Prospection par messagerie électronique : que risque une société qui ne respecte pas la loi ? | Denis JACOPINI

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

Une société commerciale ne peut envoyer de mails publicitaires sans l'accord préalable de la personne sollicitée.

Une société qui ne respecte pas cette règle risque des sanctions pénales et des amendes de 750 euros par message expédié.
De son côté, la CNIL peut prononcer des sanctions pouvant aller jusqu'à 300.000 Euros d'amende lorsque des messages sont adressés à des personnes physiques sans leur consentement.

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

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

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

Source : https://www.cnil.fr/fr/cnil-direct/question/372

Quels sont les droits et devoirs des salariés en matière de sécurité informatique | Denis JACOPINI

Il n'est pas rare que des salariés soient surpris en train, au sein de leur entreprise,d'utiliser des outils de type Keylogger – permettant l'enregistrement des touches utilisées sur le clavier – et des logiciels visant à capter et à forcer les mots de passede sessions de systèmes d'exploitation.

Or, dans la majorité des cas, aucune sanction n'est prise par les employeurs, y compris lorsque les auteurs des faits sont animés d'intentions malveillantes et non simplement ludiques.

Dans un raisonnement inspiré du droit du travail, l'employeur – arguant par exemple de ne pas disposer de charte de sécurité informatique spécifiant les comportements à respecter, ainsi que les sanctions applicables – estime qu'à défaut d'avoir porté par écrit à la connaissance de l'employé la réglementation en vigueur au sein de l'entreprise, celui-ci ne peut être légalement sanctionné.

Il est important de rappeler que le seul fait de collecter des données à caractère personnel par un moyen frauduleux est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du Code pénal) et ce, quelles que soient les intentions du salarié. De même, le fait de s'introduire frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans de prison et de 30 000 euros d'amende (article 321-1 du même code). La loi est d'application directe et ne nécessite pas d'être citée dans une charte informatique pour en assurer le respect par les salariés. Les employeurs peuvent donc prendre immédiatement les sanctions afférentes à une telle faute.
En outre, la responsabilité de l'employeur peut se voir engagée par ce type d'agissements, sur la base de plusieurs fondements :
• la personne cible/victime des menées de son/ses collègues pourra, en cas de dommage, agir contre l'employeur, responsable de ses salariés. Il reviendra alors à la société de prouver que le mis en cause a agi « hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions », ce qui est rarement admis en pratique.
• de par la jurisprudence « Sarenza c/ Jonathan » du 21 février 2013, le juge a précisé que la société devait supporter, à hauteur de 30%, son propre dommage, engendré par les lacunes dans la gestion des identifiants d'accès aux bases de données. Le juge a donc instauré l'obligation, pour l'employeur, de mettre en place des mesures de protection informatique efficaces, afin de prévenir l'installation de tout logiciel espion.
• Enfin, la plupart des logiciels utilisés à ces fins proviennent de téléchargements, susceptibles de contenir des virus. Les réseaux internes des entreprises sont régulièrement infectés par ce biais, ce qui facilite les intrusions informatiques et, partant, l'accès, l'utilisation, l'extraction, voire la destruction de données stratégiques pour l'entreprise.

Préconisations de la DGSI
La DGSI recommande à toute entreprise :
• En priorité, d'établir une charte de sécurité informatique qui permettra de sensibiliser les salariés aux enjeux numériques, tout en les responsabilisant.
• D'organiser régulièrement des conférences de sensibilisation à destination de l'ensemble des collaborateurs, qui insisteront sur leurs droits et obligations à l'ère du tout-numérique et dispenseront des mises à jour sur les évolutions technologiques en cours.
• De mettre en place des mesures de protection efficaces afin de prévenir l'utilisation potentielle de logiciels et matériels espions. L'existence de tels dispositifs de sécurité informatique permettra à l'employeur de dégager sa responsabilité juridique et d'optimiser le bon fonctionnement de son entreprise en augmentant le niveau de protection.

Vous avez besoin de recueillir des preuves, expertiser un système informatique, vérifier des contenus, Denis JACOPINI peut vous conseiller, vous accompagner et réaliser toutes les phases techniques nécessaires à la constitution d'un dossier juridique solide.
Contactez Denis JACOPINI

Quelques articles sélectionnés par nos Experts :

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« *Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services.* ».

Source : http://www.ccirezo-normandie.fr/document/104108-flash-ingerence-economique-n-15-rappel-des-droits-et-devoirs-des-salaries-en-entrepr

La cybersécurité pour les débutants – Un lexique informatique

Nous avons jugé utile de vous retaper ce lexique, bonne base pour tous ceux qui souhaiteraient se familiariser avec des termes parfois barbares.

A

ADSL
L'ADSL, Asymmetric Digital Subscriber Line, (Réseau de Raccordement Numérique Asymétrique), technologie de communication permettant de faire passer de l'information (issue d'Internet par exemple) à haut débit sur les fils de cuivre utilisés habituellement pour les lignes téléphoniques (RTC). Avec l'ADSL, il est p [illegible]

A.F.N.I.C.
Association Française pour le Nommage Internet en Coopération, elle gère le registre des noms de domaine français : .fr (France), .re (Ile de la Réunion), .pm (Saint-Pierre et Miquelon), .tf (Terres australes et antarctiques Françaises), .wf (Wallis et Futuna), .yt (Mayotte).

A.P.N.I.C.
Asia-Pacific Network Information Center, elle gère le registre régional d'adressage I.P. du continent asiatique (sauf le Moyen-Orient) et les pays du Pacifique.

A.R.I.N.
American Registry for Internet Numbers, elle gère le registre régional d'adressage I.P. du Canada, des USA et des îles des Caraïbes et de l'Atlantique.

ANONYMISEUR
C'est un service permettant de naviguer anonymement (avec des outils d'anonymisation). En général, c'est un serveur/proxy qui masque les informations personnelles (adresse IP, système d'exploitation, navigateur,…) aux sites visités. Par exemple utilisation du logiciel TOR pour une navigation anonyme.

ANONYMOUS
« Anonyme » en français est un « même internet ». Anonymous peut être qualifié comme concept, il n'y a ni leader, ni responsable, ni porte-parole. La devise des Anonymous est : « We are Anonymous, We are Legion, We do not Forget, We do not Forgive, Expect us ! » (Nous sommes les Anonymes, nous sommes Légion, nous [illegible]
On peut les qualifier d'HACKTIVISTES.

A.N.S.S.I.
L'Agence Nationale de la Sécurité des Systèmes d'Information (anciennement appelée DCSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale. Elle est rattachée au Secrétaire Général de la Défense Nationale (S.G.D.N). Elle assure la mission d'autorité nationa [illegible]

APACHE HTTP SERVER
Souvent appelé Apache, c'est un logiciel de serveur HTTP produit par l'Apache Software Foundation. Ce logiciel permet d'héberger des sites Internet. Il est le plus populaire du Web et le plus répandu. C'est un logiciel libre à licence spécifique.

ARBORESCENCE
Organisation des données informatiques de manière logique et hiérarchisée utilisant une structure algorithmique d'arbre. Le premier niveau de l'arborescence appelé « racine » contient les dossiers, les sous-dossiers et les fichiers d'un ordinateur personnel.

B

BACKBONE
Désigne la dorsale qui réalise l'interconnexion de plusieurs sous-réseaux et de lignes haut débit. C'est une autoroute numérique par laquelle passent obligatoirement les données envoyées sur un réseau.

BACKDOOR
De l'anglais « Porte dérobée », c'est un programme malicieux visant à détourner les fonctionnalités d'un service ou d'un système en ouvrant sur la machine touchée un canal d'accès masqué et utilisé par une personne malveillante.

BALAYAGE DE PORT
« Port scanning » en anglais est une technique de base pour l'administrateur réseau ou un pirate en herbes pour vérifier quels sont les ports en écoute sur un serveur de réseau. Cette technique est considérée comme une tentative d'intrusion car ce balayage sert souvent à préparer une intrusion.
Cette écoute des ports vise à déterminer si un logiciel est en écoute sur un port donné. Si c'est le cas on dit que le port est ouvert sinon qu'il est fermé.

BENCHMARK
En français « test de performance », il permet, avec des tests prédéfinis, de mesurer les performances d'un système aux fins de comparaison.

BIOS
(Basic Input Output System) Programme encapsulé dans l'EEPROM de votre ordinateur (mémoire que l'on peut reprogrammer par « flashage »). Ce programme est sollicité lorsque l'ordinateur est mis sous tension. Le BIOS est chargé de vérifier le microprocesseur, l'horloge interne, la mémoire vive, le clavier, les lecte [illegible]

BLOG
C'est un site web visible par tous constitué de billets (appelés aussi notes ou articles) mis bout à bout à l'image d'un journal de bord ou d'un journal intime.

BLUETOOTH
Bluetooth est l'équivalent d'USB mais sans fil, il sert à relier des périphériques entre eux (clavier,souris, caméra, imprimante…).

BOT
C'est la contraction de « robot ». Un « bot informatique » ou « robogiciel » est un logiciel qui agit de façon autonome pour un humain ou un autre programme informatique. Il se connecte et agit automatiquement ou semi automatiquement avec des serveurs informatiques. Utilisé principalement pour effectuer des tâ [illegible]
Les « bots » ont été détournés pour effectuer des attaques distribuées contre des services Internet. Par exemple :
- « WEBBOT » est utilisé pour la fraude au clic.
- « SPAMBOT » permet de s'inscrire sur de forums dediscussion dans le but de spammer.

BOTNET VOIR BOT
C'est un ensemble de BOTS INFORMATIQUES reliés entre eux. Leur usage bien que légitime au début fût vite détourné et désigne aujourd'hui des machines ZOMBIES.

BUFFER OVERFLOW
Le « Buffer overflow », dépassement de tampon ou débordement de tampon en français, est une attaque utilisant un bug d'un programme ou d'un système. Le « BUFFER » est une zone mémoire temporaire.
Le but de cette attaque est d'écrire plus de données que le buffer ne peut en contenir écrasant ainsi des informations nécessaires au processus.
Les conséquences sont multiples :
- Soit le bug est non intentionnel ou mal maitrisé,le résultat est un blocage du programme ou du système.
- Soit le bug est intentionnel auquel cas la personne tente de faire exécuter des instructions pour accéder au système.

Il s'agit d'une attaque redoutable. L'attaquant doit avoir des connaissances avancées sur la programmation ce qui n'est pas à la portée de tout le monde ni d'un simple « script kiddies».

BUREAU À DISTANCE (CLIENT TERMINAL SERVER)
Le bureau à distance est un logiciel client utilisant, TERMINAL SERVER EDITION (TSE), un composant de Microsoft Windows, autorisant l'utilisateur à se connecter à un serveur exécutant le service de TERMINAL. Elle permet par exemple l'administrateur réseau d'installer une base de données ou un ou des logiciel(s) s [illegible]
Elle simplifie aussi les mises à jour, le dépannage et la gestion des logiciels. Utilise le protocole réseau RDP (Remote Desktop Protocol).

BREIDBART (INDICE DE)
L'indice de Breidbart ou BI est l'unité de mesure destiné à quantifier le degré de nocivité des messages diffusés sur les NEWSGROUP USENET. On parle aussi d'EMP « Publication Multiple Abusive » (Excessive MultiPosting) ou ECP « Publication Croisée Excessive » (Excessive Cross-Posting).

C

CACHE
Mémoire tampon dans laquelle se trouvent stockées des informations que le système estime être susceptible de redemander, afin d'accélérer l'accès à la mémoire ou à un dispositif de stockage (disque dur par exemple).

CANULAR (HOAX)
Le HOAX (canular) est généralement un SPAM que l'on reçoit par courriel. Il joue avec les émotions tristes ou joyeuses afin d'inciter le destinataire à propager une rumeur, fausse nouvelle ou légendes urbaines. Même si l'objectif reste un peu flou, le HOAX sert à faire une mauvaise blague mais aussi à saturer les [illegible]

CAPTCHA
Il s'agit d'une forme de test de Turing (du nom d'Alan TURING) permettant de différencier de manière automatisée un utilisateur humain d'un ordinateur. Ce test est utilisé sur Internet dans les formulaires pour se prémunir contre les soumissions automatisées et intensives réalisées par des robots malveillants. La [illegible]
Un « captcha » usuel requiert ainsi que l'utilisateur tape les lettres et les chiffres visibles sur une image distordue qui apparait à l'écran. Certains sites web préfèrent afficher une image qui contient une opération mathématique à résoudre, identifier un dessin ou un son. Ils sont généralement utilisés pour l [illegible]
Pour aller plus loin : « Captcha » est un rétro-acronyme : le mot se prononce comme « capture » en anglais et est censé être composé des initiales de « Completely Automated Public Turing test to Tell Computers and Humans Apart », soit en français, « test public de Turing complètement automatique ayant pour but de [illegible]

CARDING
Piratage de carte bancaire.

CERTA
Le Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA) est un organisme rattaché à la Direction centrale de la Sécurité des systèmes d'information, destiné à coordonner la lutte contre les intrusions dans les systèmes d'information des administrations de l'État françai [illegible]
Créé le 19 janvier 1999, le CERTA est membre du FIRST depuis le 12 septembre 2000 et participe depuis le 25 mars 2002 à l'activité TF-CSIRT (Computer Security Incident Response Team), qui est la coordination des CERTs européens.

CHAT
Système de conversation en temps réel sur Internet.

CHEVAL DE TROIE
Logiciel d'apparence légitime qui permet de s'introduire sur les machines des utilisateurs et d'en prendre leur contrôle sans qu'ils ne s'en aperçoivent.
Le cheval de Troie se compose de deux parties distinctes : un « client » et un « serveur ».
La partie « serveur » est envoyée à la victime par mail ou sous couvert d'une amélioration logiciel, de jeux, …
La partie « clien », elle, est sur l'ordinateur dupirate en rentrant en profondeur dans le système ouvrant ainsi en grand l'ordinateur de la victime. Le pirate contrôle donc entièrement l'ordinateur de la victime.

CHIFFREMENT
Le chiffrement, parfois appelé à tort cryptage, est en cryptographie le procédé grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé) chiffrement.

CLIENT
Logiciel permettant de se connecter sur un serveur et d'effectuer des recherches de documents. Plus généralement une entité demandant un service.

CLOUD COMPUTING
C'est un concept de déportation sur des serveurs distants des traitements informatiques traditionnellement localisés sur le poste utilisateur. Les noms officiels en français sont « informatique dans le nuage », « informatique en nuage », « informatique dématérialisée », ou encore « infonuagique ».
Les utilisateurs ou les entreprises ne sont plus gérants de leurs serveurs informatiques mais peuvent ainsi accéder de manière évolutive à de nombreux services en ligne sans avoir à gérer l'infrastructure sous-jacente, souvent complexe.
Les applications et les données ne se trouvent plus sur l'ordinateur local, mais – métaphoriquement parlant – dans un nuage « cloud » composé d'un certain nombre de serveurs distants interconnectés au moyen d'une excellente bande passante indispensable à la fluidité du système. L'accès au service se fait par une a [illegible]

CLUSTER
En français « BLOC », est l'unité minimale de stockage de l'information pouvant être inscrite et manipulé par le système sur un disque dur. Sa taille varie selon le mode de formatage du disque dur et ce choix influera les performances et la capacité utile du disque dur.
Se dit aussi d'une grappe de serveurs informatiques utilisés pour une continuité de service.

COOKIE
Petit fichier incluant des paramètres (exemple : votre adresse mail si vous l'avez donnée, ou bien le type de navigateur que vous utilisez) transmis d'un serveur Internet vers la machine de l'internaute. Lors des prochaines connexions sur le même serveur, ce dernier pourra récupérer les renseignements inclus dans [illegible]

COPIE-IMAGE
Terme adapté de l'anglais « forensic copy ». L'expression « copie-image » représente une copie intégrale à l'identique de l'information numérique présente sur un support d'information, y compris les espaces non utilisés.
Elle est réalisée dans le cadre d'une investigationnumérique légale.

COURRIEL
Abréviation de l'expression courrier électronique (appelé aussi mail – email – mél) désigne l'envoi par le réseau de documents numérisés.

CPL
Le Courant Porteur en Ligne est la technique qui permet de faire circuler l'information par le réseau électrique. Cette technique permet d'être utilisé par une entreprise ou un particulier afin de créer son réseau informatique.
Elle permet donc de palier aux difficultés d'utilisation du wifi dans une zone ou une habitation où les ondes wifi passent mal.

CROSS SITE SCRIPING
En abrégé XSS, est un type de faille de sécurité des sites Web, que l'on trouve typiquement dans les applications Web qui peuvent être utilisées par un attaquant pour faire afficher des pages web contenant du code douteux.
Le principe est d'injecter des données arbitraires dans un site web, par exemple en déposant un message dans un forum, mais aussi par des paramètres d'URL, etc. Si ces données arrivent telles quelles dans la page web transmise au navigateur (par les paramètres d'URL, un messageposté, etc.) sans avoir été vérifiée [illegible]

CRYPTOGRAPHIE
Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur contenu ne soit perçu et/ou d'empêcher leur utilisation non autorisée.

CRYPTAGE
Le terme « cryptage » est utilisé à tort en informatique, puisque d'une manière générale ce mot n'existe pas. Étymologiquement, il vient de la francisation du verbe anglo-saxon « to crypt ». Le terme convenable est chiffrement ; qui signifie appliquer une cryptologie. Il est admis que le terme « crypté » est util [illegible]

CYBERCRIME
On l'utilise quand il s'agit de l'utilisation des systèmes informatiques et des réseaux comme moyen pour commettre des infractions, comme la fraude, le jeu,la diffamation, la violation du droit d'auteur, etc

CYBERTERRORISME
On l'utilise quand il s'agit de menace contre les infrastructures d'Internet et les autres systèmes informatiques comme le piratage, la diffusion de virus et l'usurpation d'identité etc. …

D

DEFACING
Un défacement, ou défaçage désigne la modification non sollicitée de la présentation d'un site Web, suite au piratage de celui-ci. Il s'agit donc d'une forme dedétournement de site Web par un pirate.

DEGROUPAGE
Le dégroupage est la technique utilisé par les FAI tiers afin d'accéder à la boucle local de l'opérateur téléphonique historique. Cette ouverture du réseau local a pour but de permettent qu'une partie des signaux téléphoniques ne soient plus gérés par l'opérateur historique rendant possible une réelle concurrence. [illegible]

DENI DE SERVICE OU DOS
(Denial of Service). C'est, d'une manière générale, l'attaque qui vise à rendre un serveur quelconque incapable de répondre aux requêtes des utilisateurs, par saturation délibérée. L'attaquant procède parl'envoi de requêtes incompréhensibles pour le serveur. Ce dernier consomme alors toutes ses ressources à leur [illegible]

DENI DE SERVICE DISTRIBUE OU DDOS
(Distributed Denial of Service). C'est une attaque informatique qui vise à rendre un ou des serveurs incapables de répondre aux requêtes des utilisateurs. Elle se déroule en deux temps :
- La première consiste à infecter un maximum d'ordinateur sur la planète (comprenez plusieurs milliers, voire dizaine de milliers) par un programme malicieux précis.
- La seconde étape consiste à envoyer simultanément, via ces machines, des paquets éventuellement résolubles, mais tellement nombreux qu'ils vont entrainer la saturation du serveur. On dit alors que le serveur « tombe ».

DEVOIEMENT
Voir PHARMING.

DIALER
Logiciel permettant de composer un numéro de téléphone.

DISCLAIMER
Vient d'un mot anglais « disclaimer » et de l'ancien français « desclamer » qui veut dire « Avis de non responsabilité ». Le disclaimer est généralement le propriétaire d'un site Internet (ou son hébergeur) qui défini, délimite ou se dédouane de sa responsabilité. Ce terme peut convenir à un créateur de logiciel [illegible]

DISQUE DUR
C'est un des organes servant à conserver les données de manière permanente dans un ordinateur.

DISQUE DUR VIRTUEL
Il s'agit précisément d'un volume de stockage en ligne (i.e. espace dédié sur un serveur distant) permettant d'être accessible partout dès lors que l'on possède une connexion à un réseau ou Internet. Ne pas confondre avec serveur virtuel.

DISTANCE DE LEVENSHTEIN (OU DISTANCE D'ÉDITION)
Cela mesure la similarité entre deux chaînes de caractères. C'est donc le nombre minimal de caractère qu'il faut supprimer, insérer ou remplacer pour passer d'une chaîne à l'autre. Elle permet en informatique de comparer deux fichiers afin de déterminer les modifications éventuelles.

DLL (EXTENSION DE FICHIER)
Les fichiers avec l'extension « .dll » (Dynamic Link Library) pouvant être traduit littéralement « bibliothèque de liaisons dynamiques », sont des fichiers systèmes exécutable permettant à des programmes de partager du code et/ou d'autres ressources nécessaires pour effectuer des tâches particulières. Un fichier D [illegible]

D.N.S.
(Domaine Name Server), que l'on peut traduire en français par « résolution du nom de domaine », a pour principe d'associer une adresse I.P. à un nom de domaine (site internet). En règle générale, chaque FAI possède son, voire ses, propres serveurs DNS. On distingue toutefois les serveurs DNS racine, qui sont au [illegible]

D.N.S. SPOOFING
Attaque informatique consistant à faire parvenir de fausses réponses à des requêtes DNS émises par une victime. La technique, dite DNS ID Spoofing, consiste à envoyer les réponses à l'internaute demandeur avant quele serveur DNS ne le fasse ; ce qui implique de prédire l'identifiant « ID » de la demande envoyée p [illegible]

D.N.S. SQUATTING
Le DNS squatting consiste, ou plutôt consistait, à acheter et enregistrer le nom de domaine d'une entreprise ou marque connue avant qu'elle-même ne l'achète. S'enchaine généralement ensuite un processus de vente au titulaire légitime du nom de domaine, dont le prix est décuplé.
Par exemple, l'achat du domaine www.nutella.com avant que cette société ne l'achète. Quand elle se manifestera, il pourra lui être revendu pour quelques milliers d'euros. Cette pratique n'existe quasiment plus, puisque d'une part les grandes marques ont toutes leur nom de domaine et d'autre part la justice consid [illegible]

D.N.S. PHARMING
Aussi appelée DNS Cache Poisoning, cette attaque consiste à compromettre le cache d'un serveur DNS par une fausse résolution. En effet, pour alléger la consommation de ses ressources, le serveur DNS va conserver cette résolution temporairement dans son cache.
Cette fausse résolution, du site www.cible.fr vers www.attaquant.fr par exemple, suivie de plusieurs interrogations va faire que la résolution IP du site www.cible.fr va s'effectuer vers www.attaquant.fr tant que des demandes seront effectuées. Ainsi un internaute voulant visiter le site original sera redirig [illegible]

DONGLE
Un « dongle » est un composant matériel se branchant sur les ordinateurs soit par le port parallèle soit de nos jours sur le port USB afin de valider le droit d'utiliser un logiciel ou un matériel. Il remplit le rôle de « verrous matériels ».

DONNEES PERSONNELLES
Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il con [illegible]

DOWNLOAD
En français, le mot téléchargement ne précise pas le sens dans lequel le transfert d'un fichier s'effectue. Or, en anglais, la distinction se fait.
Il est dont appelé download le téléchargement depuis un ordinateur (téléchargement descendant) ; c'est à dire lorsque je reçois.

DROPBOX
« DROPBOX » est un service en ligne sécurisé de stockage et de partage des fichiers proposé par la société « Dropbox, Inc. » localisée aux Etats-Unis.

DSI
Directeur des Systèmes d'Information, au sein d'une organisation (entreprise, association ou institution), il est responsable de l'ensemble des composants matériels (postes de travail, serveurs, équipements de réseaux, systèmes de stockage, de sauvegarde et d'impression…) et logiciels du système d'information, a [illegible]

DSLAM
DSLAM est le sigle anglais de « Digital Subscriber Line Access Multiplexer », soit en français, « Multiplexeur d'Accès à la Ligne d'Abonné Numérique » (plus simplement : « Multiplexeur d'accès DSL »).
C'est un appareil assurant une fonction de multiplexage, il permet d'assurer sur les lignes téléphoniques un service de type DSL (ADSL, ADSL 2+, SDSL…).

DUMP
Opération qui consiste à capturer les données d'un fichier, d'un réseau ou d'une zone de mémoire. Généralement le contenu de cette capture est affiché au format hexadécimal.

E

EBOOK
L'eBook, « Livre électronique » en français, est un fichier numérique contenant du texte qui peut être lu par tout appareil numérique comme un ordinateur, un « ordiphone » ou une tablette numérique.

E.F.I.
L'E.F.I. : Extensible Firmware Interface (traduction en français, interface micrologicielle extensible) est un logiciel intermédiaire entre le micrologiciel (firmware) et le système d'exploitation (OS) d'un ordinateur. Cette interface est appelée à être le successeur du BIOS.
Il offre de multiples avantages par rapport au BIOS :
- Prise en charge de beaucoup plus de fonctionnalités réseaux car intégrées en standard dans son Firmware.
- Propose une véritable interface graphique haute résolution.
- Offre une gestion intégrée des installations multiples de systèmes d'exploitation.

Il est développé de manière à offrir une plus grande indépendance entre le système d'exploitation et la plateforme matérielle sur laquelle il tourne.
Disponible sur AMD, American Megatrends, Dell, HP, Intel, IBM, Insyde, Microsoft et Phoenix Technologies ceux-ci constituent aujourd'hui au sein de l'UEFI forum desacteurs majeurs autour de cette technologie.
Systèmes d'exploitation utilisant l'E.F.I. :
- Les systèmes basés sur Linux sont capables de gérer l'EFI au boot depuis 2000 en utilisant le chargeur d'amorçage Elilo.
- HP-UX utilise l'EFI sur ses systèmes IA-64 depuis2002.
- Apple a, quant à lui, adopté l'EFI pour les derniers ordinateurs Apple,. Mac OS X v10.4 Tiger pour Intel et Mac OS X v10.5 Leopard prennent entièrement en charge l'EFI.
- Microsoft Windows : Les versions Itanium de Windows 2000 supportaient l'EFI 1.1 en 2002. Microsoft Windows Vista contient un système de gestion de l'UEFI depuis la version SP1. Microsoft Windows Server 2008, basé sur le noyau de Windows Vista SP1, gère également les plates-formes UEFI.

EEPROM
La mémoire EEPROM (Electrically Erasable Programmable Read-Only Memory), mémoire morte électriquement et programmable en français. Ce composant électroniquesert à enregistrer des informations qui ne s'effaceront pas lors de la mise hors tension d'un appareil.

EMP OU ECP
Voir indice de BREIDBART.

EMPREINTE NUMERIQUE(HASH VALUE)
L'empreinte numérique (hash value) est un calcul mathématique particulier qui, à partir d'une donnée fournie en entrée, détermine une empreinte servant à identifier rapidement la donnée initiale. Cette fonction, qui est mise en œuvre via un algorithme cryptographique (MD5, SHA-1, etc.), va authentifier un contenu [illegible]
Son intérêt est d'authentifier l'intégrité d'une donnée (CD-Rom saisi chez un mis en cause, clé USB remise par la victime, etc.)

ESPACE NON ALLOUE
Espace du disque dur disponible qui n'est pas assigné à une partition, à un lecteur logique ou à un volume. C'est la partie de la partition du média non utilisé. Elle peut contenir des fichiers ou des morceaux des fichiers déclarés supprimés mais toujours présent sur le disque.

ETHERNET
Norme de protocole de réseau local très répandue initialement développée par Xerox dans les années 1970. Le standard Ethernet utilise la méthode de partage du support technique CSMA/CD et correspond à la norme IEEE 802.3.

F

FACEBOOK
Le nom s'inspire des albums photo « trombinoscope » en français. C'est un site « web » permettant, à toute personne ayant créé un profil, de publier des informations textuelles et documents multimédias pour toute personne ou groupe de personne possédant un compte ou non. Il fait partie des réseaux sociaux.
Il permet aussi de commenter en direct les diverses informations publiées par le titulaire du compte.
Une fonction de messagerie instantanée est intégrée et permet de voir les membres d'un groupe en ligne. Les discutions peuvent être privées si nécessaire.

FAI
C'est une abréviation de Fournisseur d'Accès à Internet. ISP (Internet Service Provider).

FILETIME
A l'image du « timestamp », ce terme désigne un compteur numérique servant de référence temporelle. C'est une valeur de 64 bits, utilisée exclusivement sur les systèmes Windows et qui représente le nombre d'intervalles de 100 nanosecondes depuis le 1er janvier 1601 à minuit UTC.
Pour aller plus loin

FIREWALL
En français « Pare-feu ». Système protégeant le réseau local de l'entreprise contre les intrusions pouvant venir de l'extérieur (Internet). Ce système est un filtre, il peut permettre également de mettre en place des restrictions de connexion pour les machines de l'entreprise qui veulent se connecter sur certaine [illegible]

FIRMWARE
Micrologiciel en français, vient des mots anglo-saxon « software » (programme informatique) et « firm » (« ferme », état intermédiaire entre « soft » et « hard »), ou parfois par « logiciel système », « logiciel interne », « logiciel embarqué ». C'est un logiciel qui est intégré dans un composant matériel (« har [illegible]

FLASHAGE
Cette action permet d'effacer et de reprogrammer la mémoire d'un composant électronique. On s'en sert souvent pour mettre à jours le BIOS ou la mémoire EEPROM par exemple.

FLOOD
Matraquage en français, c'est une forme de « déni de service » consistant à envoyer une grande quantité de données inutiles dans un réseau (site web par exemple) provocant un ralentissement ou un crash (plantage) des machines du réseau.

FORENSIC
En français « informatique légale », elle désigne l'application de techniques ou de protocoles d'investigation numérique respectant les procédures légales afin de recueillir et d'apporter la preuve numérique. Elle regroupe donc l'ensemble des connaissances et méthodes qui permettent la conservation, la collecte et [illegible]

FLUX WEB
Un flux Web (ou « news feed ») est une technique de l'Internet pour transmettre des nouvelles ou des changements récents.

FRAMING
Vient du mot anglais « frame », cadre en français. Cette méthode consiste à incruster tout ou partie d'une autre page web ou site web dans un cadre de la page active de son propre site. Les FRAMES insérée ne laissent pas paraître leurs liens d'origine. Le FRAMING permet donc de constituer sans efforts et sans enga [illegible]
- Appropriation du travail et des efforts financiers d'autrui ;
- Contrefaçon de marque si un tel signe est reproduit ;
- Reproduction illicite d'œuvres protégées par droits d'auteur : textes, images, musique, vidéo, etc.
- Concurrence déloyale et parasitaire ;
- Détournement de clientèle ;
- Préjudice à l'image de marque (ternissement de l'image)…

FREAKING
Voir PHREAKING.

FREEWARE
Logiciel pouvant être échangé, copié sans perception de droits d'auteur. On dit aussi logiciel du domaine public.

FTP
(File Transfer Protocol) est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'administrer un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. [illegible]

G

GEEK
(Prononcez guik) stéréotype décrivant une personne passionnée, voire obsédée, par un domaine précis. Le plus souvent le terme « geek » est employé dans le domaine de l'informatique. Les geeks forment une communauté et leur passion ne se fait pas au détriment de leurs autres activités et ne joue pas vraiment sur le [illegible]

GET – POST (REQUÊTE)
Le protocole HTTP « client-serveur » utilise les commandes GET ou POST pour des requêtes sur un serveur. Une requête est une interrogation du serveur sur la ressource identifiée par l'URL qui suit le nom de la méthode. GET est la méthode la plus courante pour demander une ressource (afficher une page web). POST en [illegible]

GPRS
Le GPRS (General Packet Radio Service) offre un débit trois fois supérieur au GSM avec un maximum théorique de 170 kpbits/s. Le GPRS utilise les mêmes codages de données que le GSM et le même réseau radio, mais gagne en puissance grâce à deux nouvelles fonctions : d'abord le GPRS adapte les correcteurs d'erreurs [illegible]

GSM
GSM (Global System for Mobile communication) est un réseau radio cellulaire numérique.

H

HACKER
Ce terme est à l'origine un mot anglais signifiant « bricoleur – bidouilleur » . Il désigne une personne dont les connaissances techniques lui permettent de modifier, un objet ou un mécanisme, pour lui faire faire autre chose que ce pour quoi il a été initialement prévu. Mais il a de multiple signification en info [illegible]
- Black hat hacker, un hacker qui pénètre par effraction dans des systèmes ou des réseaux dans un objectif personnel, souvent un gain financier.
- White hat hacker, un hacker qui pénètre par effraction dans des systèmes ou des réseaux dans l'objectif d'aider les propriétaires du système à mieux le sécuriser.
- Grey hat hacker, un hacker hybride entre les chapeaux blancs et chapeaux noirs.
- Script kiddie, qui est pour l'opinion générale un hacker, souvent jeune, pénétrant par effraction dans des systèmes, généralement pour se vanter auprès de ses amis, en utilisant des programmes déjà prêts à l'emploi.

Pour les communautés underground, le script kiddie n'est pas un hacker mais un « lamer » (l'exact contraire, donc, un individu dénué de toute compétence en informatique).

HACKING
C'est l'action du hacker qui cherche à pénétrer un système pour y dérober des informations. A ce jour, le hacking regroupe un ensemble de techniques relevant de failles et vulnérabilités d'un élément ou d'un groupe d'éléments, matériels ou humains (social engineering). Les attaques informatiques à l'époque de Kevi [illegible]
De nos jours, la menace est moins virulente, mais beaucoup plus massive, notamment par l'augmentation croissante des « script kiddies ».

HACKTIVISME
Contraction de HACKER et ACTIVISME. Il infiltre les réseaux informatiques ou autre mettant ainsi son talent au service de ses convictions politiques. Il organise donc des opérations coup de poing technologique : piratage, détournement de serveurs, defacing de page d'accueil par des tracts…

HAMECONNAGE
Voir PHISHING.

HASH VALUE
Voir EMPREINTE NUMERIQUE.

HEBERGEUR
Un hébergeur Internet (ou hébergeur Web) est une entité ayant pour vocation de mettre à disposition des internautes un service d'hébergement, gratuit ou payant, fournissant ainsi un espace disque sur son serveur, afin de diffuser sur Internet des sites Web ou des pages personnelles. Il existe plusieurs types d'héb [illegible]
- *Hébergement mutualisé* : C'est l'hébergement de base d'un site web qui suffit souvent dans la plupart des cas, c'est une offre packagée et prête à l'emploi. On parle de mutualisation, car le site web partage les ressources d'un serveur avec d'autres sites web. Il existe de nombreuses offres d'hébergement offrant [illegible]
- *Hébergement dédié* : ce type d'hébergement est entièrement réservé à celui qui le loue. L'administrateur en est responsable, il choisit quels programmes et logiciels à installer. Cette solution demande du temps d'administration et des connaissances. Elle est réservée aux clients ayant une audience importante et [illegible]
- *Hébergements dédiés dits « managés », « infogérés »* : Le client dispose de son propre serveur mais les techniciens de l'hébergeur s'occupent de sa gestion système. Cette solution est parfaite si vous n'avez aucune connaissance technique sur son administration. Il suffit simplement de déposer son site. Ce type [illegible]

HIBERFIL.SYS
C'est un fichier système de Windows situé par défaut à la racine du disque système, utilisé pour stocker l'état de la mémoire vive lors d'une mise en veille prolongée (hibernation).

HOAX
Voir CANULAR.

HTML
HyperText Markup Language. Langage de description utilisé pour concevoir des documents hypertextes accessibles via un navigateur Internet.

HTTP
(Hypertext Transfert Protocol). C'est donc un protocole mis en œuvre pour le chargement des pages web. La méthode est une Commande spécifiant un type de requête, c'est-à-dire qu'elle demande au serveur d'effectuer une action. En général l'action concerne une ressource identifiée par l'URL qui suit le nom de la mét [illegible]

HUB
En anglais le mot HUB signifie « centre d'une roue » ou d'un cylindre. En informatique le HUB est utilisé pour désigner un concentrateur. C'est un appareil autorisant l'interconnexion entre plusieurs autres appareils, typiquement des ordinateurs, périphériques ou même d'autres commutateurs ou routeurs. Par exemple [illegible]

I

IEEE 802.3
C'est une norme pour les réseaux informatiques édictée par l'Institute of Electrical and Electronics Engineers (IEEE). Cette norme est généralement appelée ETHERNET.

I.E.F.
En anglais « Internet Evidence Finder » est une solution d'investigation numérique dédiée à la recherche de traces internet se trouvant aussi bien sur le disque dur que sur tout autre appareil numérique tel un téléphone ou une tablette. Conçu pour les enquêteurs spécialisés en cybercriminalité, il est aussi utili [illegible]

IFRAME (BALISE)
Iframe signifie « inline frame », en français « cadre en ligne », il s'insère dans le flot du contenu de la page. En claire cette balise est utilisée afin d'insérer dans une page HTML un autre document HTML pouvant venir d'un autre site web.

IMAP
(Internet Message Access Protocol). C'est un protocole utilisé par les serveurs de messagerie électronique, fonctionnant pour la réception. Il permet de laisser les mails sur le serveur dans le but de pouvoir les consulter de différents clients de messagerie ou en « webmail ». Il comporte des fonctionnalités a [illegible]

IMEI
International Mobile Equipment Identity. Identifiant des équipements mobiles, en particulier des téléphones portables. Chaque équipement a son propre numéro qui a la forme suivante : nnnnnn-nn-nnnnnn-n.

INCLUDE (FAILLE)
La faille « Include » est certainement la faille PHP la plus connue. Elle n'est pas liée à une vulnérabilité dans une fonction spéciale, mais est due (comme beaucoup de failles en PHP) à une erreur de programmation, en matière de sécurité, commise par un développeur. Pour aller plus loin, sa mise en œuvre touche [illegible]

INJECTION SQL (FAILLE)
C'est un type d'exploitation d'une faille de sécurité d'une application interagissant avec une base de données, en injectant une requête SQL non prévue par le systèmeet pouvant compromettre sa sécurité. Pour aller plus loin, sa mise en œuvre consiste à soumettre une requête SQL afin de contourner un élément de sé [illegible]
Par exemple, un attaquant peut envoyer une requête en utilisant l'identifiant « Toto » tout en injectantune requête SQL, sous forme de commentaire, pour le mot de passe associé. Le serveur répondra alors que l'identifiant « Toto » existe et validera l'entrée. Cette technique implique de savoir, auparavant, que le [illegible]

INODE
C'est la contraction de : Index et Node, en français « nœud d'index ». L'inode contient la totalité des informations sur le fichier, sauf le nom et sont tous de même taille. Les informations sont : le type de fichier, droits d'accès, nombre de liens, UID (User Identification), GID (Groupe Identificaton), taille, [illegible]

INTERNET
International Network. Internet est un réseau informatique, il fait communiquer tous les ordinateurs de la planète qui y sont connectés.

IP (VERSION4)
Numéro unique de la forme XXX.XXX.XXX.XXX (XXX étant un nombre entier compris entre 0 et 255) qui identifie chaque ordinateur connecté à Internet ou à tout autre réseau utilisant le protocole TCP/IP. Indispensable aux échanges d'informations entre les différentes machines, l'adresse IP peut être fixe,c'est-à-dire [illegible]
Enregistrée dans les fichiers log des serveurs visités, l'adresse IP permet généralement de remonter jusqu'à l'identité physique de l'internaute par le biais de son fournisseur d'accès, dans le cadre d'une procédure judiciaire.

IP (VERSION6)
Les adresses IP version4 sont saturées et devront être remplacé par sa version 6. En 2014, le déploiement d'IPv6 est encore limité, la proportion d'utilisateurs Internet en IPv6 étant estimée à 2%, et ce en dépit d'appels pressants à accélérer la migration adressés aux fournisseurs d'accès à Internet et aux fourni [illegible]

IPBX (OU PABX IP OU PBX IP)
Désigne un PABX utilisant le protocole internet IP que ce soit en interne sur le réseau local (LAN) ou le réseau étendu (WAN) afin d'acheminer les communications téléphonique d'une entreprise.

IRC
Internet Relay Chat. Système de conversation en temps réel sur Internet.

J

JAVASCRIPT
C'est un langage de programmation permettant l'amélioration d'une page web. Il peut être implémenté et intégré directement dans la page web, avec pour but d'exécuter des commandes sur le navigateur du poste client. C'est le navigateur web de l'internaute, et non pas le serveur web, qui prend en charge l'exécution [illegible]

K

KEYLOGGER
Programme permettant d'enregistrer dans un journal (un log) les séquences de touches frappées au clavier.

L

L.A.C.N.I.C.
Latin America and Caribbean Network Information Centre, gère le registre d'adressage IP du continent de l'Amérique latine.

LAN
Voir RÉSEAU L.A.N.

LOG
Version anglaise de journal, ou de « fichier journal ». Synonyme « logfile ». Ce terme est employé en informatique pour désigner un historique d'évènements.

M

MAC (ADRESSE)
Il s'agit de l'adresse physique d'un composant réseau (carte RJ45, dongle Wifi, FreeBox, routeur…). C'est une adresse unique permettant d'identifier un matériel sur le réseau. Une adresse MAC correspondra à une adresse IP le temps de la connexion.

MAIL
Voir COURRIEL.

MAIL-BOMBING
Le mail-bombing (bombarderie en français québécois) est une technique d'attaque visant à saturer une boîte aux lettres électronique par l'envoi en masse de messages quelconques par un programme automatisé.

MAIL DAEMON OU MAIL DELIVERY SYSTEM
Le MAIL DAEMON est un petit programme fonctionnant sur les serveurs de messagerie. Il est là pour envoyer automatiquement un courriel de retour lorsqu'un courriel n'a pu être remis à son destinataire.
Il se déclenche en général pour trois raisons :
- *USER UNKNOWN* : vous avez fait une erreur dans l'adresse du destinataire,
- *MAILBOX OVER QUOTA* : la boîte de votre destinataire est pleine,
- *DELIVERY TEMPORARILY SUSPENDED* : le serveur de messagerie est surchargé le courriel est mis dans une file d'attente pendant 6 à 8 heures.

MALWARE :
Ce terme anglo-saxon, utilisé depuis quelques années seulement, désigne toutes les familles de « logiciels malveillants » développés dans le but de nuire à unsystème informatique. Les plus connus sont les virus, les vers, les chevaux de Troie, les logiciels espions (« spyware »), les « rootkits », etc. Cliquez pou [illegible]
Il ne s'agit en aucun cas d'un nouveau type de menace.

MAN
Voir RÉSEAU M.A.N.

MBR
Le Master Boot Record ou zone d'amorçage en français est le nom donné au premier secteur adressable du disque dur. Le MBR vérifie s'il existe une partition active sur le disque et les tables de partitions. Une fois fait, il charge en mémoire le secteur de démarrage (boot) de la partition active, ce qui a pour but [illegible]

MÈME INTERNET
Le même internet est une iconographie persistante au sein d'une communauté virtuelle. Le même est moins présent sur l'internet francophone car il est souvent repris de l'anglais.

METADONNEE(S)
« Méta » vient du grec qui veut dire ce qui englobe un objet, une science. Donc une métadonnée est littéralement une donnée sur une donnée. En informatique elle sert à décrire une ressource numérique à savoir un document web, texte, photographique, sonore, etc.

MFT
(Master File Table) – Elément principal d'une partition NTFS du système de fichier de Windows. Elle contient l'ensemble de la liste des fichiers sur le disque dur et représente la structure de stockage des données de la partition.

MICROBLOG OU MICROBLOGUE
C'est un blog concis. Il permet de publier un courtarticle, bien plus court que dans un blog traditionnel. L'article peut contenir du multimédia et être diffusé en restreint à un groupe de personne. Son but est de diffuser en temps réel des informations rapidement et succinctement.
Le plus connu des « microblog » à ce jour est « TWITTER », qui fait parti du « WEB 2.0 ».

MYSQL
C'est un système de gestion de base de données. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web principalement) que par des professionnels. Sa
licence est généralement libre, mais pas exclusivement, libre. Il est une alternative à Oracle ou Microsoft SQL Server. Ce système se présente sous la forme d'un serveur (logiciel) dans lequel sont intégrées les bases de données à gérer. Cette gestion s'effectue soit par des instructions SQL (langage indépendant) [illegible]
d'administration appelée PHPMyAdmin. Pour être lues par un site Internet, les serveurs HTTP et MySQL doivent être « synchronisés ».

MODEM
MOdulateur DEModulateur, périphérique qui interprète et convertitles signaux d'une ligne téléphonique de type RTC (Réseau Téléphonique Commuté) rendant possible l'échange de données entre ordinateurs distants et connectés.

N

NERD
(Prononcez neurde) stéréotype de la culture populaire désignant une personne solitaire et intelligente, à la fois socialement handicapée (mais pas forcément isolée) et passionnée par des sujets liés à la science et aux techniques. Aujourd'hui, le terme nerd peut être employé chez les personnes qui se déclarent ge [illegible]
Ce terme est devenu plutôt péjoratif puisque l'on considère qu'un nerd est relativement asocial et polarisé sur ses centres d'intérêts ; auxquels il consacre plus de temps.

NEWSGROUP
La traduction veut dire FORUM sur internet. C'est un site Internet où n'importe qu'elle personne peut émettre des informations ou idées sur un sujet particulier.

NIBBLE
En informatique, il s'agit d'un agrégat de 4 bits, soit un demi-octet. Un nibble contenant 4 bits, il peut prendre seize (24) valeurs différentes et correspond donc à un seul chiffre hexadécimal, d'où son autre appellation de hex digit (ou hexit). Deux chiffres hexadécimaux formant un octet, ce dernier est souvent [illegible]
On trouve aussi les termes « semioctet » ou « quartet » dans les domaines du réseau ou des télécommunications. Dans certains langages, on peut également rencontrer tétrade du grec tetra (« quatre »).

NNTP
(Network News Transfer Protocol) est un protocole réseau utilisé en particulier par les forums de discussion Usenet. Les serveurs NNTP écoutent habituellement sur le port 119.

NOLIFE
Un nolife, littéralement « pas de vie » ou « sans vie », est une personne qui consacre une très grande part si ce n'est l'exclusivité de son temps à pratiquer sa passion voire son travail au détriment d'autres activités, d'une manière addictive, ce qui affecte fortement ses relations sociales et sentimentales. L [illegible]

NOMOPHOBIE
Ce mot vient de la contraction de l'expression anglaise « no mobile phobia ». Mot inventé lors d'une étude effectué par une organisation de recherche du Royaume-Uni. Cette étude montre que 53% des utilisateurs de mobile (76% chez les jeunes) en Grande-Bretagne sont anxieux quand ils ont perdu leur mobile, en court [illegible]

O

OPDS
(Open Publication Distribution System) est un protocole permettant de favoriser la diffusion de contenus sur des terminaux mobiles. Il est basé sur le format « ATOMXML » un dérivé plus élaboré du flux RSS. Le flux RSS désigne une famille de formats XML (Langage pour le web au même titre que le HTML) utilisés [illegible]
Un « ordiphone » doté d'une application de lecture peut être doté d'un logiciel compatible avec les catalogues OPDS.

ORACLE
C'est un système de gestion de base de données relationnel développé par Oracle Corporation. Il se base sur le format SQL des bases de données mais possède son propre langage ; appelé PL/SQL.

ORDIPHONE
Le « smartphone» en anglais est un téléphone mobile. La mobilité est devenu incontournable voir indispensable. Les fabricants ont du faire converger le maximum defonctionnalité.
Cet appareil doit donc lire des fichiers numériques, gérer des taches bureautiques, envoyer et/ou recevoir des courriels en temps réel, se connecter sur n'importequel réseau, aider à se déplacer géographiquement,etc.

P

P2P
Le « peer-to-peer » est un réseau d'échange et de partage de fichiers entre internautes. Le principe du « peer-topeer » (P2P) est de mettre directement en liaison un internaute avec un autre internaute qui possède un fichier convoité. Il existe 2 méthodes pour accomplir cette tâche :
- La méthode centralisée est basée sur un ou plusieurs serveurs qui possèdent la liste des fichiers partagés et qui orientent les internautes vers l'internaute possédant le fichier convoité.
- La méthode décentralisée utilise chaque internaute comme un mini-serveur et ne possède aucun serveur fixe. Cette méthode a l'avantage de répartir les responsabilités et d'éviter les actions en justice.

PABX
Private Branch eXchange. Autocommutateur privé utilisé dans les entreprises, assurant les communications internes et le lien avec le réseau téléphonique commuté global. Un autocommutateur est un central téléphonique.

PAGEFILE.SYS
C'est un fichier système de Windows situé par défaut à la racine du disque système. Ce fichier correspondant à une extension de la mémoire vive, également appelée fichier d'échange ou fichier swap, c'est une mémoire virtuelle présente sur le disque dur.

PAYPAL
C'est une plateforme de paiements sécurisés sur Internet, faisant parti du groupe eBay.com. Le titulaire d'un compte Paypal, dont l'enregistrement est gratuit et nécessite simplement une adresse e-mail valide, peut y lier sa carte de paiement. Il peut ainsi régler ses achats, sur des sites marchands ou auprès de p [illegible]

PERL
C'est un langage de programmation, créé par Larry Wall en 1985, reprenant principalement des fonctionnalités du langage C. Pour aller plus loin, il s'inspire des commandes de scripts sed, awk et shell.

PDA
Agenda électronique ou assistant numérique personnel.

PHARMING VOIR DNS PHARMING
Dévoiement en français, est une technique de piratage exploitant des vulnérabilités DNS (DNS PHARMING). Cette technique d'escroquerie consiste à rediriger le trafic Internet d'un site WEB vers un autre sitelui ressemblant afin de vous obliger à donner votre nom d'utilisateur (login) et votre mot de passe (passwo [illegible]

PHISHING (HAMECONNAGE OU FILOUTAGE)
Ce terme vient de l'expression anglaise Password Harvesting Fishingsoit en français pêche au mot de passe ou HAMECONNAGE. Technique utilisée par les escrocs en ligne, visant à usurper l'identité d'une personne ou d'une entité connue en faisant croire à la victime qu'elle s'adresse à un tiers de confiance. Le phi [illegible]

PHP
PHP Hypertext Processor : ou PHP, est un langage informatique interprété qui s'exécute du côté du serveur, et non du côté du client (votre ordinateur). Avec l'HTML, il est le langage le plus populaire pour les sites Internet. Son exécution nécessite l'installation d'un module spécifique qui doit être associé au [illegible]

PHPMYADMIN
(Prononcez « p h p mai admine »), parfois abrégé PMA, est une interface conviviale et gratuite réalisée en langage PHP pour faciliter la gestion des bases de données MySQL.

PHREAKING
Le mot anglais PHREAKING et la contraction des mots PHONE et FREAK (freak signifiant « marginal »). Le piratage téléphonique (ou phreaking en anglais) désigne le fait d'utiliser le réseau téléphonique d'une manière non prévue par l'opérateur afin par exemple de rester anonyme. On peut évoquer l'utilisation fraudul [illegible]

PROXY SERVER
En Français serveur mandataire est un serveur intermédiaire qui a pour fonction de relayer les requêtes d'utilisateurs et d'entretenir un cache des réponses. Lorsque la requête aboutit l'adresse IP de sa provenance n'est généralement pas celle du demandeur, mais celle du serveur proxy. C'est donc un bon moyen pour [illegible]

PODCAST
Le podcasting est un moyen de diffusion de fichiers multimédias (audio, vidéo ou autres) sur Internet appelés « podcasts ». Par l'entremise d'un abonnement aux flux RSS, le « podcasting » permet aux utilisateurs l'écoute ou le téléchargement automatique d'émissions audio ou vidéo pour les baladeurs numériques en [illegible]

POP3
(Post Office Protocol Version 3) est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique, donc la réception.Le port utilisé est le 110.

POP-UP
En anglais surgir. Le POP-UP désigne une « fenêtre surgissante » ou « fenêtre intruse » du navigateur internet. C'est une fenêtre secondaire qui s'ouvre sans avoir été sollicité par l'utilisateur lors de la consultation d'un site Web. Se sont en général des fenêtres publicitaires.

PORT
Porte unique destinée à l'échange entre deux ordinateurs pour un type d'application précis. Par exemple le port 80 est destiné par défaut aux échanges HTTP, c'est-à-dire pour la navigation internet, le port 21, lui, est prévu par défaut pour les échanges en FTP et 25 pour les e-mails sortants. Les ports sont numé [illegible]

R

RAM
La RAM (Random Access Memory) est la mémoire informatique d'un ordinateur.C'est l'endroit où l'ordinateur place les données pour son traitement.
Les caractéristiques de cette mémoire sont :
- sa rapidité d'accès (cette rapidité est essentielle pour fournir rapidement les données au processeur)
- sa volatilité (cette volatilité implique que les données sont perdues dès que l'ordinateur cesse d'être alimenté en électricité).

La "mémoire vive (RAM)" est généralement définie en opposition à la mémoire morte (ROM) : les données contenues dans la mémoire vive sont perdues lorsque l'alimentation électrique est coupée alors que la mémoire morte conserve ses données en absence d'alimentation électrique.
En résumé, il est donc utile de retenir, que plus l'ordinateur possède de mémoire RAM, et plus il pourra exécuter de programmes en même temps.

RAT
(Remote Administration Tool), littéralement outil d'administration distant. C'est un programme permettant la prise de contrôle totale et à distance d'un ordinateur depuis un autre ordinateur. Il existe de nombreux R.A.T. hostiles dédiés à la malveillance informatique. Ils sont constitués de deux parties : le « cli [illegible]
Ils sont implantés à l'insu de l'utilisateur, par le biais d'une faille humaine ou technique, notamment à partir des manières suivantes :
- Accès physique du pirate à l'ordinateur de la victime
- Ouverture d'un courrier piégé
- Téléchargement de fichiers vidéo, musicaux, ou images piégés
- Usage d'un trojan (Cheval de Troie)
- Usage d'une faille de sécurité système ou de sites piégés

Les RAT permettent au pirate d'observer l'activité sur le moniteur de l'ordinateur piraté comme s'il était devant, faire des captures d'écran, espionner et voir les victimes à travers leur caméra, relever les mots de passe à la volée stockés dans les navigateurs internet ou le système, enregistrés les communicati [illegible]

RECYCLE.BIN
C'est un fichier du système Windows associé à la Corbeille. Ce fichier est utilisé pour stocker temporairement les éléments de l'utilisateur avant qu'ils ne soient définitivement déclarés vacants pour le système. La Corbeille permet de garder un état temporaire des éléments avant une suppression permettant ainsi d [illegible]

REGISTRAR
Un registrar (bureau d'enregistrement en français) est une entité qui gère les noms de domaine. Les registrars sont accrédités par l'ICANN ou l'AFNIC qui les autorisent à créer des noms de domaines en ayant préalablement vérifiés qu'ils ne sont pas pris. Il est possible d'obtenir de nombreuses informations sur un [illegible]

REGISTRANT
Un registrant est une personne physique ou morale qui a enregistré un nom de domaine auprès d'un « Registrar ». Les informations sont des données déclaratives non vérifiées à l'exception de l'adresse du courriel qui doit être valide. Un contrat (entre le Registar et le Registrant) fixe le montant et la durée de j [illegible]

REMAILER
Ce sont des serveurs de mails qui font suivre votre message en enlevant dans les en-têtes de message toutes les informations qui permettent de remonter à l'expéditeur.

REMOTE DESKTOP PROTOCOL
C'est un protocole qui permet d'utiliser une application cliente spécifique à chaque système d'exploitation, permettant d'afficher, voire même de contrôler la session d'une autre machine qui exécute, elle, un serveur (TSE) compatible. Le serveur écoute par défaut le port TCP 3389. RealVNC écoute lui le port 5900. [illegible]

RESEAU : L.A.N.
(Local Area Network) est un réseau local appartenant à une même organisation, entreprise ou particulier. Il a une zone géographique restreinte.

RESEAU : M.A.N.
(Metropolitan Area Network) est une interconnexion de plusieurs L.A.N., qui peut englober une zone géographique plus étendue comme un campus ou une ville. L'interconnexion se fait alors par fibre optique.

RESEAU : W.A.N.
(Wide Area Network) est un réseau informatique couvrant une grande zone géographique, à l'échelle d'un pays, d'un continent voir de la planète, le plus grand WAN étant le réseau internet.

RESEAU SOCIAL OU SOCIAL NETWORK
C'est l'ensemble des identités sociales telles que des individus ou encore des organisations sociales reliées entre elles par des liens créés lors des interactions sociales. Cela se représente par une structure ou une forme dynamique d'un groupement social. Des réseaux sociaux peuvent être créés stratégiquement p [illegible]

RFID
De l'anglais Radio Frequency Identification qui désigne la RadioIdentification. Des radio-étiquettes contenant des éléments d'identification et de données complémentaires sont collés ou incorporés dans ou sur des objets, produits, voire même implantés dans des organismes vivants animaux ou corps humain. Exemple d' [illegible]

R.I.P.E. N.C.C.
Réseaux IP Européen – Network Coordination Centre, est un RIR(Registre Internet Régional) qui gère le registre d'adressage IP du continent Européen et du Moyen-Orient.

R.I.R.
Registre Internet Régional est un organisme qui alloue les blocs d'adressage I.P. dans sa zone géographique. Il existe aujourd'hui cinq R.I.R. : RIPE-NCC (Europe et Moyen-Orient), ARIN (Amérique du Nord), APNIC (Asie et Pacifique), LACNIC (Amérique latine et îles des Caraïbes) et AFriNIC (Afrique).

RNIS
RNIS ou Réseau Numérique à Intégration de Service, ISDN en anglais. Il permet de transporter les données numériques de l'ordinateur local à l'ordinateur distant sans emprunter aucun lien ou périphérique analogique intermédiaire tel que modem ou ligne téléphonique.

ROM
La ROM (Read-Only Memory), mémoire morte en français est la mémoire non volatile, c'est à dire une mémoire qui ne s'efface pas.
Les mémoires mortes sont utilisées, entre autres, pour stocker :
- les informations nécessaires au démarrage d'un ordinateur (BIOS, instructions de démarrage, microcode).
- des tables de constantes ou des tables de facteurs de conversion ;
- des jeux vidéo d'anciennes générations ; à cause de sa faible capacité de stockage, la mémoire mortea été remplacée par les CD-ROM et les DVD pour le stockage des jeux vidéo ;
- les équipements embarqués (relativement lents), pour contenir le programme de la partie numérique, en association avec une RAM dynamique pour traiter les données ;

ROUTEUR
Interface entre deux réseaux différents. On parle souvent de « routeur Internet », qui a pour but de relier le réseau local au réseau mondial. Cette pratique permet de mutualiser un accès Internet pour plusieurs postes.

ROOTKIT
C'est un programme malveillant dont le but est de garder le contrôle partiel ou total d'un système après une intrusion, tout en restant furtif. Le développement d'un rootkit s'effectue selon certaines contraintes : il doit s'exécuter avec des droits restreints et privilégier la furtivité, sans laisser trop de tra [illegible]

RTC
RTC ou Réseau Téléphonique Commuté est le réseau de téléphone fixe que tout le monde connait. Ce réseau d'abord conçu pour transmettre de la voix permet aussi de transporter des données.

RSS (FLUX)
RSS désigne une famille de formats XML utilisés pour la « syndication » de contenu Web. (La syndication est un mot anglais qui désigne la pratique consistant à vendre le droit de reproduire un contenu ou de diffuser un programme à plusieurs diffuseurs. Le système de la syndication a été créé par la presse écrite [illegible]
Trois formats peuvent être désignés par ces initiales :
- Rich Site Summary (RSS 0.91)
- RDF Site Summary (RSS 0.90 et 1.0)
- Really Simple Syndication (RSS 2.0)

Un flux RSS est donc un fichier dont le contenu est produit automatiquement (sauf cas exceptionnels) en fonction des mises à jour d'un site Web. Les flux RSS sont souvent utilisés par les sites d'actualité ou les blogs pour présenter les titres des dernières informations consultables en ligne.

RSSI
Responsable de la Sécurité des Systèmes d'Information (CISO en anglais) d'une organisation (entreprise, association ou institution). Personne responsable du maintien du niveau de sécurité des systèmes d'information. Il est chargé notamment des choix et des actions concernant : la sensibilisation des utilisateurs [illegible]

S

SCAM
Escroquerie pratiquée via le spam : vous recevez un message vous disant qu'une importante somme d'argent (des millions de dollars au minimum) est bloquée dans un pays riche, suite à une quelconque révolution dans un pays du tiers-monde. A vous d'envoyer de l'argent pour débloquer les fonds qui avaient été « mis à [illegible]

SCAN DE PORT
Voir BALAYAGE DE PORT.

SCRIPT
Liste de commandes ou d'instructions permettant l'automatisation d'une tâche.

SECTEUR
En informatique, il correspond à la plus petite unité physique de stockage sur un support de données numériques. Le support est donc divisé en bloc de secteur permettant l'enregistrement des données qui compose un fichier.

SERVEUR
C'est un ordinateur connecté au réseau mettant à disposition de ses utilisateurs (client) un ensemble de fichiers et d'applications. Il contribue à participer au mode de communication « client-serveur » entre des logiciels dit « client » qui envoient une requête à un logiciel dit « serveur » qui lui répond le tou [illegible]

SERVEUR DÉDIÉ VIRTUEL
C'est une méthode de partitionnement d'un serveur en plusieurs serveurs virtuels indépendant. Ces différents serveurs virtuels auront chacun les caractéristiques d'un serveur. Ils pourront fonctionner avec un système d'exploitation différent et démarrer indépendamment.

SHELL
C'est un interpréteur de commandes ; c'est à dire un programme faisant partie des composants de base d'un système d'exploitation. C'est le mode de contrôle fondamental d'un ordinateur. Ce dernier prend ses données d'entrées en ligne de commande, qui sont transmises à l'interpréteur en mode interactif. Son rôle est [illegible]
Une série de commandes précises peut être sauvegardée dans un fichier, que l'on appellera un script, ou plus précisément « Shell script ».

SIM
Sigle signifiant Subscriber Identity Module. Une carte SIM désigne la carte à puce qu'on loge dans son téléphone mobile afin qu'il puisse se connecter au réseau de l'opérateur mobile. Elle permet d'identifier personnellement l'abonné et contient des informations comme le numéro de téléphone et tout ce qui est re [illegible]

SLACK
Signifie en « forensics » la différence entre la taille du fichier logique et sa taille physique. Un secteur est la place standard que doit prend une données sur un disque dur et sa taille doit être de 512 octets. Donc si le fichier a une taille logique de 400 octets la différence avec la taille du secteur physiq [illegible]

SMARTPHONE
Voir ORDIPHONE.

SMS
Short Message Service, Service de messages courts en français est un service que peut offrir un système de communication sans fil, permettant aux usagers d'envoyer ou de recevoir des messages alphanumériques courts (autour de 160 caractères), qui s'affichent à l'écran de leur terminal mobile, généralement un télé [illegible]

SMTP
(Simple Mail Transfer Protocol) est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique, donc l'envoi. Le port utilisé est le 25.

SNIFFER
Élément matériel ou logiciel permettant de capturer à la volée les trames (paquets de données) circulant sur un réseau. Les informations peuvent être analysés pourdétecter des logins, des mots de passe, etc.

SOURCE
Code textuel (donc lisible par un être humain) à partir duquel sera généré une version exécutable du programme.

SOCIAL ENGINEERING
L'ingénierie sociale est la discipline consistant à obtenir un bien ou une information en exploitant la confiance mais parfois également l'ignorance ou la crédulité de tierces personnes. Il s'agira pour les personnes usant de ces méthodes d'exploiter le facteur humain, qui peut être considéré comme le maillon fai [illegible]
De nos jours, l'ingénierie sociale en informatique se heurte de plus en plus à l'éducation des utilisateurs. De plus en plus, les départements de gestion informatique fontcirculer un document décrivant les règles de sécurité de base : choisir un mot de passe long et ne se trouvant pas dans le dictionnaire, ne jama [illegible]

SOCIAL NETWORK :
Voir RÉSEAU SOCIAL.

SPAM
Usage abusif d'un système de messagerie électronique ou de traitement automatisé de données destiné à exposer délibérément et généralement de manière répétée tout ou partie de ses utilisateurs à des messages ou à des contenus non pertinents et non sollicités couramment appelés « spams », en faisant en sorte de l [illegible]
rapport avec le thème abordé.

SPOOFING
L'usurpation d'adresse IP (en anglais : IP address spoofing) est une technique de hacker consistant à utiliser l'adresse IP d'une machine, ou d'un équipement, afin d'en usurper l'identité. Elle permet de récupérer l'accès à des informations en se faisant passer pour la machine dont on « spoofe » l'adresse IP. De [illegible]

SPYWARE
Programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée des dits utilisateurs.

SSID
SSID est l'acronyme de Service Set IDentifier. C'est le nom donné à un réseau sans fil par un routeur wifi ou les modems des opérateurs Internet. Ce nom est fourni par l'opérateur mais peut être changé par l'utilisateur.

SSL
(Secure Socket Layer) maintenant appelé (Transport Layer Security) (TLS), est un protocole de sécurisation des échanges sur Internet, utilisé notamment pour les paiements sécurisés.

STAD
Abréviation de Système de Traitement Automatisé de Données.

STREAMING :
Le streaming, est la lecture en flux ou lecture en continu (aussi appelée lecture directe ou encore diffusion de flux continu), désigne un principe utilisé principalement pour l'envoi de contenu en « direct » (ou léger différé). Très utilisée sur Internet, elle permet la lecture d'un flux audio ou vidéo (c'est le [illegible]
nouvelles données.

SYNDICATION
La syndication est un mot anglais qui désigne la pratique consistant à vendre le droit de reproduire un contenu ou de diffuser un programme à plusieurs diffuseurs. Le système de la syndication a été créé par la presse écrite américaine, les syndicates vendant leur production (cartoons, comic-strips, chroniques, et [illegible]

SYSTEME D'EXPLOITATION (OS)
Programme fondamental permettant la gestion des différents éléments matériels de l'ordinateur et l'utilisation des logiciels.

SYSTEME VOLUME INFORMATION
C'est le nom de la banque de données où Windows XP et Windows Vista conserve son système pour la restauration des fichiers et les bases de données pour la restauration.

T

TCP/IP
Transmission Control Protocol /Internet Protocol. Protocole réseau utilisé dans de nombreuses entreprises et surtout sur Internet. C'est un protocole de remise fiable (contrairement à l'UDP) car il s'assure que le bon destinataire a bien reçu les données qui lui étaient destinées.

TIMESTAMP
En informatique, le « timestamp » désigne un compteur numérique servant de référence temporelle et représente le nombre de secondes écoulées depuis un instant deréférence. Le plus souvent l'origine choisie est le 1er janvier 1970 à minuit UTC ; instant qui marque le début de l'ère UNIX. Par exemple, le timestamp [illegible]

TOIP
Telephony over Internet Protocol, en français la téléphonie sur IP comprend tous les services de téléphonie à destination des utilisateurs finaux. (Voir aussi VoIP)

TOR
The Onion Router, en français « le routage en oignon ». C'est un logiciel libre qui permet, de manière anonyme, de transmettre des données sur un réseau basé sur le protocole « TCP » (Internet utilise ce protocole pour certains de ses échanges).
Le site https://www.torproject.org/about/overview.html.fr donne comme origine : « Tor a été initialement conçu, mis en œuvre et déployé en tant que troisième génération du projet routage en oignon du Naval Research Laboratory des États-Unis. Il a été développé avec l'US Navy, dans le but principal de protéger les [illegible]

TYPOSQUATTING
Forme de cyber-squatting se fondant principalement sur des erreurs typographiques des utilisateurs du web. Concrètement, il s'agit d'acheter tous les noms de domaines dont l'orthographe est proche de celle d'un domaine connu afin que l'utilisateur faisant une faute d'orthographe involontaire, soit dirigé vers le [illegible]

TWITTER
C'est une manière de communiquer en temps réel par des messages courts (140 caractères maximum qui équivaux à environ un à deux phrases). Un « Tweet », gazouillis en français, se dit d'un message envoyé. Cet outil de réseau social est ce que l'on appelle un microblog ou microblogue, mais à la différence d'un blog [illegible]
Donc on peut dire que « Twitter » est un réseau social asymétrique. L'asymétrie du réseau fait que chacun a accès aux informations de qui il veut sans que ces personnes soient forcément intéressées par les siennes.
Comprendre le langage utilisé avec quelques termes :
TO FOLLOW : suivre (s'abonner à l'actualité d'un membre de Twitter),
FOLLOWER : personne abonnée à un flux d'actualité,
TWEET : message public,
DM : message privé,
TWITTOS : membres de Twitter,
FOLLOWING : personne dont l'actualité est suivie par les followers,
HASHTAG : Un mot-clef précédé d'un # permet de regrouper les Tweets qui parle d'un même sujet.

U

UDP
(User Datagram Protocol) en français protocole de datagramme utilisateur, est un protocole de télécommunication utilisés pour la transmission de paquets de manière très simple entre deux entités sur le réseau. C'est un mode non fiable car il n'y a pas de moyen de vérifier si tous les paquets envoyés sont bien arr [illegible]

U.F.E.D.(UNIVERSAL FORENSIC EXTRACTION DEVICE)
Matériel associé à un logiciel permettant l'extraction et l'analyse des données enregistrées dans les téléphones cellulaires ou les tablettes. Ces données regroupent notamment les références techniques et, également, le contenu des calendriers, contacts, courriels, historiques Internet, journaux des appels, messag [illegible]

UPLOAD
En français, le mot téléchargement ne précise pas le sens dans lequel le transfert d'un fichier s'effectue. Or, en anglais, la distinction se fait. Il est dont appelé upload le téléchargement vers un ordinateur (téléchargement montant) ; c'est à dire lorsque j'envoie.

URL
Uniform Ressource Locator. C'est l'adresse d'une page Web. Elle se présente généralement sous la forme http://www.<Nomdusite>.<Domaine>.

USB
(Universal Serial Bus). C'est la version moderne du port « Série », il permet de connecter des périphériques type clavier, souris, appareil photo… à l'ordinateur. Le débit maximum est de 1.5 Mo/s, cette limite étant portée à 60 Mo/s avec l'USB2. Il en existe une version sans fildénommée « Bluetooth ».

USENET
C'est un système de réseau de forums inventé en 1979 (bien avant le World Wide Web (internet) en 1989). Vient de l'abréviation de « UNIX USER NETWORK », il permet de générer, stocker et récupérer des « articles » qui seront par la suite échangés entre les membres d'une communauté. Ces communautés sont des groupes [illegible]

V

VER (INFORMATIQUE) OU VIRUS
Le ver informatique est un logiciel malveillant qui exploite les différentes ressources d'un ordinateur hôte pour assurer sa reproduction (survie) et parvenir à son objectif malveillant (espionner, ouvrir des portes dérobées à des pirates, détruire, faire du DoS/DDoS…). Son activité a des effets indésirables visib [illegible]

VIRTUALISATION
La virtualisation est une technique consistant à simuler un ou plusieurs systèmes d'exploitation sur votre machine. Pour cela on utilise un logiciel spécifique comme VMWARE ou VIRTUALBOX.

VOIP
Voice over Internet Protocol, en français la voix sur IP est le transport d'un signal audio encapsulé dans un protocole IP. Il permet donc de téléphoner sur toutréseau utilisant le protocole TCP/IP.

VLAN
Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, c [illegible]

VMWARE
VMware est un logiciel de virtualisation. Il permet de simuler, de virtualiser tout un système et de le contenir dans un fichier unique. Il a donné son nom par extension à la gamme des programmes de virtualisation. VMware est capable de créer un environnement clos, contenu dans un fichier sur un ordinateur, dans l [illegible]
C'est à dire que l'on peut avec cette configuration, accéder de manière distante et sécurisée, à un système contenu dans une distribution VMware, et exécuter des requêtes, en laissant un minimum de traces des actions réalisées, cela contenu dans un fichier unique sur l'ordinateur du mis en cause.

VNC
Virtual Network Computing est un logiciel ouvert pour se connecter à un ordinateur distant. Il permet d'afficher sur votre écran l'écran d'un autre ordinateur et d'utiliser votre souris et votre clavier afin de contrôler à distance les autres PC connectés (via le réseau). Il permet donc de travailler sur un ordin [illegible]

VPN
Virtual Private Network , en français le réseau privé virtuel, permet de transmettre des données sécurisées en utilisant un protocole de « tunnelisation » (en anglais tunneling). Ce tunnel permet donc de faire circuler les informations de façons cryptées d'un bout à l'autredu tunnel. Il existe donc le VPN d'accès, [illegible]
Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas :
- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le Vpn auquel cas il établit directement la communication demanière cryptée vers le réseau de l'entreprise.

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuv [illegible]
L'extranet VPN permet à l'entreprise d'utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

W

WARDRIVING
De l'anglais « war » : guerre et « driving » : en conduisant, est une méthode qui consiste à balayer (scanner) les réseaux sans fil (Wifi) à l'aide d'un ordinateur portable ou d'un PDA. L'objectif de cette pratique de pénétrer sans autorisation dans ces réseaux pour obtenir librement et anonymement un accès à inte [illegible]
Pour la petite histoire, à la base les pirates utilisaient un moyen de transport, en raison de la rareté de ce type de réseau ; ce qui explique la notion de « driving ». Letemps passant, ils se sont multipliés et le déplacement des pirates n'est plus vraiment nécessaire. Certains pirates utilisaient même une sym [illegible]

WEB (OU WEB 1.0)
Par abus de langage, désigne « l'espace documentaire » de l'Internet, essentiellement composé de documents de type « texte » agrémentés d'une dose de multimédia (photos, et parfois sons ou vidéos). Ces documents utilisent la technologie de l'hypertexte.

WEB 2.0
Désigne l'évolution du WEB 1.0, qui lie non plus des pages entre elles mais aussi les personnes entre elles. Au départ cela se faisait par le courrier électronique puis la généralisation du phénomène a amené l'interconnexion avec les blogs, les forums de discussion, les réseaux sociaux…

WEB 3.0
Cette expression n'est pas encore bien définie. Elle est donc la prochaine étape de l'évolution du WEB 2.0 comme l'internet des objets, donc la rencontre du monde virtuel avec le monde réel. Par exemple l'association des étiquettes munies de codes, de puces RFID ou d'URL sot sur des objets réels ou des lieux [illegible]

WEBMAIL
Service de courriel accessible en ligne. Un webmail est une application web dotée d'une interface graphique qui permet de composer, d'envoyer, de recevoir et de lire des courriels dans une fenêtre d'un navigateur Internet.

WEP
Le Wired Equivalent Privacy (abrégé WEP) est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique. Cependant, plusieurs faiblesses graves ont été identifiées [illegible]

WPA
Wi-Fi Protected Access (WPA et WPA2) est un mécanisme pour sécuriser les réseaux sans-fil de type Wi-Fi. Il a été créé en réponse aux nombreuses et sévères faiblesses du WEP. Le WPA respecte la majorité de la norme IEEE 802.11i et a été prévu comme une solution intermédiaire pour remplacer le WEP.
Le WPA a été conçu pour fonctionner, après mise à jour de leur micro-logiciel, avec toutes les cartes Wifi, mais pas nécessairement avec la première génération des points d'accès Wifi. WPA2 quant à lui respecte la norme entière, mais ne peut pas être implémenté sur les matériels anciens.
Les deux mécanismes fournissent une bonne sécurité,si l'on respecte deux points importants :
- L'utilisateur doit encore souvent faire le choix explicite d'activer WPA ou WPA2 en remplacement du WEP, car le WEP reste habituellement le choix de chiffrement par défaut sur la plupart des équipements.
- Et lorsque le mode Personal (le choix le plus probable pour les individuels et les PME) est utilisé, une phrase secrète plus longue que les classiques mots de passe de 6 à 8 caractères utilisés par les utilisateursest nécessaire pour assurer une sécurité complète.

WIFI
(Wireless Fidelity). Technologie permettant de créer des réseaux locaux Ethernet sans fil.

WHOIS
Whois (contraction de l'anglais who is ?, signifiant littéralement qui est-ce ?) est un service de recherche fourni par les registres Internet, par exemple les Registres Internet régionaux (RIR) ou bien les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine. [illegible]

X

XSS
Voir CROSS SITE SCRIPTING.

Z

[illegible]

[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"]

Original de l'article mis en page : Lexique – La préfecture de Police

---

Ne pas avertir son employeur de propos injurieux sur Facebook peut vite devenir une faute grave | Denis JACOPINI

Ne pas avertir son employeur de propos injurieux sur Facebook peut vite devenir une #faute grave

La cour d'appel de Lyon a confirmé le mois dernier le licenciement d'une salariée accusée d'avoir tenu sur Facebook des propos dégradants et injurieux à l'égard de ses collègues de travail. L'employeur n'a pourtant pas réussi à prouver que la personne mise en cause était bien l'auteur des messages délivrés sur un groupe spécialement créé à cet effet. Explications.

Travaillant en tant que sellière maroquinière depuis 2002 chez Hermès, Madame X est licenciée en décembre 2011 pour faute grave. C'est-à-dire sans préavis ni aucune indemnité. Il faut dire que les reproches formulés par son employeur sont relativement sérieux.

La salariée est en effet accusée d'avoir ouvert en octobre 2011 un groupe Facebook intitulé « Les potins d'Hermès », sur lequel étaient relatées des « situations tenant à la vie privée de certains collaborateurs nommément désignés », « sous forme de messages et anecdotes ». C'est suite à des remontées internes que la direction a eu vent de ces commentaires jugés « profondément dégradants et injurieux » à l'égard des employés concernés, ce qui a poussé les responsables de l'entreprise à chercher à remonter jusqu'à leur auteur.

Problème : l'administrateur de ce groupe dispose d'un compte Facebook au nom de « Jules César ». Autrement dit, il s'agit d'un beau pseudonyme… Après enquête, l'employeur affirme que l'adresse IP de l'auteur de ces messages correspond à celle du domicile de Madame X. Dans un premier temps, la salariée reconnaît avoir eu connaissance de ce groupe, tout en niant en être à l'origine. Mais dans un second temps, elle finit par admettre que le compte « Jules César » et le groupe « Les potins d'Hermès » ont bien été crées depuis son ordinateur, mais par sa sœur…

« Même dans le cas où les déclarations de votre soeur (par ailleurs très limitées quant à son hypothétique implication personnelle) [seraient] avérées, et dans la mesure où vous nous avez déclaré avoir eu connaissance de la création de la page et de son contenu dès sa mise en ligne, vous auriez dû à tout le moins nous alerter au sujet d'une telle initiative dont la teneur et la portée ne pouvaient rester sans conséquence vis-à-vis de l'entreprise et de ses collaborateurs » retient ainsi l'employeur dans sa lettre de licenciement.

Impossible d'identifier le créateur du groupe

Sauf que l'ex-salariée estime avoir été remerciée à tort. Elle a donc tout d'abord saisi le conseil des prud'hommes de Lyon, lequel a confirmé le licenciement pour faute grave en novembre 2013. Madame X a ensuite saisi la cour d'appel de Lyon, qui a justement rendu sa décision le 20 octobre dernier.

Les magistrats se sont intéressés en particulier aux adresses IP fournies par Hermès. Ils ont cependant constaté que la connexion ayant servi à créer le profil Jules César et à alimenter « la plupart » des messages litigieux correspondait en fait à « une adresse IP algérienne dont l'employeur n'a pu identifier le titulaire ». En clair, il était impossible de prouver en l'état qu'il s'agissait de Madame X ou même de sa soeur.

Mais cela n'a pas empêché la cour d'appel de considérer qu'il y avait malgré tout eu faute grave de la part de la salariée. Cette faute ? Savoir que le groupe « Les potins d'Hermès » existait et n'avoir rien signalé. La décision, que nous avons pu consulter, retient en ce sens que « la faute commise par Mme X en n'alertant pas sa direction sur la création de ce groupe de discussion alors qu'à partir de son propre ordinateur étaient mis en ligne des propos déshonorants pour ses collègues de travail (…) est d'une gravité suffisante pour rendre impossible le maintien de cette salariée dans l'entreprise pendant la durée limitée du préavis ».

La cour d'appel n'a donc pas donné suite aux demandes de l'ex-salariée, qui réclamait plus de 40 000 euros d'indemnités.

La décision de la cour d'appel de Lyon évoquée dans l'article ci-dessus

Quelques articles sélectionnés par nos Experts :

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« *Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services.* ».

Source : http://www.nextinpact.com/news/91031-propos-injurieux-sur-facebook-ne-pas-avertir-son-employeur-peut-etre-faute-grave.htm

Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

2 SOLUTIONS POUR SE METTRE EN CONFORMITÉ AVEC LE RGPD

1.

Vous apprenez à vous mettre en conformité avec le RGPD en suivant une formation (ci-dessous) ;

2.

Vous faites appel à un expert / formateur qui vous accompagne dans votre mise en conformité avec le RGPD de votre établissement (Consultez notre page « Services d'accompagnement à la mise en conformité avec le RGPD »).

DÉSIGNATION N° DPO-19045

Datadock Organisme validé et référencé

Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique **spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel)**, consultant depuis 1996 et formateur depuis 1998. J'ai bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi aisé d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Pour cela, j'ai créé 3 niveaux de formation.

1. Une formation d'une journée pour les indépendants, TPE et les PME « **Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer** ». Cette formation a pour objectif de vous faire découvrir l'essentiel de ce règlement Européen, de vous apprendre les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions ;
2. Une formation de deux jours pour les DPO « **Je veux devenir le Délégué à la Protection des Données de mon établissement** ». Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement ;
3. Une formation sur 4 jours pour les consultants « **J'accompagne mes clients dans leur mise en conformité avec le RGPD** ». Vous êtes une société d'Informatique, un cabinet d'avocat, un cabinet d'expertise comptable et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation est composée de 2 jours de théorie et 2 jours de pratique dont 1 dans l'établissement de votre choix (le votre ou celui d'un client). Suivez LA formation qui vous apportera la plus grande autonomie avec le RGPD de tout notre catalogue.

et des services sur mesure.

1. Vous souhaitez tout faire -> Nous vous apprendrons à mettre votre établissement en conformité. La plupart du temps, le contenu de ces formations est personnalisé et adapté à vos besoins spécifiques ;
2. Vous ne savez pas par où commencer -> Nous ferons l'état des lieux, mettrons en place le registre puis nous vous apprendrons à maintenir la conformité des traitements ;
3. Vous ne souhaitez rien faire -> Nous nous occuperons de tout.

Plus d'information sur nos services d'accompagnement
à la mise en conformité avec le RGPD ici

Formation pour TPE/PME « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer » : 1 jour
(Découvrez et comprenez la démarche de mise en conformité)

Découvrez l'essentiel du RGPD, apprenez les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions.
Consultez les dates de nos prochaines formations
« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours
(Mettez en place une démarche de mise en conformité RGPD)

Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement.
Consultez les dates de nos prochaines formations
« Je veux devenir le Délégué à la Protection des Données de mon établissement »

Formation pour consultants « J'accompagne mes clients dans leur mise en conformité avec le RGPD » : 3 jours + 1 jour dans votre établissement
(C'est le moment ou jamais de vendre des services autour du RGPD)

Enfin, si votre objectif est avant tout de développer l'activité de mise en conformité avec le RGPD afin de vendre cette prestation auprès de vos clients, cette formation est faite sur-mesure pour vous en vous apportant l'ensemble des mesures et des cas qu'il est nécessaire de maîtriser pour que vos clients soient mis sur le chemin de la mise en conformité. Vous êtes une société d'Informatique, un cabinet d'avocat, un cabinet d'expertise comptable, un consultant et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation se passe sur 3 jours en groupe plus une journée supplémentaire en individuel pour superviser la mise en place du RGPD dans votre établissement ou chez un de vos clients (frais liés au déplacement dans cet établissement en sus). Suivez LA formation qui vous apportera la plus grande autonomie dans la mise en conformité de tout notre catalogue.
Consultez les dates de nos prochaines formations
« J'accompagne mes clients dans leur mise en conformité avec le RGPD »

Formation RGPD « Mise en conformité RGPD sur mesure » (pour TPE/PME)
(Pour ceux qui souhaitent une formation ou un accompagnement personnalisé dans la mise en conformité RGPD)

Que ayez bientôt ou déjà désigné « Délégué à la Protection des Données » ou « DPO » dans votre établissement, si vous souhaitez que nous établissions un programme de formation personnalisé dans son contenu ou dans son organisation, nous nous ferons un plaisir d'étudier votre demande et d'élaborer une proposition adaptée à vos besoins.

Accompagnement à la mise en conformité RGPD de mon établissement

Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit RGPD) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGPD) selon 3 phases principales :

1. « Analyse du contexte » en vue d'établir la liste des traitements et les mesures correctives à adopter ;
2. « Mise en place de la conformité RGPD » avec amélioration des traitements en vue de les rendre acceptables ou conformes. Ceci inclue dans bien des cas l'analyse de risque ;
3. « Suivi de l'évolution des traitements » en fonction de l'évolution du contexte juridique relatif à la protection des Données à Caractère Personnel et des risques Cyber. Ce suivi a pour principal intérêt de maintenir votre conformité avec le RGPD dans le temps.

Pour chacune des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaitez :

- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Faire » ;
- ou « Nous laisser faire ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement.

N'hésitez pas à contacter notre équipe.

Intéressé pour assister à une de nos sessions de formation en France, choisissez la ville qui vous intéresse. Vous souhaitiez que nous nous déplacions au sein de votre établissement pour une formation ou pour un accompagnement individuel, indiquez-le dans les commentaires.

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :

☐ la formation « Comprendre le RGPD » : 1 jour
☐ la formation « Je veux devenir Délégué à la Protection des Données » 2 jours
☐ la formation « Je mets en conformité mon établissement » 3+1 jours
☐ la formation « Mise en conformité RGPD sur mesure »
☐ un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs place(s) à la formation :

Formation pour TPE/PME : **« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : **« Je veux devenir le Délégué à la Protection des Données de mon établissement »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : **« J'accompagne mes clients dans leur mise en conformité avec le RGPD »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

☐Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte sera remboursé en intégralité dans les 5 jours (les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

LE FORMATEUR : Denis JACOPINI

Denis JACOPINI est Expert de Justice en informatique spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel). Il est diplômé en Cybercriminalité, e, Droit de l'Expertise Judiciaire et est Certifié en Gestion des Risques des Systèmes d' Information. IL est formateur depuis 1998 et consultant depuis 1996, il 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, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD à tout public.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

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

Datadock — Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

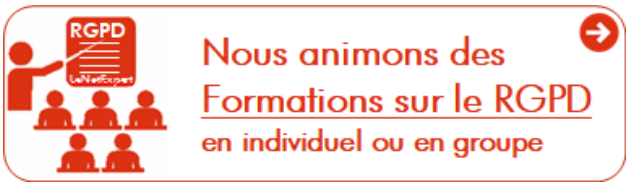
Contactez-nous

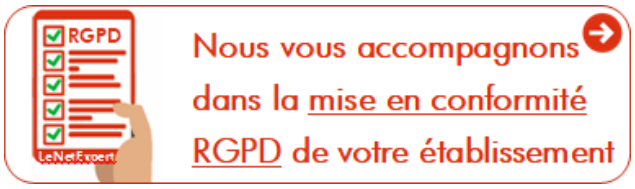
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

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

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

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

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

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

Info pratique : Attitude à adopter en cas de réception d'un e-mail étrange voire douteux
Vous recevez un e-mail étrange voire douteux, vous craignez être victime d'une arnaque ? Apprenez à les identifier et adoptez une attitude visant à contribuer à la destruction de ces réseaux.

Les meilleurs conseils pour choisir vos mots de passe | Denis JACOPINI

A l'occasion de la Journée du Mot de Passe, les meilleurs conseils aux utilisateurs pour éviter que leurs codes secrets ne soient découverts.

Le 5 mai était la Journée Mondiale du Mot de Passe. Une idée marketing lancée par des éditeurs de solution de sécurité informatique. Pour marquer cette date d'une pierre blanche, plusieurs éditeurs ont analysé les habitudes des utilisateurs. Avast Software par exemple propose des recommandations pour créer et protéger des mots de passe indéchiffrables.

Créer des mots de passe fiables et les modifier fréquemment
Une actualité ponctuée d'histoires comme celles de la faille d'Ashley Madison, le site de rencontres extra-conjugales, démontre que les gens n'utilisent pas correctement leurs mots de passe. Les utilisateurs ne créent pas de codes assez fiables et il est certain qu'ils ne les changent pas régulièrement – même face au risque de voir leurs données sensibles et leurs potentielles frasques exposées, ou leur mariage brisé. Les utilisateurs créent des mots de passe facilement déchiffrables souvent par manque d'information ou par paresse, en témoigne la liste des codes les plus souvent utilisés compilée par les chercheurs.

Dans le top 10 :
1. 123456
2. 123456789
3. password
4. 101
5. 12345678
6. 12345
7. Password1
8. qwerty
9. 1234
10. 111111

Cette liste comprend les mots de passe les plus simples, tels que 123456, password, et qwerty. D'autres se retrouvent plus bas dans la liste comme iloveyou (#19) ou trustno1 (#57) – une ironie pour un code figurant dans la liste des mots de passe les plus populaires. « ***Certains pensent qu'une liste de mots de passe seuls qui fuite en ligne n'est pas un problème – cependant, environ 50 % de ces mots de passe étaient associés à une adresse mail,*** déclare le chercheur d'Avast Michal Salat. ***Nous savons que les gens utilisent les mêmes combinaisons de mails et de mots de passe pour différents comptes. C'est pourquoi si un hacker connait le mot de passe de votre profil Ashley Madison, il connaitra également celui de votre Facebook, Amazon, eBay, etc.*** »

Comment créer des mots de passe fiables ?
Il n'y a pas de meilleure occasion que le 5 mai pour commencer à changer ses habitudes et protéger ses codes. Voici quelques conseils pour garder un mot de passe fiable et sécurisé. Je vais être honnete avec vous, si vous ne prenez pas 5 minutes pour réfléchir à votre sécurité et à la bonne gestion de vos précieux, passez votre chemin !

Domus tutissimum cuique refugium atque receptaculum sit

· Créer des mots de passe longs et complexes. Il suffit de reprendre une phrase d'un livre que vous aimez. N'oubliez pas d'y placer quelques chiffres, majuscules et signes de ponctuations.
· Utiliser un mot de passe différent pour chaque compte. Lors de les conférences, je fais sortir les clés des participants. Une clé pour chaque porte (voiture, boite aux lettres, maison, bureau…). En informatique, il faut la même régle pour ses mots de passe.
· Ne pas partager ses mots de passe. C'est peut-être une proposition idiote au premier abord, mais combien de fois, lors d'ateliers que je propose dans les écoles, j'entends le public m'expliquer avoir partager avec son ami, son voisin… sa clé wifi !
· Changer ses mots de passe régulièrement. Pour mon cas, il change tous les 35 jours. Je ne suis pas à l'abris du vol d'une base de données dans les boutiques, sites… que j'utilise.
· Utiliser un gestionnaire de mot de passe pour mémoriser ses mots de passe ? Je suis totalement contre. Il en existe beaucoup. Mais faire confiance à un outil dont on ne maîtrise ni le code, ni la sécurité, me parait dangereux. Beaucoup d'utilisateurs y trouvent un confort. L'ensemble de vos mots de passe sont regroupés dans une solution informatique qui chiffre les données. Un seul mot de passe est requis pour utiliser n'importe quel compte sauvegardé. Bref, vaut mieux ne pas perdre ce précieux cerbére !

· Verrouiller son matériel avec un mot de passe. Les systèmes existent. utilisez les. Je croise bien trop d'ordinateur s'ouvrant d'une simple pression sur la touche « Entrée ».
· Activer la double-authentification ou l'authentification forte. Indispensable aide. Téléphone portable, sites Internet, Facebook, Twitter… La double authentification renforce l'accès à vos espaces. En cas de perte, vol, piratage de votre précieux. Sans la double authentification, impossible d'accèder à vos données.

De son côté TeamViewer rappele aussi qu'il est déconseillé de fournir des informations personnelles identifiables : Utiliser plusieurs mots de passe forts peut impliquer quelques difficultés de mémorisation. Aussi, afin de s'en souvenir plus facilement, beaucoup d'utilisateurs emploient en guise de mot de passe des noms et des dates qui ont une signification personnelle. Les cyber-délinquants peuvent cependant exploiter des informations accessibles publiquement et des comptes de réseaux sociaux pour trouver ces informations et s'en servir pour deviner les mots de passe… [Lire la suite]

D'autres bons conseils pour gérer vos mots de passe sur disponibles le site de l'ANSSI ou de la CNIL.

[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 : *Générer un mot de passe indéchiffrable, possible ? –*

Les PME face à la cybercriminalité – Quelques règles de bon sens… | Denis JACOPINI

Face à l'« industrialisation » de la cybercriminalité, aucune entreprise n'est à l'abri, pas même les plus petites. Il est désormais indispensable de s'y préparer pour éviter des déconvenues qui peuvent se révéler très coûteuses.

De plus en plus variées, les techniques des cybercriminels s'industrialisent.
Un montant impressionnant : 445 milliards de dollars, soit 327 milliards d'euros, c'est le coût annuel de la cybercriminalité et de l'espionnage économique au niveau mondial, selon le Center for Strategic and International Studies (CSIS). Et il n'a sans doute pas fini de croître. « La cybercriminalité ne cesse de se développer et les attaques sont de plus en plus variées et sophistiquées, touchant toutes les entreprises, quelle que soit leur taille », assure Paul-Henri Huckel, consultant au sein du cabinet de conseil en stratégie des systèmes d'information et de la cybersécurité Lexsi.

Virus bancaire permettant d'effectuer des virements frauduleux ; destruction de sites Web d'entreprises d'e-commerce ; vol de données revendues à un concurrent ; « ransomware », autrement dit cryptage de toutes les données d'une entreprise « libérables » après versement d'une rançon… les techniques des cybercriminels s'industrialisent.

Le courrier électronique, maillon faible du système
« La première erreur est de penser que l'on est à l'abri, parce que l'on est petit », prévient Paul-Henri Huckel. Selon un rapport publié en avril 2014 par l'éditeur de logiciels Symantec, 30 % des attaques ciblées visent les PME. « Les dirigeants de petites entreprises ne sont pas suffisamment sensibilisés. Certaines sociétés n'ont même pas mis en place de système de sauvegarde de leurs données. Or, leur perte peut, dans certains cas, entraîner la fermeture de l'entreprise », remarque aussi Frédéric Desclos, responsable de l'Echangeur PME, espace de la chambre de commerce et d'industrie Paris Ile-de-France consacré à la sensibilisation et à la formation aux technologies de l'information des petites et moyennes entreprises.
Face à ce risque croissant de cyberattaque, sécuriser son système d'information est indispensable. Le courrier électronique est le maillon faible du système : selon Symantec, un message électronique sur 392 contiendrait une attaque de « phishing », ces faux courriers officiels destinés à détourner les coordonnées bancaires.

Les mots de passe doivent être modifiés au moins tous les six mois
« Il est indispensable de sensibiliser les salariés à cet aspect, ainsi qu'au caractère critique des mots de passe qui doivent être modifiés régulièrement, au moins tous les six mois », remarque Frédéric Desclos. Ce qui n'empêche pas, par ailleurs, de sécuriser au maximum son système d'information par le biais d'antivirus, d'anti-spam et de firewalls efficaces. « Un plan de sauvegarde des données est également indispensable », complète Paul-Henri Huckel. Une procédure qui n'est pas forcément coûteuse. Il suffit par exemple au dirigeant de l'entreprise de quitter chaque soir son bureau avec sa sauvegarde sous le bras…

[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 : Jean-Marc Engelhard
http://www.leparisien.fr/economie/les-pme-face-a-la-cybercriminalite-15-09-2014-4136531.php

Comment protéger son site internet des pirates informatiques ?

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

Il n’y a rien de plus stressant que de se faire hacker ou pirater un compte. Cependant, les criminels virtuels ne s’attaquent pas seulement à votre identité, ils prennent votre argent ou même la source de vos revenus. Ici, cette source ce sont les commerces en ligne et les sites web de vente. Que faire pour y remédier ?

La première précaution quand il s’agit de se protéger contre le piratage ? Mettre un plug-in de sécurité sur votre CMS. La deuxième précaution consiste à changer les droits de vos fichiers. Néanmoins, cette option n’est pas sans difficulté, car certains hébergeurs refusent ce genre de modification. Une autre astuce serait de sauvegarder régulièrement vos données pour pouvoir l’effacer en cas de piratages afin de ne laisser aucune trace de ce dernier. Dans le cas contraire, il est fort possible que vous perdiez votre crédibilité auprès de vos internautes et clients.
Pour conclure, le piratage est un sujet et un fléau courant actuellement, qu’il est toutefois possible de contrôler. Par contre, les pirates ne s’arrêtent jamais. Ils peuvent revenir pour hacker votre site ou votre serveur : une mise à jour constante de votre système de protection est donc de mise…[lire la suite]

Conseil de Denis JACOPINI :

Nous remarquons de nombreux piratages causés par une relation physique ou logique avec votre Système Informatique d’entreprise. Une autre recommandation consiste en plus de les héberger sur des machines différentes, à utiliser des identifiants et des mots de passe évidemment complexes mais aussi différents non seulement pour chacun de services du site Internet mais surtout des autres éléments de votre Système Informatique.

[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 : *Piratage informatique : comment protéger son site internet ?*

Les grands principes de la cryptologie et du chiffrement

Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage. À l'occasion du mois européen de la cybersécurité, la CNIL vous explique ce que c'est et à quoi ça sert.

Étymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός) . Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie).
La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'**authenticité** d'un message (qui a envoyé ce message ?) ou encore assurer son **intégrité** (est-ce qu'il a été modifié ?).
Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.
Pour expliquer la cryptologie, nous utiliserons dans nos exemples les personnages traditionnels en cryptographie : Alice et Bob.
Pour découvrir les grandes phases de l'histoire de la cryptologie, rendez-vous sur le webdocumentaire réalisé par l'ANSSI.

Pourquoi la cryptologie existe-t-elle ?

1.

Pour assurer l'intégrité du message : le hachage

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une « **fonction de hachage** » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2» ou « SHA256 ».
Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès (voir « **Pour assurer la confidentialité du message** »), et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.
Le hachage, pour quoi faire ?
Pour sauvegarder vos photos sur votre espace d'hébergement (de type « cloud » par exemple) et vérifier que votre téléchargement s'est bien déroulé ?
Pour sychroniser vos dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés ?

Il existe aussi des « **fonctions de hachage à clé** » qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour qu'Alice et Bob calculent la même empreinte, ils doivent tous les deux utiliser la même clé.
C'est parmi ces fonctions de hachage à clé que l'on trouve celles utilisées pour stocker les mots de passe de façon sécurisée.
Le hachage à clé, pour quoi faire ?
Votre service préféré reconnait votre mot de passe quand vous vous connectez ?
Vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire ?

2.

Pour assurer l'authenticité du message : la signature

Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la « **signature** » – numérique – permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « clé publique ». Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

La signature numérique, pour quoi faire ?
Vous voulez garantir être l'émetteur d'un courriel ?
Vous voulez vous assurer qu'une information provient d'une source sûre ?
Pour pouvoir signer, Alice doit se munir d'une paire de clés :
• l'une, dite « publique », qui peut être accessible à tous et en particulier à Bob qui est le destinataire des messages qu'envoie Alice ;
• l'autre, dite « privée », qui ne doit être connue que d'Alice.
En pratique, Alice génère sa signature avec sa clé privée qui n'est connue que d'elle. N'importe quelle personne ayant accès à la clé publique d'Alice, dont Bob, peut vérifier la signature sans échanger de secret.

3.

Pour assurer la confidentialité du message : le chiffrement

Le chiffrement d'un message permet justement de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.
Le chiffrement, pour quoi faire ?
Vous voulez vous assurer que seul le destinataire ait accès au message ?
Vous souhaitez envoyer ces informations sous enveloppe numérique et non lisible par tous comme sur une carte postale ?
Il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.
Le **chiffrement symétrique** permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.
Le **chiffrement asymétrique** suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.
Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire.
Autre point fort : plus besoin de partager une même clé secrète ! Le chiffrement asymétrique permet de s'en dispenser. Mais il est malheureusement plus lent.
Pour cette dernière raison, il existe une technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de « **chiffrement hybride** ».
Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque **vous visitez un site dont l'adresse débute par « https ».**

[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 : https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement