

PROTÉGER SA VIE NUMÉRIQUE — EN 2026 —

Le guide pratique pour sécuriser vos comptes,
vos données et vos appareils au quotidien



MOTS DE PASSE
SÉCURISÉS



ÉVITER LE
PHISHING



SAUVEGARDES
RÉGULIÈRES



OUTILS GRATUITS
FIABLES



RÉSEAU WI-FI
PROTÉGÉ



MISES À JOUR
À JOUR



APPAREILS
SÉCURISÉS



BONNES
PRATIQUES



COMPRENDRE
LES RISQUES
pour mieux
les éviter



PROTÉGER
VOS COMPTES
mots de passe
et accès



SAUVEGARDER
VOS DONNÉES
ne perdez jamais
l'essentiel



ADOPTER
LES BONS
RÉFLEXES
au quotidien



RÉAGIR
EN CAS
D'INCIDENT
avec méthode



Michel Martin

Table des matières

La sécurité numérique, un réflexe du quotidien	5
Pourquoi la protection numérique est devenue essentielle	5
Ce que vous allez apprendre dans ce manuel	5
Les outils et méthodes utilisés	6
Partie 1 — Comprendre les risques numériques.....	7
Les grandes familles de menaces	7
Comment les cybercriminels opèrent	8
Les erreurs les plus courantes des utilisateurs	8
Les signaux d’alerte que vous devez reconnaître	8
Partie 2 — Sécuriser ses comptes et ses mots de passe	10
Créez des mots de passe solides et uniques	10
Utilisez un gestionnaire de mots de passe	10
Protégez vos comptes Microsoft, Google, Apple et réseaux sociaux	12
Que faire en cas de piratage ?	12
Partie 3 — Se prémunir contre le phishing et les autres arnaques	14
Reconnaître un message frauduleux	14
Les pièges les plus fréquents	14
Vérifier les liens et les expéditeurs	15
Que faire si vous avez cliqué ou fourni des informations ?	20
Les outils gratuits pour détecter les sites dangereux	20
Partie 4 — Sauvegardez vos données sans vous tromper	26
Pourquoi la sauvegarde est votre meilleure assurance.....	26
Les trois niveaux de sauvegarde : locale, externe et cloud	26
La règle du 3-2-1 expliquée simplement	27
Sauvegarde incrémentielle	27
Automatiser les sauvegardes.....	31
Restaurer ses fichiers après un incident	36
Les erreurs les plus fréquentes.....	36
Partie 5 — Les bonnes pratiques au quotidien	38
Mettre à jour Windows, macOS, Android et iOS.....	38
Sécurisez votre navigateur et ses extensions	39
Protéger ses e-mails et ses messageries	42
Sécurisez le Wi-Fi et les appareils connectés	43

Les réflexes à adopter avant de cliquer, télécharger ou partager	44
Une routine de sécurité en moins de cinq minutes	45
Les dix réflexes à retenir	45
Partie 6 — Les outils gratuits pour vous protéger	47
Antivirus et antimalwares fiables	47
Gestionnaires de mots de passe.....	50
VPN et navigateurs sécurisés.....	50
Extensions anti-phishing et bloqueurs de traqueurs.....	58
Outils de sauvegarde et de chiffrement	59
Les erreurs à éviter	60
Partie 7 — Que faire en cas d’incident ?	61
Identifier le type d’attaque	61
Contactez les bons interlocuteurs	64
Plan d’urgence en cas d’incident	67
Partie 8 — L’avenir de la sécurité numérique.....	68
Les nouvelles technologies de protection	68
Des protections plus discrètes.....	69
La biométrie : pratique, mais à utiliser avec prudence	69
Les clés d’accès : vers la fin des mots de passe	69
Le chiffrement avancé	70
Le chiffrement post-quantique	70
L’intelligence artificielle générative	71
Les deepfakes	71
Le vol d’identité numérique	72
Restez vigilant(e) dans un monde connecté.....	72
Bonus — Routine de sécurité numérique	73
Routine quotidienne (moins de 2 minutes).....	73
Routine hebdomadaire (5 minutes)	74
Routine mensuelle (15 à 20 minutes).....	75
Routine trimestrielle (30 minutes)	76
Routine annuelle (environ une heure)	77
Votre tableau de bord de sécurité.....	78
Routine minimale en cinq minutes par semaine	79
Annexes	80
Annexe 1 — Glossaire des termes essentiels	80
Annexe 2 — Liste des sites officiels et services d’aide.....	86

Annexe 3 — Modèles de messages pour signaler une fraude	88
Le mot de la fin	91