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.

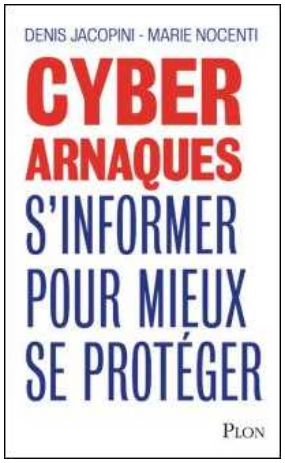
– **Utilisez une e-carte bleue.** Non seulement elle est déconnectée de vos comptes bancaires et est également assurée contre les fraudes.

– **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 ;

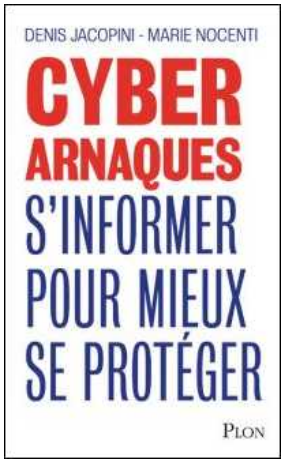
• Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

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

63% des Français redoutent de donner des informations

personnelles sur Internet | Denis JACOPINI

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

Selon une enquête réalisée par Dashlane et Opinionway, en France, au Royaume-Uni et aux États-Unis, les internautes français sont ceux qui se méfient le plus. 14% ne communiquent jamais leurs données personnelles, contre 4 % des Britanniques et 5% des Américains.

En fonction de leur identité culturelle, les internautes n'abordent pas la saisie des données personnelles sur la toile de la même manière. Selon un sondage Opinionway, réalisé en octobre 2015, les Français se montrent bien plus frileux que leurs homologues anglo-saxons: 63% d'entre eux avouent leur méfiance quand il s'agit de donner des informations personnelles sur le web contre 35 et 34% chez les Britanniques et les Américains. 14% des Français refusent de communiquer leurs informations personnelles, un chiffre qui tombe à 4 et 5% en Grande-Bretagne et aux États-Unis.
Quel que soit le pays, la donnée la plus sensible est le numéro de carte bancaire. Là encore, ce sont les Français qui arrivent en tête. 72% d'entre eux avouent leur crainte quand il s'agit de stocker cette information sur un site, contre 48% des Anglais et 41% des Américains.
Les critères qui rassurent ne sont pas les mêmes d'un pays à l'autre, selon l'enquête. Les Français se sentent en priorité protégés par le petit cadenas à côté de l'adresse qui indique une connexion sécurisée (68%), puis par l'assurance que les données ne seront pas transmises (36%). Les Britanniques et les Américains se fient, eux, à la marque ou au site Internet (53% et 47%).
En revanche, le mot de passe fait consensus. Il rime avec sécurité dans le cas de transactions pour 1/3 des Français, des Britanniques et des Américains.
Globalement, les internautes se posent beaucoup de questions quand il s'agit de payer en ligne. La vigilance reste de mise à l'égard de certains sites, de peur d'être piratés. 65% des Français évitent alors d'y utiliser leur carte. 66% des Britanniques et 70% des Américains s'abstiennent également.
Interrogés sur les systèmes sensés améliorer leur confiance, les participants se disent prêts à utiliser leur carte bancaire plus souvent, si l'utilisation une carte temporaire infalsifiable rend le piratage impossible. À cette condition, 70% des Français, 76% des Britanniques et 77% des Américains passeraient à l'acte. Autre critère jugé rassurant: une étape d'authentification supplémentaire (63% en France, 54% en Grande-Bretagne et 50% aux États-Unis).
Méthodologie : pour réaliser cette enquête, un échantillon représentatif a été constitué en fonction des critères de sexe, d'âge, de catégorie socioprofessionnelle en France, de catégorie sociale Esomar au Royaume-Uni et de revenus aux Etats-Unis. 1014 Français, 1004 Britanniques et 1009 Américains ont été soumis à un questionnaire en ligne sur système CAWI (Computer Assisted Web interview).

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

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

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

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

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

Source : http://www.boursorama.com/actualites/63-des-francais-redoutent-de-donner-des-informations-personnelles-sur-internet-419faf4a01d101ef73283fcf315c7a50

Attention ! Voici ce que les cyberdélinquants vous réservent… | Denis JACOPINI

Ingénieux, fourbes, malicieux… Des qualificatifs qui désignent bien les cyberdélinquants qui parasitent la toile, nos réseaux sociaux. Pourtant s'ils rivalisent d'astuces en tout genre, un mode opératoire se dessine sous nos yeux. A nous de savoir les identifier et de préserver l'intégrité de nos informations personnelles, et de notre portefeuille.

Dans le souci de vous faire de vous-même votre première protection contre ces cyberdélinquants, la Plateforme de lutte contre la cybercriminalité de Côte d'Ivoire (PLCC-CI) vous donne quelques types d'arnaque que ces derniers utilisent pour nous spolier.

Voici dans les grandes lignes, quelques-unes des arnaques auxquelles la PLCC fait face et que vous devez apprendre à identifier.

CHANTAGE A LA VIDEO
Cette escroquerie consiste pour le cybercriminel à :
• Faire connaissance avec sa victime sur les réseaux sociaux, site de rencontre, forum, etc.
• Établir une relation de confiance au fil des discussions
• Proposer à la victime de passer sur un service permettant la visiophonie par webcam
• Favoriser une conversation vidéo plus intime puis profiter pour capturer le flux vidéo des images susceptibles de porter atteinte à la vie privée de la victime
• Demander de fortes sommes d'argent à la victime en menaçant de diffuser ces vidéos sur internet

ARNAQUE AUX FAUX SENTIMENTS
Une arnaque classique. Elle consiste pour le cyber délinquant d'établir une relation de confiance avec sa proie pour mieux l'attendrir puis l'arnaquer ensuite.

ACHAT /VENTE :
En réponse à une offre de vente en ligne sur internet, un prétendu acheteur résidant ou en déplacement en Côte d'Ivoire demande les coordonnées bancaires ou autres du vendeur pour un virement ou l'expédition dudit marchandise avec fausse promesse de règlement des réceptions.
L'escroc passe des commandes de matériels à des exportateurs ou des entreprises en France au nom d'entreprises fictives et propose de payer soit par des cartes de crédit, soit par virement.

SPOLIATION DE COMPTE MAIL OU DE RESEAUX SOCIAUX :
Cette pratique consiste pour le cyber délinquant de prendre possession de votre compte mail ou autre dans le but de perpétrer une usurpation d'identité en envoyant des emails à vos correspondants, en leurs apprenant que soit vous a eu un accident soit vous êtes fait agressé et que vous avez besoin d'argent.

USURPATION D'IDENTITE :
Elle consiste pour le cyber délinquant de se faire passer pour vous. En pratique, c'est le fait pour l'usurpateur d'utiliser soit votre photo, votre carte d'identité ou toute autre chose vous appartenant et qui vous représente.

DETOURNEMENT DE TRANSFERT :
La pratique consiste pour l'escroc de faire le retrait de l'argent qui vous était destiné à votre insu. Pour ce faire, il collecte des informations sur les codes de transfert et aidé par d'autres personnes, il fait le retrait avec de fausse pièce.

FRAUDE SUR SIMBOX :
C'est une technique frauduleuse qui consiste à transiter les appels internationaux en appel et ce au préjudice de l'opérateur de téléphonie et du gouvernement.

FRAUDE SUR COMPTE / BANCAIRE :
C'est l'utilisation frauduleuse de numéro de carte ou compte pour réaliser des paiements sur internet.

FRAUDE INFORMATIQUE :
C'est le fait d'accéder ou de se maintenir frauduleusement dans un système dans tout ou partie d'un système de traitement pour l'entraver, soit pour le supprimer ou, modifier ou le copier.

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

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

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

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

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

Source : http://cybercrime.interieur.gouv.ci/?q=article/cybercriminalit%C3%A9-attention-voici-ce-que-les-cyberd%C3%A9linquants-vous-r%C3%A9servent%E2%80%A6

Comment empêcher Android de sauvegarder automatiquement nos données personnelles ?

Comment empêcher Android de sauvegarder automatiquement nos données personnelles ?

Nos smartphones et tablettes Android sauvegardent certaines de nos données personnelles sur les serveurs de Google sans forcément nous demander notre avis. Un système qui peut s'avérer aussi pratique pour certains qu'il peut être dérangeant pour d'autres. Encore faut-il savoir quelles sont les données sauvegardées par Google et celles qui ne le sont le pas. Nous allons donc aujourd'hui nous pencher sur la question.

N'avez-vous jamais remarqué que lorsque vous entrez-vos identifiants Google dans un nouvel appareil Android, ce dernier retrouvait automatiquement certaines de vos informations personnelles, notamment vos contacts. Pourtant, vous n'avez jamais rien fait pour, et pour cause puisque cette option est activée par défaut. Ce qui signifie que vous pouvez également la désactiver. La plupart des utilisateurs la conservent néanmoins activée pour des raisons de praticité.

Il faut dire que cette sauvegarde automatique peut s'avérer utile lorsque vous changez de smartphone, lorsque vous disposez de plusieurs appareils Android ou si par malheur, vous vous faisiez voler votre téléphone. Mais certains ne veulent pas que leur vie privée se retrouve sur le cloud de Google. Ce tutoriel est pour eux mais avant de passer à la pratique, un peu de théorie.

Les données automatiquement sauvegardées par Google

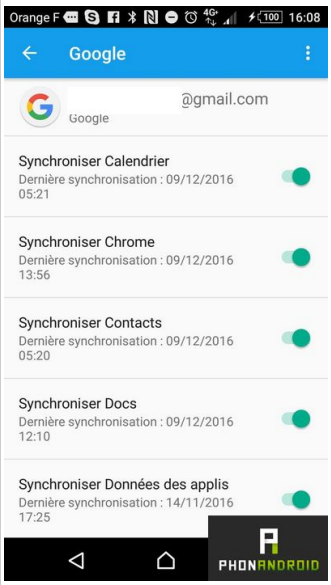
Au sein de son OS, Google a intégré un outil du nom d'Android Backup Service qui sauvegarde certaines données liées aux services que vous utilisez. Ces données sont les suivantes :

• **Contacts** qui sont sauvegardés au sein de Google Contacts. Vous pouvez ainsi les retrouver sur tous vos appareils et même sur votre PC en vous connectant simplement à votre compte.
• **Emails** qui sont sauvegardés au sein de Gmail
• **Documents**, ce qui vous permet d'ailleurs d'éditer vos documents sauvegardés dans le cloud à partir de n'importe lequel de vos appareils
• **Calendriers**
• **Chrome** : vos favoris et votre historique de navigation sont synchronisés avec votre compte. Idem pour vos mots de passe si vous avez activé la fonction Smart Lock
• **Hangouts** : vos conversations sont sauvegardées
• **Google Play Store** : les applications que vous avez téléchargées sont automatiquement sauvegardées. Vous pouvez ensuite les retrouvez dans l'onglet « Mes applications » de la boutique. C'est très pratique lorsque vous changez de smartphone car vous n'avez pas besoin de les rechercher une par une, en outre, les applications achetées sont également sauvegardées
• Vos **photos** et vidéos, à condition d'utiliser l'application Google Photos et d'avoir activé la sauvegarde automatique de vos médias
• Certaines **données d'applications**

Comment empêcher Google de sauvegarder vos données

Vous n'êtes pas ravis à l'idée que Google en sache autant sur vous et vous souhaiteriez que certaines de vos données ne soient pas sauvegardées ? Et bien rassurez-vous, c'est possible et en quelques clics. Il vous suffit pour cela de :

• Vous rendre dans le menu **Paramètres > Personnel > Comptes de votre smartphone**
• Sélectionner votre compte Google
• Décocher toutes les données que vous ne voulez pas que Google sauvegarde



Et pour aller plus loin, n'hésitez pas à jeter un œil à notre tutoriel comment préserver sa vie privée sur Android.

Les données non sauvegardées par Google

Les données listées ci-dessous ne sont pas sauvegardées par Google. Pour éviter de les perdre en changeant de smartphone, il faudra donc utiliser une application tierce mais nous y viendrons après.

• Les SMS, il est néanmoins possible de sauvegarder ses SMS sur Android en utilisant une application
• Google Authentificator : pour des raisons de sécurité, les données d'authentification Google en deux étapes ne sont pas sauvegardées
• Réglages : les paramètres personnalisés de de votre smartphone ne sont pas sauvegardés
• Bluetooth : Android ne synchronise pas les périphériques Bluetooth appairés vers votre smartphone

Comment sauvegarder toutes ses données personnelles

Bien que Google ne le permette pas par défaut, il est tout à fait possible de sauvegarder toutes les données de votre smartphone Android à l'aide de notre précédent tutoriel. Certaines de vos données iront directement sur votre support externe, d'autres seront sauvegardées en ligne afin de pouvoir ensuite être réintégrées à votre nouveau smartphone si votre but est de sauvegarder vos données pour les retrouver sur un nouvel appareil.

N'oubliez pas non plus de jeter un œil à notre sélection d'applications pour sauvegarder ses données personnelles. Certaines nécessiteront que votre téléphone soit rooté, d'autres non, et elles vous permettront de sauvegarder toutes vos applications et pas seulement les données.

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 ?

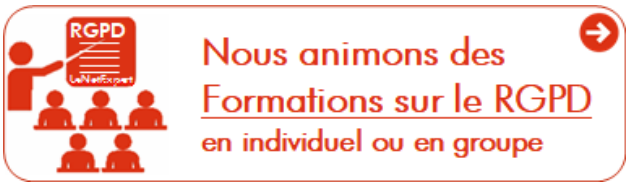
Contactez-nous

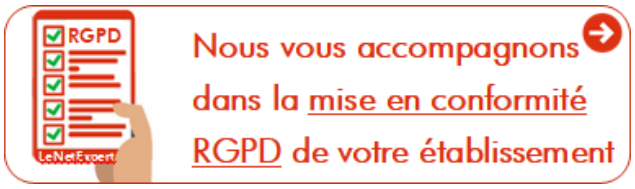
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

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 :





Quelques articles sélectionnés par nos Experts :

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

en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Source : http://www.phonandroid.com/comment-empecher-android-sauvegarder-automatiquement-donnees-personnelles.html

---

Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone

Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone

Interviewé par Atlantico, Denis JACOPINI nous parle d'une nouvelle forme de Phishing. Le APP (Authorised Push Payment Fraud – fraude au paiement par autorisation) serait une des techniques de fraude en forte croissance au Royaume Uni, et combinerait des techniques sophistiquées, au travers de SMS et d'appels, pour soutirer de l'argent aux victimes.

Le APP (Authorised Push Payment Fraud – fraude au paiement par autorisation) serait une des techniques de fraude en forte croissance au Royaume Uni, et combinerait des techniques sophistiquées, au travers de SMS et d'appels, pour soutirer de l'argent aux victimes. 19 370 cas auraient été répertoriés au Royaume Uni au cours de ces 6 derniers mois selon le daily mail. Quelles sont les techniques ici employées ? La France est-elle touchée ?
Denis Jacopini : Cette technique de fraude utilise de nombreux ingrédients de base :
• L'ingénierie sociale (pratique utilisant des techniques de manipulation psychologique afin d'aider ou nuire à autrui)
• L'usurpation (d'identité);
• Le passage en mode émotionnel par la peur ;
• L'interlocuteur est votre sauveur et est là pour vous aider.

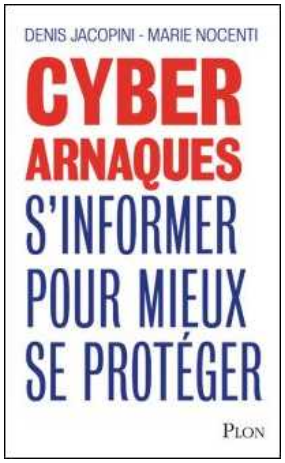
Dans le cas précis, nous avons aussi :
• L'usurpation du nom de la banque ;
• L'usurpation du numéro de téléphone de la banque ;
• Le passage en mode émotionnel de la victime basé sur la peur du piratage mais heureusement elle est en ligne avec un sauveur (baisse de la prudence, confiance aveugle…) ;
• La création d'une ambiance téléphonique de centre d'appel ;
• Un excellent comédien qui joue le rôle de l'employé de banque ;
• Une excellente connaissance des procédures internes des banques dont la banque usurpée.
En France, ce type d'arnaque n'est pas encore médiatisé. En effet, les banques n'aiment pas tellement communiquer sur leurs failles car :
• Ce n'est pas bon pour leur image ;
• Elles sont ensuite obligées de dépenser beaucoup pour corriger ;
• Elles préfèrent investir lorsque la fraude commence à leur coûter plus cher que les mesures de sécurité à mettre en place (gestion du risque).

Ces nouvelles techniques de fraude marquent elles une réelle professionnalisation de cette forme de criminalité ?
Denis Jacopini : Cette forme de criminalité existe depuis très longtemps et n'a pas attendu l'informatique et Internet pour se développer et se professionnaliser. Prétexter un gros risque et usurper l'identité des pompiers, des policiers, du plombier en utilisant leur costume, leur jargon, leur outils pour vous rassurer et reviennent ensuite pour mieux vous arnaquer ou vous cambrioler existe depuis que les escrocs existent.
Plus récemment, Gilbert Chikli Pionnier de l'arnaque au faux président, utilisait des techniques de manipulation psychologique et se servait de sa parfaite connaissance des procédures internes aux très grandes entreprises et sa maîtrise du langage juridique ou financier en fonction de l'identité de la personne usurpé pour obtenir de ses victimes des virements définitifs pour des sommes détournées de plusieurs dizaines de millions d'euros.
Chaque fois que des techniques d'arnaque ou d'escroquerie sont déjouées, décortiquées et dévoilées au grand jour, il y a des millions d'escrocs du dimanche vont analyser l'arnaque pour la reproduire et l'utiliser pour eux. Une fois que l'arnaque commence à être connue et de plus en plus de gens sont sensibilisés, les escrocs professionnels et utilisant leur génie à des fins illicites modifient leurs techniques pour toujours utiliser des moyens basés sur les ingrédients de base + des failles inexploitées utilisant ou non la technologie.
Comme les banques ont mis en place des mesures de sécurité utilisant l'internet, le SMS, le téléphone, les escrocs utilisent ces mêmes technologies en recherchant le moyen d'exploiter les failles qui ne seront jamais suffisamment protégées : Les failles du cerveau humain.

Quels sont les réflexes à avoir pour éviter tout problème de ce type ?
Denis Jacopini : Le seul moyen que nous avons pour nous protéger est d'une part la prudence ultime en plus de la sensibilisation. Selon moi, les médias devraient signaler ce type d'arnaque afin de sensibiliser le plus grand nombre. Cependant, cette solution ne plait pas aux banques qui considèrent inutile de répandre la peur car cela risquerait d'écorcher de manière irréversible la confiance que nous avons mis des années à avoir envers les moyens de paiement électronique sur Internet.
A notre niveau, si j'ai un conseil à vous donner pour éviter tout problème de ce type, si vous vous trouvez dans une situation anormale qui vous est présenté par un interlocuteur, contactez directement l'établissement à l'origine de l'appel à partir des coordonnées dont vous disposez, et allez jusqu'au bout de la vérification AVANT de réaliser des opérations financières irréversibles et partagez le plus possible les cas d'arnaques.
Quand on sait à quoi ressemble le loup, on ne le fait pas rentrer dans sa bergerie. Par contre, s'il met un nouveau costume, le piège fonctionnera tant que ce nouveau costume ne sera pas connu du plus grand nombre. (d'où l'utilité de mon livre CYBERARNAQUES
https://www.amazon.fr/Cyberarnaques-Denis-JACOPINI/dp/2259264220

[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 : *Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone | Atlantico.fr*

Notre avis sur le choix des logiciels de sécurité | Denis JACOPINI

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

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

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

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

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

1. http://assiste.com.free.fr/p/abc/a/pirates_informatiques.html
2. http://www.imprimer-dematerialiser.fr/la-cybercriminalite-2015-en-8-chiffres

---

Vol de données : cinq conseils pour se protéger

contre les intrusions | Denis JACOPINI

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

Ransomware, chevaux de Troie et logiciels malveillants : les entreprises ne sont guère à l'abri des attaques de pirates qui représentent un grand risque pour leur sécurité. Mais contrairement aux idées préconçues, les menaces ne proviennent pas uniquement de l'extérieur. Les employés de l'entreprise peuvent ainsi mettre à profit les nombreuses possibilités qu'ils ont d'accéder aux systèmes de l'entreprise pour une utilisation frauduleuse des données, et cela sans beaucoup d'effort. Les organisations sont d'ailleurs rarement aussi bien protégées des attaques venant de l'interne que de celles extérieures.

Les cinq recommandations suivantes peuvent aider les entreprises à se protéger efficacement contre le vol de données par des employés.

1. Octroyer des droits d'accès différents

Pour protéger les données sensibles, il est nécessaire de donner aux employés travaillant dans différents départements des droits d'accès appropriés. Ainsi, le niveau de securité est determiné par le besoin de connaissances d'un projet : un employé n'a accès à certains documents et dossiers que si ceux-ci sont nécessaires pour effectuer une tâche qui tombe sous sa responsabilité. Ces divers cloisonnements mis en place au sein de l'entreprise sous la forme de « murailles de Chine » empêchent l'échange d'informations non nécessaire entre les différents départements, permettant de limiter la perte de données.

2. Utiliser une double authentification forte

Afin de limiter tout risque, l'étape supplémentaire recommandée est une authentification à deux facteurs. Pour accéder au système, l'utilisateur doit, par exemple, non seulement entrer son mot de passe, mais aussi recevoir un SMS contenant un mot de passe unique, valable pour une seule session. Ainsi, il n'est pas possible d'accéder à l'information et aux données sensibles, même si le mot de passe a été volé.

3. Durcir la protection des informations

Les fonctionnalités en terme de sécurité doivent inclure la protection des données. Le fournisseur ne devrait en aucun cas avoir accès aux fichiers et documents, par exemple. En outre, les droits des administrateurs doivent être limités aux informations pertinentes à leurs activités.

4. Mettre en œuvre une gestion des droits d'information

Les technologies de gestion des droits d'information des documents sensibles peuvent contrôler et protéger contre le téléchargement non autorisé. Celles-ci assurent un contrôle efficace des documents même si les utilisateurs sont autorisés à accéder à l'information. Le filigrane empêche, en outre, une capture d'écran des informations. Il n'y a aucun risque de perte de données dans cet environnement protégé et elles ne tombent pas entre de mauvaises mains.

5. Enregistrer toute modification

Pour éviter le vol de données par un employé de l'entreprise et de s'en rendre compte après coup, il est conseillé d'enregistrer tous les changements effectués afin que ceux-ci soient répertoriés dans un historique. Cela permet un flux d'informations toujours clair et transparent.

Sofia Rufin, Vice Présidente Régionale de Brainloop, commente la menace croissante que reprèsentent les employés de l'entreprise dans le cadre de vols de données : « Nous avons observé au cours des dernières années, une augmentation du nombre des pertes de données dues à des failles en interne, les entreprises faisant encore trop souvent confiance à des standards de sécurité déficients. L'impact peut pourtant s'avérer désastreux sur l'image de l'entreprise, et les conséquences financières et légales peuvent menacer son développement économique… [Lire la suite]

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

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

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

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

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

Source : *Vol de données : cinq conseils pour se protéger contre les intrusions – Global Security Mag Online*

Un technique d’attaque informatique très répandue : Le « Watering Hole » | Denis JACOPINI

Les motivations des attaquants sont diverses. Les plus répandues sont le gain financier, la gloire personnelle, la malveillance ou encore l'espionnage.Quelle que soit la finalité de l'attaque, cette dernière passe le plus souvent par la compromission d'un système. Pour parvenir à leur fin, les attaquants disposent d'un large arsenal comprenant le contournement des mécanismes de sécurité, l'accès physique à la machine ou encore l'exploitation de vulnérabilités. Au sein de cet arsenal, l'exploitation de vulnérabilités constitue sans aucun doute le principal vecteur d'intrusion. Les méthodes d'infection employées peuvent alors prendre différentes formes :• Infection par média amovible (CD, USB, cartes SD, …)
• Infection par e-mail (pièce jointe ou un lien malicieux notamment)
• Infection via le réseau interne (fichiers partagés)
• Infection par visite d'un site Web

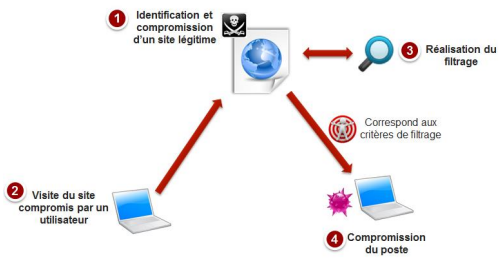
Le « Watering Hole » fait partie de la dernière catégorie : «Infection par site Web », autrement appelé «Drive-By Download». Cette dernière repose sur le principe suivant :
1. Création ou compromission d'un site Web par l'attaquant (accès à l'interface d'administration, compromission des régies publicitaires pour injecter du code au sein des publicités affichées, découverte d'une vulnérabilité de type XSS…)
2. Dépôt du malware sur le site (Ex : code JavaScript offusqué s'exécutant au chargement de la page, iframe contenant un ActiveX ou un applet Java malicieux hébergé sur un autre site, …)
3. Compromission de la machine cliente. La victime est incitée à se rendre ou redirigée de manière automatique sur le site Web hébergeant le malware. Son navigateur exécute le code malicieux et un malware est installé à son insu sur son poste de travail ou son Smartphone, très souvent de manière transparente. L'attaquant dispose alors d'un accès partiel ou complet sur l'appareil infecté.
Simple attaque de type « Drive-by Download » ?
La subtilité de cette attaque réside dans le choix des sites Web initialement compromis (cf étape 1). En effet, en fonction de la cible, le choix est principalement réalisé en fonction de la localité de l'entité ciblée ou en lien avec son métier.

Plusieurs cas concrets récents peuvent être cités en exemple :
• Professionnel : (politique/religieux/syndical…) Dans le cas d'Apple, de Microsoft ou de Facebook en février dernier, le site Web compromis était un site Web consacré au développement sur iPhone (iphoneDevSDK), site susceptible d'être visité par les développeurs des trois sociétés. La population cible peut également être plus restreinte comme l'illustre la compromission du site « http://www.rferl.org (Radio Free Europe Radio Liberty) ».
• Géographique : En Septembre 2012 lors de l'attaque VOHO[1], les cybercriminels avaient compromis un site gouvernemental local au Maryland, celui d'une banque régionale dans le Massachusetts afin de compromettre les machines de populations spécifiques résidant ou travaillant dans les localités ciblées.
• Et pourquoi pas Personnel : Il est tout à fait possible de voir le site du club de sport ou de musique où les enfants de la victime sont inscrits, être compromis…

Pourquoi utiliser cette méthode plutôt qu'une autre ?
En comparaison de l'envoi de phishing par exemple, cette méthode présente de nombreux avantages pour les attaquants :watering hole – scalable

Scalable :
Elle permet de couvrir un grand nombre de victimes « facilement ». Le «Drive-By Download» est largement utilisé dans le domaine de la #cybercriminalité permettant de compromettre un très grand nombre de machine rapidement ;
L'exploitation de vulnérabilités Java ou Adobe Flash récentes, peuvent permette de contourner les mécanismes de cloisonnement au sein des navigateurs Web et ainsi de couvrir de nombreux systèmes d'exploitation et navigateurs Web vulnérables différents
Efficace :
Couplée avec l'exploitation d'une vulnérabilité de type « 0-day », le taux d'infection peut être très élevé. Le rapport sur la campagne « VOHO »[2] publié par RSA et portant sur des attaques par « Watering Hole » recensait 32 160 machines infectées appartenant à 731 organisations pour un taux d'infection de 12%.
Discret :
Aucune action de l'utilisateur n'est nécessaire si ce n'est d'aller visiter ses sites Web habituels. L'absence de signaux rend également l'identification de la source de l'infection difficile. Enfin, la possibilité de filtrer les postes infectés (classe IP, langue du navigateur, localité …) permet de restreindre les dommages collatéraux et donc de limiter la visibilité de l'attaque.

Cette méthode présente cependant un certain nombre d'inconvénients :
• Potentiellement, une phase de reconnaissance, consistant à identifier sur quels sites se rendent les futures victimes
• Une phase de compromission de sites légitimes est nécessaire : les attaquants peuvent cependant identifier les sites vulnérables via des scans automatisés.
• Les attaquants doivent réaliser une analyse post-infection afin de déterminer, pour chaque poste compromis, quel type de profil a été infecté et si le profil correspond à la cible (société, fonction, …)



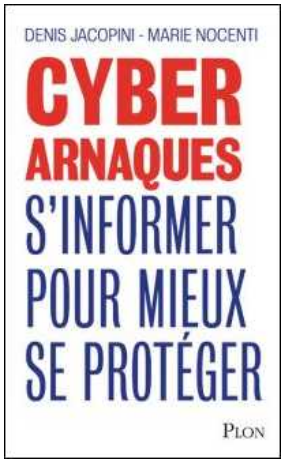
A noter que le filtrage effectué afin de réduire le périmètre des postes compromis émergent également au sein des attaques par phishing.

Quels sont les mécanismes de défense ?
Face à ce type de menace, il n'existe pas de solution « miracle ». Il convient donc d'appliquer des bonnes pratiques afin de limiter les risques d'infection et d'être réactif en cas de compromission :
1. [Mise à jour du parc] – On constate que les vulnérabilités exploitées sont le plus souvent liées aux technologies Java ou à Adobe Flash. A minima, il convient de maintenir à jour le parc applicatif. Cependant, cette mesure peut ne pas être suffisante (cas des 0-day). Nous recommandons donc de les désinstaller lorsqu'ils ne sont pas nécessaires.
2. [Filtrage Web] – Mettre à jour régulièrement en ajoutant automatiquement et au besoin manuellement les sites connus comme hébergeant des malwares au sien des listes noire des équipements de filtrage Web (nécessite de disposer d'un service de veille). De manière plus radicale, il est envisageable d'imposer la navigation Web pour des populations sensibles depuis des postes séparés du reste du réseau de l'entreprise.
3. [Durcissement des postes] – Des mécanismes de contournement peuvent également être mis en place. Pour Java par exemple, il est possible de configurer le niveau de sécurité sur « high » de manière à n'exécuter les applets non signés qu'après validation manuelle de l'utilisateur. Des mesures similaires peuvent être appliquées sur le plug-in Flash. Il est aussi possible de pousser des plugins comme « NoScript » afin d'interdire l'exécution de code JavaScript, Flash, Java …

Conclusion
La compromission par « Watering Hole » partage les mêmes objectifs que par « **spear-phishing** » et la même méthode d'infection que les attaques par « **Drive-by download** ».
Cette combinaison est ainsi surtout utilisée pour des attaques cherchant à s'introduire au sein d'une organisation, quel que soient les postes compromis.
Avec le temps et grâce aux campagnes de sensibilisations, les utilisateurs et en particulier les populations VIP sont de plus en plus précautionneuses quant à l'ouverture des pièces jointes aux courriels. Les attaques par « Spear-phishing » sont ainsi complétées par des attaques de type « Watering-Hole » qui ne nécessitent aucune action de la part de la victime si ce n'est de visiter ses sites Web habituels…

[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 : http://www.lexsi-leblog.fr/cert/watering-hole-et-cyberc riminalite.html

---

« Vous avez été en contact

avec une personne testée positive au Covid-19 » : Attention aux arnaques sur les smartphones

MÉFIEZ-VOUS ! – La crise sanitaire liée à la pandémie est perçue comme une opportunité par les pirates informatiques qui jouent sur les craintes et les angoisses des citoyens pour les piéger. Attention donc si vous recevez des messages liés au Covid-19 sur votre téléphone.

A l'approche de la levée du confinement, profitant de l'inquiétude qui règne au sein de la population, les pirates informatiques agissent, multipliant fraudes et arnaques sur le web, notamment à travers la pratique de l'hameçonnage (ou « phishing » en anglais), particulièrement lucrative. Pour rappel, cette technique consiste à « piéger » une personne en le poussant à cliquer sur un lien dans le but d'installer un logiciel malveillant sur son appareil ou de collecter ses informations personnelles. …[lire la suite]

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

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

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

Source : *« Vous avez été en contact avec une personne testée positive au Covid-19 » : attention aux arnaques sur les smartphones | LCI*