# Les objets connectés représentent-ils un risque ? | Denis JACOPINI

Les #objets connectés représentent-ils un risque ?

**Contrôler sa maison ou son appartement du bout des doigts, voici la promesse des fameux objets connectés. Des réfrigérateurs aux téléviseurs, en passant par les thermostats, les caméras de surveillance, les serrures, ou encore les éclairages… de plus en plus d'équipements du foyer peuvent être pilotés à distance à l'aide d'un smartphone via un réseau local et Internet. Mais derrière ce rêve de la maison intelligente et connectée, encore inimaginable il y a quelques années, se cachent d'inquiétants problèmes de sécurité. État des lieux.**

**Un marché en ébullition**

Longtemps réservée aux technophiles fortunés, la #domotique commence vraiment à se démocratiser grâce à l'émergence des appareils et objets connectés. Après les équipements multimédias (Smart TV, systèmes Hi-Fi, imprimantes…), les appareils électroménagers connectés – réfrigérateurs, lave-linge, cafetières, réveils, etc.– commencent à débarquer sur le marché. Mais ce sont surtout les systèmes prêts à l'emploi ou les modules adaptables permettant de connecter l'éclairage, les serrures de portes, les stores, les systèmes de surveillance (caméras, détecteurs de mouvements/fumée, alarmes…), ou encore le chauffage qui rencontrent un succès grandissant.
L'embellie du marché de la domotique s'explique notamment par la simplicité d'installation et d'usage de ces nouveaux produits, mais également par leur prix de plus en plus abordable. Toutefois, comme n'importe quel appareil qui se connecte à un réseau Wi-Fi et à Internet, ils s'exposent de fait à toutes sortes de risques. D'autant que pour la plupart, ils ne possèdent aucun système de protection de type antivirus, antimalware, etc. Des failles de sécurité, plus ou moins importantes en fonction de la nature des objets, ont été soit démontrées par des experts de sécurité, soit exploitées par des hackers. Nous verrons les cas les plus effrayants qui donnent matière à réflexion.

**Des appareils sous haute surveillance**

Outre les incidents révélés ici et là, la sécurité des objets connectés est devenue un sujet particulièrement sensible depuis la médiatisation d'un moteur de recherche public étonnant baptisé Shodan. Créé par un Américain du nom de John Matherly, ce dernier explore le Web en continu pour référencer et regrouper tous les appareils qui y sont connectés. Quelques clics suffisent pour trouver aussi bien des systèmes domotiques, que des imprimantes, des caméras, des alarmes, voire des installations industrielles sensibles telles que des centrales électriques, des raffineries, ou encore, des réacteurs.

Pas de quoi rassurer les utilisateurs, même si à l'origine Shodan n'aurait pas été créé pour nuire, mais au contraire pour aider les experts en sécurité à identifier les vulnérabilités des logiciels et infrastructures réseau des entreprises. Le service se targue de garder une trace de tous les faits et gestes de ses utilisateurs, qui doivent obligatoirement s'identifier et souscrire à un abonnement au-delà d'un certain nombre de recherches. Il n'en reste pas moins que désormais, tout objet connecté ayant une adresse IP peut être localisé, identifié, voire détourné.

**Les promesses de la maison intelligente et connectée**

Contrôler et gérer divers équipements de la maison à l'aide d'un smartphone, d'une tablette ou d'un ordinateur n'est plus une utopie. Inutile d'avoir à tirer des câbles partout et d'entreprendre de lourds et coûteux travaux avec des spécialistes. Tout le monde peut en principe concevoir une installation domotique soi-même grâce à la nouvelle génération de produits disponibles sur le marché. Au-delà du confort qu'offrent ces nouvelles technologies au quotidien, elles permettent de réaliser de substantielles économies d'énergie, de renforcer la sécurité du foyer, ou encore de se prémunir d'accidents domestiques (incendie, inondation…).

Confort, sécurité, prévention, économie d'énergie…

**Domotique**

Les produits ont évolué, mais la promesse de la domotique est toujours la même : centraliser et automatiser grâce à diverses technologies l'ensemble ou une partie des équipements électriques du foyer. Des serrures qui se ferment à distance, des caméras et des détecteurs de mouvements capables de s'animer en votre absence et de vous envoyer des SMS en cas d'intrusion, des thermostats intelligents permettant de gérer la température au degré près dans chaque pièce, des stores électriques qui s'ouvrent et se ferment automatiquement en fonction de la lumière, des détecteurs de fumée (obligatoires dans toute l'Union européenne à partir de mars 2015) qui lancent des alertes en cas de départ d'incendie, des éclairages qui créent différentes ambiances lumineuses selon les heures de la journée… Les possibilités sont quasi-infinies.

Réaliser une installation domotique est maintenant à la portée du plus grand nombre grâce, notamment, à ce qu'on appelle les box domotiques. Ces systèmes prêts à l'emploi que l'on trouve dans tous les magasins de bricolage et d'électronique (Castorama, Leroy Merlin, Electro Dépôt…) et même dans certains hypermarchés permettent de connecter et de contrôler à distance des équipements de la maison via une seule et même interface. Ces packs se composent d'un serveur domotique / multimédia (relié au réseau Wi-Fi du foyer), et d'un éventail plus ou moins important d'équipements de surveillance, d'automatisation, de loisirs, etc.

Ces dispositifs communiquent entre eux par le biais de différentes technologies sans fil comme le courant porteur (CPL), le Wi-Fi, les radiofréquences, ou des protocoles propriétaires. Pour les contrôler à l'aide d'une tablette ou d'un smartphone depuis le réseau local du foyer ou à distance par Internet, l'utilisateur n'a plus qu'à jouer du bout des doigts avec les icônes représentant les équipements connectés pour planifier des actions immédiates ou différées.

**Créer des scénarios**

Dans le jargon de la domotique, un scénario désigne un ensemble d'actions programmées pour différents moments de la journée, de la semaine, du mois, voire de l'année. Les fabricants ont réalisé d'énormes progrès pour faciliter la gestion des produits domotiques et la création de scénarios en développant des applications très intuitives. Exit les lignes de code informatique, ou les menus interminables au vocabulaire incompréhensible, place aux icônes visuelles, aux photomontages représentant les différentes parties du foyer, et à des menus dynamiques inspirés de ceux des smartphones. Quelques clics suffisent pour créer plusieurs scénarios pour la journée, la nuit, le week-end, et les combiner entre eux.

Point d'orgue des maisons intelligentes, les applications mobiles facilitent la compréhension et l'utilisation des équipements domotiques

On peut imaginer, par exemple du lundi au vendredi, un scénario qui consisterait à déclencher une série d'actions à partir de 7 heures : ouvrir les stores, allumer le ballon d'eau chaude, faire chauffer la cafetière, lancer la radio, déverrouiller les portes, démarrer les caméras de surveillance, etc. Bien entendu, toutes les solutions domotiques n'offrent pas les mêmes possibilités. Les fabricants distillent généralement des packs spécialisés dans un domaine précis (surveillance, automatisation, éclairage, chauffage…) à compléter au fur et à mesure. En parallèle, il existe d'innombrables objets connectés autonomes (stations météo, balances Wi-Fi, réveils intelligents, ampoules connectées…) qui se connectent directement au réseau du foyer, sans passer par un serveur propriétaire.

Aura, le réveil intelligent de Withings qui analyse votre sommeil pour vous réveiller en douceur

Le problème, c'est que tout ce petit monde ne parle pas le même langage. Les standards universels, que rêvent de concevoir Apple et Google pour que tous les appareils connectés puissent communiquer entre eux via leurs plateformes mobiles respectives, ne sont pas encore d'actualité. À moins de choisir du matériel très haut de gamme comme la box universelle Lifedomus Vision (2 988 euros) compatible avec la plupart des protocoles de communication des solutions domotiques (KNX, EnOcean, MyHome, Zwave, Modbus, Zigbee…), mieux vaut s'équiper chez le même fabricant pour pallier les éventuels problèmes de compatibilité.

**Quels risques pour la sécurité ?**

Depuis quelques mois, la sécurité de l'Internet des objets fait couler beaucoup d'encre. Aux quatre coins de la planète, des experts en sécurité prennent le sujet à bras le corps : ils multiplient les démonstrations pour montrer les vulnérabilités de certains produits et la façon dont les cybercriminels pourraient les exploiter pour réaliser des attaques. Les spécialistes n'ont pas tort d'alerter les fabricants, car les risques ne sont plus seulement virtuels. Depuis quelques mois, quelques cas concrets d'attaques basées sur des objets connectés prouvent le bien-fondé de leurs craintes.

**Failles et vulnérabilité des objets connectés**

La division de sécurité Fortify on Demand du constructeur HP a récemment publié un rapport alarmant sur la sécurité des objets connectés. Elle a ainsi annoncé avoir découvert plus de 25 vulnérabilités sur 10 objets connectés parmi les plus populaires (Smart TV, thermostats intelligents, webcams, boxs domotiques…). Sans donner plus de précisions sur les marques concernées, elle déclare que la plupart ne crypte pas les données échangées sur le réseau et n'exige pas de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance. Ces dispositifs autorisent des mots de passe comme « 123456 » particulièrement vulnérables (un fait que nous avons effectivement pu vérifier après quelques recherches sur Shodan). Par ailleurs, la protection de leurs logiciels serait insuffisante, car non chiffrée, et certaines interfaces Web ne sont pas du tout sécurisées.

Toujours selon ce rapport, 90 % des produits évalués collectent des informations personnelles sensibles (adresse email/postale, date de naissance…) susceptibles de circuler en clair sur Internet à cause du manque de protection. Difficile néanmoins de contester un rapport ne précisant pas les modèles et les marques des appareils incriminés. À travers cette étude, la division déclare vouloir sensibiliser les acteurs du marché, mais elle souhaite aussi promouvoir sa solution de sécurité Fortify on Demand auprès des fabricants.

Ce n'est pas la seule étude de ce type. Le groupe de chercheurs indépendant d'AV-Test avait mis en lumière d'importantes failles de sécurité, notamment sur les systèmes domotiques iComfort de REVRitter, et XAVAX MAX ! d'Hama, permettant de contrôler le chauffage, l'électricité, les prises de courant avec interrupteur, ou encore l'éclairage. Aussi incroyable que cela puisse paraître, leur communication n'était pas sécurisée sur le réseau lors des mises à jour logicielle ou firmware, mais en plus, la solution iComfort ne nécessitait aucune authentification que cela soit pour l'accès local ou via Internet.

Avec un moteur de recherche comme Shodan, n'importe qui aurait pu repérer les dispositifs de la marque sur Internet et en prendre le contrôle à distance… Effrayant. Gageons que les deux fabricants ont pris les mesures qui s'imposent pour sécuriser un tant soit peu leurs systèmes.

**Le lapin Karotz sécurisé ? Pas tout à fait.**

Dans la sécurité informatique, les experts réalisent des « exploits », c'est-à-dire des tests (appelés Proof-of-concept, preuve de concept) visant à démontrer la présence de vulnérabilités sur des systèmes ou des logiciels pour proposer des patchs. Certains exemples sont particulièrement croustillants. La spécialiste Jennifer Savage avait ainsi montré comment elle avait réussi à exploiter une faille de sécurité du fameux lapin multifonctions Karotz qu'elle avait offert à sa fille. Cela lui avait permis de prendre le contrôle à distance de l'appareil à son insu, à l'aide d'un ordinateur, et d'utiliser sa caméra et son micro pour l'espionner.

**Des ampoules qui éclairent et déverrouillent les réseaux Wi-Fi**

Plus récemment, des chercheurs sont parvenus à prendre le contrôle d'ampoules connectées Lifx en exploitant une faille de leur protocole de communication. Ils ont pu démontrer qu'ils pouvaient théoriquement s'introduire dans un rayon de 30 mètres dans le réseau Wi-Fi domestique auquel elles sont connectées et accéder à des données privées stockées sur d'autres appareils du foyer, par exemple. Depuis cette découverte, le fabricant s'est empressé de publier un correctif.

**Des Smart TV qui espionnent les téléspectateurs**

Les démonstrations les plus impressionnantes ont souvent lieu lors des conférences Black Hat organisées chaque année à Las Vegas, mais aussi à Amsterdam ou à Tokyo. Elles réunissent aussi bien des chercheurs, des experts en sécurité, que des hackers de haut vol. En 2013, plusieurs conférenciers ont exposé les vulnérabilités des TV connectées. L'un d'entre eux a prouvé notamment qu'il était possible de prendre le contrôle de la caméra et du micro d'une Smart TV et d'espionner leur propriétaire à leur insu. Et cela, même quand l'appareil était éteint.

**Le thermostat Nest Lab qui joue les « Big Brother »**

À l'occasion de la dernière édition qui s'est déroulée au mois d'août 2014 à Las Vegas, des chercheurs d'une université de Floride ont montré comment pirater le thermostat intelligent de Nest (la start-up rachetée par Google). Avec un accès physique à l'appareil (uniquement), ils ont pu prouver qu'il est possible d'insérer un code pour détourner et récupérer les informations récoltées par l'appareil, sans que son propriétaire s'en aperçoive.

**Nouvelle génération de cyberattaques**

La sécurité et la protection des données privées ne sont clairement pas la priorité de certains acteurs du marché des objets connectés. Sans vouloir dresser un tableau catastrophiste de la situation, les cyberattaques sur les objets connectés présentant des failles de sécurité ont tendance à se multiplier ces derniers mois. Caméras de vidéosurveillance, réfrigérateurs, babyphones, Smart TV, voici quelques exemples connus d'appareils qui ont fait l'objet d'attaques diverses et variées.

**Des caméras au service des voyeurs**

Impossible de ne pas citer la faille de sécurité qui avait permis à des hackers de diffuser sur Internet le flux vidéo de milliers de webcams et caméras de vidéosurveillance Trendnet, installées chez des particuliers. Malgré la publication rapide d'un correctif par le fabricant après sa découverte, de nombreux utilisateurs continuaient un an plus tard à être espionnés à leur insu, car ils n'avaient toujours pas fait la mise à jour.

**Un hack jusque dans… le berceau d'un nourrisson !**

Début 2014, la société spécialisée en sécurité PenTPoint a révélé pour la première fois une cyberattaque réalisée à partir de toutes sortes de dispositifs connectés dont des Smart TV, des NAS, des consoles de jeux vidéo, un réfrigérateur, etc. Les pirates auraient exploité leur vulnérabilité pour installer un serveur de spams (botnet) et envoyer plus de 750 000 emails frauduleux. Dans l'État de l'Ohio aux États-Unis au mois d'avril dernier, un hacker n'a rien trouvé de mieux que de pirater un babyphone pour terroriser un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, il s'est mis à hurler des insanités sur le nourrisson.

**Analyse et collecte de données en règle**

En Grande-Bretagne, le blogueur spécialisé en développement informatique connu sous le nom de DoctorBeet's a fait une étonnante découverte. Suite à l'acquisition d'une Smart TV de la marque LG, il a remarqué l'apparition de publicités ciblées comme on peut en voir sur des services Web tels que Gmail. Il en a donc déduit que la TV devait forcément analyser ses habitudes, les programmes qu'il regarde, les sites qu'il visite, etc. En cherchant à en savoir plus, il constate en effet que son téléviseur dispose d'une fonction activée par défaut de collecte d'informations de visionnage.

Même après avoir désactivé cette fonction, le téléviseur continuait de transmettre des informations à son insu à LG. Le constructeur ne se contentait pas de scruter ses habitudes de consommation, mais il récupérait également des données personnelles telles que des vidéos de famille qu'il avait projetées sur son écran depuis son ordinateur. Un scandale dont se serait bien passé LG qui aurait, depuis, décidé de permettre à ses clients de « vraiment » désactiver l'option de collecte de données. Outre le manque de sécurité constaté sur de nombreux objets connectés, il faudra donc aussi redoubler d'attention et se méfier des pratiques intrusives de certains fabricants !

Source DoctorBeet's Blog

**Sous l'œil de Shodan**

En faisant un tour d'horizon des objets connectés pour la maison, susceptibles de présenter des risques, on se rend compte qu'ils sont tous potentiellement vulnérables. Certains ne sont pas sécurisés ou pas suffisamment, tandis que d'autres présentent des failles de sécurité plus ou moins importantes pouvant être exploitées pour mener des attaques externes ou à courte distance. Mais la principale faille qu'exploitent les hackers est encore trop souvent l'absence de vigilance des utilisateurs. Beaucoup n'ont pas conscience des risques et n'utilisent pas de mots de passe pour protéger l'accès à distance de leurs équipements, ou se contentent de laisser les identifiants par défaut fournis par les fabricants. Un vrai problème, d'autant qu'avec un moteur de recherche comme Shodan, tous les appareils connectés ayant une adresse IP visible sont désormais répertoriés sur le Web.

D'une efficacité redoutable, ce service permet d'effectuer des recherches globales, ou par pays, en saisissant une simple requête pour identifier, localiser, voire prendre le contrôle des appareils connectés non protégés par un mot de passe. Il suffit de saisir le nom d'une marque de produits connectés connue (DLink, Netgear, Samsung…) ou de cliquer sur les mots recherchés les plus populaires (Webcam, Camera, Netcam…) pour voir apparaître leurs adresses IP et s'y connecter. Le service indique de surcroît de nombreux détails sur les dispositifs, comme leur système d'exploitation, s'ils sont connectés, protégés ou non par des identifiants, etc.

Comme cela avait été démontré dans une enquête baptisée Null CTRL, réalisée par deux journalistes norvégiens pour le site Dagbladet en 2013, d'innombrables équipements connectés référencés par Shodan ne possèdent aucune protection. Quelques clics suffisent pour les repérer et visionner, par exemple, le flux vidéo de caméras de surveillance chez des particuliers, jouer avec le tableau électrique ou le thermostat d'un immeuble, s'introduire dans des bases de données, etc. Gageons qu'à terme, cette surexposition des objets connectés permette de sensibiliser les utilisateurs sur l'importance de sécuriser leur accès.

**Qu'en pensent les experts ?**

Au-delà des rapports alarmants, des exploits des chercheurs et des affaires relatées dans les médias, nous avons souhaité donner la parole à un expert en sécurité ainsi qu'à un fabricant de solutions domotiques. Tous deux apportent une vision concrète sur les risques que représentent les objets connectés à l'heure actuelle, et donnent quelques conseils aux utilisateurs pour mieux se protéger.

**Cybermesures sur les maisons intelligentes**

Pour en savoir un peu plus sur les menaces qui planent sur les maisons intelligentes et leurs installations domotiques, nous avons rencontré un expert en sécurité qui travaille depuis plus de dix ans pour Kaspersky Lab Angleterre. Il dresse un portrait plus nuancé que celui des cabinets d'experts en sécurité que nous avons évoqué précédemment.

David Emm

**Clubic : Que pouvez-vous nous dire sur la sécurité des objets connectés pour la maison ?**

David Emm : Les gens utilisent Internet pour faire des achats, gérer leurs comptes en banque, aller sur les réseaux sociaux mais aussi pour chercher des informations liées à tous les aspects de leur vie quotidienne. Et cela va encore plus loin maintenant que nous utilisons les technologies informatiques pour réaliser des actions qui étaient, par le passé, purement mécaniques, voire manuelles. Malheureusement, lorsque de nouvelles technologies voient le jour, ou lorsque la technologie génère de nouveaux usages, la sécurité n'est souvent pas l'une des priorités. Ce n'est pas un phénomène nouveau et si l'on regarde en arrière, on remarque que les évolutions sont portées par une volonté de simplicité, de réduction des coûts ou d'autres bénéfices, alors que la sécurité n'est envisagée qu'après l'émergence d'un problème. Les risques sont multiples, allant du vol à la manipulation des données. Il est facile d'imaginer par exemple qu'un compteur intelligent soit manipulé pour falsifier la consommation électrique. Pour l'instant, cela reste de l'ordre du possible plus que de celui du réel car à ma connaissance il n'y a eu aucune attaque réelle visant des compteurs électriques.

**Clubic : Selon vous, quels sont les types d'appareils domotiques les plus vulnérables ?**

David Emm : Lorsqu'ils entendent parler de l'Internet des objets ou de maisons intelligentes, la plupart des gens imaginent leurs appareils traditionnels disposant de nouvelles fonctionnalités (réfrigérateur, contrôle des portes, chauffage central, etc.). Pourtant, ces appareils ne sont pas encore massivement connectés et pour l'instant, leur vulnérabilité a été démontrée le plus souvent au travers d'exploits d'experts dans le cadre de tests. Bien sûr, lorsque ces appareils seront plus courants dans nos vies, je pense qu'ils deviendront régulièrement la cible d'attaques. Mais il faut surtout s'inquiéter de la vulnérabilité d'appareils qui sont aujourd'hui des incontournables, comme par exemples les modems Internet, les tablettes, les smart TV, etc.

**Clubic : À quel type d'attaques les maisons intelligentes (Smart Home) sont-elles exposées ?**

David Emm : Je dirais qu'il y a trois principales catégories :
1 – Obtenir l'accès à un appareil et l'utiliser pour prendre le contrôle d'autres systèmes connectés dans la maison
2 – Avoir accès à des informations privées ou sensibles, y compris des mots de passe
3 – Falsifier des informations reçues / envoyées par un appareil à l'insu des personnes du foyer

**Clubic : Quelles sont les vulnérabilités que vous avez pu constater ?**

David Emm : L'un de mes collègues David Jacoby a publié un rapport pour alerter sur les dangers de l'exécution de code à distance et des mots de passe faibles sur les appareils de stockage NAS, mais aussi la possibilité d'orchestrer une attaque de type « man-in-the-middle » (NDRL : l'attaque de « l'homme du milieu » consiste à s'infiltrer sans être vu dans un réseau et y intercepter des informations) via une Smart TV. Il a également découvert des fonctionnalités d'analyses non référencées intégrées dans les routeurs par les constructeurs (sans doute pour des raisons légitimes), mais qui pourraient être exploitées par un attaquant. Un appareil sans fil est repérable et potentiellement vulnérable aux attaques lorsque ses communications ne sont pas cryptées, et que le mot de passe d'accès utilisé est celui par défaut ou faible.

**Clubic : Est-ce que Kaspersky envisage de proposer des solutions de sécurité pour les objets connectés ?**

David Emm : Ce n'est pas parce qu'il est possible d'installer une solution de sécurité sur les terminaux traditionnels (PC, tablettes, smartphones…), que cela sera possible sur tous les appareils du quotidien qui sont connectés à Internet. Ces appareils pourraient recevoir et envoyer des données sans pour autant autoriser l'installation de code ou disposer de suffisamment d'espace pour le faire. Ils pourraient être verrouillés (par exemple si une Smart TV tourne sous un OS standard, il est possible que le code ne puisse être modifié que par le constructeur). En plus, le vendeur n'est pas toujours le constructeur des composants informatiques intégrés. Cela signifie qu'il pourrait être impossible de patcher ces appareils; même en cas de mise à jour de sécurité disponible via le constructeur des composants. On comprend mieux pourquoi il est primordial que les constructeurs et les entreprises qui les exploitent prennent en compte la sécurité dès le début de la fabrication d'un produit. Il est essentiel de pouvoir établir un dialogue entre experts en sécurité et développeurs d'appareils informatiques pour maisons connectées.

**Clubic : Que peuvent faire les utilisateurs pour protéger au mieux leurs systèmes domotiques ?**

David Emm : La première chose est de lister tous les objets connectés de la maison et de savoir comment et à quoi ils sont connectés (à Internet, ou à d'autres objets de la maison). Ensuite, il est impératif de mettre des obstacles sur la route du hacker. Pour ce faire, il faut tout d'abord installer régulièrement les mises à jour de sécurité et les mises à jour logicielles, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle. Pour finir, il faut limiter l'accès d'un objet connecté aux autres objets connectés dans la maison. Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple…).

**Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?**

David Emm : C'est une question difficile, car LE scénario catastrophe impliquant un seul individu n'aura pas forcément le même impact au niveau d'une communauté. Pour les individus, le risque qui importe c'est le #vol de données personnelles – par exemple, les noms d'utilisateurs, les mots de passe, etc. Ou encore, le fait que l'on puisse vous espionner vous ou votre famille (comme le hack du babyphone survenu dans l'Etat de Ohio). Il y aussi le risque qu'une application contrôlant la sécurité de votre porte d'entrée puisse être hackée, vous laissant enfermé dehors. Du point de vue de la communauté, l'impact peut être plus important. Si un hacker arrive par exemple à intercepter des données d'un compteur intelligent (Smart Meter), cela peut affecter les relevés : ils peut remettre les compteurs à zéro, voire créer une panne générale d'électricité.

**Le point de vue d'un spécialiste de la domotique**

Pour compléter ce dossier, nous avons voulu donner également la parole à un fabricant de solutions domotiques. Somfy, l'un des leaders du marché de la domotique, a bien voulu répondre à nos questions sur la sécurité des maisons intelligentes.

**Clubic : Comment la box Somfy et les appareils qu'elle permet de piloter à distance sont-ils protégés ?**

Somfy : En tant que spécialiste de solutions domotiques, notre box prend en compte les problématiques de sécurité. L'ensemble des actions effectuées avec nos solutions Tahoma et Somfy Box transite sur un serveur sécurisé et est chiffré sur 128 bits. Le protocole RTS propriétaire de Somfy (10 millions de systèmes installés dans le monde) qui est utilisé pour la commande radio est sécurisé grâce à un code tournant de 16 millions de combinaisons.

**Clubic : En tant que fabricant, que pensez-vous du remous médiatique autour de la vulnérabilité supposée ou avérée de certains objets connectés pour la maison ?**

Somfy : Nous sommes aujourd'hui en plein boom des objets connectés, avec de nombreux nouveaux acteurs qui lancent parfois des solutions un peu trop vite et pas suffisamment abouties. Il faut veiller à bien se renseigner sur le fabricant et sa légitimité sur le secteur. Somfy possède une expertise en matière de radio et d'IP qui nous rend légitimes sur ce secteur. Depuis que nous avons lancé notre box il y a quatre ans, aucun piratage ne nous a été signalé.

**Clubic : Quels sont selon vous les points faibles d'une installation, ou quels pourraient-ils être ?**

Somfy : Les points faibles de l'installation seraient de ne pas avoir de système de protection, d'avoir positionné les détecteurs de mouvements aux mauvais endroits ou de ne pas couvrir tous les accès de la maison.

**Clubic : Selon vous, quel serait LE scénario catastrophe pour une maison intelligente ?**

Somfy : Le scénario catastrophe, s'il y en a un, serait de se faire voler son téléphone sans code pour le déverrouiller en laissant ainsi libre accès à l'application qui commande la maison intelligente. Il faut donc prendre les précautions nécessaires.

**Conclusion**

En moins de deux ans, la domotique est passée d'un marché de niche à un nouvel eldorado convoité par la plupart des géants de l'industrie high-tech. Apple, Google, Microsoft ou encore Samsung, pour ne citer qu'eux, se sont lancés tour à tour sur ce marché promis à une très forte croissance en multipliant les partenariats et les rachats de start-up spécialisées. Début 2014, Google n'a pas hésité par exemple à faire la troisième acquisition la plus importante de son histoire, en rachetant Nest Labs pour la bagatelle de 3,2 milliards de dollars et, plus récemment, le spécialiste de caméras IP Dropcam pour 555 millions de dollars.

Courant 2014, Samsung s'est offert la start-up spécialisée SmartThings (montant de l'achat non divulgué), Microsoft a noué un partenariat avec Insteon, un des leaders de la domotique aux USA, et Apple a dévoilé à l'occasion de la WWDC la plateforme HomeKit pour iOS8 qui permettra de contrôler les objets connectés de nombreux fabricants via Siri (l'assistant vocal d'Apple). En attendant les solutions des poids lourds des nouvelles technologies, le marché est déjà bien occupé par les acteurs historiques – Somfy, Philips, Haier, Legrand, etc. –, une foule de nouveaux fabricants de tous horizons, des fournisseurs d'électricité ou encore des opérateurs comme Orange et SFR, qui commercialisent en France des kits de domotique pour accompagner leurs box. Si tout ce monde frappe à la porte de nos foyers, c'est que le potentiel est énorme.

Il ne fait aucun doute que les produits du quotidien vont être de plus en plus connectés (comme nous avons pu le voir au CES cette année), mais pas toujours bien sécurisés. Les acteurs comme Google, Apple et Microsoft, qui ambitionnent qu'un maximum d'objets connectés puissent fonctionner à l'avenir avec leurs plateformes mobiles respectives, vont sans doute imposer aux fabricants un cahier des charges drastique en matière de sécurité s'ils veulent obtenir une certification. Cela pourrait peut-être permettre d'augmenter le niveau de protection des objets connectés, même si comme nous l'avons vu, il n'est pas toujours possible de patcher des produits comprenant des composants provenant de différents fabricants.

Le nombre croissant d'objets connectés risque d'intéresser de plus en plus les cybercriminels pour entreprendre des diffusions de spams ou de logiciels malveillants à grande échelle, par exemple. Mais le plus effrayant serait qu'ils puissent prendre le contrôle total des maisons intelligentes, espionner leurs habitants à l'aide des caméras de surveillance, s'introduire ni vu ni connu dans le foyer en déverrouillant la porte à l'aide d'un smartphone, couper l'électricité ou le chauffage en plein hiver, ou encore, déclencher l'alarme au beau milieu de la nuit…

Pour que les maisons intelligentes tiennent vraiment toutes leurs promesses, il est indispensable qu'à l'avenir leur sécurité soit garantie. En attendant, côté utilisateur, il faudra être de plus en plus vigilant, se renseigner sur le système de protection des produits, faire systématiquement les mises à jour, ou encore instaurer un mot de passe fort pour l'accès à distance de tous les appareils connectés. Le prix à payer pour que le rêve de posséder une maison intelligente ne tourne pas au cauchemar.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : #http://www.clubic.com/antivirus-securite-informatique/article-723729-1-objets-connectes-representent-risque.html
Par Jérôme Cartegini

# 10 conseils pour garder vos appareils protégés pendant les vacances | Denis JACOPINI

## 10 conseils pour garder vos appareils protégés pendant les vacances

**Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, voici un mini-guide conçu par les experts ESET pour voyager et surfer en toute tranquillité.**
Brosse à dents ? ok.
Serviette de bain ? ok.
Ordinateur, téléphone, tablette ? ok.
Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, méfiez-vous des menaces lorsque vous utilisez un Wi-Fi public pour vous connecter à votre banque en ligne, boutique en ligne ou tout simplement pour vérifier vos e-mails. Pas de panique ! Stephen Cobb et d'autres professionnels ESET ont créé un guide pour vous permettre de voyager en toute sécurité et garder ainsi toutes vos données personnelles et vos appareils protégés.

**Conseils**


1. Avant de prendre la route, assurez-vous d'exécuter sur vos appareils une mise à jour complète du système d'exploitation ainsi que des logiciels, et de posséder une solution de sécurité de confiance.
2. Sauvegardez vos données et placez-les dans un endroit sûr. Pensez à déplacer les données sensibles du disque dur de votre ordinateur portable sur un disque dur externe chiffré le temps de vos vacances.
3. Ne laissez jamais vos appareils sans surveillance dans les lieux publics. Activez la fonction antivol de vos appareils pour tracer les appareils volés ou perdus, et au besoin d'effacer les contenus à distance.
4. Mettez un mot de passe fort et activez la fonction « délai d'inactivité » sur tous vos appareils, que ce soit votre ordinateur portable, votre tablette ou votre téléphone. Retrouvez tous nos conseils pour un mot de passe efficace en cliquant ici.
5. Dans la mesure du possible, utilisez uniquement des accès internet de confiance. Demandez à votre hôtel ou l'endroit où vous logez le nom de leur Wi-Fi et utilisez exactement le même nom : faites attention aux arnaques qui essaient de ressembler aux Wi-Fi publics en ajoutant le mot « gratuit » au nom de la connexion Wi-Fi.
6. Si l'Internet de votre hôtel vous demande de mettre à jour un logiciel afin de pouvoir vous connecter, déconnectez-vous immédiatement et informez-en la réception.
7. Ne vous connectez pas à des connexions Wi-Fi qui ne sont pas chiffrées avec WPA2. Toutes les normes inférieures à celle-ci ne sont tout simplement pas assez sûres et peuvent être facilement piratées.
8. Si vous devez utiliser le Wi-Fi public pour vous connecter à votre réseau d'entreprise, utilisez toujours votre VPN (réseau virtuel privé).
9. Si ce n'est pas urgent, évitez les banques et boutiques en ligne quand vous utilisez le Wi-Fi public. Sinon, nous vous conseillons d'utiliser le partage de connexion de votre téléphone et de surfer en utilisant internet sur votre téléphone portable.
10. Si vous n'utilisez pas encore d'antivirus de confiance et suspectez votre ordinateur portable d'être infecté, vous pouvez utiliser gratuitement le scanner ESET Online qui ne nécessite aucune installation et peut être utilisé pour détecter et retirer des logiciels malveillants
Article original de ESET
Cliquez ici

---

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 Liberté) ;
- 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 : ESET — Actualités

---

# Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

**Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.**

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.
Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant… Les accès gratuits pullulent et se généralisent.
Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « **Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit** » assure-t-il. « **Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants…** »

## Des sniffeurs de données

Il exagère ? Non. « **L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés !** » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

## Les données sur le Wi-Fi ne sont pas chiffrées

« **Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter.** » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « **Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi** ».

## Conseils

Alors quels conseils ? « **Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites.** » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.
Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Androïd.
Article original de Samuel NOHRA.

**Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]**

---

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 : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

# Fausses applications Pokémon GO. Comment se protéger ? | Denis JACOPINI


Fausses applications Pokémon GO. Comment se protéger ?

**Les chercheurs ESET découvrent des fausses applications sur Google Play qui cible les utilisateurs de Pokémon GO. L'une d'entre elles utilise pour la première fois une application qui verrouille l'écran (Lockscreen) sur Google Play. Les deux autres applications utilisent la fonctionnalité scareware qui oblige l'utilisateur à payer pour des services inutiles.**

Toutes les fausses applications découvertes par ESET et détectées grâce à ESET Mobile Security (application lockscreen nommée « Pokémon GO Ultimate » et les applications scareware « Guide & Cheats for Pokémon GO » et « Install Pokemongo ») ne sont plus disponibles sur Google Play. Elles ont été retirées de l'app Store suite à l'alerte donnée par ESET.

Même si ces fausses applications ne sont pas restées longtemps sur le Google Play, elles ont généré quelques milliers de téléchargements. L'application « Pokémon GO Ultimate », a piégé entre 500 et 1.000 victimes, « The Guide & Cheats for Pokémon GO » en a atteint entre 100 et 500, et la plus dangereuse d'entre elles, « Install Pokemongo » a atteint entre 10.000 et 50.000 téléchargements.

« Pokémon GO Ultimate » cultive son extrême ressemblance avec la version officielle du célèbre jeu mais ses fonctionnalités sont très différentes : elle verrouille l'écran automatiquement après le démarrage de l'application. Dans de nombreux cas, réinitialiser le téléphone ne fonctionne pas parce que l'application se superpose à toutes les autres, ainsi qu'aux fenêtres du système. Les utilisateurs doivent redémarrer leurs appareils en retirant la batterie ou en utilisant Android Device Manager. Après la réinitialisation, l'application malveillante fonctionne en arrière-plan, à l'insu de sa victime, en cliquant silencieusement sur des annonces à caractère pornographique. Pour se débarrasser de l'application, l'utilisateur doit aller dans Réglages -> Gestion des Applications -> PI Réseau et la désinstaller manuellement.

« Pokémon GO Ultimate » est la première fausse application sur Google Play qui utilise avec succès une fonction de verrouillage d'écran. Comme la fonctionnalité principale de cette application est le clic sur des annonces pornographiques, il n'y a pas de réels dommages. Mais il suffit de peu pour que la fonction de verrouillage d'écran évolue et ajoute un message de rançon, pour créer le premier ransomware par lockscreen sur Google Play.», explique Lukáš Štefanko, Malware Researcher chez ESET.

Alors que l'application « Pokémon GO Ultimate » porte les signes d'un screenlocker et d'un pornclicker, les chercheurs ESET ont également trouvé un autre malware sur Pokémon GO dans Google Play. Les fausses applications nommées « Guide & Cheats for Pokemon GO » et « Install Pokemongo » sur Google Play, appartiennent à la famille des Scarewares. Ils escroquent leurs victimes en leur faisant payer des services inutiles. En leur promettant de leur générer des Pokecoins, Pokeballs ou des œufs chanceux – jusqu'à 999.999 chaque jour – ils trompent les victimes en leur faisant souscrire à de faux services onéreux. (Cette fonctionnalité a récemment été décrite dans un article publié sur WeLiveSecurity).

« Pokémon GO est un jeu si attrayant que malgré les mises en garde des experts en sécurité, les utilisateurs ont tendance à accepter les risques et à télécharger toutes applications qui leur permettraient de capturer encore plus de Pokémons. Ceux qui ne peuvent pas résister à la tentation devraient au moins suivre des règles de sécurité élémentaires. » recommande Lukáš Štefanko.

**Conseils des experts en sécurité ESET pour les afficionados de Pokémon GO :**

– téléchargez uniquement ce qui vient d'une source connue
– lisez les avis en prêtant attention aux commentaires négatifs (gardez en tête que les commentaires positifs ont pu être créés par le développeur)
– lisez les termes et conditions de l'application, concentrez-vous sur la partie qui concerne les permissions requises
– utilisez une solution de sécurité mobile de qualité pour vérifier toutes vos applications

**Conseils de Denis JACOPINI**

Pour anticiper et vous protéger pour moins de 10€ (10€ est prix de la licence initiale. Une forte réduction sera appliquée au moment du renouvellement au bout d'un an)


Article original de ESET

---

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

---

# Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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

LE NET EXPERT AUDITS & EXPERTISES

EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES
LENETEXPERT.fr

RGPD CYBER
LE NET EXPERT MISES EN CONFORMITÉ

SPY DETECTION
Services de détection de logiciels espions

LE NET EXPERT FORMATIONS

LE NET EXPERT ARNAQUES & PIRATAGES

# Formation RGPD : l'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Contenu de nos formations :

Le Règlement Général sur la Protection de Données (RGPD) entre en application le 25 mai 2018 et les entreprises ne s'y sont pas préparées. Or, elles sont toutes concernées, de l'indépendant aux plus grosses entreprises, et risqueront, en cas de manquement, des sanctions pouvant aller jusqu'à 4% de leur chiffre d'affaires. Au delà des amendes pouvant attendre plusieurs millions d'euros, c'est aussi la réputation des entreprises qui est en jeu. Quelle valeur lui donnez vous ? Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

**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.**

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

---

**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 :

Nous animons des Formations sur le RGPD en individuel ou en groupe

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

**Quelques articles sélectionnés par nos Experts :**
Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

---

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

---

# Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s'en protéger ?

Le contexte de l'Internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos comportements au quotidien.
Avons-nous raison d'avoir peur ? De quoi doit-on avoir peur ? Comment se protéger ?
Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des attitudes responsables seront les clés permettant d'enrayer le phénomène.

**OBJECTIF DE LA FORMATION EN CYBERCRIMINALITE :**

La formation en cybercriminalité a pour but de créer des déclics chez les utilisateurs, mettre à jour les connaissances des informaticiens et faire prendre conscience aux chefs d'entreprises des risques en couvrant les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer le phénomène de la cybercriminalité.

**PROGRAMME :**

• Etat des lieux de la cybercriminalité en France et dans le monde;
• Les principaux cas de piratages et d'arnaques expliqués ;
• Les bonnes pratiques au quotidien pour limiter les risques ;
• Etude de vos témoignages, analyse de cas et solutions.
• PUBLIC CONCERNÉ : Utilisateurs, chefs d'entreprise, présidents d'associations, élus….

**MOYENS PÉDAGOGIQUES :**

• **Support de cours pour prise de notes**
• **Résumé remis en fin de cours.**
• **Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.**

**CONDITIONS D'ORGANISATION**

• Formations individuelles ou en groupe
• Formations dispensées dans vos locaux ou organisées en salle de formation partout en France en fonction du nombre de stagiaires.

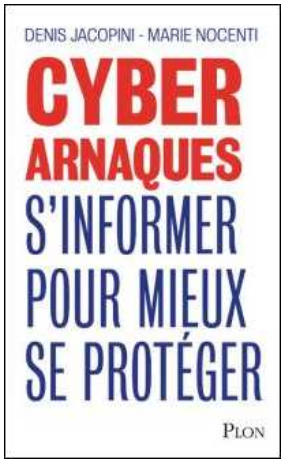
Téléchargez la fiche de présentation / Contactez-nous

**QUI EST LE FORMATEUR ?**

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.
Il anime dans toute le France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.
A ce titre, il intervient régulièrement sur différents médias et sur La Chaine d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.
Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).
Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.
Denis JACOPINI peut facilement être contacté sur :
http://www.leNetExpert.fr/contact

[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

---

# 10 bonnes pratiques pour des soldes sur Internet en

# sécurité

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

# 10 bonnes pratiques pour des soldes sur Internet en sécurité

**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.

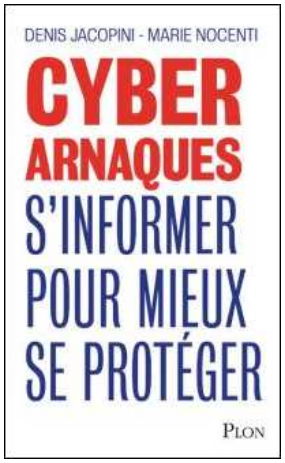
– **Utilisez une e-carte bleue.** Non seulement elle est déconnectée de vos comptes bancaires et est également assurée contre les fraudes.

– **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.

[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

Article original de ESET

---

# Victime d’un piratage

# informatique, quelles sont les bonnes pratiques ?


---

**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 ;

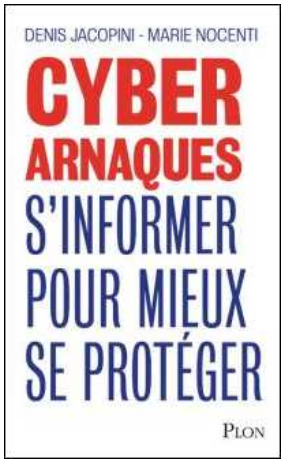
• Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

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.

[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

---

# Objets connectés : les inquiétantes failles de

# sécurité dont vous n’avez pas conscience | Denis JACOPINI

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

**Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ? Télévision, pèse-personne, thermostat et autres hubs domotiques… les objets connectés tentent d'envahir nos maisons et de s'infiltrer au coeur même de leur réseau numérique.**

Pourtant, malgré leur objectif de nous simpliflier la vie, leur développement semble encore assez poussif ; en raison sans doute de leur manque criant de sécurité. C'est ce que révèle une étude menée par la division Sécurité de Hewlett Packard : rien de moins que 250 vulnérabilités ont été relevées par les experts d'HP Fortify au sein des 10 objets connectés les plus populaires.
Ces failles de sécurité seraient, selon Mike Amistead, le manager général d'HP Fortify, le symptome de la ruée des entreprises sur le créneau des objets connectés. Il estime en effet que les start-ups se lançant sur ce marché tenteraient de commercialiser leur produit le plus rapidement possible avant la concurrence… au mépris de la garantie d'un niveau de sécurité suffisant des réseaux et des données personnelles.
Vos données personnelles en clair sur la toile Parmi les failles de sécurité relevées, HP a constaté que :
• 90 % des objets connectés étudiés solliciteraient une information personnelle sensible (ex : adresse email ou postale, nom, date de naissance, etc) ; une information ensuite véhiculée en clair sur la toile ;
• 70 % des objets connectés ne crypteraient pas les données échangées avec le réseau ;
• 80 % des objets connectés ne nécessiteraient pas de mot de passe complexe pour identifier les demandes de connexion tierces ;
• 60 % des objets connectés seraient vulnérables aux attaques dites de « cross-site scripting » (type de faille de sécurité permettant d'injecter du contenu dans une page, et provoquant ainsi des actions sur les navigateurs web visitant la page).

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

[block id="24881" title="Pied de page Contenu Cyber"]

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

Source : http://www.archimag.com/vie-numerique/2014/07/30/objets-connectes-internet-failles-securit

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

**Il 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.

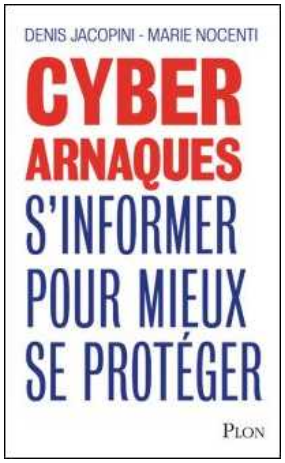
**Et si on dispose d'un Mac plutôt que d'un PC ?**
Il y a quelques années, avoir un Mac « garantissait » d'être un peu à l'abris des virus et des pirates informatiques. En effet, pouquoi un pirate informatique perdrait du temps à développer un logiciel malveillant et prendrait des risques pour seulement 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