

Hygiène numérique de base – Gameplon

1. Objectif de la plaquette

Elle sert à :

- Sensibiliser les utilisateurs aux risques numériques
- Proposer des gestes simples pour sécuriser leur poste
- Montrer que tu maîtrises les bases de l'hygiène numérique

2. Introduction

L'hygiène numérique regroupe les pratiques essentielles pour protéger un poste informatique contre les menaces courantes (malwares, fuites de données, intrusions). Dans le cadre du projet Gameplon, ces mesures garantissent la sécurité des machines utilisées en environnement pédagogique.

3. Bonnes pratiques techniques

- Mises à jour régulières du système et des logiciels Antivirus actif et à jour
- Pare-feu activé sur tous les profils réseau
- BitLocker activé pour chiffrer les disques
- Comptes utilisateurs non administrateurs pour les élèves
- Mot de passe fort et renouvelé régulièrement
- Sauvegardes régulières des données critiques

4. Bonnes pratiques comportementales

- Ne pas installer de logiciels non autorisés Ne pas ouvrir de pièces jointes suspectes
- Ne pas partager ses identifiants
- Verrouiller sa session en cas d'absence
- Utiliser des clés USB vérifiées ou désactivée

5. Outils utilisés dans Gameplon

- Script d'audit PowerShell pour vérifier l'état du poste Export CSV des composants critiques
- Vérification automatique des services essentiels (WinDefend, BITS...

6. Conclusion

Ces gestes simples permettent de maintenir un environnement sécurisé, stable et conforme aux recommandations de l'ANSSI. Ils doivent être appliqués systématiquement dans le cadre du projet Gameplon.