Achats de Noël et hausse de la cybercriminalité : 4 conseils pour éviter d’être piraté | Denis JACOPINI

La fin d’année arrive à grands pas et les français se sont déjà lancés dans la course aux cadeaux de Noël, notamment en ligne. Et cette frénésie de l’achat ne risque pas de s’atténuer puisqu’à partir du 6 janvier ce sera au tour des soldes d’hiver de prendre le relai. Les périodes d’achats massifs font le bonheur des e-commerçants… et des cybercriminels ! Tour d’horizon des mesures à prendre pour éviter une attaque informatique.

Les mois de décembre et janvier représentent une période de forte activité, les e-commerçants vont voir leurs ventes augmenter et cela ne manquera pas d’attirer les cybercriminels en tout genre. Chaque année à cette période, les tentatives de piratage envers les entreprises mais aussi les particuliers se multiplient.
L’essor du commerce en ligne, et également du commerce sur terminaux mobiles, constitue une aubaine pour les hackeurs. Pour se prémunir de ces attaques, les particuliers peuvent prendre quelques précautions simples mais pourtant essentielles :
1. Veiller à toujours avoir les dernières mises à jour de ses applications, de son système d’exploitation et des logiciels de sécurité.
Des failles sont régulièrement enregistrées par les acteurs du secteur, et les correctifs sont présents dans les mises à jour. Un logiciel non mis à jour risque fortement d’être vulnérable face à des failles pourtant déjà identifiées et corrigées.

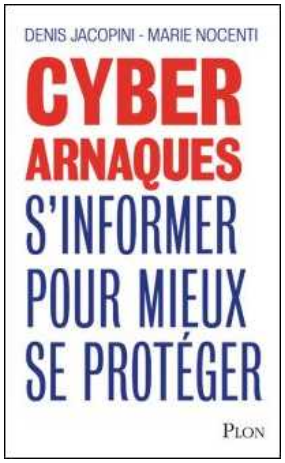
2. S’en tenir aux règles d’or : ignorer ou bloquer les pop-ups ;
utiliser un mot de passe original et sécurisé contenant à la fois des majuscules, des chiffres et des caractères spéciaux, ne pas utiliser les mêmes identifiants sur plusieurs sites car le mot de passe pourrait être compromis ; commander sur des sites fiables et via des connexions sécurisées en https.

3. Eviter de cliquer sur les liens directement depuis un emailing :
le phishing est une technique de cyberattaque à la mode, et elle est particulièrement efficace en période de fin d’année – lorsque des dizaines d’emails propose quotidiennement aux internautes des bons plan pour Noël et pour les soldes. Si l’offre est alléchante, au lieu de cliquer directement sur le lien, mieux vaut effectuer une nouvelle recherche dans son navigateur et s’assurer qu’il s’agit du site réel.

4. Eviter les transactions depuis des réseaux Wi-Fi publics.
La plupart des réseaux publics (gares, cafés, etc) ont un niveau de cryptage faible, et donc une moindre sécurité. Les informations bancaires pourraient atterrir dans les mains d’une tierce personne. Que l’on soit connecté depuis un ordinateur, une tablette, ou un mobile, mieux vaut donc se méfier des réseaux ouverts.

Autre point sensible : les achats via smartphones et tablettes sont de plus en plus communs, mais il est important d’être encore plus vigilent depuis ces terminaux. En effet, ces terminaux font face à de nombreuses menaces et sont souvent moins bien sécurisés que les ordinateurs.
Ici aussi des règles d’or s’appliquent : ne pas télécharger d’applications gratuites de propriétaires inconnus afin d’éviter les trojans, acheter et visualiser les comptes bancaires seulement via des applications propriétaires (celles de sa banque ou celles d’e-commerçants de renom), mais aussi supprimer l’historique de navigation, le cache et les cookies régulièrement afin de supprimer les données sensibles.

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

Mise en conformité RGPD, formations et conférences

Cybercriminalité et en protection des données personnelles, Expertises et Recherche de preuves

Denis JACOPINI est Expert en Cybercriminalité et en Protection des Données à Caractère Personnel.
Notre métier :

Animation de formations et de conférences

Cybercriminalité (virus, espions, piratages, fraudes, arnaques Internet)
Protection des Données à Caractère Personne (mise en conformité avec la CNIL etle RGPD)
Audits sécurité, Expertises techniques et judiciaires

Audit sécurité (ISO 27005) ;
ID Swatting

Recherche de preuves (Investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
Expertises de systèmes de vote électronique ;

Victime d’usurpation d’identité sur facebook,

tweeter ? Portez plainte mais d'après quel article de loi ? | Denis JACOPINI

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

Vous vous retrouvez victime d’usurpation d’identité, quelqu’un s’est fait passer pour vous sur Facebook, twitter, viadeo, linkedin et vous voulez porter plainte. Sur quelle loi s’appuyer ?

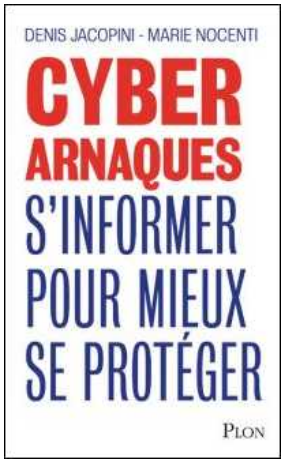
Je ne suis pas avocat, cependant, une fois au commissariat de police ou en brigade de gendarmerie, il se peut que l’officier ne sache pas sur quelle loi et quel article s’appuyer. Sachez que s’il vous décourage de porter plainte sous le motif que c’est inutile dans la mesure ou le responsable de l’acte malveillant ne sera jamais retrouvé, il a tout de même l’obligation d’enregistrer la plainte que vous souhaitez déposer.

Pour vous aider, pour l’aider.
Selon la Loi LOPPSI 2 (LOI n° 2011-267 du 14 mars 2011 d’orientation et de programmation pour la performance de la sécurité intérieure)
Article 226-4-1 du Code de Procédure Pénale : « Le fait d’usurper l’identité d’un tiers ou de faire usage d’une ou plusieurs données de toute nature permettant de l’identifier en vue de troubler sa tranquillité ou celle d’autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d’un an d’emprisonnement et de 15 000 € d’amende.
Cette infraction est punie des mêmes peines lorsqu’elle est commise sur un réseau de communication au public en ligne. »
Voir cet article sur Légifrance :
www.legifrance.gouv.fr/affichCodeArticle.do;?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000023709201

Si par la suite vous souhaitez rechercher ou recueillir des preuves, afin de garantir leur recevabilité, notamment en matière d’intégrité du respect de la preuve, nous pouvons vous aider pour vous accompagner dans toutes ces démarches.
Contactez-vous

[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

Comment supprimer une informations gênante sur

Internet ? | Denis JACOPINI

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

LE NET EXPERT AUDITS & EXPERTISES

EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LE NET EXPERT .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

Comment supprimer une information gênante sur Internet ?

Victime d'usurpation d'identité, d'insultes ou de propos diffamatoires, vous désirez faire disparaître une information compromettante d'Internet ? Il est temps d'agir sur votre e-réputation. Les conseils de Denis JACOPINI, expert informatique assermenté.

1 Où supprimer

Nous pouvons considérer plusieurs niveaux de suppression :
– Au niveau des supports (sites Internet) stockant les informations à supprimer vers lesquels pointent les outils permettant de trouver l'information ;
– Au niveau des outils permettant de trouver les informations ;
– Au niveau des supports ayant une copie des informations à supprimer vers lesquels pourraient pointer les outils permettant de trouver l'information ;
–
Supprimer la totalité des informations ne peut être garanti
En effet, les actions menées sur Internet par les utilisateurs sont Internationales. En 2016, dans le monde, nous comptons un peu plus de 3,3 milliards d'internaute et un peu plus d'un milliard de sites Internet. C'est autant d'utilisateurs susceptibles d'enregistrer une information dans leur ordinateur ou la diffuser sur Internet, sur un blog ou un forum dans le plus grand secret.
A ce jour, les seuls moyens à notre disposition pour trouver de l'information sur Internet sont :
• soit de connaître l'url (Uniform Resource Locator) utilisées pour identifier les pages et les sites web (par exemple : https://www.lenetexpert.fr/contacter-denis-jacopini-expert-judiciaire-en-informatique-correspondant-cnil-cil/)
• soit on passe par des outils permettant de rechercher de l'information (ex : http://www.google.fr et on recherche « Contacter Denis JACOPINI »)
• soit on passe par des outils spécialisés dans la recherche d'information qui vont scruter dans différents type de services Web (annuaires, réseaux sociaux, espaces de partage, de microblogage…)
Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
1.1 Suppression d'informations à une adresse précise
Prendre contact avec le responsable du site Internet ou le propriétaire du compte contenant l'information est la première étape que nous recommandons.
Par exemple, si une information fausse ou compromettante est constatée à l'adresse suivante : https://www.lenetexpert.fr/contacter-denis-jacopini-expert-judiciaire-en-informatique-correspondant-cnil-cil, le plus simple est de contacter la personne en charge du site internet racine soit http://www.lenetexpert.fr en expliquant la raison de notre demande de suppression d'informations
Retrouver la personne responsable du contenu du site Internet peut s'avérer simple (dans le meilleur des cas, le site dispose d'une rubrique « Contact » ou « contactez-nous », ou bien d'une rubrique « Mentions légale » contenant un numéro SIREN, SIRET, l'identité d'un « responsable de la publication »…) ou parfois compliquée (aucune rubrique précédemment citée n'est présente). Il sera alors nécessaire de trouver les coordonnées de la personne en charge de l'hébergement du site internet en question par d'autres moyens en fonctions des informations pouvant être trouvées sur le site Internet ou sur des sites proposant des services de « Whois », répertoriant les informations administratives et techniques relatives au noms de domaines.
Enfin, vous pouvez aussi contacter le responsable d'un site internet en recherchant le nom du site, de la marque ou du service dans des annuaires internet, des moteurs de recherche ou sur des réseaux sociaux ou d'anciennes versions du site internet.
Notez toutefois qu'en France, tous les sites internet édités à titre professionnel ont l'obligation de créer une rubrique « mentions légales » dans laquelle vous pourrez peut-être aussi trouver un numéro SIREN ou SIRET si le site Internet appartient à un professionnel ou une association déclarée à l'INSEE.
Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
1.2 Suppression d'informations dans les outils de recherche
–
Supprimer une information sur un site Internet n'a pas d'action directe et immédiate sur le contenu des annuaires et des moteurs de recherche. Cependant, supprimer une information sur un site Internet peut avoir des actions à posteriori comme c'est le cas pour les moteurs de recherche, tels que Google, qui disposent de Bots (par exemple les robots GoogleBot) qui scrutent le contenu des sites Internet et le contenu derrière leurs liens, à la recherche de toute modification, ajout ou suppression d »informations.
Supprimer une information sur un site Internet peut ainsi avoir pour effet de supprimer l'information dans l'index de recherche du moteur de recherche mais ceci sera sans garantie en terme de réalisation ou de délai.
Cependant, si le préjudice porte sur la présence sur Internet d'une information compromettante, il ne faut pas perdre de vue qu'un internaute lambda recherche sur Internet dans la quasi totalité des cas en passant par un moteur de recherche.
Notez qu'en France, le moteur de recherche Google est utilisé dans plus de 93% des cas et draine chaque mois un plus de 40 millions de recherches, Bing est utilisé dans un peu plus de 4% des cas et Yahoo dans un peu plus de 2% des cas. Cela laisse très peu de place (moins de 1%) aux autres moyens utilisés pour rechercher de l'information sur Internet.
De plus, une étude de Advanced Web Ranking de février 2015 nous informe que sur la première page de google, le premier résultat récoltera 33% des clics, le second résultat 15,6% des clics, le troisième résultat 10% des clics, le 4ème résultat 7% des clics, le 5ème résultat, 6% des clics, les 5 derniers résultats récoltant seulement 4% des clics.
Il est donc facile de remarquer que 75% des consultations seront réalisées sur la 1ère page. Les liens présents sur la seconde page des résultats de Google récolteront 5% des clics.
Ainsi, plus de 80% des recherches ne concernant que les deux premières pages de Google et ces habitudes de consultation étant quasiment similaires sur appareils mobiles et sur d'autres moteurs de recherche,
compte tenu qu'il sera impossible d'agir sur tous les annuaires, tous les moteurs de recherche et tous les sites Internet,
compte tenu que du coup, les prétendants à l'existence numérique concentrent leurs efforts pour être présents sur ces outils de recherche,
compte tenu que ne pas y être présent sur ces outils de recherche revient à ne tout simplement pas avoir d'existence numérique,
alors, concentrer ses efforts pour disparaître des 3 premières pages des 3 principaux moteurs de recherches sur Internet permettra de faire disparaître 98% des informations indésirables.
A la suite d'une plainte déposée en 2010 auprès de l'Agence espagnole de protection des données, dans son Arrêt du 13 mai 2014, la Cour de Justice de l'Union Européenne accorde aux individus le droit de s'opposer au traitement de leurs données personnelles.
À la suite de cette décision, Google a publié un formulaire en ligne le 31 mai 2014 permettant à chaque citoyen européen de demander le déréférencement des liens qui apparaissent dans une recherche associée à leur nom, tout en prenant en compte l'intérêt prépondérant du public à avoir accès à l'information.
Le mercredi 16 juillet 2014, le moteur de recherche Bing a mis à disposition son formulaire de demande de blocage des résultats de recherches sur Bing en Europe et en décembre de cette même année, Yahoo a mis à disposition son formulaire.

Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
–
2 Comment supprimer

2.1 En résumé, pour supprimer une information sur un site Internet à une adresse précise :
A) Aller sur le site Internet et rentrer en contact avec le site Internet ou avec le responsable de la publication
– rubrique « Contact », « Contactez-nous » ou similaire ;
– rubrique « Mentions légales » ou similaire ;
B) Rechercher le représentant légal de l'activité professionnelle associée au site Internet à partir de son numéro SIREN ou SIRET (liste non exhaustive)
– www.infogreffe.fr
– www.societe.com
– www.europages.com
– www.hoovers.com
C) Rechercher la personne en charge de l'hébergement de l'information avec des outils de Whois (liste non exhaustive)
– www.afnic.fr/fr/produits-et-services/services/whois/
– www.gandi.net/whois?lang=fr
– www.whois-raynette.fr/
– http://whois.domaintools.com
D) Rechercher la personne en charge de l'hébergement de l'information sur les réseaux sociaux (liste non exhaustive)
– plus.google.com
– www.facebook.com
– www.twitter.com
– www.linkedin.com
– www.viadeo.com
E) Rechercher la personne en charge de l'hébergement de l'information dans les annuaires et les moteurs de recherche (liste non exhaustive)
– www.google.com
– www.google.fr
– www.bing.com
– www.yahoo.com
– www.yahoo.fr
F) Rechercher d'anciennes versions du site Internet qui pourraient contenir des informations par la suite supprimées
– http://archive.org/web (Wayback machine)
Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
Si l'information à supprimer est personnelle, en France, vous disposiez d'un droit d'accès, de modification ou de suppression à cette information (Article 34 et suivants de la Loi Informatique et Libertés du 6 janvier 1978).
La CNIL met à votre disposition un générateur de courrier (https://www.cnil.fr/modeles/courrier) destiné à vous aider à faire exercer vos droits auprès des responsables de sites Internet.
Exemple de courrier :
Conformément à l'article 40 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, je vous prie de [objet_de_la_demande]
Vous voudrez bien m'adresser copie de l'enregistrement ainsi modifié.
Je vous rappelle que vous disposez d'un délai maximal de deux mois suivant la réception de ce courrier pour répondre à ma demande, conformément à l'article 94 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée.
Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.
Si l'information à supprimer fait l'objet d'une demande de suppression judiciaire, l'Expert informatique désigné pour réaliser cette mission pourra directement contacter le responsable du site internet pour lui communiquer l'ordonnance justifiant son action et demander le retrait pur et simple de l'information.
En cas de difficulté, remontez la au juge en charge du suivi de votre affaire.
Enfin, si vous n'arriver pas à trouver ou à contacter une personne en charge du site Internet contenant l'information à supprimer, vous avez la possibilité de signaler un acte d'injure ou de diffamation sur le site Internet du ministère de l'Intérieur : http://www.internet-signalement.gouv.fr ou saisir une juridiction de proximité (https://www.service-public.fr/particuliers/vosdroits/F1785).

2.2 En résumé, pour supprimer une information dans les 3 moteurs de recherche les plus utilisés en France :
A) Google : Accéder au formulaire de demande de suppression de résultats de recherche au titre de la législation européenne en matière de protection des données :
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr
B) Bing : Accéder au formulaire de de demande de blocage des résultats de recherches sur Bing en Europe
https://www.bing.com/webmaster/tools/eu-privacy-request
C) Yahoo :
https://fr.aide.yahoo.com/kb/search/Demande-de-blocage-de-r%C3%A9sultats-de-recherche-sur-Yahoo-Search–Formulaire-pour-r%C3%A9sidents-europ%C3%A9ens-sln24378.html
D) Une technique appelée le Flooding consiste à produire beaucoup de contenus et de liens pour apparaître dans les premiers résultats et de faire passer le contenu incriminé sur les pages moins consultées.

Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
2.3 Si vous pouvez modifier le contenu des pages Web du site Internet :
A) Supprimez les fichier sou les dossiers contenant l'information
B) Modifiez la ou les pages d'index ou d'accueil en rajoutant dans l'entête « <meta name= »robots » content= »noindex » /> »
C) Par le biais d'un fichier .htaccess vous pouvez aussi rendre privé et protégé par mot de passe l'accès à un dossier
Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
Bien évidemment cette liste de conseils pas exhaustive et n'attend que vos avis et commentaires pour l'enrichir

[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"]

Etude et publication de Denis JACOPINI
LIENS SOURCES
Utilisation des moteurs de recherche en France
http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/
Taux de clic en fonction de la position dans les résultats
http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fonction-des-positions-dans-google/544

Attaques informatiques : comment les repérer ? | Denis JACOPINI

Attaques informatiques : comment les repérer ?

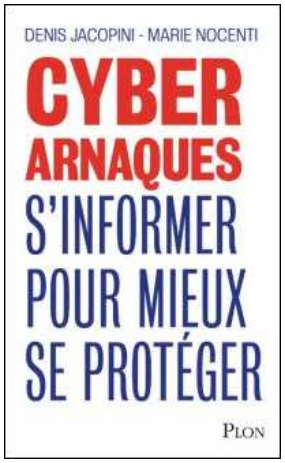
Une entreprise met souvent plusieurs mois avant de s'apercevoir qu'elle est victime d'une attaque informatique. Certains signes doivent néanmoins l'alerter.

Deux cent jours, c'est en moyenne le temps nécessaire à une entreprise pour découvrir qu'elle a été victime d'une attaque informatique. Et encore, à condition qu'elle le découvre. A cela s'ajoute le temps de réparation, qui est presque aussi long. Pourquoi une telle durée ? Parce qu'au fil des années, les attaques se sont sophistiquées et les objectifs des pirates ont évolué.
S'il y a dix ou quinze ans, les hackers voulaient absolument montrer leurs exploits, ils sont aujourd'hui plus discrets. Le but n'est plus de « faire un coup » mais de récupérer des données personnelles, financières ou d'endommager subrepticement un système sans que la victime s'en aperçoive immédiatement.
C'est pourquoi, si certaines attaques peuvent être assez rapidement perceptibles comme les dénis de service (la saturation du système qui devient inopérant), la plupart des menaces restent ignorées des utilisateurs. Ce qui peut être extrêmement dommageable puisque pendant cette période, l'entreprise risque de se faire voler ses secrets industriels et surtout peut donner accès, involontairement, aux systèmes de ses fournisseurs ou de ses donneurs d'ordre : « En général, ce sont des tiers qui détectent les attaques.
Les grands comptes, qui ont les outils pour faire cette surveillance, remarquent des anomalies chez leurs sous-traitants » souligne Jérôme Billois, directeur du pôle Cyber-sécurité chez Solucom.

Mais comment, lorsque l'on est une PME, que l'on n'a pas d'expert en interne, déceler une attaque informatique et la distinguer par exemple d'une panne de machines ou de réseau ?
Pour Gérôme Billois, la première parade est la vigilance. « Il faut sensibiliser les utilisateurs et remonter les comportements anormaux » explique l'expert.
Des anomalies qui peuvent être protéiformes, pas toujours synonymes d'attaques, mais qu'il convient de vérifier : ralentissement soudain du poste de travail ; ordinateur qui doit fréquemment être redémarré ; taux d'activité inhabituel des sites Web avec des accès fréquents aux bases de données… « Il faut être attentif au système d'information, voir si les volumes de données sont cohérents et regarder les destinations », rappelle Gerôme Billois. Autres éléments à surveiller : le nombre et l'activité des comptes autorisés à administrer le système. « Les pirates, parfois, se créent un compte administrateur. Or, s'il y en a plus que le nombre initialement autorisé, cela peut être le signe d'une intrusion. Il faut également regarder les heures où ces comptes ont été actifs, les comptes malveillants agissant plutôt en dehors des heures habituelles de travail. Mais attention, précise Gérôme Billois, si l'on mène une telle surveillance, il faut que cela soit mentionné dans la charte informatique et signalé à la Commission nationale informatique et libertés (Cnil) via une déclaration simplifiée. »
L'entreprise sera également attentive au rapport que lui envoie son anti-virus, car, même si celui-ci n'arrête pas toutes les attaques, il demeure le premier rempart. Il faut vérifier que sur tous les postes, les antivirus sont bien activés, sachant que certains utilisateurs n'hésitent pas à désactiver ces solutions accusées de ralentir les opérations ou d'empêcher le téléchargement de logiciels. Les Smartphones et les tablettes, particulièrement ceux qui fonctionnent sous le système Androïd, peuvent être aussi attaqués. Il existe en effet de nombreuses (fausses) applications dont l'objectif est de récupérer des données ou de faire payer l'utilisateur : « Il faut se méfier quand l'application demande des droits élevés alors qu'elle n'en a pas besoin. Par exemple, une application de bureautique qui va requérir de la géolocalisation. »
Heureusement, les entreprises, même les plus petites, disposent d'une palette d'outils pour se protéger. Outre l'antivirus, elles ont la possibilité d'acquérir des systèmes de détection d'intrusion (IDS) qui écoutent le trafic réseau de manière furtive, afin de repérer des activités anormales ou suspectes. « Elles peuvent également avoir une approche pro-active et souscrire auprès de prestataires spécialisés des services qui vont faire la surveillance interne de leur système d'information », précise Gérôme Billois. Mais la première protection (comme le principal risque) reste l'humain. « Il faut bien gérer le départ des employés, surtout s'ils sont partis en mauvais termes ». Et ne pas oublier de faire régulièrement les mises à jour des logiciels de sécurité et de vérifier, via la solution d'administration de système, que tout fonctionne correctement.

[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.leparisien.fr/economie/business/attaques-informatiques-comment-les-reperer-07-12-2015-5348215.php

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

Attention ! Voici ce que les cyberdélinquants vous réservent

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

Des policiers en formation de lutte contre la cybercriminalité | Le Net Expert Informatique

Des policiers en formation de lutte contre la cybercriminalité

Une session de formation sur la prévention et la lutte contre la cybercriminalité a été lancée dimanche au profit de cadres spécialisés de la Police algérienne à l'Institut national de la police criminelle de Saoula (Alger), indique un communiqué de la Direction générale de la Sûreté nationale (DGSN).

La session de formation « s'inscrit dans le cadre de la mise en oeuvre des démarches du directeur général de la sûreté nationale, le général-major Abdelghani Hamel à travers des sessions de formation technique de haut niveau au profit des cadres de la Sûreté nationale dans le domaine de la lutte contre la criminalité sous toutes ses formes », précise la même source.

Cette session de cinq jours, encadrée par des experts de la police iranienne, porte notamment sur l'échange d'expériences en matière de législations internationales et les meilleures pratiques et techniques de la coopération internationale en la matière en vue de renforcer la lutte contre ce type de criminalité ».

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.lexpressiondz.com/linformation_en_continue/222512-lutte-contre-la-cybercriminalite-des-policiers-en-formation.html

---

Victime d'une fraude sur

votre carte de paiement ? L’état met à votre disposition une nouvelle plateforme : Percev@l

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

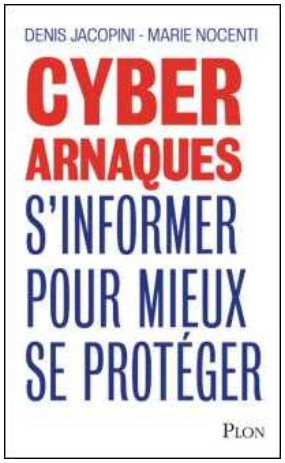
LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES LENETEXPERT.fr | RGPD CYBER LE NET EXPERT MISES EN CONFORMITÉ | SPY DETECTION Services de détection de logiciels espions | LE NET EXPERT FORMATIONS | LE NET EXPERT ARNAQUES & PIRATAGES

Victime d’une fraude sur votre carte de paiement ? L’état met à votre disposition une nouvelle plateforme : Percev@l

Depuis quelques jours, un nouveau téléservice est disponible sur service-public.fr. Il permet aux victimes de fraude à leur carte de paiement de se signaler auprès des autorités.
Un tel service était nécessaire et attendu depuis longtemps. En effet, la fraude aux cartes de paiement a lieu essentiellement sur Internet aujourd'hui (à plus de 70% selon les statistiques publiées par l'Observatoire de la sécurité des moyens de paiement). Cela veut dire que le lieu où se commet réellement l'infraction n'a en général aucun rapport avec l'endroit où se trouve la victime. De surcroît, c'est le cumul des informations provenant des nombreuses victimes qui permettra d'identifier les fraudeurs et leur mode opératoire et facilitera la coopération internationale (plus facile si on peut identifier un préjudice conséquent lié aux mêmes auteurs).
Lorsqu'on constate un paiement frauduleux avec son numéro de carte bancaire (en consultant son relevé de compte en ligne, ou encore en étant prévenu par sa banque ou son prestataire de paiement), les opérations suivantes peuvent maintenant être réalisées par les victimes:
• Mettre sa carte en opposition en contact son organisme de paiement (en général par un simple appel téléphonique)
• Réaliser son signalement sur le téléservice Percev@l (on le retrouve simplement sur le site service-public.fr en cherchant Percev@l ou « fraude carte bancaire »)
• Transmettre le récépissé fourni par Percev@l à sa banque pour faciliter les opérations de remboursement
[lire la suite]

[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 : *Percev@l – plateforme de signalement des fraudes aux cartes de paiement – est ouverte! – Investigation & transformation numériques*

Commet se prémunir du phishing | Denis JACOPINI

Comment se prémunir du phishing

Le phishing, francisé sous le nom de „hameçonnage », est une méthode de fraude qui sévit sur le Web depuis 2005. Cette dernière permet de soutirer des données sensibles en exploitant les failles informatiques pour piéger les internautes.

[popup show= »ALL »]

Un phénomène actuel omniprésent

L'actualité ne cesse d'en rapporter les méfaits :l'attaque de TV5 Monde, la création d'un phishing Google qui ressemble comme deux gouttes d'eau au célèbre moteur de recherche et l'élaboration d'une opération phishing pour s'évader d'une prison sont autant de phénomènes d'actualité qui démontrent que ce genre de fraude est de plus en plus perfectionné. Il est d'ailleurs estimé qu'un Internaute sur 10 se laisserait prendre au piège, c'est ce que révèle un article de Metronews. Afin de contrer ce phénomène,l'association Phishing-Initiative a été créée dans le but de protéger les internautes et de freiner les tentatives de phishing, toujours plus nombreuses.

Comment reconnaître un mail frauduleux ?

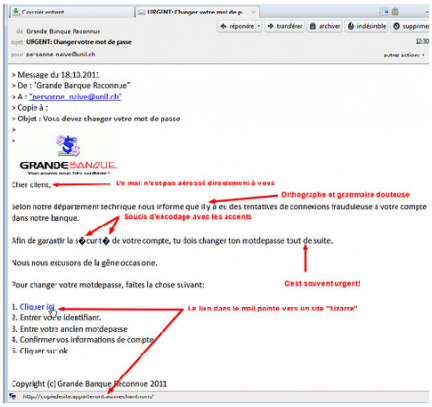
Comment repérer le vrai du faux ? Voici quelques méthodes qui permettent de voir si vous avez à faire à une tentative de phishing par e-mail :

• Votre e-mail semble provenir de votre banque et a l'air d'en être une copie originale, avec son logo et ses couleurs. Commencez par lire le message, si vous trouvez des erreurs d'orthographe ou des erreurs d'affichage, vous saurez qu'il ne s'agit alors que d'une pâle copie.

• Un message vous invite à vous rendre sur une page externe. Méfiance ! Avant de cliquer sur le lien, passez la souris sur le lien sans cliquer dessus. En bas à droite, vous découvrirez une URL « bizarre », qui n'a rien à voir avec l'entreprise.

• Le mail est trop insistant (dans le pire des cas, vous prédit une catastrophe) et vous demande expressément de donner vos codes bancaires et informations personnelles.

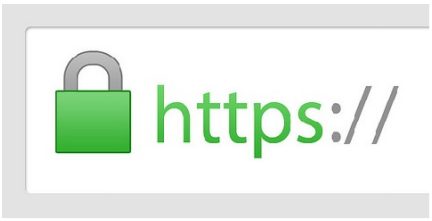
En voici un exemple type :



Flicker – phishing_exemple hameconnage pardownloasource.fr, CC BY 2.0, Certains Droits Réservés

Comment effectuer un paiement en ligne sécurisé ?

• Comment éviter la fraude et payer en toute sécurité quand vous faites vos achats en ligne ? Comment savoir s'il ne s'agit pas d'une tentative de phishing ? Vérifiez toujours lors de votre paiement que le site est sécurisé : l'URL débute par « https» et est accompagnée d'un petit cadenas, de cette façon :



Flickr – https par Sean MacEntee, CC BY 2.0, Certains Droits Réservés Et si vous ne souhaitez pas livrer vos coordonnées bancaires lors d'un achat en ligne, il existe des modes de paiements alternatifs qui ne nécessitent pas vos données bancaires. Pus sûrs, ils ne sont toutefois pas infaillibles :

• PayPal, que l'on ne présente plus, permet de la même manière d'acheter ou de vendre en ligne sans livrer le moindre code bancaire grâce à un compte virtuel qu'il est possible de remplir selon vos besoins. Si des systèmes tels que PayPal sont régulièrement confrontés à des tentatives de phishing (vigilance donc !), le fraudeur ne peut cependant remonter à votre compte en banque, ce qui vous offre une sécurité supplémentaire.

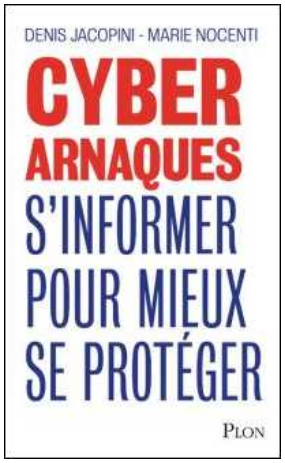
• La carte virtuelle prépayée autorise un paiement en ligne sécurisé puisqu'en aucun cas vous ne livrez vos coordonnées bancaires sur Internet. Pour comprendre comment cela fonctionne, vous pouvez vous fier aux instructions de Paysafecard.

• Concernant le m-paiement, soit le paiement par mobile, Apple Pay utilise les concepts de jetons de paiement et l'identification biométrique pour une protection optimale. Mais, malgré la technologie développée par Apple, des hackers ont réussi à mener une vaste fraude bancaire en volant des données bancaires et en les installant sur de nouveaux Iphone.

Quel que soit votre moyen de paiement en ligne, restez vigilants !

[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 : https://www.globalsecuritymag.fr/Cybercriminalite-se-premunir-du,20150429,52544.html

Céder au chantage finance et renforce l’infrastructure des attaques DDoS | Denis JACOPINI

La cybercriminalité peut prendre plusieurs formes (attaques DDOS, arnaques, spam…), les pirates peuvent avoir plusieurs motivations (idéologie, vengeance, argent…) mais la technique qui aura le mieux fonctionné en 2015 et qui devra encore battre des records en 2016, c'est l'attaque par cryptolockers.

Je prends la peine d'écrire cet article car ces formes d'attaques feront dans les prochains mois, toujours partie non seulement des techniques les plus simples pour les pirates (2 milliards d'e-mails sont envoyés dans le monde chaque seconde dont la très grande majorité par des serveurs piratés), des plus rentables (même si seulement 0,01% des personne se font infectées, je vous laisse calculer ou imaginer le nombre colossal de victime chaque jour), et des moins risqués (en raison des technonologies d'anonymisation facilement accessibles).

Qu'est-ce que les crypto lockers

Ce sont des programmes malveillants qui peuvent se cacher dans des pièces jointes de mails ouqui peuvent s'attraper en consultant des pages WEB infectées (des mails peuvent aussi transporter des pages WEB).
A l'ouverture des informations piégées, ces programmes malveillants se lancent automatiquement et commencent à crypter (coder les informations dans un code incompréhensible par l'humain), avec un code qui peut parfois être inconnu par les pirates eux-même, la totalité des informations de vos disques durs (internes, amovibles, externes, réseaux…) et vous affichent, vers la fin de son travail, un message vous demandant de passe à la caisse.
Un règlement en bitcoins (monnaie virtuelle et anonye de rigueur) vous sera demandé en échange du code permettant de décrypter vos données.
Si vous ne payez pas, vous êtes sur que vos données ne seront pas décryptées; si vous payez, vous avez peut-être une chance de recevoir en échange de votre obole (quelques centaines d'euros) le code permettant de retrouver vos données comme avant.

Ces logiciels sont aussi appelés des rançongiciels ou des ransomwares (logiciel à rançon en français)

Comment s'en protéger

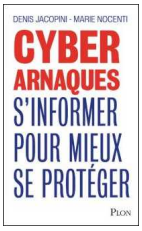
• Avoir des sauvegardes dignes de ce nom (automatisées, externalisées, historisées, contrôlées…) au cas ou vou svous faîtes infecter ;
• Avoir une suite de sécurité capable de de bloquer les logiciels malveillants, les mails infectés ou les sites malveillants ;
• Redoubler de vigilance, surtout sur les sites proposant gratuitement des choses payantes (multimédia mais aussi pornographique).

Une solution que nous recommandons depuis plusieurs années :

Et si c'est trop tard

• Profiter enfin des sauvegardes que vous avez réalisées contraint et forcé sans vraiment croire qu'un jour vous en aurez besoin ;
• Vous tourner vers un professionnel ou un service ayant l'outil de décryptage de vos données
• Payer en espérant :
• 1 : que vos données seront bien décryptées après paiemetn de la rançon;
• 2 : qu'un seul logiciel malveillant ait crypté vos données (et qu'il n'y ait pas un logiciel qui vous a crypté des données déjà cryptées)
• 3 : qu'aucun autre logiciel malveillant viendra vous refaire la même chose dans quelques jours car même si vous payez, rien ne vous garanti que, sans avoir activé des protections efficaces, vous ne vous rafassiez pas infectree.
[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 Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.
Commandez sur Fnac.fr

---

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