

Sommaire

Edito 2

Avant-propos 3

Objectifs 3
Les outils 4
L'organisation du livre 4
A qui s'adresse l'ouvrage 4
Pré requis 4

Problèmes et solutions 5

Inspecter ses défenses 1 7

Système et sécurité 7
Le centre de maintenance 8

Sauvegarder 2 11

Pourquoi sauvegarder ? 11
Que sauvegarder ? 11
Où sauvegarder ? 12
Les types de sauvegarde 13

Sauvegarde de Windows 3 15

Pourquoi Windows ? 15
Le point de restauration 15
L'image système 17

Sauvegarde des données 4 19

Quelles données sauvegarder ? 19
Différents types de sauvegardes 19
Sauvegarde avec Windows 7 20
Sauvegarder avec SyncBack 22
CrashPlan 25
Paramétrer CrashPlan 28

Les virus 5 31

Virus ? 31
L'infection 31
L'antivirus 32
Analyser l'ordinateur 34
Mise à jour de la liste de virus 35
En cas d'infection 35
Et si ça ne suffit pas ? 36
Les types de virus 37
Security Essential de Microsoft 37

Le pare-feu 6 39

A quoi sert un pare-feu ? 39
Les types de pare-feu 40
Le pare-feu de Windows 7 40
ZoneAlarm 42
Norton Internet Security 45

Les espions 7 47

Que font les logiciels espions ? 47
Les logiciels de défense 47
Windows Defender 48
Ad-Aware 50
Spybot Search & Destroy 53
Norton Internet Security 55
Choisir 56

Le spam 8 57

Le Spam, cette plaie 57
L'adresse email, une mine d'or 58
Le filtre antispam 58
Réagir au spam 59
Un exemple de filtre 60

Le hameçonnage 9 63

Qu'est-ce que le hameçonnage ? 63
Comment la fraude fonctionne 63
Comment se protéger 64

Protéger vos données 10 67

Les dommages possibles 67
Le mot de passe 68
KeePass 70
Les comptes utilisateurs 74
Empêcher l'accès à vos données 74
TrueCrypt 75

Mises à jour 11 81

Windows Update 81
La mise à jour automatique 81
La recherche de mises à jour 82
La mise à jour d'autres produits 83

La connexion Wi-Fi 12 85

Le WiFi 85
Clé de sécurité 86
Chiffrer la connexion Wi-Fi 87
Le filtrage MAC 88
Se protéger avec un VPN 89

Glossaire 93

Index 96