Guide pédagogique de sécurité informatique

Introduction : pourquoi ce guide est essentiel

Selon le rapport Verizon, **81 % des violations de données sont causées par des mots de passe faibles ou volés**. Cette statistique montre que la majorité des cyberattaques exploitent des erreurs humaines simples et évitables.

L'objectif de ce guide est de fournir des **règles claires, compréhensibles et applicables immédiatement**, afin d'améliorer la sécurité numérique d'utilisateurs non techniques, aussi bien dans un cadre personnel que professionnel.

---

1. Les mots de passe : première ligne de défense

1.1 Principe fondamental

Règle clé : la longueur est plus importante que la complexité.

Un mot de passe long augmente de manière exponentielle le temps nécessaire pour être cassé par force brute, même s'il utilise des mots simples.

1.2 Comparaison de deux modèles

Mot de passe complexe mais faible :

Tr0ub4dor&3

- 11 caractères
- Structure prévisible
- Vulnérable aux attaques automatisées

Phrase de passe robuste :

correct horse battery staple

- 28 caractères
- Facile à mémoriser
- Extrêmement résistante au cassage

Modèle	Exemple	Sécurité	Mémorisation
Complexe mais faible	Tr0ub4dor&3	**Facile à deviner** (~28 bits d'entropie)	**Difficile**
Phrase de passe robuste	correct horse battery staple	**Difficile à deviner** (~44 bits d'entropie)	**Déjà mémorisée**

---

2. Stockage sécurisé des mots de passe

2.1 Méthodes à proscrire absolument

- Fichiers texte ou tableurs
- Carnets papier
- Post-it visibles
- Enregistrement dans le navigateur sans mot de passe maître

Ces pratiques exposent l'ensemble des accès en cas de perte ou de compromission du poste.

2.2 Solution recommandée : le gestionnaire de mots de passe

Un gestionnaire de mots de passe fonctionne comme un **coffre-fort numérique chiffré**.

Principe de fonctionnement : - Un seul mot de passe maître - Accès à un coffre chiffré en **AES-256** (standard cryptographique de niveau militaire) - Tous les autres identifiants sont stockés de manière sécurisée

Avantages principaux : - Génération automatique de mots de passe longs et uniques - Suppression de la réutilisation des mots de passe - Synchronisation sécurisée entre appareils

2.3 Outils recommandés

- Bitwarden : gratuit, open-source, recommandé par les professionnels
- 1Password : solution commerciale reconnue pour son ergonomie

---

3. Authentification à deux facteurs (2FA)

3.1 Principe

L'authentification à deux facteurs ajoute une barrière supplémentaire. Même si un mot de passe est compromis, l'accès reste bloqué sans le second facteur.

3.2 Les trois facteurs d'authentification

1. Ce que vous savez : mot de passe
2. Ce que vous avez : téléphone, clé physique
3. Ce que vous êtes : biométrie

3.3 Comparaison des méthodes 2FA

• **Méthode**	• **Niveau de Sécurité**	• **Recommandation**
• **Clé physique (YubiKey)**	• Maximale	• Idéal pour les comptes critiques.
• **Application (Authy/TOTP)**	• Élevée	• Recommandé pour tous les usages.
• **SMS**	• Faible	• À éviter (vulnérable au SIM Swapping).
• **E-mail**	• Très faible	• Déconseillé.

---

4. Phishing : la principale menace actuelle

Le phishing consiste à se faire passer pour un service légitime afin de voler des identifiants ou des informations sensibles.

Signes d'alerte fréquents

- Message créant un sentiment d'urgence
- Fautes d'orthographe ou de syntaxe
- Liens suspects ou raccourcis
- Demande d'identifiants ou de paiement

Règle absolue : aucun service sérieux ne demande un mot de passe par e-mail.

---

5. Hygiène numérique : bonnes pratiques quotidiennes

- Verrouiller son poste lors des absences
- Vérifier systématiquement l’adresse du site avant connexion
- Ne jamais transmettre d’identifiants par e-mail
- Éviter les réseaux Wi-Fi publics sans protection
- Utiliser des mots de passe uniques pour chaque service

---

6. Mises à jour : un enjeu critique

La majorité des cyberattaques exploitent des failles connues pour lesquelles un correctif existe déjà.

Les mises à jour corrigent ces vulnérabilités. Ne pas les appliquer revient à laisser une porte ouverte.

Éléments à maintenir à jour : - Systèmes d’exploitation - Navigateurs web - Applications critiques et professionnelles

---

7. Protection logicielle

Un logiciel de protection (antivirus ou anti-malware) permet de détecter et bloquer les menaces telles que les ransomwares ou chevaux de Troie.

Il doit être : - Installé - Activé - Régulièrement mis à jour

---

8. L'Ingénierie Sociale et les Menaces Avancées

- **Le Risque d'Autorité :** Les attaquants ne créent pas seulement de l'urgence ; ils utilisent souvent une position d'autorité (faux patron, faux technicien) pour demander des transferts d'argent ou des codes[1].
- **Deepfakes et IA :** Avec l'essor de l'IA, il faut désormais se méfier des appels ou vidéos non sollicités. La règle d'or est d'exiger une vérification écrite par un autre canal pour toute action critique demandée oralement[2].

9. La Sécurité des Objets et de la Mobilité

Nos environnements sont remplis d'appareils connectés qui sont souvent des maillons faibles :

- **Smart Home & IoT :** Il est crucial de changer les mots de passe par défaut de ces appareils et, si possible, de les isoler sur un réseau Wi-Fi "invité"[3].
- **Le Bluetooth :** Maintenez-le désactivé lorsqu'il n'est pas utilisé pour éviter le "Bluebugging" (piratage via Bluetooth)[4].
- **Perte ou Vol :** Configurez systématiquement les fonctions de localisation et d'effacement à distance sur vos smartphones[5].

10. Le Partage de Secrets (Alternative à l'E-mail)

- **Liens Éphémères :** Pour partager un identifiant ponctuellement, utilisez des outils comme **PrivateBin** ou **OneTimeSecret**, qui créent des liens s'autodétruisant après la première lecture[6].

11. Le Principe du Moindre Privilège

C'est une règle de base souvent oubliée par les particuliers :

- **Comptes Administrateurs :** N'utilisez pas votre ordinateur avec un compte "Administrateur" pour vos tâches quotidiennes (navigation web, mails). Utilisez un compte "Utilisateur Standard" et ne basculez en administrateur que lorsque c'est strictement nécessaire[7].

Tableau de Synthèse de l'Hygiène Numérique

Domaine	Action Prioritaire	Objectif
Accès	Phrase de passe de 12+ caractères[8].	Rendre le cassage par force brute lent[9].
Stockage	Utiliser un gestionnaire chiffré (Bitwarden)[10].	Garantir l'unicité des accès[11].
Connexion	Activer la 2FA (Application de préférence)[12].	Protéger le compte même si le code est volé[13].
Maintenance	Mises à jour immédiates des logiciels[14].	Fermer les failles de sécurité connues[15].

Conclusion

La sécurité informatique repose sur une combinaison de bonnes pratiques simples mais rigoureuses.

- Utiliser des phrases de passe longues et uniques
- Stocker ses accès dans un gestionnaire sécurisé
- Activer l'authentification à deux facteurs
- Rester vigilant face au phishing
- Mettre à jour régulièrement ses systèmes

La cybersécurité n'est pas un outil, mais un comportement. En appliquant ces principes, l'utilisateur réduit considérablement son exposition aux menaces les plus courantes.

Glossaire pour les Non-Techniciens

- **AES-256 :** Un standard de chiffrement de niveau militaire. Imaginez un coffre-fort dont la combinaison est si complexe qu'il faudrait des milliards d'années au superordinateur le plus puissant pour l'ouvrir sans la clé.
- **Force Brute :** Méthode d'attaque basique qui consiste à essayer toutes les combinaisons possibles de mots de passe jusqu'à trouver la bonne. Contrée par la longueur du mot de passe.
- **Phishing (Hameçonnage) :** Technique d'escroquerie envoyant de faux e-mails ou SMS semblant provenir d'une entreprise de confiance (banque, impôts) pour voler des identifiants.
- **Ransomware (Rançongiciel) :** Logiciel malveillant qui prend vos fichiers en otage en les chiffrant et demande une rançon pour les débloquer.
- **SIM Swapping :** Attaque où le pirate parvient à tromper votre opérateur mobile pour transférer votre numéro de téléphone sur sa propre carte SIM, lui permettant d'intercepter vos SMS de validation 2FA.
- **TOTP (Time-based One-Time Password) :** Le standard utilisé par les applications comme Google Authenticator. C'est un code à 6 chiffres qui change toutes les 30 secondes, généré localement sur votre téléphone sans avoir besoin de réseau.
- **VPN (Réseau Privé Virtuel) :** Outil qui crée un "tunnel" sécurisé et chiffré pour votre connexion internet, protégeant vos données, surtout sur les Wi-Fi publics.