Denis JACOPINI est Expert de Justice en informatique spécialisé en Cybercriminalité et en RGPD (protection des Données à Caractère Personnel).

Diplômé en Cybercriminalité, en Droit de l'Expertise Judiciaire et Certifié en Gestion des Risques des Systèmes d' Information (ISO 27005), il est également formateur depuis 1998 et consultant depuis 1996 dans le domaine de la sécurité informatique et a 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 dans la sécurité informatique, Expert de Justice en Informatique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, il est praticien de la mise en conformité en matière de sécurité informatique et RGPD.

« Mon objectif est de mettre à votre disposition mon expérience et mes connaissances acquise lors de diplômes, certifications, formations et veille permanente. »

CONFIDENTIEL

Interventions réalisées en France et étranger pour :

- Adecco Groupe France (Vote électronique) ;
- Banque Populaire Caisse d'Épargne Mutuelle Vote électronique) ;
- Addecco Training (Vote électronique) ;
- Etablissement Français du Sang (Vote électronique) ;
- Adecco Réunion (Vote électronique) ;
- Engie IT (Vote électronique) ;
- Adecco Antilles Guyanne (Vote électronique) ;
- Conseil Départemental du Haut-Rhin (Vote électronique) ;
- CoE (Conseil de l'Europe) ;
- CSOEC (Conseil Supérieur de l'Ordre des Experts Comptables) (Vote électronique) ;
- IFAR (Institut de Formation des Agent de Recherche) ;
- Master 2 Spécialité Lutte contre la Criminalité Financière et Organisée ;
- CNFPT (Centre National de la Fonction Publique Territoriale) ;
- CERI (Centre d'Enseignement et de Recherche en Informatique) ;
- CNIL du Bénin ;
- CNIl du Burkina Fasso ;
- CEJCARIOM (Compagnie d'Experts Judiciaires près la Cour d'appel de RIOM) ;
- CEJCANIMES (Compagnie d'Experts Judiciaires près la Cour d'appel de Nîmes) ;
- AFDIT (Association Française de Droit de l'Informatique et de la Télécommunication) ;
- EFACS (Ecole de Formation des Avocats Centre Sud) ;
- EDA (Ecole des Avocats) ;
- EBBS Business School Bordeaux ;
- SCIENCES-U ;
- Différents centres de Formation : (PLB Formation, M2i, CG).

PUBLICATIONS DE Denis JACOPINI

ANIMATION D'UN BLOG DEPUIS MARS 2014 :
http://www.lenetexpert.fr

CRÉATEUR DES FORMATIONS :

« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

« Je veux devenir Délégué à la Protection des Données »

« Je mets en conformité mon établissement »

« Arnaques sur Internet à connaître »

« Victime d'un ransomware, quelle attitude adopter pour mettre toutes les chances de son coté ? »

« Victime d'un prélèvement frauduleux sur votre compte bancaire, que faire ? »

« Virus, arnaques et piratages informatiques, risques et solutions pour nos entreprises »

« Tous ciblés par les cybercriminels - Comment se protéger des pirates du Web ? »

« La cybercriminalité, un vrai risque pour les entreprises »

« Les professionnels de santé face aux Pirates Informatiques »

« Mettre son établissement en conformité avec la CNIL, mode d'emploi »

« Est-ce que votre site Internet est en règle avec la CNIL ? »

PUBLICATIONS ET TRAVAUX :

CYBERARNAQUES S'INFORMER POUR MIEUX SE PROTEGER
mars 2018 Plon ISBN 2259264220

Et si le RGPD était une opportunité pour les Avocats ?
Conseil National des Barreaux

Le RGPD, une révolution dans la protection des données ?
Le Quotidien du Pharmacien

Les enfants face aux dangers des réseaux sociaux
Publication en cours de rédaction

atlantico

Décryptages

PROTECTION TROP FAIBLE

Ces applis qui pillent vos données personnelles sans vous le dire en abusant de votre consentement

Expedia, Hollister, Air Canada... sont autant d'applications disponibles sur iPhone et qui enregistreraient l'activité des utilisateurs sans leur permission. Ces données sont renvoyées aux développeurs pour " améliorer leurs services"

Denis Jacopini

Atlantico : Clics, données de saisie, changement de pages. Ces données ne seraient pas suffisamment masquées selon une enquête de TechCrunch. Elles permettraient de reproduire l'activité des utilisateurs. Concrètement quel est l'intérêt pour les entreprises outre l'optimisation des services ?

Denis Jacopini : On ne veut pas forcément imaginer qu'elles font ça pour revendre nos données puisque la plupart confirment le contraire. Par contre, une chose certaine, c'est que l'exploitation de ces données par leurs services permet d'en savoir plus sur nos comportements et là nous pouvons devenir des cibles qualifiés pour des partenaires qui ne vont pas forcément disposer de données personnelles (mails, contacts...) mais par contre ils auront nos choix et il suffira qu'ils entrent en contact avec un partenaire intéressé par certains profils pour qu'ils puissent directement vous contacter pour le compte de ces partenaires.

Ces pratiques sont-elles admises en Europe malgré le RGPD, les utilisateurs n'ayant pas donné leur consentement explicite ?

A partir du moment où ce ne sont pas des données à caractère personnel qui sont partagées, la RGPD ne s'applique pas. Si ce sont des clics, des consultations, des choix d'achat de commande, d'intérêt, cela ne concerne pas les données à caractère personnel. Dans le cadre du RGPD, il faut voir les termes convenus avec l'utilisateur et les finalités qui ont été convenues. En général, lorsque l'utilisateur donne ses informations, on a eu son accord auparavant. A partir du moment où il y a accord, y compris sur des données sensibles, de manière volontaire, transparente, avec une connaissance des

Ces applis qui pillent vos données personnelles sans vous le dire en abusant de votre consentement
L'article complet sur :
https://www.atlantico.fr/decryptage/3565655/ces-applis-qui-pillent-vos-donnees-personnelles-sans-vous-le-dire-en-abusant-de-votre-consentement-denis-jacopini

ARNAQUES

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

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.

Denis Jacopini

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 ?

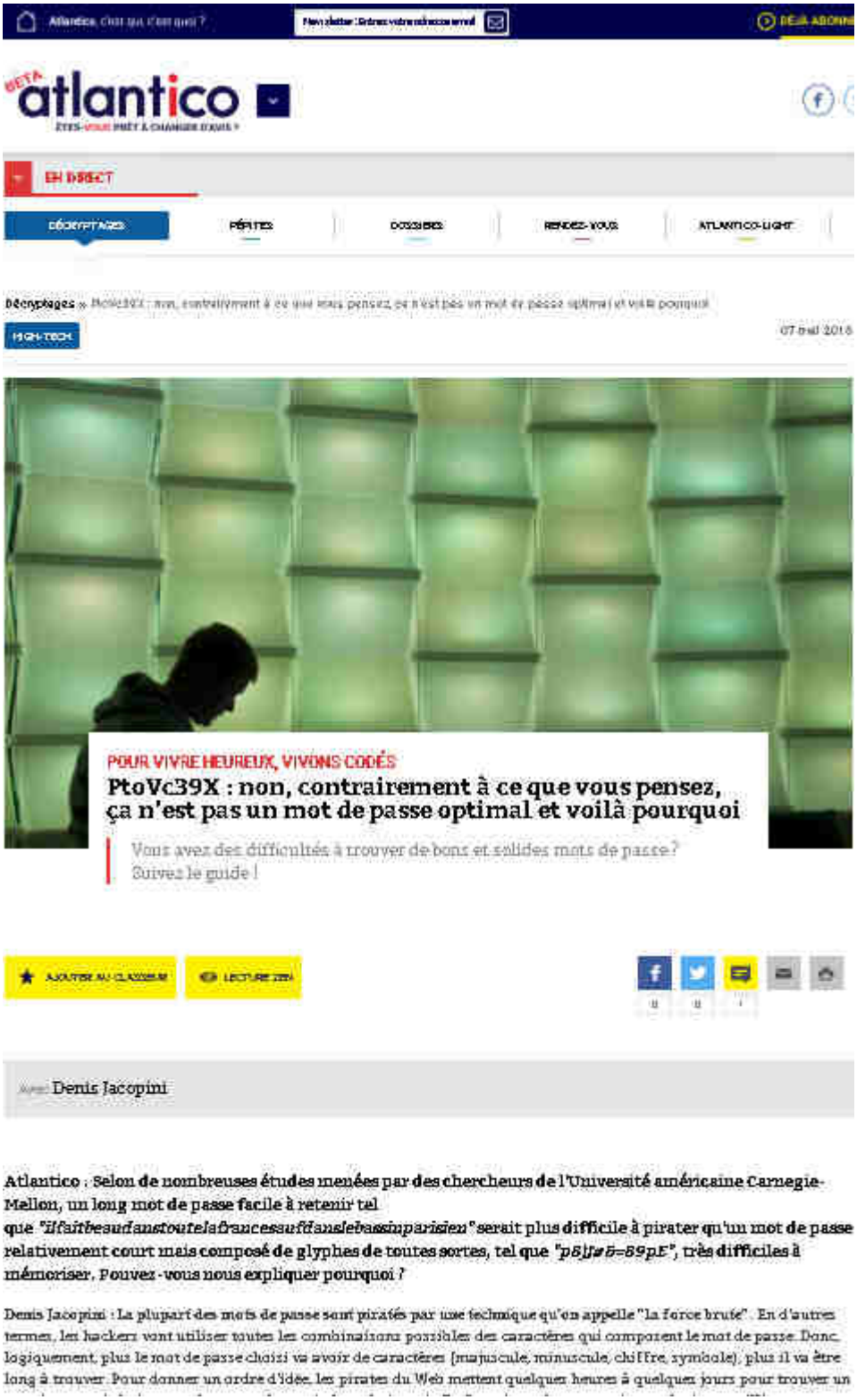
Denis Jacopini : Cette technique de fraude utilise de nouveaux ingrédients de base :

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 :

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

L'article complet sur :
http://www.atlantico.fr/decryptage/fraudes-au-paiement-autorisation-dans-lesquelles-on-fait-dire-ok-telephone-denis-jacopini-3401993.html



POUR VIVRE HEUREUX, VIVONS CODÉS

PtoVc39X : non, contrairement à ce que vous pensez, ça n'est pas un mot de passe optimal et voilà pourquoi

Vous avez des difficultés à trouver de bons et solides mots de passe ? Suivez le guide !

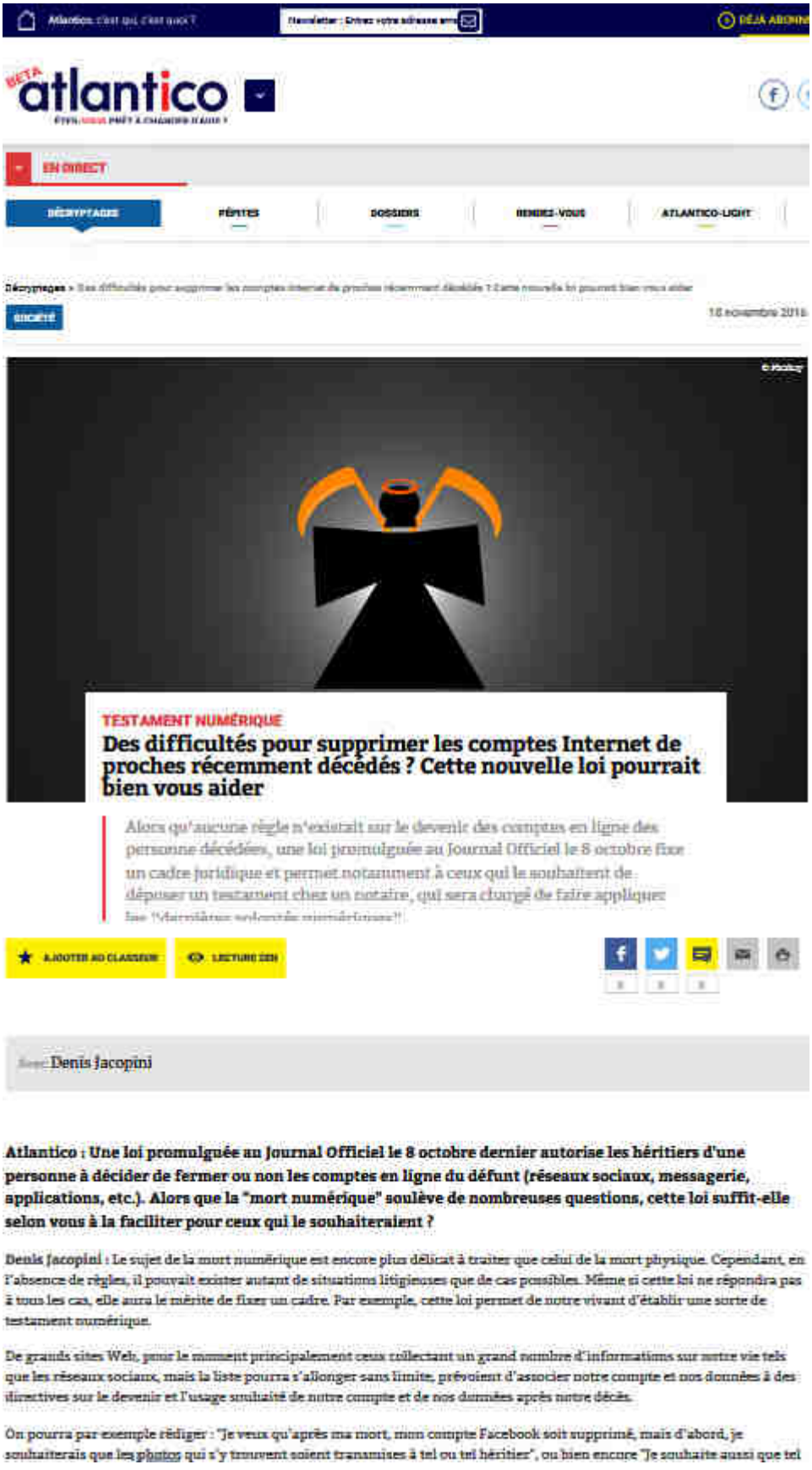
Denis Jacopini

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que *"il faitbeaudanstoutelafrancesaufdanslebassinparisien"* serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que *"p8lJ*5=89pE"*, très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle "la force brute". En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe. Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un

PtoVc39X : non, contrairement à ce que vous pensez, ça n'est pas un mot de passe optimal et voilà pourquoi

L'article complet sur :
http://www.atlantico.fr/decryptage/ptovc39x-non-contrairement-que-pensez-est-pas-mot-passe-optimal-et-voila-pourquoi-3385250.html



TESTAMENT NUMÉRIQUE

Des difficultés pour supprimer les comptes Internet de proches récemment décédés ? Cette nouvelle loi pourrait bien vous aider

Alors qu'aucune règle n'existait sur le devenir des comptes en ligne des personne décédées, une loi promulguée au Journal Officiel le 8 octobre fixe un cadre juridique et permet notamment à ceux qui le souhaitent de déposer un testament chez un notaire, qui sera chargé de faire appliquer

Denis Jacopini

Atlantico : Une loi promulguée au Journal Officiel le 8 octobre dernier autorise les héritiers d'une personne à décider de fermer ou non les comptes en ligne du défunt (réseaux sociaux, messagerie, applications, etc.). Alors que la "mort numérique" soulève de nombreuses questions, cette loi suffit-elle selon vous à la faciliter pour ceux qui le souhaiteraient ?

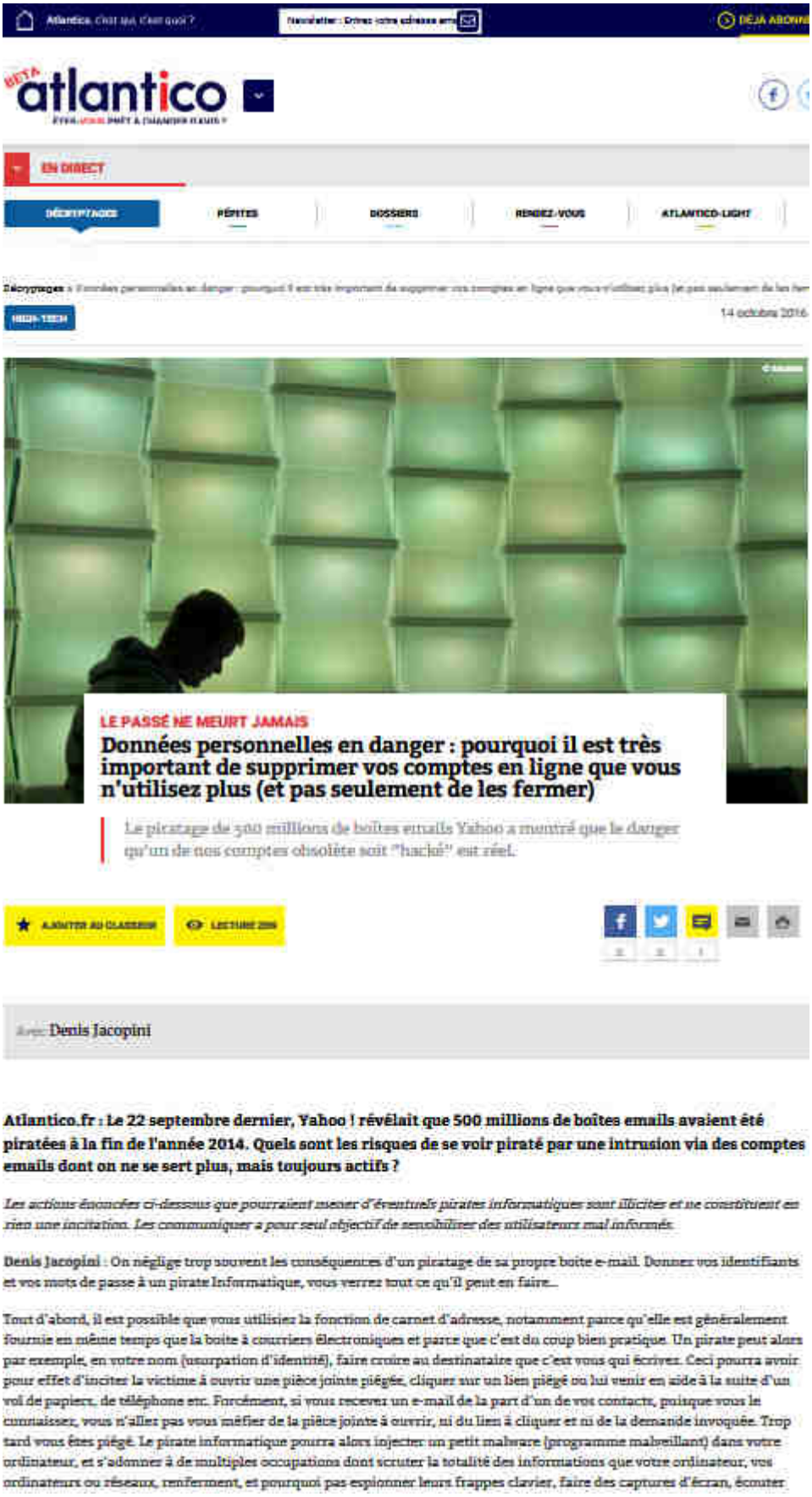
Denis Jacopini : Le sujet de la mort numérique est encore plus délicat à traiter que celui de la mort physique. Cependant, en l'absence de règles, il pouvait exister autant de situations litigieuses que de cas possibles. Même si cette loi ne répondra pas à tous les cas, elle aura le mérite de fixer un cadre. Par exemple, cette loi permet de notre vivant d'établir une sorte de testament numérique.

De grands sites Web, pour le moment principalement ceux collectant un grand nombre d'informations sur notre vie tels que les réseaux sociaux, mais la liste pourra s'allonger sans limite, prévoient d'associer notre compte et nos données à des directives sur le devenir et l'usage souhaité de notre compte et de nos données après notre décès.

On pourra par exemple rédiger : "Je veux qu'après ma mort, mon compte Facebook soit supprimé, mais d'abord, je souhaiterais que les photos qui s'y trouvent soient transmises à tel ou tel héritier", ou bien encore "Je souhaite aussi que tel

Des difficultés pour supprimer les comptes Internet de proches récemment décédés ? Cette nouvelle loi pourrait bien vous aider

L'article complet sur :
http://www.atlantico.fr/decryptage/difficultes-pour-supprimer-comptes-internet-proches-recemment-decedes-cette-nouvelle-loi-pourrait-bien-aider-denis-jacopini-2879559.html



atlantico

EN DIRECT

DÉCRYPTAGES | PÉPITES | DOSSIERS | RENDEZ-VOUS | ATLANTICO-LIGHT

Décryptages

14 octobre 2016

HIGH-TECH

LE PASSÉ NE MEURT JAMAIS

Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n'utilisez plus (et pas seulement de les fermer)

Le piratage de 500 millions de boîtes email Yahoo a montré que le danger qu'un de nos comptes obsolète soit "hacké" est réel.

AJOUTER AU CLASSEUR | LECTURE 20H

Avec Denis Jacopini

Atlantico.fr : Le 22 septembre dernier, Yahoo ! révélait que 500 millions de boîtes emails avaient été piratées à la fin de l'année 2014. Quels sont les risques de se voir piraté par une intrusion via des comptes emails dont on ne se sert plus, mais toujours actifs ?

Les actions énoncées ci-dessous que pourraient mener d'éventuels pirates informatiques sont illicites et ne constituent en rien une incitation. Les communiquer a pour seul objectif de sensibiliser des utilisateurs mal informés.

Denis Jacopini : On néglige trop souvent les conséquences d'un piratage de sa propre boite e-mail. Donnez vos identifiants et vos mots de passe à un pirate Informatique, vous verrez tout ce qu'il peut en faire...

Tout d'abord, il est possible que vous utilisiez la fonction de carnet d'adresse, notamment parce qu'elle est généralement fournie en même temps que la boite à courriers électroniques et parce que c'est du coup bien pratique. Un pirate peut alors par exemple, en votre nom (usurpation d'identité), faire croire au destinataire que c'est vous qui écrivez. Ceci pourra avoir pour effet d'inciter la victime à ouvrir une pièce jointe piégée, cliquer sur un lien piégé ou lui venir en aide à la suite d'un vol de papiers, de téléphone etc. Forcément, si vous recevez un e-mail de la part d'un de vos contacts, puisque vous le connaissez, vous n'allez pas vous méfier de la pièce jointe à ouvrir, ni du lien à cliquer et ni de la demande invoquée. Trop tard vous êtes piégé. Le pirate informatique pourra alors injecter un petit malware (programme malveillant) dans votre ordinateur, et s'adonner à de multiples occupations dont scruter la totalité des informations que votre ordinateur, vos ordinateurs ou réseaux, renferment, et pourquoi pas espionner leurs frappes clavier, faire des captures d'écran, écouter

Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n'utilisez plus (et pas seulement de les fermer)

L'article complet sur :
http://www.atlantico.fr/decryptage/donnees-personnelles-en-danger-pourquoi-est-tres-important-supprimer-vos-comptes-en-ligne-que-utilisez-plus-et-pas-seulement-2836897.html

Atlantico : Selon une enquête de la FAU (*University of Erlangen-Nuremberg*), près de la moitié des internautes cliqueraient sur des liens d'expéditeurs inconnus (environ 56% d'utilisateurs de boîte mail et 40% d'utilisateurs de Facebook), tout en étant parfaitement conscients des risques de virus ou d'autres infections. Pourquoi donc, selon vous, le font-ils malgré tout ? Qu'est-ce qui rend un mail d'un inconnu si attirant, quitte à nous faire baisser notre garde ?

Denis Jacopini : Cela vous est très probablement déjà arrivé de recevoir un e-mail provenant d'un expéditeur anonyme ou inconnu. Avez-vous résisté à cliquer pour en savoir plus ? Quels dangers se cachent derrière ces sollicitations inhabituelles ? Comment les pirates informatiques peuvent-ils se servir de nos comportements incontrôlables ?

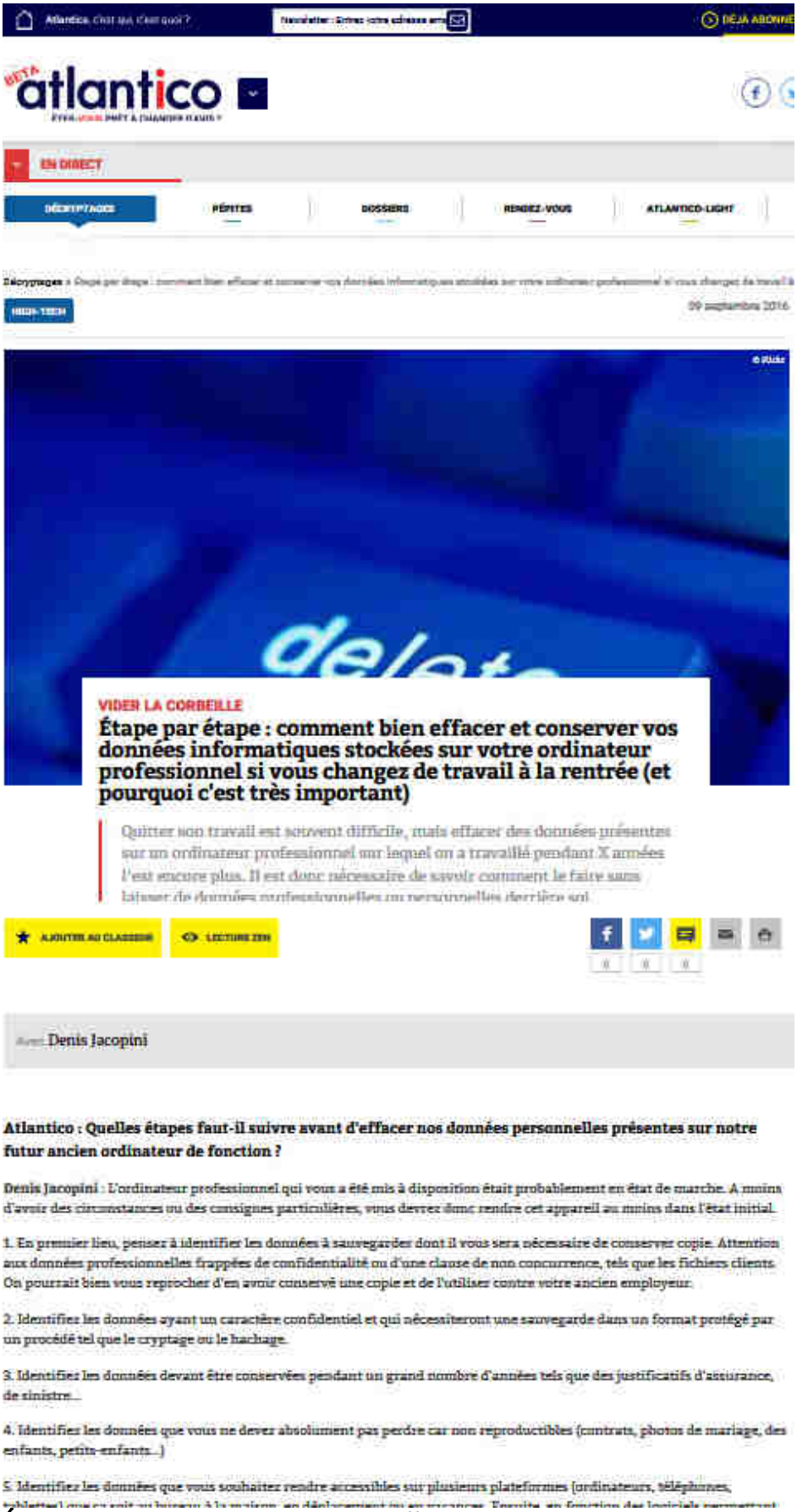
Aujourd'hui encore, on peut comparer le courrier électronique au courrier postal.

Cependant, si l'utilisation du courrier postal est en constante diminution (-22% entre 2009 et 2014), l'usage des messages électroniques par logiciel de messagerie ou par messagerie instantanée a lui par contre largement augmenté.

Parmi les messages reçus, il y a très probablement des réponses attendues, des informations souhaitées, des messages de personnes ou d'organismes connus nous envoyant une information ou souhaitant de nos nouvelles, et quelques autres messages que nous recevons avec plaisir de personnes connues, et puis il y a tout le reste : les messages non attendus, non

Le phishing, cette redoutable technique qui nous pousse à cliquer sur des mails inconnus alors même qu'on est bien conscient des risques

L'article complet sur :
http://www.atlantico.fr/decryptage/phishing-cette-redoutable-technique-qui-pousse-cliquer-mails-inconnus-alors-meme-qu-on-est-bien-conscient-risques-denis-jacopini-2817278.html



VIDER LA CORBEILLE

Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important)

Quitter son travail est souvent difficile, mais effacer des données présentes sur un ordinateur professionnel sur lequel on a travaillé pendant X années l'est encore plus. Il est donc nécessaire de savoir comment le faire sans laisser de données confidentielles ou personnelles derrière soi.

Avec Denis Jacopini

Atlantico : Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction ?

Denis Jacopini : L'ordinateur professionnel qui vous a été mis à disposition était probablement en état de marche. A moins d'avoir des circonstances ou des consignes particulières, vous devrez donc rendre cet appareil au moins dans l'état initial.

1. En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tels que les fichiers clients. On pourrait bien vous reprocher d'en avoir conservé une copie et de l'utiliser contre votre ancien employeur.

2. Identifiez les données ayant un caractère confidentiel et qui nécessiteront une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hachage.

3. Identifiez les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre...

4. Identifiez les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits-enfants...)

5. Identifiez les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones,

Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important)

L'article complet sur :
http://www.atlantico.fr/decryptage/etape-etape-comment-bien-effacer-et-conserver-vos-donnees-informatiques-stockees-votre-ordinateur-professionnel-changez-travail-2808429.html

Piratage informatique : bien plus sûre que le "mot de passe", la "phrase de passe" (à condition que...)
http://www.atlantico.fr/decryptage/piratage-informatique-bien-plus-sure-que-mot-passe-phrase-passe-condition-que-denis-jacopini-2806246.html

l'Expert Informatique obligatoire pour valider les systèmes de vote électronique
http://www.lenetexpert.fr/expert-informatique-obligatoire-systeme-vote-electronique

3 points à retenir pour vos élections par Vote électronique
https://www.lenetexpert.fr/3-points-a-retenir-pour-vos-elections-par-vote-electronique

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
https://www.lenetexpert.fr/organisation-des-elections-professionnelles-des-nouveautes-editions-tissot/
Les dangers des jouets connectés
https://www.lenetexpert.fr/les-dangers-des-jouets-connectes-denis-jacopini

Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n'utilisez plus ?
https://www.lenetexpert.fr/donnees-personnelles-en-danger-pourquoi-il-est-tres-important-de-supprimer-vos-comptes-en-ligne-que-vous-nutilisez-plus

Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d'expéditeurs inconnus ?
https://www.lenetexpert.fr/pourquoi-malgre-le-danger-connu-cliquons-nous-sur-des-e-mails-dexpediteurs-inconnus

Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?
https://www.lenetexpert.fr/quoi-et-comment-supprimer-vos-donnees-si-vous-rendez-votre-ordinateur-professionnel-a-votre-employeur

Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur
https://www.lenetexpert.fr/etapes-a-suivre-si-vous-comptez-rendre-votre-ordinateur-professionnel-a-votre-employeur

Bien plus sûre que le "mot de passe", la "phrase de passe
https://www.lenetexpert.fr/piratage-informatique-bien-plus-sure-que-le-mot-de-passe-la-phrase-de-passe-a-condition-que-denis-jacopini

Votre responsabilité engagée en cas de piratage de vos données
https://www.lenetexpert.fr/votre-responsabilite-engagee-en-cas-de-piratage-de-vos-donnees

Mise en place d'un système de vote électronique, quelques conseils
http://www.lenetexpert.fr/mise-en-place-dun-systeme-de-vote-electronique-quelques-conseils

10 techniques de cybercriminels pour vous pirater votre carte bancaire
http://www.lenetexpert.fr/10-techniques-de-cybercriminels-pour-vous-pirater-votre-carte-bancaire

Contacter Interpol en cas d'arnaque … est une arnaque
http://www.lenetexpert.fr/contater-interpol-en-cas-darnaque-est-une-arnaque

Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité
http://www.lenetexpert.fr/des-solutions-pour-la-sensibilisation-et-formation-des-salaries-face-a-la-cybercriminalite-le-net-expert-informatique

Arnaques par mail (scam, phishing) : quelles précautions prendre ?
http://www.lenetexpert.fr/arnaques-par-mail-scam-phishing-quelles-precautions-prendre-le-net-expert-informatique

Utilisation juridique des documents numériques . Peuvent-ils constituer une preuve ?
http://www.lenetexpert.fr/utilisation-juridique-documents-numeriques-peuvent-constituer-preuve

La Méthode EBIOS désormais adaptée aux traitements de données à caractère personnel et à la CNIL
http://www.lenetexpert.fr/la-methode-ebios-desormais-adaptee-aux-traitements-donnees-caractere-personnel-cnil

La cybercriminalité, un vrai risque pour les chefs d'entreprises
http://www.lenetexpert.fr/la-cybercriminalite-un-vrai-risque-pour-les-chefs-dentreprises

Le Crowdfunding, risques, pièges et précautions à prendre
http://www.lenetexpert.fr/crowdfunding-risques-pieges-precautions-prendre

Attaque informatique TV5 Monde -Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8
http://www.lenetexpert.fr/attaque-informatique-tv5-monde-denis-jacopini-interviewe-par-canal-plus-pour-le-jt-de-direct8-le-net-expert-informatique

Procédure à suivre pour demander l'aide juridictionnelle
http://www.lenetexpert.fr/procedure-a-suivre-pour-demander-l-aide-juridictionnelle

Comment vérifier si votre site Internet a été victime d'un Hackeur
http://www.lenetexpert.fr/comment-verifier-si-votre-site-internet-a-ete-victime-dun-hackeur

Utilisation des données personnelles dans le cas de la prospection Téléphonique – Rappel des règles
http://www.lenetexpert.fr/utilisation-des-donnees-personnelles-dans-le-cas-de-la-prospection-e-mailing-rappel-des-regles-copie

Mise en place d'un système de vidéosurveillance – Rappel des règles
http://www.lenetexpert.fr/mise-en-place-dun-systeme-de-videosurveillance-rappel-des-regles

Emailing – Rappel des règles d'utilisation des données personnelles dans le cas de la prospection
http://www.lenetexpert.fr/emailing-rappel-regles-dutilisation-donnees-personnelles-cas-prospection

Les obligations des Associations vis à vis de la CNIL
http://www.lenetexpert.fr/les-obligations-des-associations-vis-a-vis-de-la-cnil

Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité
http://www.lenetexpert.fr/nouvelles-formations-en-cybercriminalite-et-en-declarations-a-la-cnil-le-net-expert-informatique

Usurpation d'identité, propos diffamatoires, concurrence déloyale, atteintes à votre E-réputation – Nous pouvons vous aider
http://www.lenetexpert.fr/usurpation-didentite-propos-diffamatoires-concurence-deloyale-atteintes-a-votre-e-reputation-nous-pouvons-vous-aider

Vote électronique – Mode d'emploi
http://www.lenetexpert.fr/vote-electronique-mode-demploi

Comment bien sécuriser ses e-mails ? | Le Net Expert Informatique
http://www.lenetexpert.fr/comment-bien-securiser-ses-e-mails-le-net-expert-informatique

Denis JACOPINI interviewé par une journaliste de Ouest France
http://www.lenetexpert.fr/denis-jacopini-interviewe-par-une-journaliste-de-ouest-france-le-net-expert-informatique-replay

Quelles sont les mentions obligatoires sur un site internet ?
http://www.lenetexpert.fr/quelles-sont-les-mentions-obligatoires-sur-un-site-internet-le-net-expert-informatique

Victime d'un prélèvement frauduleux sur votre compte bancaire ? Que faire ?
http://www.lenetexpert.fr/victime-dun-prelevement-frauduleux-sur-votre-compte-bancaire-le-net-expert-informatique

Se mettre en conformité avec la CNIL – Oui mais comment ?
http://www.lenetexpert.fr/se-mettre-en-conformite-cnil-comment

Info pratique : Attitude à adopter en cas de réception d'un e-mail étrange voire douteux

http://www.lenetexpert.fr/info-pratique-attitude-adopter-en-cas-reception-dun-e-mail-etrange-voire-douteux

Protection des données personnelles : Les entreprises ne respectent pas la Loi et jouent avec les données de leur clients. Ca pourrait bien leur coûter cher !
http://www.lenetexpert.fr/les-entreprises-respectent-pas-loi-jouent-les-donnees-contacts-ca-bien-couter-cher

La cybercriminalité, un vrai risque pour les administrations
http://www.lenetexpert.fr/la-cybercriminalite-un-vrai-risque-pour-les-administrations

12/12/2018 sur RTL
Denis JACOPINI sur la grande radio Nationale Française RTL dans l'émission de Julien Courbet « Ça peut vous arriver » vous donne quelques conseils pour détecter les arnaques sur Internet

20 juin 2018 JT TF1
20/06/2018 – Un rapport officiel publié le 20 juin par le ministère de l'Intérieur montre l'augmentation considérable du nombre de cyberattaques. TF1 a demandé l'avis de Denis JACOPINI.

12 avril 2018 sur C8 avec Valérie BENAÏM - Présentation de son livre CYBERARNAQUES
https://www.youtube.com/watch?v=lDw3kI7ra2s

"atlantico
UN VENT NOUVEAU SUR L'INFO

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

PtoVc39X : non, contrairement à ce que vous pensez, ça n'est pas un mot de passe optimal et voilà pourquoi (07 mai 2018)

Des difficultés pour supprimer les comptes Internet de proches récemment décédés ? Cette nouvelle loi pourrait bien vous aider (15 novembre 2016)

Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n'utilisez plus (et pas seulement de les fermer) (04 octobre 2016)

Le phishing, cette redoutable technique qui nous pousse à cliquer sur des mails inconnus alors même qu'on est bien conscient des risques (19 septembre 2016)

Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) (6 septembre 2016)

[Piratage informatique : bien plus sûre que le "mot de passe", la "phrase de passe" (à condition que...) (31 août 2016)]

Un nouveau règlement européen

Le RGPD, une révolution dans la protection des données ?

Le RGPD risque fort de bouleverser les pratiques en matière d'exploitation de données

Sur le papier, le nouveau règlement européen relatif à la protection des données personnelles n'est que le prolongement de la loi informatique et libertés dont il s'est inspiré. Mais les sanctions prévues seront beaucoup plus lourdes et la notion de coresponsabilité des acteurs responsables de la sécurité des données qu'il introduit risque fort de modifier leurs relations contractuelles.

● Le 25 mai prochain, entre en application le Règlement européen sur la protection des données personnelles, le déjà fameux RGPD.

Ce règlement, qui date du 27 avril 2016, a pour but de donner à l'ensemble des citoyens de l'Union européenne le contrôle de leurs données personnelles et de responsabiliser l'ensemble des acteurs traitant ces données. Cela concerne donc à peu près tout le monde. D'où l'effervescence récente qui entoure l'application prochaine du RGPD, dont on estime qu'il va impacter de façon importante l'écosystème des professionnels. Et plus particulièrement tous ceux qui traitent des données sensibles dont font partie les données de santé.

Une effervescence que d'aucuns jugent tardive, les entreprises ont eu deux ans pour se préparer car le RGPD promulgué en avril 2016 n'a pas bougé dans sa substance depuis. Et plus encore, pour les entreprises françaises soumises à la loi informatique et libertés, vieille d'une quarantaine d'années, dont le RGPD s'inspire très largement. C'est en tout cas la position de Denis Jacopini, expert informatique assermenté spécialisé RGPD. « *Il n'y a pas de changements fondamentaux par rapport à cette loi* », estime-t-il. Et pourtant, le RGPD risque fort de bouleverser les pratiques en matière d'exploitation de données, un paradoxe que Denis Jacopini explique par une forme de réactualisation de la loi informatique et libertés qu'entraîne, *de facto*, le RGPD. Les articles 50 à 52 de cette loi prévoient des sanctions pénales en cas d'infraction, mais en réalité, ces sanctions n'étaient pas utilisées. « *Les entreprises se sont dit que de toute façon la CNIL n'avait pas les moyens de contrôler les contrôler toutes* », explique Denis Jacopini. C'est là que le RGPD entre en scène et va modifier ce statu quo.

Des sanctions très lourdes

« *Ce n'est pas la CNIL qui va contrôler comment les données sont exploitées, mais les consommateurs eux-mêmes* », précise l'expert. Ils vont pouvoir saisir l'instance dès lors qu'ils voient leurs données sur Internet. Et toutes les plaintes seront traitées par la Commission. Avec un risque financier pour le moins important désormais puisque l'un des changements apportés par le RGPD est le montant des sanctions qui pourra atteindre jusqu'à 4 % du chiffre d'affaires de l'entreprise par qui les données se sont retrouvées sur Internet. Or, compte tenu des risques croissants liés aux données de santé, de plus en plus convoitées par les cybercriminels, la probabilité pour que cela se produise est loin d'être infime. Tout est fait actuellement pour porter à la connaissance de tout un chacun ses droits sur cette question des données personnelles. Et plus encore dans le domaine des données de santé, où la question de l'exploitation non désirée de telles données peut revenir au premier plan.

Ces données peuvent par exemple arriver chez un assureur, lequel peut les utiliser dans le sens contraire de l'intérêt d'un assuré, ou tout simplement se retrouver sur le Net par simple acte de malveillance. « *Plusieurs mutuelles dans le sud de la France ont été victimes de cybercriminels qui ont récupéré leurs données et demandé une rançon, ce qu'elles ont refusé, les données en question ont été mises sur Internet* », raconte Denis Jacopini. Ce risque n'est pas qu'une hypothèse, c'est la réalité d'aujourd'hui.

La coresponsabilité du pharmacien et de ses sous-traitants

Non seulement les sanctions seront plus lourdes, mais les patients lésés pourront se retourner contre l'ensemble des acteurs qui ont failli à la sécurité de leurs données de santé. Le RGPD introduit en effet la notion de coresponsabilité. Le pharmacien, en tant que professionnel de santé, a le droit de recueillir et d'abriter des données de santé, un aménagement prévu aussi bien par la loi informatique et libertés que par le nouveau règlement européen. Mais de ce fait, il est responsable de ces données et doit en assurer la sécurité. Si elles se trouvent par mégarde ou par malveillance là où elles ne devraient pas être, la responsabilité du professionnel de santé est engagée, tout comme celle de ses sous-traitants. Pour le pharmacien, il s'agit bien évidemment des éditeurs de LGO, des hébergeurs et des acteurs du Web dans leur globalité, parfois même des groupements qui peuvent exploiter des données.

Certes, le monde de la santé est très réglementé et le législateur français a veillé à ce que tous les organismes et les entreprises qui hébergent des données soient habilités à le faire, c'est l'objet de l'agrément hébergeur de données de santé émis par l'ASIP Santé. Les éditeurs de LGO, tout en notant l'évolution réglementaire, estiment être déjà dans les clous du fait de cette législation très stricte. « *Le RGPD n'est pas une révolution et s'inscrit dans la continuité de la réglementation existante*, explique Virginie Molle Rousier, directrice marketing et communication de Smart Rx, *les LGO étant déjà tenus, avant le règlement, de se conformer à des référentiels et cahiers des charges très rigoureux en matière de sécurité des données. Les applicatifs contenant des données de santé sont, en outre, d'ores-et-déjà hébergés dans un environnement agréé HDS.* » Pour Denis Jacopini, l'enjeu n'est pas que technique, il est juridique et commercial. « *Cela va remuer le monde professionnel dans sa totalité, les relations contractuelles entre les entreprises, quelles qu'elles soient, et leurs sous-traitants, vont être impactées, c'est un chantier énorme.* »

Un traitement commercial des données de santé à l'insu des pharmaciens ?

On peut ainsi imaginer que le sujet du traitement commercial des données de santé à l'insu des pharmaciens, qui avait été dénoncé par certains d'entre eux, sera remis à l'ordre du jour. « *Les pharmaciens seront dans le devoir de réclamer aux éditeurs de logiciels la preuve de leur bonne conformité avec le RGPD, notamment l'usage fait de leurs données de santé* », estime ainsi Hélène Decourteix, consultante et fondatrice de La Pharmacie Digitale.

Dans l'immédiat, les pharmaciens auront à améliorer la sécurité de leur informatique, avec notamment des systèmes d'authentification précis, et des outils professionnels, antivirus et pare-feu, voire des procédures pour par exemple empêcher la prise de contrôle à distance d'un ordinateur. Beaucoup de travail reste à faire, il n'est pas certain que les pharmaciens puissent être prêts en l'état d'autant qu'ils n'ont pas beaucoup d'aide pour l'instant. La CNIL fait cependant un effort important d'information, elle a notamment mis en ligne sur son site Internet le logiciel Pia, un outil pour simuler les études d'impact sur la vie privée concernant les risques liés à la sécurité des données. Pour sa part, le Conseil national de l'Ordre des pharmaciens n'a pour l'instant pas communiqué sur le sujet, mais il affirme travailler dessus. L'instance attend notamment les modifications de la loi française qui vont résulter de l'application du RGPD. ● **Hakim Remili**

ID Swatting : Septembre 2016, deux adolescents sont à l'origine d'un canular téléphonique ayant entraîné une opération antiterroriste à Paris.
Malgré le fait d'avoir utilisé une messagerie chiffrée, LCI demande lors de son JT à Denis JACOPINI comment la police les a retrouvé ?

https://youtu.be/B0wApuNyAFQ

Découvrez comment vous vous feriez facilement piéger par phishing ?
Réponse de Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité (arnaques, virus, phishing...) en Direct sur LCI le 23 mai 2016 dans l'émission « Ca nous Concerne » de Valérie Expert.

https://youtu.be/hk9rQDa_zXc

Arnaques Phishing et Crypto Virus en Direct sur LCI le 23 mai 2016.
Arnaques, Phishings, 4 Experts se sont penchés sur ces pièges d'Internet :
– Denis JACOPINI, Expert informatique assermenté spécialisé en Cybvercriminalité
– Vincent HINDERER, Secrétaire Général de Phishing Initiative
– Colonel Nicolas DUVINAGE, Commandant du CLCCN de la Gendarmerie Nationale
– Cyril BROSSET, journaliste au magazine Que Choisir

https://youtu.be/rcOpjxRPX7I

Les fraudes par Carte Bancaire en direct sur LCI le 7 mars 2016 avec Denis JACOPINI expert Informatique spécialisé en Cybercriminalité , Serge MAÎTRE Secrétaire Général de l'AFUB et Nicolas CHATILLON Directeur du Développement Fonctions Transverses du Groupe BPCE
Denis JACOPINI vous explique que quoi que l'on fasse, les fraudeurs auront une longueur d'avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.Consultez notre article 10 techniques de Cybercriminals pour pirater votre carte Bancaire

https://youtu.be/zPOt_h5Qb84

https://youtu.be/kRjXLdfJCYY

Augmentation de la cybercriminalité : Faisons le point

Chiffre alertant : la cybercriminalité évolue globalement de 51% et, la France à elle seule, enregistre 36% de hausse des actes cybercriminels. Avec *Denis Jacopini*, expert en justice informatique, détaillons les « nouveautés » de ce monde, trouvons les raisons et expliquons cette hausse inquiétante.

Denis Jacopini : expert et consultant

Dans cet article, Denis Jacopini nous donnera son point de vue sur les points abordés. Disposant d'un cursus technique solide, expert en justice informatique, il a fait évoluer au fil des années sa structure (www.lenetexpert.fr) pour la tourner vers des secteurs plus porteurs, dont la cybercriminalité qu'il n'estime pas assez « **sensibilisée** » par les donneurs d'ordre.

2016, une année de mouvementée

La cybercriminalité n'est pas un fait inconnu, elle perdure déjà depuis quelques années. Le problème se trouverait dans le fait que le cybercriminel redouble d'ingéniosité, explique D.Jacopini, notamment par de **petites actions**, en passant par **des intermédiaires**. Les hackers savent très bien que les utilisateurs se méfient de plus en plus, au fur et à mesure que les technologies évoluent. Ils ne s'attaquent plus à l'entreprise mais aux **prestataires** en relation avec l'entreprise. Pour 2016, **les cybercriminels développent leurs techniques** en même temps que l'utilisateur augmente sa vigilance.

Comment lutter contre la cybercriminalité ?

« **L'hygiène informatique n'est pas encrée dans les mentalités** » poursuit D.Jacopini, qui fait de son mieux pour changer le comportement des utilisateurs, y compris les entreprises. Il regrette le long temps de réaction face aux failles trouvé par les hackers et **conseil les utilisateurs d'être prudent** sur les **pièces jointes des mails**, il conseille aussi de faire les **mises à jour de ses systèmes** multimédia et conseil **d'acheter un anti-virus**, car ce-dernier a un devoir de résultat. Les anti-virus doivent obligatoirement protéger l'appareil de manière efficace. Si nous, les utilisateurs, mettraient ces conseils en place, beaucoup moins de personnes se feraient piégé. Dites-vous bien que tout le monde est concerné par les actes malveillants !

Pourquoi une évolution aussi importante ?

La cybercriminalité a des caractéristiques assez favorables car sur le net on peut être facilement et sans grosse difficulté **anonyme**. Comme D.Jacopini l'a dit ci-dessus, le hacker redouble d'ingéniosité, il recherche constamment à évoluer. Il est donc difficile, voire quasi impossible de retrouver les auteurs de ses actes. Ce qui a pour principale cause qu'ils sont **rarement punis**, et donc continuent à agir... De plus nous mettons trop de temps à trouver les solutions aux failles trouvé par les hackers. Ils ont donc le temps de peaufiné leurs méthodes et de les **améliorer,** poursuit D.Jacopini.

En conclusion :

Si vous voulez éviter les problèmes : **protégez-vous**. Une fois que cette tâche sera accomplis, vous n'auriez plus besoin de pensé au danger auxquelles vous êtes susceptible d'être victime, à condition de **rester un minimum vigilant !** Que ce soit des entreprises aux consommateurs, les cybercriminels **n'épargnent personne !** Tout le monde peut endosser le rôle de la victime !

Vers une nouvelle cybercriminalité

En 2016, les objets connectés devront faire face à l'augmentation du nombre de cyberattaques. Denis Jacopini, expert en cybercriminalité, nous livre son point de vue sur l'évolution d'un phénomène qui prend de l'ampleur.

Laurène Delaunay, Alexis Vellayoudom Conéricaondin

Comment définiriez-vous la cybercriminalité ?

Ce sont toutes les infractions rencontrées dans la vie courante qui sont liées à l'usurpation d'identité et aux arnaques mais qui utilisent les données informatiques. Ces infractions existent depuis l'arrivée du minitel en 1981. La cybercriminalité concerne également tous les délits et infractions qui utilisent les réseaux électroniques et numériques

Plusieurs médias ou entreprises spécialisées prédisent une augmentation des cyber-attaques pour 2016, comment l'expliquez-vous ?

Il y a une augmentation qui est inexorable. Quand je préviens des risques, les entreprises me répondent qu'elles ne risquent rien ou qu'il n'y a rien d'important dans leurs systèmes informatiques. Mais elles n'ont toujours pas compris qu'à partir du moment où elles détiennent des informations personnelles qui ne leur appartiennent pas, elles prennent des risques. Elles pensent qu'à partir du moment où on leur donne une information on peut en faire ce que l'on veut. Or ce n'est pas le cas : il y a la loi sur les libertés informatiques. Il y a des risques importants de vols de données personnelles et de détournement d'argent (données bancaires).

En 2016, les pirates vont exploiter la faiblesse des sous-traitants.

Des grosses sociétés comme Target (Ndlr : chaîne de distribution américaine) ont déjà été piratées par l'intermédiaire des sous-traitants qui s'occupent de la vidéo surveillance ou de la climatisation. Les sous-traitants sont moins bien protégés que les entreprises.

Il y a des actions établies qui ne correspondent pas à ce qui devrait être fait. L'une des clés pour enrayer le phénomène, c'est une bonne coopération internationale. Il faudrait que les pays s'entendent pour traquer les pirates informatiques. Or aujourd'hui seuls 47 pays sur 197 ont ratifié la Convention de Budapest (Ndlr : coopération internationale pour lutter contre la cybercriminalité). L'objectif est de rechercher, de retrouver et de punir les pirates informatiques. Sur 47 pays, pas un seul pays d'Afrique ne l'a ratifié. Quant à la Russie, elle protège des cybercriminels et ne signera jamais la Convention.

Pourtant, depuis des années, la cybercriminalité rapporte plus que la drogue, parce que c'est plus rapide et plus facile. Tant qu'on ne met pas en place une coopération internationale, le nombre de cybercriminels va augmenter. Les cybercriminels ne risquent rien, donc le phénomène se développe.

N'y a-t-il pas un manque de législation vis à vis des objets connectés ?

Il y a un manque de législation certain. En France on interdit de commercialiser un logiciel de cryptage sans autorisation donc si je ne le commercialise pas, j'ai le droit de le diffuser ! Ca me paraît un peu aberrant. Il va y avoir une évolution en matière d'outils de cryptage et d'outils de communication car il a été démontré, aujourd'hui, que les réseaux terroristes commencent à développer et créer leurs propres logiciels.

Mais ce n'est pas seulement un problème Français ou européen, c'est un problème mondial. Il faut penser à la définition d'une charte mondiale de lutte contre la cybercriminalité qui serait abritée par une organisation internationale. Elle obligerait à définir des règles strictes de sécurité et aux constructeurs de les respecter. Si les fabricants n'ont pas signé la charte où ne respectent pas ces conditions, alors ils seront automatiquement sanctionnés.

N'est-il pas nécessaire aussi de sensibiliser les jeunes auprès de l'utilisation des objets connectés ?

Pour ce qui concerne les objets connectés, il faut bien évidemment sensibiliser les jeunes. Il faut prendre conscience qu'un objet connecté mal utilisé met les jeunes en danger. Quand on sait que 90% des objets connectés collectent des informations personnelles, c'est-à-dire des informations qui sont censées être tenues secrète, il y a lieu de s'interroger. Car ces informations ne devraient pas être diffusées ou être divulguées. Quand on sait également que 90% des objets connectés ne nécessitent pas de mots de passe complexes pour protéger les accès. Par exemple : 1,2,3,4,5,6 est encore le mot de passe le plus utilisé dans le monde en 2015. L'objet connecté, l'accepte. Or les informaticiens auraient dû rendre obligatoires, dans leurs systèmes de sécurité, au minimum un chiffre, une majuscule et un symbole.

Chiffre impressionnant encore, 70% des objets connectés ne crypteraient pas leurs échanges avec le réseau. Ce qui veut dire que quelqu'un qui est connecté sur ce Wifi-Public peut capter ces informations. Par ailleurs, 60% des objets connectés ne sont pas protégés contre les « attaques par force brute », c'est-à-dire tester plein de mots de passe différents. Il y un gros problème au niveau des fabricants. Ils n'ont pas du tout intégré la nécessité de sécuriser leurs objets. La priorité des fabricants, c'est de faire de l'argent.

Il est donc urgent de pratiquer de la prévention auprès des jeunes. Un pirate va chercher, au travers de différents moyens, des portes d'entrées pour pénétrer un système informatique. Et l'objet connecté est une porte d'entrée supplémentaire. Donc cette augmentation du nombre d'objets connectés ralentie la lutte contre la cybercriminalité.

AVIS D'EXPERT

CYBERCRIMINALITÉ

Denis Jacopini,
expert en cybercriminalité

i-Petite Entreprise a rencontré Denis Jacopini, spécialiste dans la protection des données personnelles et en cybercriminalité. Il acte des formations auprès des dirigeants d'entreprises et des salariés, pour leur donner des conseils et détecter les attaques. Il nous donne son avis d'expert pour aider les entreprises dans la prévention des cyberattaques.

IPE : Quels sont les risques de la cybercriminalité ?
Denis Jacopini : La cybercriminalité prend plusieurs formes : des pirates qui ont message à faire passer et dont le but est la défiguration de sites internet, et d'autres qui recherchent l'aspect pécuniaire de la cybercriminalité. Une attaque entraine une mauvaise image et une perte de confiance autant auprès des clients que des salariés. Ces derniers risquent de moins s'engager dans l'entreprise et de perdre confiance dans la sécurité informatique avec la peur de voir leurs données personnelles volées.

IPE : Que conseillerez-vous aux entreprises pour améliorer leur sécurité ?
DJ : Les entreprises ont conscience de la cybercriminalité mais se font toujours avoir. Il faut absolument éduquer. Toutes les entreprises risquent de se faire pirater. L'élément souvent négligé est la charte informatique qui va lier le salarié aux usages des outils informatiques.

IPE : Et concrètement ?
DJ : Concrètement, pour anticiper, l'entreprise doit faire un audit de la sécurité de son système d'information (analyses des mesures de sécurité existantes, test d'intrusion, analyse des usages illicites internes ou externes à l'entreprise) et prévoir une sensibilisation des salariés par un organisme extérieur. Les actions qui en ressortent souvent sont : l'amélioration d'outils et de mesures de sécurité, la mise en place d'une charte informatique, d'outils de cryptage des e-mails ou de cryptage des données. Enfin, la mise à niveau tous les 12 mois des employés car ils doivent connaître les nouvelles techniques couramment utilisées par les cybercriminels.

IPE : Quel est le plus grand danger pour les entreprises ?
DJ : La plus grande menace reste le mail piégé. Dans la précipitation, l'employé va l'ouvrir et cliquer sur une page web usurpée. A partir de là, le pirate peut s'infiltrer, c'est ce qu'il s'est passé avec TV5 Monde. Contre ce genre d'attaque, appelée « *spear-phising* », la technologie arrive à ses limites. La question désormais, est celle du comportement. La sensibilisation des salariés est très difficile mais il est possible de leur apprendre toutes les formes d'attaques, grâce à des formations.

> UNE ATTAQUE ENTRAINE UNE MAUVAISE IMAGE ET UNE PERTE DE CONFIANCE AUTANT AUPRÈS DES CLIENTS QUE DES SALARIÉS.

Cyber-attaques : « Les sociétés ne se protègent pas »

Entretien | Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.

Contexte

Après les attentats du 7 janvier, de nombreux sites internet d'institutions locales ou religieuses en France ont été piratés par des groupes de hackers se présentant comme des islamistes, dont celui du palais des Papes à Avignon, victime d'un "défaçage" (remplacement de la page d'accueil du site) par un groupe dénommé Fallaga team (lire notre édition du 16 janvier). Ces phénomènes de piratage ne sont pas nouveaux et s'accentuent. Ils sont imputables à différents types de malfaiteurs et se matérialisent de manière très différente. Décryptage des cyber-attaques avec Denis Jacopini, expert judiciaire près la cour d'appel de Nîmes et des juridictions du Gard, du Vaucluse, de l'Ardèche et de la Drôme.

■ Denis Jacopini : « Les chefs d'entreprise ne sont pas assez sensibilisés. » DR

Qu'est-ce qu'une cyber-attaque ?

C'est une attaque informatique et cela existe depuis qu'Internet s'est répandu dans le monde. Il existe des formes différentes réparties en trois grandes catégories par l'Union européenne. D'abord celle des arnaques et escroqueries par le biais de faux e-mails qui vous disent que vous avez gagné au loto ou que vous avez hérité d'une somme et vous demandent votre numéro de carte bleue. Ensuite, il existe les attaques sur les Stad (Système de traitement automatisé des données), c'est le fait de rendre inopérant un système informatique comme un serveur. Ces serveurs sont calibrés pour répondre à un certain nombre de requêtes en même temps. Si on le sature de demandes, il ne peut plus répondre.

C'est ce qui s'est passé pour Sony récemment, des dizaines de milliers d'ordinateurs infectés ont saturé en même temps le serveur qui est tombé en panne. Si, par exemple, le serveur d'une entreprise commerciale tombe en panne à Noël, ce sont des centaines de milliers d'euros de perdu. Les malfaiteurs peuvent faire du chantage en disant "je vous bloque ou vous me payez 100 000 €".

« On peut stopper le phénomène si on change les mentalités »

Dans le cas de Sony, des données avaient aussi été supprimées du système. La dernière forme consiste à déposer sur des systèmes informatiques des informations illicites, comme des contenus faisant l'apologie du terrorisme, pédopornographiques, et ce en utilisant les failles d'un système, ce qui est arrivé sur différents sites internet de la région récemment.

Il semble impossible, quelle que soit la structure attaquée, de s'en prémunir.

Il faut d'abord des victimes pour pouvoir analyser le mode opératoire, de manière à ce que les forces de l'ordre et les informaticiens se tiennent informés et puissent ensuite se protéger. Il y a des génies dans toutes les catégories d'attaque. Le groupe KPMG (situé en région Rhône-Alpes, NDLR) en 2012 s'est fait voler 7,6 M € et Michelin 1,6 M € en 2014, selon la méthode de l'"arnaque au président" (en faisant ordonner des virements au nom du président de la société sur de faux comptes en banque. NDLR). Mais tous les jours, des gens se font arnaquer sur des sites de rencontre par des personnes qui se trouvent à l'étranger. Elles leur demandent des petites sommes d'argent à de nombreuses personnes toute la journée pour acheter un billet de train et au final empochent plusieurs dizaines de milliers d'euros. Pour se protéger de cela, il n'y a que le bon sens et la formation. Un éditeur est actuellement en train de développer un logiciel d'analyse comportementale qui va alerter l'utilisateur dès qu'il détectera un élément étrange par rapport à ses habitudes, pour provoquer sa suspicion. Souvent, lorsque les sites se font attaquer, c'est parce que le système de traitement de données n'était pas à jour ou que le client n'a pas voulu payer un informaticien pour le faire. Tous les programmes ont des dysfonctionnements, des fonctions qui ne marchent pas, notamment pour leur sécurité. Il faut donc sans arrêt introduire de nouvelles fonctions pour corriger les défaillantes.

A-t-on une idée du nombre de victimes que font ces attaques ?

C'est très difficile à recenser car tout le monde peut être une cible. Or le gros souci, c'est qu'une entreprise qui a perdu de l'argent à cause d'une cyber-attaque ne va pas le dire, car elle ne veut pas passer pour une société non fiable vis-à-vis des salariés ou des banques. Les individus non plus ne vont pas porter plainte puisqu'ils se font rembourser par leur banque. J'estime à plus de 30 % d'entreprises touchées en France. Et si on compte les virus, ça fait 80 %. On peut stopper le phénomène si on change les mentalités. Les premiers fautifs, ce sont les chefs d'entreprise et les informaticiens qui ne sont pas sensibilisés à la sécurité. Ces derniers n'ont pas convaincu les chefs d'entreprise de se protéger. Or la loi informatique et liberté de 1978 oblige les entreprises à déclarer à la Cnil le traitement de données personnelles et à les protéger (durée de conservation, lieux de stockage, etc.). Elles ne sont donc pas en règle et ne protègent pas leurs données. C'est arrivé à deux reprises chez Orange qui s'est fait voler 100 000 données clients.

Mais cette lutte coûte cher pour de petites structures comme une mairie !

Ce sont des budgets qui doivent être prévus. Les entreprises ou collectivités prévoient des systèmes informatiques mais la notion de sécurité n'est pas prise en compte. Ceux qui n'ont pas de politique de sécurité devront débloquer des budgets pour ça. Une réglementation européenne relative à la protection des données est d'ailleurs en projet pour obliger toutes les entreprises à déclarer un piratage à la Cnil dans les 24 heures afin que les clients en soient informés. Les entrepreneurs peuvent se former à la sécurité sur internet, il existe des prises en charge par les organismes paritaires.

Recueilli par HÉLÈNE AMIRAUX

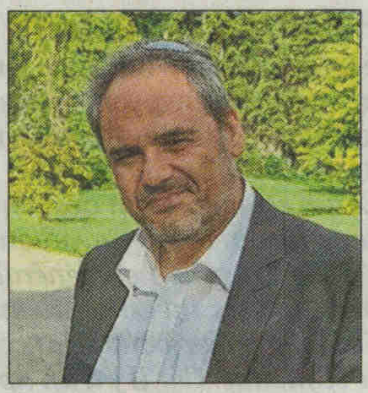
GROS PLAN

La e-reputation

« La e-réputation existe parce que google existe et n'oublie rien ». Un piratage révélé peut vite faire passer l'entreprise pour une *« passoire »* et ruiner sa crédibilité. Des sociétés se sont spécialisées dans le "nettoyage" de e-reputation. *« Le seul moyen d'agir est de rendre plus visible les informations positives, on joue sur le nombre d'informations pour noyer le poisson. On peut faire oublier un piratage en publiant un don à une association. Mais l'algorithme de google ne prend pas uniquement en compte la fraîcheur de l'information mais aussi le nombre de clics ».*

3 QUESTIONS À **Denis Jacopini** expert en informatique

"Nous sommes tous des proies potentielles des pirates d'internet"



Denis Jacopini est à Cavaillon ce soir./ PHOTO DR

Ce soir à Cavaillon, Denis Jacopini, expert informatique assermenté, animera une conférence sur le piratage des sites internet. Au lendemain de l'attentat de Charlie Hebdo, plus de 25 000 sites ont été "défigurés" en France, dont quelques-uns en Vaucluse, à l'instar de celui du Palais des papes ou de certaines communautés de communes. Pour ce spécialiste de la cyber-criminalité et de la protection des données personnelles, il est important que les sociétés comme les collectivités reconsidèrent leur sécurité numérique.

Si l'on peut voir dans le piratage du site du Palais des papes un acte symbolique, pourquoi "hacker" celui d'une communauté de communes ?
Là, c'était une opération de communication. C'est l'institution dans son ensemble qui est la cible. Les pirates ont cherché, avec l'aide de robots, des sites faciles qui sont soit à l'abandon soit gérés avec peu de moyens. L'idée du piratage est de récolter des données ou juste se contenter de dire "on est passé par là".

Ces attaques sont de plus en plus nombreuses. Doit-on faire face à une nouvelle criminalité ?
Les attaques ont toujours existé mais aujourd'hui elles sont très nombreuses, et nous sommes tous des proies potentielles. C'est facile pour les malfaiteurs de réaliser ces actions de masse dans l'anonymat. La plus répandue reste le vol de données.

Comment se préserver ?
Il est impératif de reconsidérer la question de la sécurité informatique pour les élus ou les entreprises, il en va aussi de l'image et de la réputation des sociétés et des collectivités. Les pirates n'ont pas forcément besoin du numéro de carte bancaire, ils peuvent faire des transactions avec votre banque juste avec votre mail et votre mot de passe. Il est donc important de changer de mot de passe régulièrement, d'avoir un anti-virus performant mais cela ne suffit pas. Il y a d'autres actions pour se protéger...

Recueilli par Mélodie TESTI

Pour en savoir plus, rendez-vous ce soir à 18h30 dans les locaux de Initiative Cavare et Sorgues, 111, boulevard Paul-Doumer, à Cavaillon.

AVI_001

SALON PROFESSIONNEL DU NUMERIQUE

(http://www.salon-du-numerique.fr/)

Le Salon du Numérique 2014 s'est déroulé une fois de plus cette année à Avignon.

Mais cette fois, le 18/03/2014, a été dans des locaux bien plus grand avec accès facilités et parking gratuit (Rue Felicien Laurent Zone Agroparc – Avignon).

A 15h00, Denis JACOPINI a animé avec Lionel FOUQUET une conférence de présentation intitulée « **Le juridique et le Web**« .

Les usages de l'informatique évoluent mais les lois du numérique et les risques des chefs d'entreprise aussi. Partant du fait qu'un abonné à Internet a une obligation de surveillance de l'usage qu'il en est fait par ses utilisateurs et que l'employeur peut être pénalement responsable à titre personnel de l'agissement de ses salariés, cette conférence a pour objectif d'informer les chefs d'entreprise de l'ensemble des nouveaux usages de l'informatique risquant de les rendre pénalement responsables. En raison des surveillances de plus en plus efficaces et automatiques de l'Internet à notre domicile, ces pratiques interdites se sont désormais déportées sur le lieu de travail. Pendant un peu moins d'une heure, vous seront présentés les usages quotidiens de l'informatique dans le milieu professionnel pouvant vous rendre pénalement responsable. Les solutions à mettre en œuvre pour minimiser ces risques seront également dévoilées à cette occasion.

L'Hebdo Le Comtadin N°3605 du 19 septembre 2013

L'actualité

Prévenir les risques liés à l'informatique

Jeudi 26 septembre à 19h30, le restaurant «les Ombrages», à Montfavet, accueille une conférence sur le risque informatique donnée par un expert judiciaire.

La révolution de l'information, figurez-vous, nous sommes en plein dedans. Les deux pieds dedans, même. Il y a encore 10 ans, qui aurait pensé envoyer ses factures par mail ? Faire son rapprochement bancaire par le biais d'Internet ? Informer 1500 personnes d'un seul coup d'une offre promotionnelle en appuyant juste quelques fois, du bout du doigt, sur la souris de son ordinateur ? De nouvelles pratiques, de nouvelles modalités de production et d'échanges de l'information, qui ont aussi leur côté obscur. Certes, les dirigeants des petites et très petites sociétés se pensent protégés, par leur petite taille, des problèmes de virus ou de vol des données. Mais pourtant, il existe des risques bien concrets, qui concernent au premier chef les petites entreprises. C'est en tout cas la démonstration que fait Denis Jacopini, expert juridique du risque informatique près la cour d'appel de Nîmes.

Denis Jacopini, expert du risque informatique

Après une licence en ingénierie électrique, Denis Jacopini gérera durant 17 ans une société d'informatique à Cavaillon, spécialisée dans le service aux entreprises. *«J'ai assisté au gonflement de la bulle informatique, dans les années 2000, puis à son dégonflement juste après. C'est alors que je me suis dit que la structuration du secteur allait générer des problèmes particuliers, bien au-delà des problèmes de maintenance technique : les risques juridiques ».*

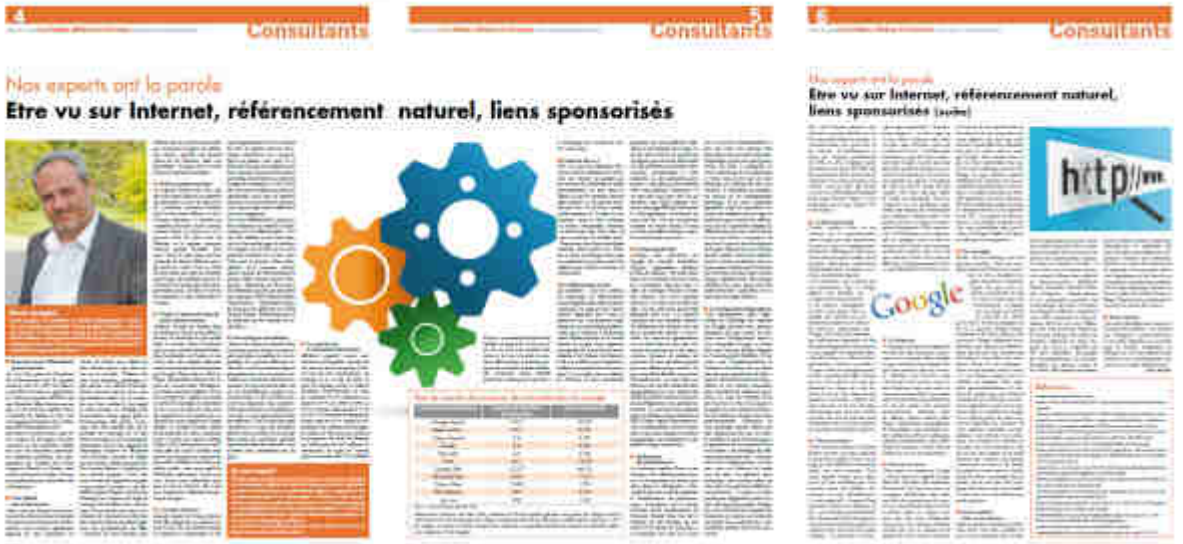
Après une formation de droit de l'expertise judiciaire à l'université d'Avignon, il intervient donc dans l'expertise de dossiers judiciaires. Mais il développe aussi un volet préventif, pour éviter précisément aux chefs d'entreprises de se retrouver devant les juges.

Pour cela, il propose des conférences. L'agence de communication Hélios Média, à Sarrians, a pris la décision d'en organiser une, le 26 septembre prochain, dans le superbe cadre des Ombrages, à Monfavet. Au programme de cette conférence, deux des risques les plus courus par les entreprises : la question des base de données et de leur déclaration à la CNIL, et la question plus récente de l'arrivée du téléchargement illégal dans le cadre de l'entreprise. *« Partant du fait qu'un abonné à Internet a une obligation de surveillance de l'usage qu'il en est fait par ses utilisateurs et que l'employeur peut être pénalement responsable à titre personnel de l'agissement de ses salariés, cette conférence a pour objectif d'informer les chefs d'entreprise de l'ensemble des risques encourus en rapport avec les nouveaux usages de l'informatique»*, explique l'expert. *« En raison des surveillances de plus en plus efficaces et automatiques de l'Internet à notre domicile, ces pratiques interdites se sont désormais déportées sur le lieu de travail».*

La cerise sur le gâteau étant que Denis Jacopini ne fait pas qu'attirer l'attention des décideurs sur l'existence des risques, mais qu'il peut aussi proposer des solutions, allant du simple réglage d'un Firewall pour empêcher l'usage des réseaux sociaux, jusqu'à la formation qui permet de mettre en place des bases de données en toutes légalité. De quoi surfer et travailler l'esprit plus tranquille !

Pierre Nicolas

Entrée libre - Réservation et information : 06 26 39 16 57 www.helios-medias-communication.com



Nos experts ont la parole

Le Crowdfunding, risques, pièges et précautions à prendre