GUIDE ULTIME DE CYBERSÉCURITÉ

Protéger ses données et se prémunir des cybermenaces

# Introduction à la Cybersécurité

La cybersécurité est aujourd’hui un enjeu majeur pour les particuliers et les entreprises. Les cyberattaques sont de plus en plus fréquentes et sophistiquées, ciblant aussi bien les multinationales que les PME ou les particuliers. L’objectif de ce guide est de fournir les clés pour comprendre les principales menaces et adopter des comportements sécurisés.

## Pourquoi ce guide ?

* Sensibiliser aux dangers numériques
* Fournir des réponses aux questions des QCM "Débutant", "Pro", "Avancé"
* Donner des outils pratiques pour sécuriser ses données

# 1. Comprendre les Cyberattaques

## A. Phishing (Hameçonnage)

Le phishing est une méthode utilisée par les hackers pour récupérer des informations personnelles (identifiants, mots de passe, coordonnées bancaires) via des emails, SMS ou sites frauduleux.

### Comment le reconnaître ?

* Fautes d’orthographe
* Demandes urgentes d’agir rapidement
* Adresses d’expéditeur suspectes
* Liens suspects (vérifiez toujours l’URL !)

### Exemple :

Email "Votre compte est suspendu. Cliquez ici pour vérifier vos informations."

**Sources :**

* ANSSI : https://www.ssi.gouv.fr/
* Cybermalveillance.gouv.fr

## B. Vishing et Smishing

* \*\*Vishing\*\* : Appels frauduleux simulant des services techniques ou des banques
* \*\*Smishing\*\* : SMS contenant des liens malveillants

Réflexe : Ne jamais divulguer d’informations personnelles par téléphone ou SMS.

# 2. Logiciels Malveillants

## A. Ransomware

Malware qui chiffre vos données et demande une rançon pour les récupérer.

### Protection :

* Sauvegardes régulières
* Ne jamais ouvrir de pièces jointes inconnues

## B. Keylogger

Logiciel espion qui enregistre les frappes clavier.

### Détection et prévention :

* Utiliser des antivirus réputés
* Sensibiliser à l’installation de logiciels douteux

## C. Trojan et Malware Polymorphe

* Se fait passer pour un logiciel légitime
* Change de forme pour contourner les antivirus

# 3. Attaques Réseau et Web

## A. Man-in-the-Middle (MITM)

Interceptent les communications sur un réseau non sécurisé. Préférez le VPN.

## B. DNS Spoofing

Redirige vers de faux sites via la manipulation des DNS.

## C. Man-in-the-Browser

Malware modifiant les transactions bancaires en temps réel dans le navigateur.

# 4. Méthodes d’Accès aux Comptes

## A. Attaque par Force Brute et Dictionnaire

Essai automatique de mots de passe jusqu’à trouver le bon. Utilisez des mots de passe longs et complexes.

## B. MFA (Authentification Multi-facteur)

Ajoutez une couche de sécurité (code SMS, applications comme Google Authenticator).

# 5. Sécurité des Données et des Réseaux

## A. Chiffrement de Bout en Bout

Permet de protéger les communications, même contre le fournisseur de service.

## B. Sauvegardes régulières

Testez régulièrement vos sauvegardes pour garantir leur fiabilité.

## C. Journalisation et Sandbox

Surveillez les accès aux systèmes (logs) et testez les fichiers suspects en environnement isolé (sandbox).

# 6. Attaques Avancées et Menaces

## A. Supply Chain Attacks

Attaques sur des fournisseurs pour atteindre les clients finaux.

## B. Zero-Day Exploits

Exploitation de failles inconnues du fournisseur.

## C. Deepfakes

Utilisés pour usurper l’identité et manipuler (fraudes au président).

# 7. Bonnes Pratiques Quotidiennes

* Vérifiez l’URL des sites (typosquatting)
* Limitez les permissions des applications mobiles
* Désactivez les macros dans les documents Office
* N’acceptez pas les invitations d’inconnus sur les réseaux sociaux

# 8. Cas Concrets et Scénarios

* \*\*Email frauduleux d’une banque\*\* : ne jamais cliquer, vérifier directement sur le site officiel.
* \*\*Appel d’un faux technicien\*\* : raccrocher et contacter l’entreprise par ses canaux officiels.
* \*\*Wi-Fi public\*\* : utiliser un VPN.

# 9. Ressources et Outils Recommandés

## Gestionnaires de mots de passe :

* Bitwarden, Dashlane

## VPN :

* ProtonVPN, NordVPN

## Antivirus :

* Bitdefender, ESET

## Sources fiables :

* ANSSI : https://www.ssi.gouv.fr/
* CNIL : https://www.cnil.fr/
* Cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/
* MITRE ATT&CK : https://attack.mitre.org/

# 10. Glossaire

* \*\*Phishing\*\* : Hameçonnage
* \*\*Ransomware\*\* : Logiciel de rançon
* \*\*Zero-Day\*\* : Faille inconnue
* \*\*MFA\*\* : Authentification multi-facteur

# 11. Conclusion

La cybersécurité est un enjeu collectif. En suivant ces conseils et en restant vigilant, vous renforcez votre sécurité et celle de votre environnement professionnel ou personnel.