

Les bases de la cybersécurité et les bonnes pratiques

Fondamentaux indispensables pour protéger les comptes, les postes et les données.

1. Les trois objectifs fondamentaux

Confidentialité	Empêcher les personnes non autorisées d'accéder aux informations.
Intégrité	Garantir que les données ne sont pas modifiées de manière non autorisée.
Disponibilité	Maintenir les systèmes et les données accessibles lorsqu'ils sont nécessaires.

2. Menace, vulnérabilité et risque

Menace : élément susceptible de provoquer un incident (malware, attaquant, phishing, erreur humaine, vol).

Vulnérabilité : faiblesse pouvant être exploitée (logiciel non corrigé, mot de passe faible, droits excessifs, mauvaise configuration).

Risque : possibilité qu'une menace exploite une vulnérabilité et provoque un impact.

À retenir : menace + vulnérabilité → risque

3. Menaces courantes

Malware	Terme générique pour un logiciel malveillant.
Virus / ver	Infecte des fichiers ou se propage, parfois automatiquement par le réseau.
Cheval de Troie	Programme qui paraît légitime mais contient une fonction malveillante.
Ransomware	Chiffre ou bloque des données et peut demander une rançon.
Spyware	Collecte des informations à l'insu de l'utilisateur.
Ingénierie sociale	Manipule une personne pour lui faire réaliser une action dangereuse.

4. Comptes, mots de passe et MFA

Mot de passe : privilégier la longueur, éviter les informations évidentes et ne pas réutiliser le même mot de passe sur plusieurs services.

Gestionnaire de mots de passe : permet d'utiliser des mots de passe longs et différents, avec une solution autorisée par l'organisation.

MFA : combine plusieurs facteurs (ce que l'on connaît, possède ou est) pour renforcer l'authentification.

Demande MFA inattendue : ne pas valider et signaler l'événement selon la procédure.

5. Les protections essentielles

Mises à jour	Corrigent notamment des vulnérabilités connues.
Antivirus	Détecte et bloque certaines menaces ; il ne suffit pas à lui seul.
Pare-feu	Contrôle les communications réseau selon des règles.
Moindre privilège	Attribuer uniquement les droits nécessaires.
Sauvegardes	Permettent de restaurer les données après un incident.

6. Sauvegarde : règle 3-2-1

3	copies des données
2	types de supports différents
1	copie hors site ou isolée

Une sauvegarde n'est utile que si elle est restaurable. Vérifier régulièrement les résultats et tester la restauration.

7. Phishing : les signaux d'alerte

- adresse d'expéditeur ou domaine inhabituel ;
- urgence, menace ou pression ;
- demande de mot de passe ou d'informations sensibles ;
- lien vers une adresse inhabituelle ;
- pièce jointe inattendue ;
- demande de paiement ou changement de coordonnées bancaires.

Bon réflexe : ne pas cliquer. Accéder directement au service par une adresse connue ou vérifier par un autre canal.

8. Supports USB, téléchargements et scripts

- Ne pas brancher un support USB inconnu sans respecter les procédures de l'organisation.
- Installer les logiciels depuis une source officielle ou un outil de déploiement approuvé.
- Être vigilant face aux fichiers exécutables et scripts : .exe, .msi, .bat, .cmd, .ps1, .js, .vbs, .scr.
- Afficher les extensions de fichiers permet de repérer des noms trompeurs comme facture.pdf.exe.

9. Poste potentiellement compromis

Signes possibles :

- fichiers renommés, chiffrés ou devenus inaccessibles ;
- message de rançon ;
- alertes antivirus inhabituelles ;
- logiciels inconnus ;
- demandes MFA répétées ;
- activité ou comportement anormal du poste.

Réflexe incident : limiter → identifier → documenter → escalader → analyser

Ne pas payer, ne pas improviser un nettoyage, ne pas réinstaller immédiatement le poste sans consigne adaptée. Préserver les informations utiles et appliquer la procédure de l'organisation.

10. Les réflexes à retenir

- Utiliser des mots de passe robustes et différents.
- Activer le MFA lorsqu'il est disponible.
- Maintenir les systèmes et logiciels à jour.
- Conserver antivirus et pare-feu actifs.
- Limiter les droits au strict nécessaire.
- Sauvegarder et tester les restaurations.
- Vérifier avant de cliquer, télécharger, brancher ou exécuter.
- Face à un incident : limiter, documenter et escalader.