GUIDE ULTIME DE CYBERSÉCURITÉ

*Protéger ses données et se prémunir des cybermenaces*

# Introduction

Pourquoi ce guide ?

La cybersécurité est une responsabilité partagée : que vous soyez utilisateur individuel ou professionnel, vous êtes une cible potentielle.

Ce guide vous apporte une compréhension pratique des menaces numériques et des bonnes pratiques à adopter.

# I. Les Données Personnelles

## A. Définition

Une donnée personnelle est toute information permettant d'identifier une personne physique, directement ou indirectement.

* Nom et prénom
* Adresse postale ou e-mail
* Numéro de téléphone
* Numéro de carte bancaire
* Adresse IP
* Photos, vidéos, empreinte digitale

## B. Pourquoi les protéger ?

* Prévenir l'usurpation d'identité
* Éviter la fraude financière
* Respecter la vie privée

## C. Réglementation

Le RGPD (Règlement Général sur la Protection des Données) encadre la collecte, le traitement et la protection des données personnelles en Europe.

# II. Sécurisation des Comptes en Ligne

## A. Créer un mot de passe robuste

* Longueur minimale : 12 caractères
* Inclure des majuscules, minuscules, chiffres et symboles
* Éviter les informations personnelles et les suites logiques

Exemple sécurisé : T!gR@9Xz#K

## B. Gestionnaire de mots de passe

Un gestionnaire de mots de passe génère et stocke des mots de passe complexes, accessibles avec un mot de passe maître sécurisé.

* Bitwarden
* Dashlane
* 1Password

## C. Authentification à Deux Facteurs (2FA)

La 2FA combine un mot de passe et un second facteur d'authentification (code SMS, app mobile) pour renforcer la sécurité des comptes.

# III. Les Risques sur Internet et Comment s’en Protéger

## A. Le Phishing

Technique de fraude visant à voler des informations personnelles (identifiants, coordonnées bancaires) via des e-mails ou sites frauduleux.

* Fautes d'orthographe
* Demandes urgentes
* Adresses d'expéditeur suspectes

Exemple : E-mail prétendant venir de votre banque vous demandant de confirmer vos identifiants via un lien piégé.

## B. Liens et Pièces Jointes Suspectes

Ne jamais cliquer sur un lien ni ouvrir une pièce jointe provenant d'un expéditeur inconnu ou suspect.

Vérifier l'URL en survolant le lien sans cliquer.

## C. QR Codes Inconnus

Ne jamais scanner un QR code dont la source est inconnue ou non vérifiée.

# IV. Sécurité des Réseaux

## A. Wi-Fi Public

* Utiliser un VPN
* Éviter les transactions sensibles sur un réseau public
* Privilégier la 4G/5G

## B. Réseaux Domestiques

* Modifier le mot de passe par défaut du routeur
* Désactiver le WPS
* Mettre à jour le firmware du routeur

# V. Mises à Jour et Sauvegardes

## A. Mises à Jour

Installer immédiatement les mises à jour pour corriger les vulnérabilités de sécurité.

## B. Sauvegardes

Sauvegardez régulièrement vos fichiers sur plusieurs supports (disque dur externe, cloud).

* Sauvegarde hebdomadaire recommandée
* Conserver une copie hors ligne (déconnectée)

# VI. Les Menaces Courantes

## A. Ransomware

Un logiciel malveillant qui chiffre vos fichiers et demande une rançon pour récupérer l'accès.

## B. Attaques par Force Brute

Tentative de deviner un mot de passe en testant toutes les combinaisons possibles.

## C. SIM Swapping

Usurpation de votre numéro de téléphone pour intercepter des SMS 2FA.

# VII. Sécurité Mobile et IoT

## A. Sécurité des Smartphones

* Verrouiller l'écran (code, empreinte, reconnaissance faciale)
* Désactiver la géolocalisation si non nécessaire
* Vérifier les permissions des applications

## B. Objets Connectés

* Changer les mots de passe par défaut
* Mettre à jour les appareils régulièrement
* Isoler les objets connectés sur un réseau dédié

# VIII. Bonnes Pratiques en Environnement Professionnel

* Verrouiller son ordinateur lorsqu'on quitte son poste
* Ne jamais partager ses mots de passe, même avec des collègues
* Utiliser un mode invité ou une session temporaire pour les prêts d'appareil
* Vérifier toute demande urgente par téléphone ou en face à face

# IX. Outils Indispensables

|  |  |  |
| --- | --- | --- |
| Outil | Fonction | Exemple |
| Gestionnaire de mots de passe | Stocker et générer des mots de passe complexes | Bitwarden, Dashlane |
| VPN | Chiffrer la connexion et sécuriser les réseaux Wi-Fi publics | ProtonVPN, NordVPN |
| Antivirus | Protéger contre les malwares et ransomwares | Bitdefender, ESET |
| Pare-feu | Filtrer le trafic réseau entrant et sortant | Pare-feu Windows, pfSense |
| Chiffrement de disque | Protéger les données en cas de vol d’appareil | BitLocker, FileVault |

**🔗 Sources et ressources utiles :**

* ANSSI : https://www.ssi.gouv.fr/
* CNIL : https://www.cnil.fr/
* Cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/

# X. Cas Pratiques et Simulations

* Détecter un e-mail frauduleux : vérifier l'adresse, les fautes, le lien URL
* Réagir à un SMS suspect : ignorer, bloquer, signaler
* Créer un mot de passe sécurisé : utiliser un générateur, éviter les informations personnelles
* Scanner un QR code en toute sécurité : vérifier la source
* Effectuer une sauvegarde régulière : planifier sur plusieurs supports

**🔗 Ressources pour approfondir :**

* Cybermalveillance.gouv.fr : fiches pratiques
* ANSSI : guides de bonnes pratiques numériques
* CNIL : recommandations sur la protection des données personnelles

# Glossaire

|  |  |
| --- | --- |
| Terme | Définition |
| Phishing | Technique visant à récupérer des informations confidentielles par la ruse |
| 2FA | Authentification à deux facteurs |
| VPN | Réseau privé virtuel permettant de sécuriser les connexions Internet |
| Ransomware | Logiciel malveillant bloquant l'accès aux données contre une rançon |
| Pare-feu | Outil filtrant les connexions réseau autorisées ou interdites |

# Conclusion

La cybersécurité est l'affaire de tous. Adoptez ces bonnes pratiques et partagez-les autour de vous pour un environnement numérique plus sûr.