

# Table des matières

## 1. VOTRE PRINCIPAL ENNEMI : LA NÉGLIGENCE ..... 1

- Un problème malheureusement classique • 2
- Causes possibles à la perte des données électroniques • 3
  - Arrêt brutal du système • 3
  - Obésité du système de fichiers • 4
  - Système corrompu • 5
  - Noms de fichiers à rallonge • 5
  - Bogues des logiciels • 6
- Méthode simple et efficace pour lutter contre la perte des données • 7
- Sauvegarder des données • 7
  - Activer et paramétrer l'enregistrement automatique des documents • 7
  - Ce qu'il faut sauvegarder • 8
  - Supports de sauvegarde et d'archivage • 10
  - Sauvegarde manuelle • 11
    - Sauvegarder la messagerie • 11
    - Sauvegarder le carnet d'adresses personnel • 13
    - Sauvegarder le bureau et les favoris • 14
  - Sauvegarde automatique • 14
    - Sauvegarde normale, incrémentielle, différentielle ou quotidienne • 16
    - Planifier une sauvegarde automatique • 17
  - Vérifier si une sauvegarde s'est bien passée • 19
  - Outils de sauvegarde • 21
- Restaurer des données • 21
  - Restaurer un document de bureautique • 21
  - Restaurer un document supprimé par inadvertance • 21
  - Restaurer la messagerie • 22
  - Restaurer les données avec l'utilitaire de sauvegarde • 23
- Quand le système ne démarre plus... • 24
  - Identifier la panne • 25

- Se préparer à une panne du processus de démarrage • 26
- Réparer un système gravement endommagé par un virus • 26
- Réactiver la dernière bonne configuration connue • 27
- Le mode sans échec • 27
- Réparer une installation endommagée • 28
- Récapitulatif : les dix commandements à l'usage de l'utilisateur d'informatique • 28

## 2. CONFIGURER SA MACHINE DE FAÇON SÉCURISÉE ..... 31

- Configurer le système d'exploitation • 33
  - Windows, un système sécurisé ? • 33
  - Étapes essentielles d'une configuration sécurisée • 34
- Configuration de base : formater les disques en NTFS • 34
  - Convertir une partition en NTFS • 35
  - Formater une partition en NTFS • 36
- Sécuriser le Registre • 37
  - Risques encourus • 37
  - Modifier les permissions du Registre • 37
- Restreindre l'accès aux applications • 39
  - Créer un compte restreint • 39
  - Choisir les programmes accessibles par le menu Démarrer • 40
- Protéger l'accès à votre machine • 41
  - Définir un mot de passe utilisateur • 41
  - Fiabilité des mots de passe Windows • 42
  - Choisir un mot de passe robuste • 43
  - Protéger votre machine lorsque vous vous absentez : écran de veille et mot de passe • 43
- Partager des informations sur un réseau • 45
  - Visualiser les partages présents sur votre ordinateur • 45
  - Régler les autorisations d'un partage • 46
  - Mettre fin au partage d'un dossier • 47
  - Partages « fantômes » • 47

**Petites mesures anodines... • 49**

- Vider la liste Mes documents récents • 49
- Vider les historiques et paramètres sensibles du navigateur • 51
- Rendre les fichiers « invisibles » • 53

**Le plus : préserver la confidentialité des fichiers par chiffrement • 54**

- Chiffrer une information • 54
- Chiffrer des fichiers sur son ordinateur • 56
- Chiffrer un fichier ou un volume sous Windows 2000/XP avec EFS (Encrypted File System) • 58
- Limites des solutions natives de chiffrement fournies par Windows • 60
- Alternatives possibles pour un chiffrement plus robuste • 61
- Mettre en œuvre et utiliser GnuPG pour chiffrer fichiers et répertoires • 62

**Récapitulatif • 67**

**3. SE PROTÉGER CONTRE LES VIRUS**

**ET AUTRES CODES MALVEILLANTS.....69**

**Connaître son ennemi • 71**

- Définition d'un virus • 71
- Principaux types de virus • 71
  - Virus • 71
  - Vers • 72
  - Chevaux de Troie ou Troyens • 72
  - Autres formes de malveillances • 73

**Agissements des virus • 73**

- S'installer discrètement sur votre ordinateur • 73
- Pervertir votre système • 74
- Ouvrir toutes grandes les portes de votre PC • 74
- Lancer des attaques de grande envergure • 75

**Agissements des logiciels espions • 75**

**Infection de la machine • 79**

- Clic sur une pièce jointe infectée • 79
- Exploitation d'une faille logicielle • 79
- Image piégée • 80
- Macro infectée • 80

**Propagation des virus • 81**

- Périodicité d'apparition de nouveaux virus • 82
- Auteurs des virus • 82

**Fonctionnement d'un logiciel antivirus • 84**

- Fichier de définitions de virus • 84
- Détection des menaces • 85
  - Détection par reconnaissance de la signature d'un virus • 85
  - Détection par vérification de l'intégrité des fichiers • 85

**Surveillance du comportement des processus de l'ordinateur • 86**

**Méthode heuristique • 86**

**Fonctionnalités importantes d'un logiciel antivirus • 87**

**Principaux antivirus du marché • 88**

**Choisir un antivirus • 89**

- F-Secure Antivirus • 90
- Kaspersky Anti-Virus • 92
- BitDefender • 93
- McAfee VirusScan • 95
- Panda Titanium Antivirus • 95
- PC-cillin Internet Security • 96
- Norton Antivirus • 97
- AntiVir Personal Edition Classic • 99
- Sophos antivirus • 100

**Installer un nouveau logiciel antivirus • 101**

**Mise à jour et première analyse • 102**

**Configurer le logiciel antivirus • 107**

- Optimiser au quotidien la protection de votre ordinateur • 109
- Procéder à une analyse complète du système • 110

**Éradiquer un virus • 112**

**Code malveillant reconnu par l'antivirus • 112**

**Nettoyer une machine contaminée • 113**

**Votre machine ne démarre plus • 113**

Votre antivirus propose une fonction de démarrage à partir du support d'installation • 113

Votre antivirus ne propose pas de fonction de démarrage à partir du support d'installation • 114

**Votre machine démarre encore • 114**

Mettez à jour votre antivirus • 114

C'est un nouveau virus • 114

Votre antivirus ne sait pas éradiquer le virus • 114

Vous n'avez pas d'antivirus • 115

**Créer un jeu de disquettes d'urgence • 116**

**Mesures complémentaires à prévoir pour éviter l'infection par un virus • 117**

**Peut-on se passer d'un antivirus ? • 118**

**Expulser les logiciels espions • 118**

**Récapitulatif • 121**

**4. LES RÉSEAUX, AUTOROUTES DE L'INTRUSION ..... 123**

**Messagerie, forums ou navigation sur Internet : les risques induits par les protocoles de transmission • 125**

Rôle majeur des protocoles « IP » dans les communications sur Internet • 125

Adressage IP • 125

Transmission d'informations avec le protocole IP • 126

- Réseau IP • 127
- Protocole TCP • 128
- Couches fonctionnelles : modèle OSI • 129
  - Couches 1 (physique) et 2 (liaison) • 130
  - Couche 3 (réseau) • 130
  - Couche 4 (transport) • 131
  - Couche 7 (application) • 131
  - Modèle simplifié TCP/IP • 131
- Protocoles UDP et ICMP • 132
- Comment l'attaquant perçoit-il un protocole de communication ? • 134
- Attaques perpétrées via les protocoles réseau • 134**
  - Derrière leur apparente innocence, les protocoles IP sont de redoutables vecteurs d'intrusion • 134
  - Utilisation de TCP, UDP ou ICMP pour analyser une installation à distance • 135
    - Exploitation de ICMP • 135
    - Ouverture de session TCP • 136
    - Balayage de ports • 136
    - Exploitation du TTL • 138
  - Telnet, FTP, TFTP et SNMP, facteurs de risque • 139
    - Telnet • 139
    - TFTP • 139
    - SNMP • 140
  - Risques liés aux protocoles NetBIOS • 141
- Attaques perpétrées via les protocoles applicatifs • 143**
  - Dangers liés à HTTP • 143
    - Encapsulation de protocole • 144
    - Téléchargement de codes mobiles • 144
    - Détournement des flux chiffrés • 145
  - Piratage par courrier électronique • 145
- Risques liés aux applications sur Internet • 147**
  - Applications sur Internet : des vecteurs potentiels d'intrusion • 147
  - Se protéger des attaques dirigées contre les applications • 149
- Mention spéciale pour le Wi-Fi • 150**
  - Réseau Wi-Fi • 150
  - Risques liés au Wi-Fi • 151
  - Localisation des points d'accès • 152
  - Intrusion au cœur de votre système • 152
  - Mesures de protection • 153
    - Installez un pare-feu personnel • 153
    - Utilisez WPA, voire WPA2 • 153
    - Activez la traduction d'adresse (NAT) • 154
    - Masquez le SSID • 154
    - Ayez recours aux tunnels VPN (Virtual Private Network) • 154
    - Désactivez le Wi-Fi lorsque vous vous raccordez au réseau filaire • 155
- Récapitulatif • 155**
- 5. METTRE EN PLACE ET CONFIGURER SON PARE-FEU PERSONNEL..... 157**
- Notions générales sur les pare-feux • 159**
  - Qu'est-ce qu'un pare-feu ? • 159
  - Antivirus et pare-feu • 160
  - Cible du pare-feu • 161
  - Différents types de pare-feux • 161
    - Pare-feux de niveau 4, dits « stateful inspection » • 162
    - Pare-feux applicatifs • 163
  - Fonctionnement d'un pare-feu • 163
  - Limites des pare-feux • 165
  - Choisir un type de pare-feu • 165
  - Pare-feux logiciels disponibles gratuitement ou dans le commerce • 167
  - Choisir un pare-feu logiciel • 168
  - Sécurité assurée par les fournisseurs d'accès • 168
- Configurer son pare-feu personnel • 170**
  - Installer un pare-feu logiciel • 170
  - Définir la politique de filtrage des flux d'information • 170
  - Principales règles de filtrage protocolaire proposées par les pare-feux logiciels • 172
  - Filtrage du trafic ICMP • 174
  - Politique de filtrage des protocoles du Web et de la messagerie • 175
  - Politique de filtrage des ports TCP et UDP • 176
  - Filtrer les applications avec un pare-feu • 176
  - Traduction d'adresses • 181
  - Créer ses propres règles de filtrage • 184
  - Réagir aux alertes affichées par les pare-feux • 187
  - Journaux du pare-feu • 188
  - Trouver le juste équilibre entre le niveau de protection délivré par un pare-feu et la facilité d'emploi • 190
  - Protéger l'accès aux fonctions d'administration du pare-feu • 191
- Les pare-feux matériels • 191**
  - Nécessité d'un pare-feu matériel • 191
  - Emplacement du pare-feu matériel • 192
  - Avantages d'un pare-feu matériel par rapport à un pare-feu logiciel • 192
  - Principaux pare-feux matériels disponibles sur le marché • 194
    - Cyberguard Firewall (US) • 194
    - Arkoon Network Security France) • 195
    - Netasq (France) • 196

- Check Point (Israël) • 197
- Choisir un pare-feu matériel • 197
- Détection et prévention d'intrusion • 199**
  - Détecter une tentative d'intrusion • 199
  - Apport d'un logiciel spécifique de détection et de prévention d'intrusion en complément du pare-feu • 200
  - Principales sondes en matière de détection et de prévention d'intrusion • 201
  - Règles natives des IDPS • 201
  - Écrire une règle de détection d'intrusion avec Snort • 202
    - Type d'action • 202
    - Type de protocole • 202
    - Adresses IP, ports source et destination • 203
    - Opérateur de direction • 203
    - Options • 204
- Récapitulatif • 204

## **6. RECONNAÎTRE L'AUTHENTICITÉ SUR INTERNET AVEC LES CERTIFICATS .....207**

- Certifier une clé publique • 209
- Certificat, signature et autorité de certification • 210
- Déchiffrer un certificat • 211
  - Exemple concret • 211
  - Processus d'authentification d'un correspondant • 212
- Principe de confiance • 214
- Réseaux de confiance • 214
  - Infrastructures centralisées X.509 • 215
  - Organismes habilités à établir un certificat • 215
    - Autorité de certification racine • 215
    - Chaîne de certification • 216
    - Modèle réel composé de nombreuses autorités de certification • 218
- Listes de révocation • 219
- Récapitulatif • 220

## **7. CONFIGURER SON NAVIGATEUR INTERNET DE FAÇON SÉCURISÉE.....223**

- Un pare-feu et un antivirus ne sont pas suffisants. • 224
- Risques liés aux navigateurs • 225
  - Codes mobiles présents dans les pages web • 225
  - Contrôles ActiveX • 226
    - Protection par Authenticode • 228
    - Contrôle ActiveX reconnu sûr pour l'écriture de scripts • 231
  - Applets Java • 231
  - Autres formes de risques liés aux contenus exécutables • 233

- Modules externes ou plug-ins • 234
- Scripts • 234

Cookies • 235

## **Fonctions de sécurité offertes par les navigateurs • 236**

- Sécuriser Internet Explorer • 237
  - Zones de sécurité prédéfinies • 238
  - Paramètres de sécurité affectés à chaque zone • 240
  - Affecter un site web à une zone de sécurité • 244
  - Paramètres de « confidentialité » • 244
- Sécuriser Netscape Navigator • 246
  - Préférences concernant les cookies • 246
  - Préférences concernant les scripts et plug-ins • 248
  - Préférences liées à l'interprétation des pages web • 248
  - Préférences concernant les scripts • 249
- Sécuriser Mozilla Firefox • 250
  - La gestion des cookies • 251
  - Gestion des mots de passe de sites web • 252
  - Paramètres de sécurité liés aux fonctionnalités web • 252

## **Gérer les certificats • 254**

- Afficher la liste des certificats stockés dans votre navigateur • 255
  - Sous Internet Explorer • 255
  - Sous Netscape • 255
  - Sous Firefox • 256
- Modifier la liste des certificats présents par défaut dans le navigateur • 257
- Attitude à adopter lorsqu'un certificat ne peut être vérifié • 258
- Déterminer si le certificat d'une nouvelle autorité de certification est fiable • 260
- Gérer les listes de révocation • 262
  - Sous Internet Explorer • 262
  - Sous Netscape Navigator • 262
  - Sous Firefox • 266

Récapitulatif • 266

## **8. SÉCURISER SON COURRIER ÉLECTRONIQUE ..... 269**

- Lutter contre les messages non sollicités • 270
  - Le spam • 270
    - Divulgarion de votre adresse de courrier électronique • 272
    - Protéger son adresse électronique contre le spam : quelques mesures simples • 272
      - Un compte public et un compte privé • 272
      - Une adresse résistant au spam • 274
      - Un domaine peu usité • 274
      - Plutôt l'image que le texte • 274
  - Le phishing • 276

Éviter de se faire piéger avec le phishing • 277	Installer les extensions de sécurité • 313
Filtrer les messages indésirables • 277	Configurer Enigmail • 314
Mode opératoire d'un filtre antispam • 277	Diffuser votre clé publique OpenPGP • 317
Services proposés par les clients de messagerie pour filtrer les spams • 278	Obtenir la clé OpenPGP d'un correspondant • 318
Bloquez ou déplacez les indésirables • 278	Signer ou chiffrer un message avec OpenPGP • 318
Règles de filtrage des messages • 279	Récapitulatif • 320
Installer un filtre antispam additionnel • 281	<b>9. TRANSACTIONS ÉLECTRONIQUES</b>
Principaux filtres antispam disponibles actuellement • 281	<b>ET PAIEMENT SUR INTERNET ..... 323</b>
Configurer un filtre antispam • 281	<b>Acheter et payer sur Internet • 325</b>
Une solution simple pour une protection efficace • 284	Principes mis en œuvre au cours d'une transaction électronique sécurisée • 325
<b>Réduire les risques d'infection virale ou de pénétration via la messagerie • 284</b>	Déroulement d'une transaction électronique sécurisée • 326
Optimiser la configuration de son antivirus vis-à-vis de la messagerie électronique • 285	Niveau de sécurité réel offert au consommateur lors d'une transaction SSL • 329
Bloquer images et contenus externes dans les messages HTML • 285	Moyens mis à votre disposition pour rendre vos transactions plus sûres • 331
<b>Préserver la confidentialité et garantir l'authenticité d'un message électronique • 286</b>	Vigilance • 331
Principes de fonctionnement des échanges sécurisés • 287	Législation française favorable au consommateur en ligne • 331
Chiffrement d'un message • 287	Modèle de transaction avec tiers • 332
Signature d'un message • 289	<b>Étude de cas : la sécurité dans le cadre de la déclaration des revenus sur Internet • 334</b>
Chiffrer et signer à l'aide des certificats • 291	Obtenir votre certificat • 335
Échanger des messages signés et/ou chiffrés avec un correspondant • 291	Vérifier le certificat • 336
Obtenir un certificat et l'intégrer dans votre client de messagerie • 292	Importer les certificats des AC signataires • 339
Diffuser votre certificat à vos interlocuteurs • 295	Utiliser les services sécurisés • 340
Récupérer et intégrer le certificat d'un correspondant • 296	Récapitulatif • 342
Signer ou chiffrer un message • 298	<b>10. ET WINDOWS VISTA ? ..... 345</b>
Lire un message chiffré par votre correspondant • 300	Conséquences du contrôle d'accès généralisé aux contenus • 346
Vérifier la signature et donc l'authenticité d'un message • 300	Signature des pilotes et des exécutables • 348
Authentification de l'expéditeur via un certificat • 302	Dépendance vis-à-vis du fournisseur • 349
Niveau de protection réel délivré • 304	Dépendance technologique et absence d'interopérabilité • 350
Problème de la fiabilité des clés secrètes et privées • 305	TCPA, Palladium et NGSCB • 350
Renforcer la sécurité des échanges par voie de messagerie électronique • 307	La sécurité, je fais tout seul • 353
Valeur juridique de la signature d'un message électronique • 308	Améliorations de la sécurité du système • 354
Sécuriser son courrier sous Thunderbird avec OpenPGP • 308	L'ombre du piratage plane toujours • 355
Modèle de confiance d'OpenPGP • 308	Faut-il migrer ? • 356
Réseau de confiance • 308	<b>A. NOTIONS DE CRYPTOLOGIE ..... 357</b>
Niveaux de confiance • 310	<b>B. DIFFÉRENTS TYPES D'ATTAQUES ..... 377</b>
	<b>INDEX ..... 381</b>