Comment sécuriser vos données et systèmes d’information ? | Denis JACOPINI

5

La cyberattaque, dont a été victime la chaîne TV5 Monde, puis ultérieurement le journal Belge Le Soir et d'autres médias, appelle à s'interroger quant à la sécurité des systèmes d'information.

La #sécurité des données informatiques représente un enjeu quotidien particulièrement important pour les sites d'e-commerce, les médias, les hébergeurs et les éditeurs de sites internet. Les banques et les compagnies d'assurances sont également concernées, en raison des multiples données qu'elles sont amenées à traiter dans le cadre de leurs activités.
La cyberattaque, dont a été victime la chaîne « TV5 Monde », puis ultérieurement le journal Belge « Le Soir » et d'autres médias, en témoigne et appelle à s'interroger quant à la sécurité des systèmes d'information, face au volume colossal des échanges de données sur les réseaux[1].
Outre les mesures préventives d'ordre technique à mettre en place, il est des mesures juridiques qu'il est hautement recommandé d'instaurer. Qu'à l'origine de l'attaque on identifie une faille interne à l'entreprise, ou externe (sous-traitant, hébergeur, etc.), il existe différents moyens juridiques à mettre en œuvre pour l'éviter. Les acteurs peuvent en effet être nombreux (éditeur, intégrateur, consultant, sous-traitant, prestataire, etc.) et la chaîne des responsables potentiels apparaît complexe.
Face au risque croissant de cyberattaque et aux enjeux du Big Data, il est indispensable de sécuriser l'ensemble des moyens techniques, humains et juridiques qui permettent de garantir la sécurité d'un système informatique.

1) La mise en place d'une stratégie en interne

a) En premier lieu, il est conseillé de procéder à un audit (juridique et technique) de sécurité du système d'information. L'objectif de cet audit sera de répertorier les points forts, et surtout les axes d'amélioration du système d'information dans son ensemble. Dans un monde en « hyper connexion » analyser une partie du système d'information n'a pas de sens car les risques peuvent venir d'un réseau ou d'une filiale non revus. Le but est de vérifier la sécurité du système afin d'identifier les mesures de réaction à une attaque, de tester un nouvel équipement, et surtout de mettre en place un planning de mise en conformité.
Les interventions liées aux opérations de maintenance corrective et évolutive doivent être régulièrement planifiées, notamment par l'application de correctifs de sécurité.

b) Ensuite, il est recommandé de rédiger une Charte de sécurité informatique, visant à sensibiliser chacun à la confidentialité et à l'importance de l'intégrité des données d'un système d'information. Une telle Charte représente une étape indispensable dans le processus de sécurisation des données. Elle doit viser les postes fixes, les mobiles, les tablettes, etc… et traiter, notamment, de la gestion des mots de passe, mais aussi de l'accès au réseau de l'entreprise depuis l'extérieur.

c) Soulignons qu'il convient d'instaurer une politique de gestion des mots de passe. L'utilisation d'un mot de passe dit « fort » est un élément fondamental dans la sécurisation d'un système d'information. Or, bien souvent, les mots de passe sont trop communs ou configurés par défaut. Il est donc essentiel de mettre en œuvre une politique de gestion des mots de passe afin de protéger tant l'utilisateur final, que le système d'information lui-même.
La surveillance des logs de connexion et de l'accès via des hotspot et/ou VPN est à encadrer également avec minutie.

d) Enfin, il est opportun de prévoir des clauses spécifiques dans les contrats de travail de l'ensemble des salariés au-delà des seuls administrateurs système, Directeurs des Systèmes d'Information (DSI).

2) Le développement d'une stratégie en externe

a) Avant tout accord, il convient de mettre en place une politique efficace de confidentialité en signant des accords de non divulgation (« Non-Disclosure Agreement ») avec l'ensemble de la chaîne des sous-traitants.

b) En parallèle de cela, il est nécessaire :
• de rédiger de solides contrats avec les différents prestataires techniques dont le non-respect sera sanctionné par des clauses pénales ;
• de vérifier régulièrement les contrats conclus avec les hébergeurs.

La rédaction des contrats informatiques nécessite en effet une expertise toute particulière. On pense notamment aux contrats de maîtrise d'œuvre, d'intégration, de sous-traitance, de licence d'utilisation, etc.
Pour ce qui concerne les obligations et garanties des parties, le contrat doit refléter la réalité des responsabilités. Le risque juridique est donc associé à la personne qui est effectivement responsable des traitements et des usages qui sont faits des données et des résultats.
L'application du régime du contrat de fourniture de prestations de services, complété par des obligations accessoires de surveillance et de respect de la confidentialité des données stockées, assure une protection optimale au bénéficiaire du service. Tout en servant les intérêts des utilisateurs, ce régime est également opportun à l'égard des prestataires car il correspond à leur nature juridique et à leur responsabilité sur le Web.

c) Il demeure indispensable de veiller au respect des recommandations de la CNIL. Il est nécessaire de procéder à toute déclaration requise en fonction de la nature des données et des modalités du traitement (déclaration simplifiée, déclaration normale, ou autorisation préalable) ; les formalités préalables étant allégées en cas de désignation d'un Correspondant Informatique et Libertés ou « CIL ».
Au sein de sa structure, ou en externe pour les petites structures, le responsable du traitement désigne une personne qui sera chargée de (i) tenir à jour un registre des traitements mis en œuvre au sein de l'organisme et (ii) veiller au respect des dispositions de la loi « informatique et libertés » au sein de l'organisme. Le CIL ainsi désigné peut être notamment être un salarié de la société, ou le conseil de cette société.

d) Le contrat doit également permettre la possibilité aux acteurs de la DSI d'auditer leur prestataire (droit d'audit). Cela permet de contrôler que les mesures contractuelles, par exemple sur la sécurisation de données, sur l'hébergement des données au sein de l'espace Européens, sont respectées.

e) Enfin, il est toujours possible de solliciter l'intervention de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui veille quotidiennement au renforcement de la Cyber sécurité en accompagnant les entreprises par des actions de conseil, de politique industrielle et de réglementation.

3) En phase contentieuse

En cas de conflit, il est nécessaire de faire dresser des constats informatiques aux fins de préserver la matérialité de l'infraction et surtout de retracer l'origine de l'attaque ou de l'intrusion.
Par conséquent, la sécurité des données implique la mise en place d'une stratégie juridique renforcée, que ce soit tant au niveau des systèmes d'information que des réseaux de communications électroniques (mails et réseaux sociaux).

[1] En 1 minute, voici notamment ce qui s'échange sur la toile :
– 204 millions d'emails expédiés ;
– 1.875.000 likes sur Facebook ;
– 278 000 Tweets expédiés ;
– 694 445 recherches sur Google ;
– 70 noms de domaine enregistrés ;
– 13 000 applications téléchargées.

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

Source : http://www.journaldunet.com/solutions/expert/60588/cyberattaque–comment-securiser-vos-donnees-et-systemes-d-information.shtml

Windows 8 : Identifier les applications malveillantes à partir des services par défaut | Denis JACOPINI

	Windows 8 : Identifier les applications malveillantes à partir des services par défaut

Afin de vérifier si votre ordinateur dispose d'applications malveillantes ou non, nous vous mettons en ligne la liste des services lancés par défaut de Windows 8.

Exécutez Services.msc

Nom du service	Fichier	Démarrage par défaut	Démarrage conseillé	Remarques
Acquisition d'image Windows (WIA)	stisvc	Manuel	Manuel	Fournit des services d'acquisition d'images pour les scanners et les appareils photos. Si votre scanner ou webcam ne fonctionne pas correctement, utilisez le démarrage automatique.
Agent de protection d'accès réseau	napagent	Manuel	Désactivé	Le service Agent de protection d'accès réseau (NAP) recueille et gère les informations d'intégrité pour les ordinateurs clients d'un réseau. Les informations recueillies par l'agent NAP sont utilisées pour s'assurer que l'ordinateur client possède les logiciels et paramètres nécessaires.
Agent de stratégie IPsec	PolicyAgent	Manuel	Manuel	La sécurité du protocole Internet (IPSec) prend en charge l'authentification de l'homologue réseau, l'authentification de l'origine des données, l'intégrité des données, la confidentialité des données (chiffrement) et la protection de la relecture.
Alimentation	Power	Automatique	Automatique	Gère la stratégie d'alimentation et la remise de notification de stratégie d'alimentation.
AMD External Events Utility	atiesrxx	Automatique	Désactivé	Fait partie des pilotes graphiques AMD. Permet de modifier les réglages de votre carte graphique à partir d'événements externes comme des raccourcis clavier par exemple.
Appel de procédure distante (RPC)	RpcSs	Automatique	Automatique	Ce service est le Gestionnaire de contrôle des services pour les serveurs COM et DCOM. Il traite les demandes d'activation d'objets, les résolutions d'exportateur d'objets et le nettoyage de la mémoire distribuée pour les serveurs COM et DCOM. Ce service est indispensable, de nombreux autres services en dépendant. Laissez-le donc sur automatiq[illegible]
Application système COM+	COMSysApp	Manuel	Manuel	Gère la configuration et le suivi des composants de base COM+ (Component Object Model).
Assistance IP	iphlpsvc	Automatique	Désactivé	Fournit une connectivité de tunnel à l'aide des technologies de transition IPv6.
Assistant NetBIOS sur TCP/IP	lmhosts	Automatique	Désactivé	Utilisé pour partager et imprimer des fichiers à travers le réseau local. Activez le service si vous avez plusieurs ordinateur dans votre réseau local et que vous échangez des fichiers entre eux.
Assistant Connectivité réseau	NcaSvc	Manuel	Manuel	Fournit la notification du statut DirectAccess aux composants de l'interface utilisateur.
Assistant Connexion avec un compte Microsoft	wlidsvc	Manuel	Désactivé	Utilisé pour autoriser les utilisateurs à ouvrir une session avec un compte utilisateur Microsoft en ligne. Si vous utilisez uniquement des comptes locaux, désactivez ce service.
Audio Windows	AudioSrv	Automatique	Automatique	A moins de ne pas avoir de carte de son dans votre ordinateur, laissez ce service en démarrage automatique sinon, plus aucun son ne pourra être joué par votre ordinateur.
BranchCache	PeerDistSvc	Manuel	Désactivé	Ce service met en cache le contenu réseau à partir d'homologues sur le sous-réseau local.
Cache de police de Windows Presentation Foundation	FontCache	Manuel	Manuel	[illegible]
Carte à puce	SCardSvr	Manuel	Désactivé	[illegible]
Carte de performances WMI	wmiApSrv	Manuel	Manuel	[illegible]
Centre de sécurité	wscsvc	Automatique	Automatique	[illegible]
Cliché instantané des volumes	VSS	Automatique	Automatique	[illegible]
Client de stratégie de groupe	gpsvc	Automatique	Automatique	[illegible]
Client de suivi de lien distribué	TrkWks	Automatique	Désactivé	[illegible]
Client DHCP	Dhcp	Automatique	Automatique	[illegible]
Client DNS	dnscache	Automatique	Automatique	[illegible]
Collecteur d'événement Windows	Wecsvc	Automatique	Automatique	[illegible]
Configuration automatique de réseau câblé	dot3svc	Manuel	Manuel	[illegible]
Configuration automatique des périphériques connectés au réseau	NcdAutoSetup	Manuel	Manuel	[illegible]
Configuration des services Bureau à distance	SessionEnv	Manuel	Manuel	[illegible]
Connaissance des emplacements réseau	NlaSvc	Automatique	Automatique	[illegible]
Connexions réseau	Netman	Manuel	Manuel	[illegible]
Contrôle parental	WPCSvc	Manuel	Désactivé	[illegible]
Coordinateur de transactions distribuées	MSDTC	Manuel	Manuel	[illegible]
Découverte SSDP	SSDPSRV	Manuel	Manuel	[illegible]
Détection de services interactifs	UI0Detect	Manuel	Manuel	[illegible]
Détection matériel noyau	ShellHWDetection	Automatique	Automatique	[illegible]
Disque virtuel	vds	Manuel	Manuel	[illegible]
Dossiers de travail	workfolderssvc	Manuel	Manuel	[illegible]
Ecouteur du groupement résidentiel	HomeGroupListener	Manuel	Manuel	[illegible]
Evénements d'acquisition d'images fixes	WiaRpc	Manuel	Manuel	[illegible]
Expérience audio-vidéo haute qualité Windows	QWAVE	Manuel	Manuel	[illegible]
Expérience d'application	AeLookupSvc	Manuel	Manuel	[illegible]
Explorateur d'ordinateurs	Browser	Manuel	Manuel	[illegible]
Extensions et notifications des imprimantes	PrintNotify	Manuel	Manuel	[illegible]
Fichiers hors connexion	CscService	Manuel	Manuel	[illegible]
Fournisseur de cliché instantané de logiciel Microsoft	swprv	Manuel	Manuel	[illegible]
Fournisseur du Groupement résidentiel	HomeGroupProvider	Manuel	Manuel	[illegible]
Générateur de points de terminaison du service Audio Windows	AudioEndpointBuilder	Automatique	Automatique	[illegible]
Gestion à distance de Windows (WSM)	WinRM	Manuel	Désactivé	[illegible]
Gestion d'applications	AppMgmt	Manuel	Désactivé	[illegible]
Gestion des clés et des certificats d'intégrité	hkmsvc	Manuel	Désactivé	[illegible]
Gestionnaire d'identité réseau homologue	p2pimsvc	Manuel	Désactivé	[illegible]
Gestionnaire d'informations d'identification	VaultSvc	Manuel	Désactivé	[illegible]
Gestionnaire d'installation de périphérique	DsmSvc	Manuel	Manuel	[illegible]
Gestionnaire de comptes de sécurité	SamSs	Automatique	Automatique	[illegible]
Gestionnaire de session locale	LSM	Automatique	Automatique	[illegible]
Gestionnaire des connexions automatiques d'accès à distance	RasAuto	Manuel	Manuel	[illegible]
Gestionnaire des connexions Windows	RasMan	Manuel	Manuel	[illegible]
Groupement de mise en réseau de pairs	p2psvc	Manuel	Manuel	[illegible]
Hôte de DLL de compteur de performance	PerfHost	Manuel	Manuel	[illegible]
Hôte de périphérique UPnP	upnphost	Manuel	Manuel	[illegible]
Hôte du fournisseur de découverte de fonctionsfdPHost		Manuel	Désactivé	[illegible]
Hôte système de diagnostics	WdiSystemHost	Manuel	Désactivé	[illegible]
Identité de l'application	AppIDSvc	Manuel	Manuel	[illegible]
Information d'application	Appinfo	Manuel	Manuel	[illegible]
Infrastructure de gestion Windows	Winmgmt	Automatique	Automatique	[illegible]
Interface de services d'invité Hyper-V	vmicguestinterface	Manuel	Désactivé	[illegible]
Interruption SNMP	SNMPTRAP	Manuel	Désactivé	[illegible]
Isolation de clé CNG	KeyIso	Manuel	Manuel	[illegible]
Journal d'événement Windows	EventLog	Automatique	Automatique	[illegible]
Journaux & alerte de performance	pla	Manuel	Manuel	[illegible]
Lanceur de processus serveur DCOM	DcomLaunch	Automatique	Automatique	[illegible]
Localisateur d'appels de procédure distante (RPC)	RpcLocator	Manuel	Désactivé	[illegible]
Mappage de découverte de topologie de la couche de liaison	lltdsvc	Manuel	Désactivé	[illegible]
Mappeur de point de terminaison RPC	RpcEptMapper	Automatique	Automatique	[illegible]
Microsoft Keyboard Filter	MsKeyboardFilter	Désactivé	Désactivé	[illegible]
Modules de génération de clés IKE et AuthIP	IKEEXT	Manuel	Manuel	[illegible]
Moteur de filtrage de base	BFE	Automatique	Automatique	[illegible]
Netlogon	Netlogon	Manuel	Désactivé	[illegible]
Optimiser les lecteurs	defragsvc	Manuel	Manuel	[illegible]
Ouverture de session secondaire	seclogon	Manuel	Désactivé	[illegible]
Pare-feu Windows	MpsSvc	Automatique	Automatique	[illegible]
Partage de connexion Internet (ICS)	SharedAccess	Manuel	Désactivé	[illegible]
Planificateur de classes multimédias	MMCSS	Automatique	Automatique	[illegible]
Planificateur de tâches	Schedule	Automatique	Automatique	[illegible]
Plug and Play	PlugPlay	Manuel	Manuel	[illegible]
Préparation des applications	AppReadiness	Manuel	Manuel	[illegible]
Prise en charge de l'application Rapports et solutions aux problèmes du Panneau de configuration	wercplsupport	Manuel	Désactivé	[illegible]
Programme d'installation ActiveX	AxInstSV	Manuel	Désactivé	[illegible]
Programme d'installation pour les modules Windows	TrustedInstaller	Manuel	Manuel	[illegible]
Propagation du certificat	CertPropSvc	Manuel	Désactivé	[illegible]
Protection logicielle	sppsvc	Manuel	Manuel	[illegible]
Protocole EAP (Extensible Authentification Protocol)	Eaphost	Manuel	Manuel	[illegible]
Protocole PNRP	PNRPsvc	Manuel	Désactivé	[illegible]
Publication des ressources de découverte de fonctions	FDResPub	Automatique	Désactivé	[illegible]
Redirecteur de port du mode utilisateur des services Bureau à distance	UmRdpService	Manuel	Désactivé	[illegible]
Registre à distance	RemoteRegistry	Manuel	Désactivé	[illegible]
Requête du service VSS Microsoft Hyper-V	vmicvss	Manuel	Désactivé	[illegible]
Routage et accès distant	RemoteAccess	Désactivé	Désactivé	[illegible]
Serveur	LanmanServer	Automatique	Automatique	[illegible]
Serveur de priorité des threads	THREADORDER	Manuel	Manuel	[illegible]
Service Arrêt de l'invité Microsoft Hyper-V	vmicshutdown	Manuel	Désactivé	[illegible]
Service Broker des événements système	SystemEventsBroker	Manuel	Désactivé	[illegible]
Service Broker pour les connexions réseau	NcbService	Manuel	Désactivé	[illegible]
Service Broker pour les événements horaires	TimeBroker	Manuel	Désactivé	[illegible]
Service Collecteur ETW d'Internet Explorer	IEEtwCollectorService	Manuel	Désactivé	[illegible]
Service d'administration IIS	IISADMIN	Automatique	Automatique	[illegible]
Service d'association de périphérique	DeviceAssociationService	Automatique	Automatique	[illegible]
Service d'énumération de périphériques de carte à puce	ScDeviceEnum	Manuel	Désactivé	[illegible]
Service d'historique des fichiers	fhsvc	Manuel	Manuel	[illegible]
Service d'infrastructure de localisation Windows	lfsvc	Manuel	Désactivé	[illegible]
Service d'infrastructure des tâches en arrière-plan	BrokerInfrastructure	Automatique	Automatique	[illegible]
Service d'installation de périphérique	DeviceInstall	Manuel	Manuel	[illegible]
Service de biométrie Windows	WbioSrvc	Manuel	Désactivé	[illegible]
Service de cache de police Windows	FontCache	Manuel	Manuel	[illegible]
Service de chiffrement de lecteur BitLocker	BDESVC	Manuel	Désactivé	Le chif[illegible]
Service de configuration automatique WLAN	WlanSvc	Manuel	Manuel	[illegible]
Service de configuration automatique WWAN	WwanSvc	Manuel	Désactivé	[illegible]
Service de découverte automatique de Proxy Web pour les services http Windows	WinHttpAutoProxySvc	Manuel	Manuel	[illegible]
Service de déploiement AppX	AppXSvc	Manuel	Manuel	[illegible]
Service de l'assistant Compatibilité des programmes	PcaSvc	Automatique	Désactivé	[illegible]
Service de la passerelle de la couche Application	ALG	Automatique	Désactivé	[illegible]
Service de moteur de sauvegarde en mode bloc	wbengine	Manuel	Manuel	[illegible]
Service de notification d'événement système	SENS	Automatique	Automatique	[illegible]
Service de partage de ports Net.Tcp	NetTcpPortSharing	Désactivé	Désactivé	[illegible]
Service de prise en charge Bluetooth	bthserv	Manuel	Désactivé	[illegible]
Service de profil utilisateur	ProfSvc	Automatique	Automatique	[illegible]
Service de publication des noms d'ordinateurs PNRP	PNRPAutoReg	Manuel	Désactivé	[illegible]
Service de rapport d'erreurs Windows	WerSvc	Manuel	Désactivé	[illegible]
Service de stockage	StorSvc	Manuel	Désactivé	[illegible]
Service de stratégie de diagnostic	DPS	Automatique	Désactivé	[illegible]
Service de surveillance des capteurs	SensrSvc	Manuel	Désactivé	[illegible]
Service de transfert intelligent en arrière-plan	BITS	Automatique	Automatique	[illegible]
Service de virtualisation Bureau à distance Hyper-V	vmicrdv	Manuel	Désactivé	[illegible]
Service du clavier tactile et du volet d'écriture manuscrite	TabletInputService	Manuel	Manuel	[illegible]
Service du périphérique d'interface utilisateur	hidserv	Manuel	Manuel	[illegible]
Service Echange de données Microsoft Hyper-V	vmickvpexchange	Manuel	Désactivé	[illegible]
Service énumérateur d'appareil mobile	WPDBusEnum	Manuel	Désactivé	[illegible]
Service hôte du fournisseur de chiffrement Windows	WEPHOSTSVC	Manuel	Manuel	[illegible]
Service hôte WDIServiceHost	WdiServiceHost	Manuel	Désactivé	[illegible]
Service Initiateur iSCI de Microsoft	MSiSCSI	Manuel	Désactivé	[illegible]
Service inspection du réseau Windows Defender	WdNisSvc	Manuel	Manuel	[illegible]
Service interface du magasin réseau	nsi	Automatique	Automatique	[illegible]
Service KtmRm pour Distributed Transaction Coordinator	KtmRm	Manuel	Manuel	[illegible]
Service Liste des réseaux	netprofm	Manuel	Manuel	[illegible]
Service mains libres Bluetooth	BthHFSrv	Manuel	Désactivé	[illegible]
Service Partage réseau du Lecteur Windows Media	WMPNetworkSvc	Automatique	Désactivé	[illegible]
Service Pulsation Microsoft Hyper-V	vmicheartbeat	Manuel	Désactivé	[illegible]
Service Synchronisation date/heure Microsoft Hyper-V	vmictimesync	Manuel	Désactivé	[illegible]
Service Windows Defender	WinDefend	Automatique	Automatique	[illegible]
Service Windows Store (WSService)	WSService	Manuel	Manuel	[illegible]
Service SSTP (Secure Socket Tunneling Protocol)	SstpSvc	Manuel	Manuel	[illegible]
Services Bureau à distance	TermService	Manuel	Désactivé	[illegible]
Services de chiffrement	CryptSvc	Automatique	Automatique	[illegible]
SMP de l'espace de stockages Microsoft	smphost	Manuel	Désactivé	[illegible]
Spouleur d'impression	Spooler	Automatique	Automatique	[illegible]
Station de travail	LanmanWorkstation	Automatique	Automatique	[illegible]
Stratégie de retraite de la carte à puce	SCPolicySvc	Manuel	Désactivé	[illegible]
Superfetch	SysMain	Automatique	Automatique	Gère et améliore les performances du système dans le temps.
Système d'événement COM+	EventSystem	Automatique	Automatique	Prend en charge le service de notification d'événements système.
Système de couleurs Windows	WcsPlugInService	Manuel	Désactivé	Le service WcsPlugInService héberge des modules de plug-in tiers du modèle de périphérique couleurs et du modèle de gamme de couleurs du système de couleurs Windows.
Système de fichiers EFS (Encrypting File System)	EFS	Manuel	Manuel	Fournit la technologie de chiffrement des fichiers de base utilisée pour stocker les fichiers chiffrés sur les volumes NTFS.
Télécopie	Fax	Manuel	Désactivé	Vous permet d'envoyer et de recevoir des télécopies, d'utiliser les ressources de télécopie disponibles sur cet ordinateur ou le réseau.
Téléphonie	TapiSrv	Manuel	Manuel	Prend en charge l'interface TAPI (Telephony API) pour les programmes qui contrôlent les périphériques de téléphonie sur l'ordinateur local et, via le réseau local (LAN), sur les serveurs qui exécutent également le service.
Temps Windows	W32Time	Manuel	Manuel	Conserve la synchronisation de la date et de l'heure sur tous les clients et serveurs sur le réseau.
Thèmes	Themes	Automatique	Automatique	Fournit un système de gestion de thème de l'expérience utilisateur.
Vérificateur de points	svsvc	Manuel	Manuel	Vérifie les endommagements éventuels du système de fichiers
WebClient	WebClient	Manuel	Désactivé	Permet à un programme fonctionnant sous Windows de créer, modifier et accéder à des fichiers Internet.
Windows Connect Now – Registre de configuration	wcncsvc	Manuel	Désactivé	Héberge la configuration de connexion immédiate Windows pour le protocole WFP. Utilisé pour configurer rapidement une connexion sans fil.
Windows Driver Foundation – Infrastructure de pilote mode-utilisateur	wudfsvc	Manuel	Manuel	Gère les processus hôtes de pilote mode-utilisateur.
Windows Installer	msiserver	Manuel	Manuel	Ajoute, modifie et supprime des applications fournies en tant que package Windows Installer (*.msi).
Windows Search	Wsearch	Automatique	Désactivé	Fournit des fonctionnalités d'indexation de contenu, de mise en cache des propriétés, de résultats de recherche pour les fichiers, les messages électroniques et autres contenus. Si vous utilisez beaucoup la fonction Recherche de Windows, laissez le service activé. Sinon, désactivez-le. La recherche sera toujours poss[illegible]
Windows Update	wuauserv	Automatique	Automatique	Active la détection, le téléchargement et l'installation des mises à jour de Windows et d'autres programmes.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.winhelponline.com/blog/windows-8-services-default-startup-type/

Règlement européen sur la protection des données : Renforcement des droits des personnes

	Règlement européen sur la protection des données : Renforcement des droits des personnes

Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci.

Consentement renforcé et transparence

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

De nouveaux droits

Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

Des conditions particulières pour le traitement des données des enfants : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

source : CNIL

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

Un oeil sur vous, citoyens

sous surveillance – Documentaire 2015 | Denis JACOPINI

	Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 2h24

Des milliards de citoyens connectés livrent en permanence – et sans toujours s'en rendre compte – des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la #cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Victime d’une arnaque vous demandant de régler par coupons recharges PCS ? Pas de panique !

Les escroqueries à la Carte prépayée et aux coupons recharges PCS Mastercard (ou Transcash ou Tonéo) se développent de plus en plus et ont tendance à remplacer certaines arnaques plus anciennes, mais désormais mieux détectées par les internautes

Par mail ou via Facebook, ils envoient tout d'abord soit un appel au secours venant d'une personne proche ou toute autre raison aboutissant à un chantage.

Ils demandent ensuite de recharger leur carte de crédit par ce nouveau moyen très moderne qu'est la carte prépayée PCS Mastercard. Souvent les personnes ne connaissent même pas le principe de rechargement de carte de crédit mais lorsque l'interlocuteur nous explique qu'il suffit simplement de descendre au bureau de tabac en bas de chez nous, d'acheter 1, 2, 3 ou 4 tickets de rechargement (coupons recharges), puis de lui envoyer les codes pour répondre à a demande, beaucoup commencent à flairer le piège.

Ce moyen de paiement vient en remplacement des mandats cash ou des versement par Western Union qui ont aujourd'hui une telle mauvaise réputation que leur nom seul éveille des soupçons pour la plupart d'entre nous.. Il permet de rendre impossible de remonter jusqu'au destinataire par la voie judiciaire habituelle.

Ainsi, que ça soit quelqu'un qui se fait passer pour un ami qui vous signale avoir perdu ses papiers ou son téléphone en vous suppliant de l'aide par ce moyen de paiement ou une personne qui exerce sur vous un chantage :

• N'hésitez pas à porter plainte en commissariat de Police ou en Brigade de Gendarmerie (en fonction de votre résidence) ;

• Vous pouvez utilisez un site internet de pré-plainte sur Internet (https://www.pre-plainte-en-ligne.gouv.fr)

• Ne répondez plus à ses messages ;

• Signalez ses agissements sur www.internet-signalement.gouv.fr ;

Si vous avez du temps à perdre, vous pouvez aussi vous amuser à les mener en bateau, **les capacités de nuisance de ces arnaqueurs du dimanche étant très limitées** à seulement pouvoir vous envoyer des e-mails ou vous téléphoner si vous avez commis l'imprudence de leur communiquer votre numéro. Vous pouvez rétorquer en leur faisant croire que vous allez les payer ou que vous avez vous aussi besoin d'un coupon de recharge PCS pour vous déplacer pour aller en acheter un !

Attention :

Si vous êtes en contact avec une personne se présentant comme victime s'étant faite arnaquer par un escroc et que cette dernière vous communique ensuite les coordonnées d'un contact chez Interpol présenté comme son sauveur, fuyez ! Il s'agit aussi d'une arnaque.

Interpol ne rentre jamais en contact directement avec les victimes !

Ceux qui vous soutiennent le contraire ou qui vous contactent directement en se faisant passer pour Interpol ont malheureusement aussi pour objectif de vous soutirer de l'argent.

Plus d'infos sur : https://www.lenetexpert.fr/contater-interpol-en-cas-darnaque-est-une-arnaque/

Remarque :

Il est possible qu'au moment ou vous êtes sur le point de déposer plainte, la personne en face de vous cherche à vous dissuader. C'est normal, face au faibles changes de retrouver l'auteur de l'acte délictueux, ils considèrent comme une perte de temps le fait de devoir traiter votre demande sous forme de plainte et vous inviteront à déposer une main courante.

Insistez pour déposer plainte car sans cette acte citoyen qu'on ne peut vous refuser (en faisant bien attention de le faire en mentionnant la bonne qualification juridique), vous ne laisserez pas passer la moindre chance (même si elle est minime) de faire arrêter l'escroc.

Pour information

• Les délits d'usurpation d'identité, pouvant être associé au phishing selon l'article 226-4-1 du code pénal sont punis d'un an d'emprisonnement et de 15 000 € d'amende.

• Selon l'article Article 312-1 du code pénal, le délit d'extorsion ou de tentative d'extorsion (demande d'argent en échange de ne pas supprimer des données ou de ne pas divulguer des secrets volés) est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.

• Les délits d'escroquerie ou tentative d'escroquerie, selon les articles 313-1, 313-2 et 313-3 du code pénal, sont punis de cinq ans d'emprisonnement et de 375 000 euros d'amende.

[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 : *Comment fonctionne une escroquerie à la Carte prépayée et aux coupons recharges PCS Mastercard, Transcash ou Tonéo? | Ms2i On Air*

Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?

Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de trace sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé (effacer l'historique de ses comptes mails et personnelles, formatage complet, logiciel d'aide à la suppression etc…) ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage.
Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :
• Des programmes ajoutés ;
• Nos e-mails ;
• Nos traces de navigation ;
• Nos fichiers téléchargés ;
• Divers identifiants et mots de passe ;
• Les fichiers temporaires

Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes ajoutés
Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :
• soit par le raccourcis de désinstallation que le programme a créé ;
• s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
• Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (gratuit).

Concernant les e-mails
Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :
• fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
• fichiers dans « » »% »'AppDataLocalMicrosoftWindows Live Mail » pour le logiciel « Windows Live Mail » ;
• les fichiers contenus dans ' » »% »'APPDATA%ThunderbirdProfiles » pour le programme Mozilla Thunderbird
• le dossier contenu dans « ..Local SettingsApplication DataIMIdentities » pour le programme Incredimail.

Concernant nos traces de navigation
En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».

Concernant les fichiers téléchargés
En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Concernant divers identifiants et mots de passe
Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaitre et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».
Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans vote ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires
En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).
En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Pour finir
Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore »…

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : 5 applications pour effacer des données de façon sécurisée – ZDNet

---

Quelles formalités une pharmacie doit déclarer à la CNIL ? | Denis JACOPINI

Quelles formalités une pharmacie doit déclarer à la CNIL ?

Les fichiers relatifs à la gestion d'une pharmacie doivent être déclarés à la CNIL :Par une déclaration simplifiée de conformité à la norme n°52 si le fichier correspond aux caractéristiques énoncées dans ce texte ;
Par une déclaration normale si le fichier sort du cadre de cette norme.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=193E337DAA685A15B25C9E90E19E80BF?name=Activit%C3%A9+d%27une+pharmacie+%3A+quelles+formalit%C3%A9s+%C3%A0+la+CNIL+%3F&id=545

Votre boite e-mail a été piratée. Quelle attitude adopter ? | Denis JACOPINI

Votre boite e-mail a été piratée. Quelle attitude adopter ?

Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée ?Quelle attitude adopter ?

Un choix s'offre à vous :
Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

Vous protéger et faire cesser le piratage
Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée. Quels sont les éléments qui vous font penser ça ?
– Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails ?
– Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?
– Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la votre ?
1°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.
Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions… Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur www.antivirus.lenetexpert.fr.
2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulèrement (e-mail, banque, blog, réseaux sociaux…).
Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

Rechercher l'auteur et porter plainte
Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.
Soit vous avez les éléments techniques pouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.
Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet www.internet-signalement.gouv.fr. Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachat que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

Source : Denis JACOPINI

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

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

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

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

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

1. En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tel que les fichiers clients.

On pourrait bien vous reprocher d'en avoir conservé une copie et de l'utiliser contre votre ancien employeur.

2. Identifiez les données ayant un caractère confidentiel et qui nécessiteront une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hachage.
3. Identifiez les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre…
4. Identifiez les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits-enfants…)
5. Identifiez les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ça soit au bureau à la maison, en déplacement ou en vacances. Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifiez les fonctions de « Sauvegarde », « Enregistrer sous » ou d' »Export ». Vous pourrez alors choisir le support adapté.

Enfin, en fonction des critères de sécurité choisis, vous pourrez sauvegarder sur des supports adaptée soit :

– à la confidentialité (tout support numérique en utilisant un logiciel de cryptage ou de hachage tel de Truecrypt, Veracrypt, ou AxCrypt…) ;
– à l'intégrité (multiplier le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à n'absolument pas perdre) ;
– à la longévité en utilisant des supports avec une durée de vie adapté à vos attentes. Sachez qu'à ce jour, il est difficile de garantir la lecture d'une information numérique au-delà de plusieurs dizaines d'années (en raison de l'altération des supports avec le temps, mais aussi de l'évolution des versions, des formations et des logiciels). Qui peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
– à la disponibilité sur plusieurs plateformes et sur plusieurs lieux, comme le proposent les solutions *cloud* qui sont éclos il y a quelques dizaines d'années seulement ;
– à la quantité (car vous devez rapidement stocker pour ensuite trier et choisir un support adapté) en choisissant par exemple un disque dur USB externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

Les risques :

Les clés USB sont des outils permettant de conserver une copie facilement accessible et aisément transportable. 100% des clés USB tomberont un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.

Idem pour les disques durs. 100% des disques durs tomberont un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettront plus facilement de récupérer leur contenu en cas de panne.

Les supports de type lecteurs ZIP, lecteur JAZ, lecteurs magnéto-optiques, lecteurs de bandes etc. sont de plus en plus rares. Conserver des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginez un instant jour ou vous souhaitez y accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vies de vos données numériques entre les mains du *Bon Coin*…

Voilà, en fonction de tous ces critères et à partir de ces conseils, il ne vous reste plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Comparatif :

Disque dur : Quelques Go à quelques To – Bon marché, rapide mais fragile.
Clé USB : Quelques Go – Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.
Cloud : Quelques Mo à quelques To – Accessible de n'importe où mais aussi par tous ceux qui ont le mot de passe (risqué) – Dépend du fonctionnement et de la rapidité d'Internet – Les services de cloud gratuits peuvent s'arrêter du jour au lendemain et vous perdrez tout.
Disques optiques (CD, DVD,Magnéto Optique) : Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (pérennité des lecteurs de disques) jusqu'à quand ?
Supports spéciaux (ZIP/Jazz/QIC/DAT/DLT/DDS/SDLT) : Supports fragiles, lecteurs trop rares pour garantir une lecture au dela de 5 ans.

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de traces sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage. Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :

– Des programmes ajoutés ;
– Nos e-mails ;
– Nos traces de navigation ;
– Nos fichiers téléchargés ;
– Divers identifiants et mots de passe ;
– Les fichiers temporaires

Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes ajoutés :

Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :

– soit par le raccourcis de désinstallation que le programme a créé ;
– s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
– Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (gratuit).

Concernant les e-mails :

Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :

– fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
– fichiers dans » » « % »'AppDataLocalMicrosoftWindows Live Mail » pour le logiciel « Windows Live Mail » ;
– les fichiers contenus dans ' » »% »'APPDATA%ThunderbirdProfiles » pour le programme Mozilla Thunderbird
– le dossier contenu dans « …Local SettingsApplication DataIMIdentities » pour le programme Incredimail.

Concernant nos traces de navigation :

En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».

Concernant les fichiers téléchargés :

En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Concernant divers identifiants et mots de passe :

Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».

Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires :

En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).
En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Pour finir :

Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore »…

Ne pas effacer ses données personnelles sur so ordinateur de fonction est-il dommageable ? Si oui, pourquoi ?

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :

– Accéder à vos documents et découvrir les informations qui peuvent soit être professionnelles et être utilisées contre vous, soit personnelles permettant à un voyou de les utiliser contre vous soit en vous demandant de l'argent contre son silence ou pour avoir la paix ;
– Accéder aux identifiants et mots de passe des comptes internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes facebook, twitter, dropbox… ;
– Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement déposer des commentaires ou envoyer des e-mails en utilisant votre identité.

Auteur : Denis JACOPINI

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

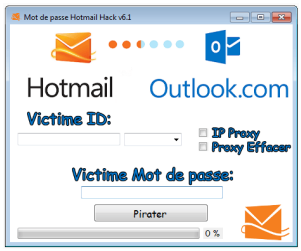
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c’est très important) | Atlantico.fr

---

Arnaques, spams, phishing, sextape. Comment se protéger ? | Denis JACOPINI



Arnaques, spams, phishing, sextape. Comment se protéger ?

Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée ?Quelle attitude adopter ?

Un choix s'offre à vous :
Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

Vous protéger et faire cesser le piratage
Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée. Quels sont les éléments qui vous font penser ça ?
– Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails ?
– Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?
– Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la votre ?
1°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.
Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions… Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur www.antivirus.lenetexpert.fr.
2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulèrement (e-mail, banque, blog, réseaux sociaux…).
Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

Rechercher l'auteur et porter plainte
Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.
Soit vous avez les éléments techniques prouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.
Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet www.internet-signalement.gouv.fr. Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachat que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

Denis JACOPINI est Expert Informatique assermenté, pratiquant à la demande de particuliers d'entreprises ou de Tribunaux. Il est consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI