JACOPINI sur Europe 1 parle de son livre « CYBERARNAQUES S'informer pour mieux se protéger » ce jeudi 12 avril 2018 en direct dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel WIZMAN

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. Denis JACOPIN en parle ce jeudi 14 avril 2018 en direct sur Europe 1 dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel Wizman

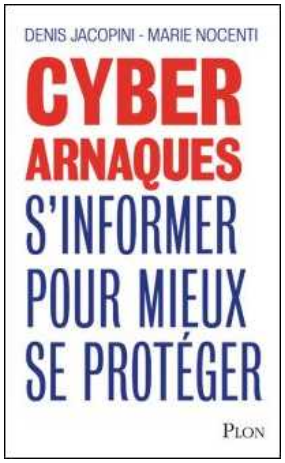
http://www.europe1.fr/emissions/bonjour-la-france



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.

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

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

Commandez sur Fnac.fr

---

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

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

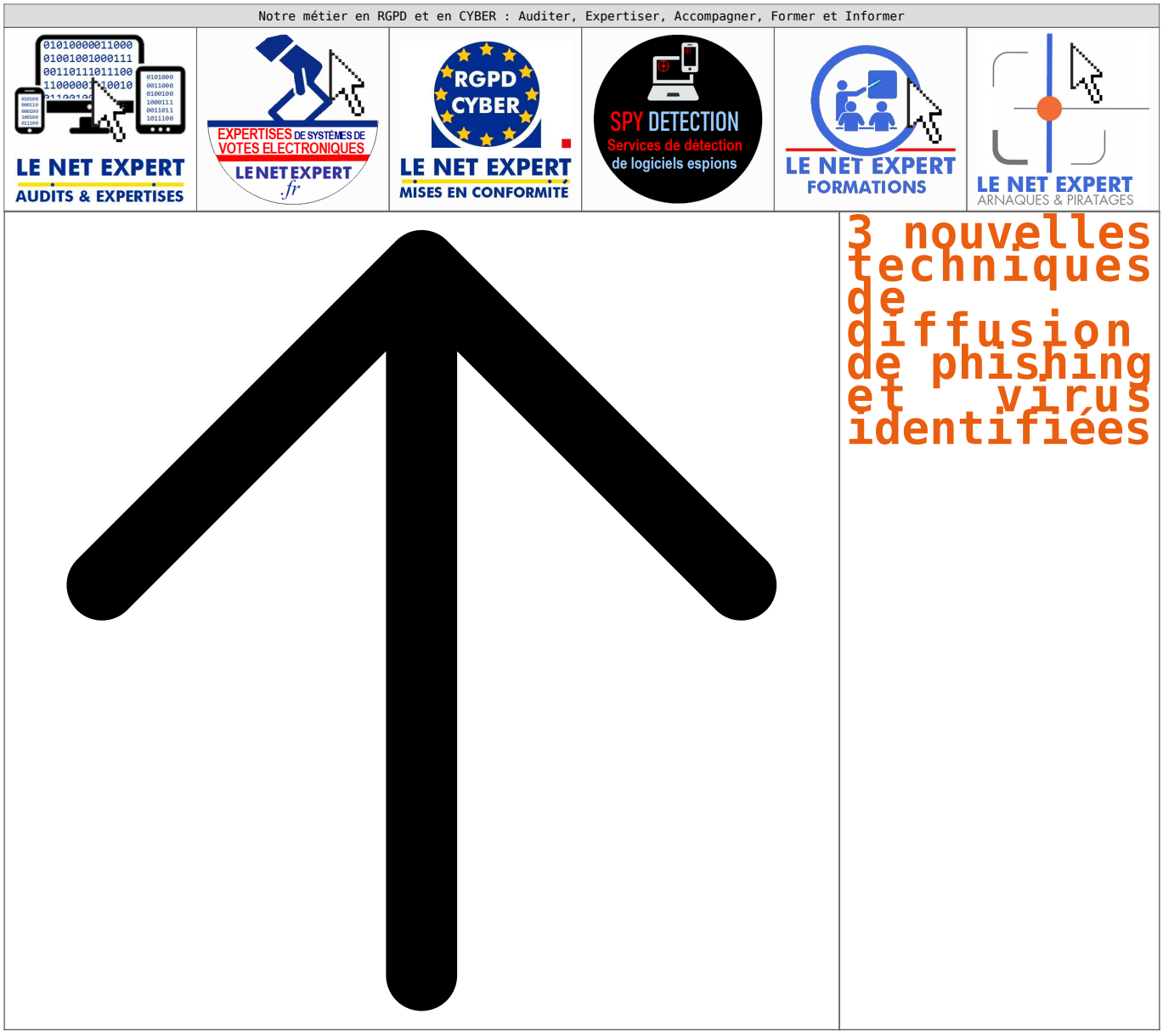
Commandez sur amazon.fr

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

Commandez sur Fnac.fr

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

3 nouvelles techniques de diffusion de phishing et virus identifiées | Denis JACOPINI



Alors qu'auparavant le spam était essentiellement source de désagréments et de baisse de productivité, il sert également aujourd'hui à véhiculer des virus et des attaques par phishing très dangereuses.

L'e-mail reste la porte d'entrée préférée des hackers sur les réseaux d'entreprise. Ainsi, près de 90% des e-mails envoyés sur les adresses de messagerie professionnelles sont des spam. Alors qu'auparavant ces spam étaient essentiellement source de désagréments et de baisse de productivité, ils servent également aujourd'hui à véhiculer des virus et des attaques par phishing très dangereuses, qui gagnent continuellement en intensité et en intelligence.
Plusieurs finalités à ces attaques : voler des données (identifiants personnels, coordonnées bancaires, propriété intellectuelle, etc.), et de l'argent (via des trojan banking par exemple ou des cryptolocker et demandes de rançons) mais également infiltrer des réseaux pour mener des attaques ultérieures de plus grande envergure et développer des réseaux de botnets de plus en plus puissants pour diffuser encore plus de spam, virus et phishing.

3 nouvelles techniques identifiées

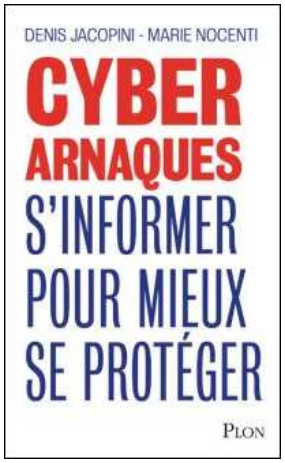
> Des vagues qui utilisent des adresses IP non reconnues
Les cybercriminels se servent de réseaux de botnets/spambots (réseaux de PC zombies) dont ils ont considérablement développé la puissance ces derniers mois. Grâce à ces réseaux, les cybercriminels sont en mesure d'envoyer régulièrement des vagues massives et intenses de spam – jusqu'à plusieurs millions de spam simultanément pour les plus gros réseaux. La force de ces campagnes de spam massives est qu'elles sont basées sur des réseaux de PC bénéficiant d'adresses IP non reconnues, que les outils de filtrages antispam classiques par signatures ou réputation ne sont pas en mesure d'identifier comme spam dans un premier temps.
L'utilisation d'adresses IP non blacklistées permet aux spam, et potentiellement aux virus et phishing de franchir les systèmes de filtrage – traditionnels basés sur les signatures ou réputation- qui ont besoin de temps pour identifier et blacklister ces nouvelles adresses. Pour les hackers, cela suppose toutefois de renouveler leurs réseaux de PC zombies non identifiés entre chaque attaque. On observe ainsi une période de 6 à 10 jours entre chaque très grosse vague de spam. Entre-temps les hackers se livrent surtout à de petites attaques pour infecter de nouveaux postes et ainsi faire croître leur réseau de PC zombies. Le seul moyen de bloquer efficacement ces vagues est d'utiliser le filtrage heuristique qui permet d'analyser le contenu des e-mails plutôt que de se baser uniquement sur son origine (réputation) ou sa propagation sur les réseaux et l'internet (signature).

> Des virus à tout faire (polymorphes)
Illustration de la nouvelle ère de l'industrialisation du hacking, les virus sont également de plus en plus intelligents. Alors qu'auparavant chaque virus était programmé pour une action précise, les virus actuels sont commandés à distance. Après avoir pénétré le réseau le plus discrètement possible, un virus actuel peut être commandé à distance et être utilisé au besoin par exemple comme actif d'un spambot de grande envergure voire même pour une attaque de cryptolockage.

> Activation des liens URL de phishing après le passage du filtre
En matière de phishing (phishing ciblé), les cybercriminels font également preuve de plus en plus d'intelligence pour faire évoluer leurs techniques. Ainsi, certains cybercriminels envoient des e-mails de phishing utilisant des liens URL activables à distance, une fois les outils de filtrage franchis. Cette technique permet aux e-mails de phishing de franchir le filtrage sans être détectés puisque les liens URL renvoient vers un contenu totalement légitime. Ce n'est qu'une fois les barrières franchies que les hackers vont les activer pour les faire renvoyer vers des sites de phishing frauduleux.
Cette technique de plus en plus utilisée est très efficace mais cependant encore peu répandue car elle n'est techniquement pas à la portée de tous les hackers.

Le hacking s'est fortement industrialisé ces dernières années. Les techniques utilisées pour diffuser du spam massivement et des virus sont de plus en plus intelligentes et dangereuses pour les entreprises. Pour se protéger mieux, l'éducation et la formation des utilisateurs sont des axes primordiaux d'où l'importance de rappeler quelques règles de base :
• N'ouvrir les pièces jointes suspectes (fichiers .zip, .xls ou .doc.) que si l'expéditeur est confirmé.
• Supprimer le message d'un expéditeur suspect inconnu sans y répondre.
• Refuser de confirmer l'accusé de réception dans le cas d'un expéditeur inconnu suspect. Cela risquerait de valider et diffuser l'adresse e-mail de l'utilisateur à son insu.
• Remonter les emails identifiés comme spam auprès de son service informatique. Ils seront ensuite transmis à l'entreprise chargée de la protection des messageries pour une prise en compte dans la technologie de filtrage.
• Et en cas de doute, contacter son service informatique.

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 : http://www.journaldunet.com/solutions/expert/62660/diffusion-de-phishing-et-virus—3-nouvelles-techniques-identifiees.shtml

Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boites mail se fassent pirater ? | Denis JACOPINI

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

Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boites mail se fassent pirater ?

I**l est très difficile de savoir si un ordinateur est piraté / piratable ou pas. Qu'il soit PC ou Mac, il possède ses failles qui peuvent sans limite être exploitées.**
Il n'y a plus beaucoup de protections qui résistes aux plus grands hackers.
La divulgation de documents dévoilant les techniques qu'utilise la NSA pour nous espionner (c.f. http://www.lenetexpert.fr/les-10-outils-les-plus-incroyables-utilises-par-la-nsa-pour-nous-espionner-le-net-expert-informatique) et les dessous de société d'espionnage informatique Hacking Team récemment piratée (c.f. http://www.lenetexpert.fr/les-dessous-de-la-societe-despionnage-hacking-team-le-net-expert-informatique) nous ont récemment démontré qu'il n'y a aucune limite au piratage.

Mais alors, comment se protéger ?
Comme pour votre maison ou votre appartement, il n'existe aucun moyen d'empêcher les voleurs de rentrer. Les moyens qu'ils utiliseront seront généralement à la hauteur de l'intérêt qu'ils y trouveront.
Cependant, les conseils que je peux donner, sont comme pour les moyens de protection de vos habitions. Au plus on met des barrières de sécurité, au plus on retarde l'intrusion et au plus on décourage l'auteur. Il sera en effet plus difficile de rentrer chez vous si vous avez la dernière serrure de protection avec les volets anti-effraction dernier cri, avec une alarme ultra perfectionnée etc. plutôt qu'un simple cadenas pour vous protéger.

Pour sécuriser un système informatique
1) J'analyse généralement ce qui, dans nos habitudes quotidiennes correspond à une attitude numérique dangereuse ou irresponsable. Pour cette phase, il est difficile de vous dire quoi faire exactement, puisque c'est généralement notre expérience, nos connaissances passées et notre intuition qui servent à produire une bonne analyse.

2) La phase suivante va consister à détecter la présence d'espions dans votre ordinateur. Compte tenu que la plupart des outils d'espionnage sont capables de détecter qu'on est en train de les détecter, vaut mieux déjà, faire des sauvegardes, puis couper d'internet votre appareil (du coup, il sera nécessaire de télécharger les logiciels de détection à partir d'un autre ordinateur, et les copier sur l'ordinateur à analyser à partir d'une clé USB par exemple).
Cette phase de détection est très difficile. En effet, les logiciels espions, programmés pour espionner ce que vous tapez au clavier, ce que voit votre webcam ou entend votre micro, sont aussi programmés pour ne pas être détectés.
Le dernier outil connu pour réaliser une détection de logiciels espions est le logiciel **Detekt**. Ce logiciel a pour but de détecter des logiciels espions (spywares) sur un système d'exploitation Windows.
Les spywares actuellement détectés sont :
• DarkComet RAT ;
• XtremeRAT ;
• BlackShades RAT ;
• njRAT ;
• FinFisher FinSpy ;
• HackingTeam RCS ;
• ShadowTech RAT ;
• Gh0st RAT.
Attention, car les développeurs de ce logiciels précisent cependant :
« Certains logiciels espions seront probablement mis à jour en réponse à la publication de Detekt afin d'éviter la détection. En outre, il peut y avoir des versions existantes de logiciels espions […] qui ne sont pas détectés par cet outil ».
Vous trouverez plus d'informations et le lien de téléchargement sur http://linuxfr.org/news/detekt-un-logiciel-de-detection-de-logiciels-espions
Sur Mac, il n'existe pas un tel outil. Vous pouvez cependant utiliser le logiciel MacScan pou des antispaywares du commerce.
Cependant, que ça soit sur PC ou sur Mac, ce n'est qu'une analyse approfondie (et souvent manuelle) des fichiers systèmes, des processus en mémoire et qui se lancent au démarrage qui permettra de détecter les applications malveillantes installées sur votre ordinateur.

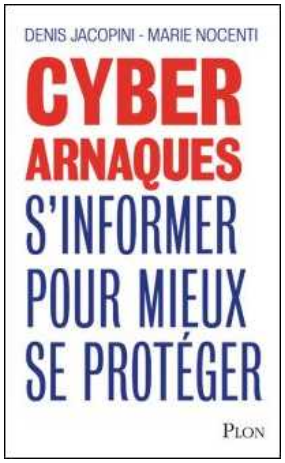
Et si on dispose d'un Mac plutôt que d'un PC ?
Il y a quelques années, avoir un Mac « garantissait » d'être un peu à l'abris des virus et des pirates informatiques. En effet, pouquoi un pirate informatique perdrait du temps à développer un logiciel malveillant et prendrait des risques pour seulement 5% de la population numérique mondiale. Désormais, avec l'explosion d'Apple, de ses téléphones, tablettes et aussi ordinateur, les systèmes IOS se sont répandu sur la planète numérique. De plus, c'est très souvent les plus fortunés qui disposent de ces types d'appareils… une aubaine pour les pirates qui trouvent tout de suite un intérêt à développer des dangereuxwares.

3) La troisième et dernière phase de ces recommandations est la protection. Une fois votre système considéré comme sain (il est complètement inutile de protéger un système qui est infecté car ça ne soignera pas l'équipement et les conséquences pourraient être pires), il est temps d'adopter l'attitude d'un vrai utilisateur responsable et paranoïaque.
• Mettez à jour votre système d'exploitation (Windows, MasOs, IOS, Androis, Linux…) avec la version la plus récente. En effet, l'enchaînement des mises à jour des systèmes d'exploitation est peu souvent fait pour améliorer le fonctionnement ou ajouter des fonctions à votre appareil. Le ballet incessant des « updates » sert prioritairement à corriger les « boulettes » qu'ont fait volontairement ou involontairement les informaticiens « développeurs » détectées par d'autres informaticiens plus « contrôleurs ».
• Mettez à jour vos logiciels avec leurs versions les plus récentes (et particulièrement pour vos navigateurs Internet et les logiciels Adobe). En effet, la plupart des intrusions informatiques se font pas des sites Internet malveillants qui font exécuter sur votre ordinateur un code informatique malveillant chargé d'ouvrir un canal entre le pirate et vous. Ces codes informatiques malveillants utilisent les failles de vos logiciels pour s'exécuter. Lorsque l'utilisation d'une faille inconnue (sauf par les pirates) d'un logiciel est détectée par les « Gardiens de la paix numérique », un correctif (ou patch) est généralement développée par l'éditeur dans les jours qui suivent leur découverte. Ceci ne vous garantira pas une protection absolue de votre ordinateur, mais renforcera son blindage.Les pirates utilisent parfois d'anciens serveurs ou d'anciens postes de travail connecté sur le réseau, qui ont de vieux systèmes d'exploitation qui ne se mettent plus à jour et qui ont des failles ultra-connues pour pénétrer votre réseau et des postes pourtant ultra-sécurisés. Pensez donc à les déconnecter du réseau ou à copier le contenu ou les virtualiser sur des systèmes plus récents et tenus à jour.
• Mettez à jour les firmwares des matériels et objets connectés. Pour les mêmes raisons qu'il est important de mettre à jour vos logiciels avec leurs versions les plus récentes, il est aussi important de mettre à jour les logiciels de vos matériels et objets connectés (routeurs, modems, webcams etc.).
• Adoptez une politique sécurisée dans l'utilisation des mots de passe. Vos mots de passe doivent êtres longs, complexes et doivent changer souvent. Conseil primordial dans l'utilisation des mots de passe au bureau : Il doit être aussi précieux et aussi secret que le code de votre carte bancaire. Personne ne doit le connaître, sinon… quelqu'un pourra facilement se faire passer pour vous et vous faire porter le chapeau pour ses actes malveillants.
• Méfiez-vous des sites Internet proposant des vidéos gratuites, du streaming gratuit ou autres services inespérément gratuit. Les sites sont souvent piégés et ont destinés soit à collecter des données personnelles, soit contaminer votre ordinateur par des petits codes malveillants.
• Méfiez-vous également des e-mails douteux de demande d'aide (même d'un ami) ou autre participation humanitaire utilisant le paiement par Manda Cash, Western Union ou monnaie virtuelle telle le Bitcoin. Ce sont des moyen de paiement qui sont généralement utilisés par les pirates pour se faire payer et disparaître dans la nature. Les emails destinés à vous hameçonner auront aussi quelques détails qui devraient vous mettre la puce à l'oreille (Faute d'orthographe, huissier ou directeur ayant une adresse e-mail yahoo ou gmail).
• Vous avez un doute, vous pensez que votre ordinateur ou votre boite e-mail est victime d'intrusion, changez immédiatement de mot de passe. Certains systèmes de messagerie permettent d'avoir un historique des accès et des connexions. L'analyse de cet historique pourrait bien vous donner une indication pour savoir si quelqu'un d'autre à accès à votre messagerie (alias, double diffusion, collecte d'un compte mail sur un autre compte etc).

Conclusion
Voila, vous avez maintenant toute une liste de recommandations qui peut vous rassurer (ou non) et vous permettre de prendre conscience de la complexité qu'est à ce jour la lutte de la #cybercriminalité.
Si maintenant tout ceci vous semble complexe, rassurez-vous, c'est notre métier. Nous seront donc en mesure de vous accompagner dans la sensibilisation des utilisateurs, la détection ou la protection contre ces « ennuiwares ».
Contactez-moi

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

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

Commandez sur Fnac.fr

---

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

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

Commandez sur amazon.fr

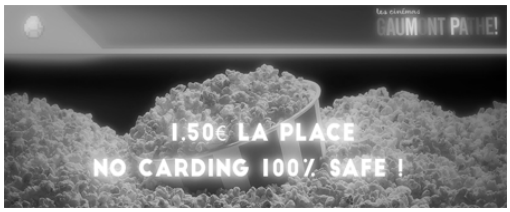
Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le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

Commandez sur Fnac.fr

Source : Denis JACOPINI

Place de ciné pas chère : une

faille pour Gaumont Pathé ? | Denis JACOPINI

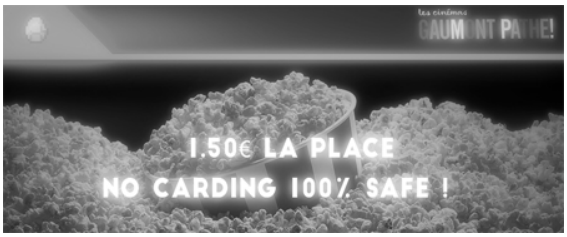


Place de ciné pas chère : une faille pour Gaumont Pathé ?

Place de ciné pas chère ? Bluff, escroquerie ou piratage informatique ? Une boutique du black market francophone propose de payer ses places de cinéma 5 fois moins chères que le prix initial. Une possibilité pirate qui ne viserait que les cinémas Pathé Gaumont !

Les amateurs de cinémas ne me contrediront pas, le cinéma est devenu un petit luxe loin d'être négligeable dans un budget. Même si des cartes de réductions existent, cela fait rarement la sortie cinéma (deux adultes, deux enfants) à moins de 50€ (si on rajoute quelques friandises), et à la condition ou la séance n'est pas en 3D, ce qui fait gonfler la note. Bref, tout le monde n'a pas la chance d'aller au cinéma deux fois par semaine. Bilan, ce qui est mon cas, les cartes de réduction sont un bon moyen d'assouvir son plaisir de salle obscure. D'autres internautes, beaucoup plus malhonnêtes, n'hésitent pas à revendre des entrées à un prix défiant toutes concurrences.

Place de ciné pas chère ?

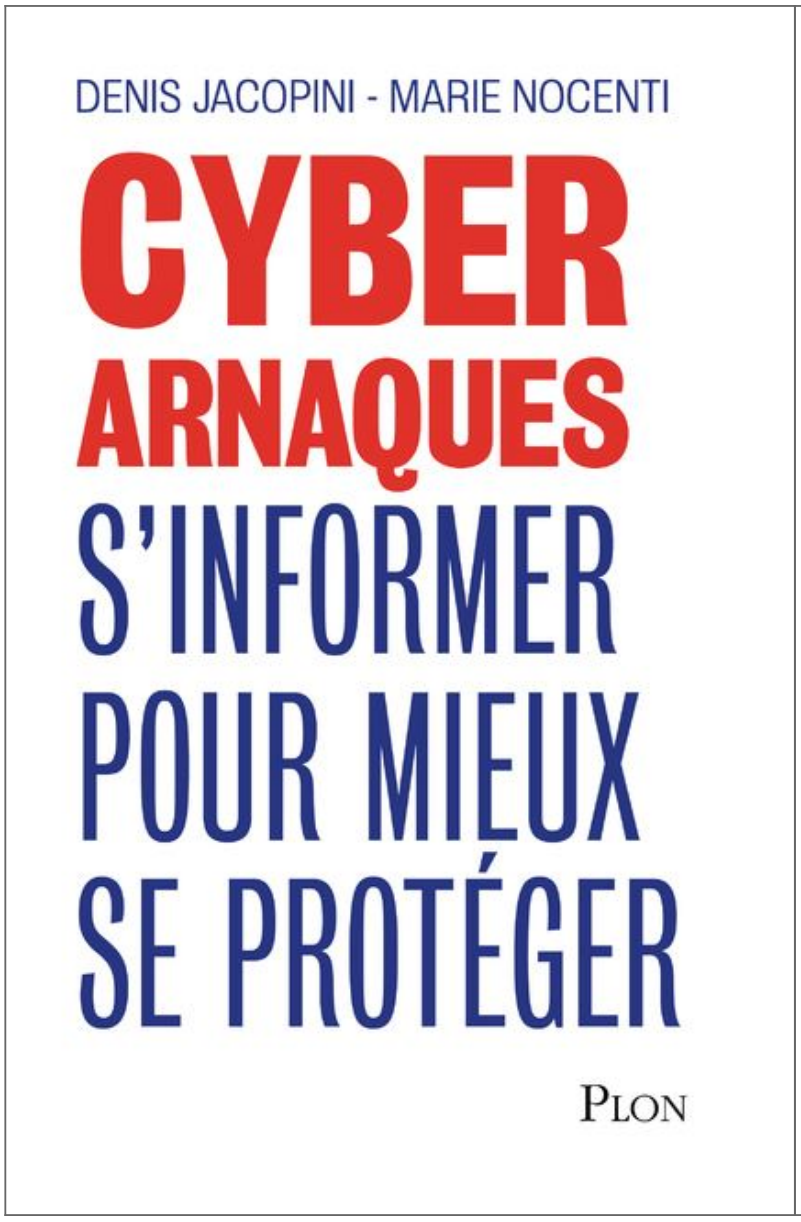


Dans une boutique du black market francophone, je suis tombé sur une publicité annonçant proposer des places de cinéma à 1,5€/2€. Des places ne pouvant être utilisées que dans les cinémas Gaumont Pathé! Le président des cinémas Pathé, Jérôme Seydoux et Nicolas Seydoux, président de Gaumont (Grand Père et Oncle respectifs de la dernière James Bond Girl, Léa Seydoux) auraient-ils décidé de faire des réductions aussi inattendues qu'impossibles ? Malheureusement pour les cinéphiles, ce n'est pas le cas.Il semble que le vendeur derrière cette proposition alléchante de Place de ciné pas chère a trouvé une méthode pour escroquer l'entreprise. « ***J'ai des places de cinéma gratuites et illimitées valables dans tous les Pathé de France,*** indique ce commerçant. ***Ces places ne sont pas cardées*** [comprenez acquises avec des données bancaires piratées, NDR], ***juste ma tête***« . Le vendeur indique ne pas vouloir donner plus d'informations sur sa méthode. Une technique qu'il utiliserait depuis deux ans « ***pour moi et mes amis et qu'il n'est jamais rien arrivé***« . D'après ce que j'ai pu constater, le pirate semble être capable de générer des codes « invitation ». Le pirate a même créé un shop (boutique automatisée) qui permet d'acquérir autant de place que le black marketeur est capable de générer contre la somme demandée. Paiement en bitcoins… [Lire la suite]

Réagissez à cet article

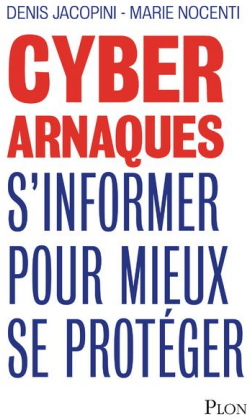
Source : *ZATAZ Place de ciné pas chère : une faille pour Gaumont Pathé ? – ZATAZ*

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)

LE NET EXPERT
• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)
- **ANALYSE DE VOTRE ACTIVITÉ**
- **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
- **IDENTIFICATION DES RISQUES**
- **ANALYSE DE RISQUE (PIA / DPIA)**
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
• FORMATIONS / SENSIBILISATION :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**
• RECHERCHE DE PREUVES (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES
• EXPERTISES & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous
Notre Expert, Denis JACOPINI, est 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).

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 ;

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

Contactez-nous

Réagissez à cet article

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

Cyber-Sécurité : des menaces de plus en plus présentes, mais des collaborateurs pas assez formés | Le Net Expert Informatique

La Cyber-Sécurité de plus en plus menacante, mais des collaborateurs pas assez formés

Les entreprises ont encore trop souvent tendance à sous-estimer le #risque lié au manque de formation de leurs équipes (hors services informatiques) à la cybersécurité. La preuve…

Une enquête réalisée par Intel Security montre que si les collaborateurs de la DSI restent les plus #exposés aux cyberattaques (26 % au niveau européen contre 33 % en France, ce taux étant le plus élevé), les équipes commerciales et les managers (top et middle management) le sont aujourd'hui de plus en plus. En France, 18 % des commerciaux, 17 % du middle management et 14 % des dirigeants sont des #cibles potentielles. Viennent ensuite les personnels d'accueil (5 % en France, taux identique à la moyenne européenne), et le service client (seulement 7 % en France, contre 15 % au niveau européen).
Or ces types de personnel restent tous #mal formés à la sécurité informatique. Le risque est particulièrement fort au niveau des équipes commerciales avec 78 % de professionnels non formés et 75 % des personnels d'accueil. Ces taux descendent un peu pour le top management (65 % de non formés) et pour les équipes du service client (68 %). Côté middle management, la moitié est formée (51 % en France, 46 % au niveau européen).
L'enquête souligne également qu'au-delà des attaques ciblant les personnes non averties via leurs navigateurs avec des liens corrompus, les #attaques de réseaux, les #attaques furtives, les #techniques évasives et les #attaques SSL constituent une menace croissante pour les entreprises. On en recense plus de 83 millions par trimestre. Pour les contrer, les professionnels informatiques français réévaluent la stratégie de sécurité en moyenne tous les huit mois, en ligne avec les pratiques des autres pays européens sondés. 21 % mettent par ailleurs à jour leur système de sécurité moins d'une fois par an (contre 30 % en moyenne au niveau européen). Et 72 % d'entre eux (et 74 % en moyenne en Europe) sont persuadés que leur système de sécurité pourra contrer ces nouvelles générations de cyberattaques.
Or, ils se trompent. Les #attaques DDoS par exemple. Conçues pour créer une panne de réseau et permettre aux hackers de détourner l'attention de l'entreprise, tandis qu'ils se faufilent dans son système et volent des données, elles ne sont pas vraiment prises au sérieux (malgré leur augmentation +165% et leur dangerosité), puisque seuls 20 % des professionnels informatiques français estiment qu'elles constituent la principale menace pour le réseau de leur entreprise.
Au final, il existe un profond décalage entre l'évolution des attaques et la perception qu'en ont les entreprises qui ne peuvent plus négliger la formation de leurs équipes non IT.

Source : http://www.itchannel.info/index.php/articles/157059/cyber-securite-menaces-plus-plus-presentes-mais-collaborateurs-pas-formes.html

---

Que faire en cas de fraude sur sa carte bancaire ?

Que faire en cas de fraude sur sa carte bancaire ?

De plus en plus d'usagers de la banque sont victimes de l'utilisation frauduleuse de leur carte alors même qu'ils ne l'utilisent pas pour leur achat sur le net. Pourtant il arrive de plus en plus fréquemment que certains d'entre eux constatent des sommes prélevées sur leur compte bancaire en consultant leur relevé bancaire.

Que faire en cas de fraude sur sa carte ? Quelles sont les démarches pour déclarer une utilisation frauduleuse de sa carte bancaire ?

Selon les disposition de l'article L 133-24 du Code Monétaire et Financier, la responsabilité du propriétaire d'une carte bancaire n'est pas engagée dans le cas où la carte a été contrefaite ou si l'achat contesté n'a pas été effectué avec l'utilisation physique de la carte.

Les titulaires de carte victimes d'une utilisation frauduleuse sur Internet ont un délai de 13 mois pour contester les sommes prélevées sur leur compte bancaire. Ils doivent se rendre auprès de sa banque et s'opposer formellement aux transactions effectuées ou au paiement des opérations en question.

Quelles sont les démarches à faire auprès de sa banque ?

En cas d'usurpation des données de sa carte bancaire, il faut :

• Appeler sa banque le plus rapidement possible pour le signaler par téléphone.

• Envoyer à sa banque une lettre qui confirme la mise en opposition de la carte utilisée frauduleusement,

– Un document qui décrit toutes les opérations contestées, les coordonnées bancaires et le motif de l'opposition de la carte,

– Une attestation (AFFIDAVIT) certifiant que la carte a toujours été en sa possession et qu'elle n'a jamais été cédée ou prêtée.

La loi de 2001 sur la protection du consommateur n'exige pas de dépôt de plainte auprès de la gendarmerie. Il n'est donc pas nécessaire de porter plainte pour que la banque procède aux remboursement des sommes usurpées.

Selon les articles L133-19 et L 133-20, la banque doit rembourser toutes les sommes prélevées à compter de la date d'opposition ainsi que tous les frais liés à l'opposition de la carte bancaire.

Pour éviter une usurpation de sa CB, voici quelques conseils et certaines mesures de sécurité à prendre :

– ne jamais laisser la carte bancaire à la vue d'un quelconque public (ex :
– exposée la CB dans la voiture ou sur un bureau),

– penser à reprendre sa carte bancaire dans les terminaux de paiement après chaque achat,

– détruire les tickets de paiement avant de les jeter car ils comportent le code de la carte bancaire,

– ne jamais dire le numéro ni le code secret de la carte bancaire à quiconque,

– ne pas oublier de signer au dos de la carte bancaire.

Source : Banque-en-ligne.fr *Que faire en cas de fraude sur sa carte bancaire ?*

Réagissez à cet article

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

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Conseils de prévention sur Internet / Cybercrime / Dossiers / Actualités – Police nationale – Ministère de l’Intérieur

---

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

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

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