

Acculturation à la cybersécurité et respect des règles de sécurité

14.1. Introduction à l'acculturation à la cybersécurité

L'un des rôles fondamentaux de l'administrateur AIS est d'être **ambassadeur de la sécurité numérique au sein de son organisation**. Il ne suffit pas d'installer des pare-feux : il faut aussi **accompagner les utilisateurs, promouvoir les bonnes pratiques, et faire respecter la politique de sécurité**.

Objectifs :

- Sensibiliser tous les collaborateurs
 - Diffuser une culture sécurité active
 - Réduire les risques humains (phishing, erreurs)
 - Créer un climat de vigilance constructive
-

14.2. Pourquoi la cybersécurité est l'affaire de tous

Faits marquants :

- 90 % des incidents proviennent d'une erreur humaine
- Le phishing est la **1re porte d'entrée des ransomwares**
- L'usage personnel d'outils pro (shadow IT) est en forte hausse

Risques encourus :

- Vol ou fuite de données sensibles
 - Interruption de l'activité
 - Perte financière (amendes, rançon, réparations)
 - Perte de confiance client ou usager
 - Responsabilité juridique (ex : RGPD)
-

14.3. Notions clés à transmettre aux utilisateurs

Sujet	Explication simple
Mots de passe	Complexes, uniques, jamais partagés
MFA	Double authentification = sécurité renforcée
Emails suspects	Ne jamais cliquer sans vérifier l'expéditeur
Supports amovibles	Risques d'infection, usage réglementé

Sujet	Explication simple
Sites web	Privilégier le HTTPS, éviter les téléchargements
Réseaux Wi-Fi publics	Ne jamais s'y connecter sans VPN
Télétravail	VPN, verrouillage poste, confidentialité

14.4. Bonnes pratiques du quotidien numérique

- **Verrouillage automatique des postes**
 - **Mise à jour régulière des systèmes**
 - **Utilisation d'antivirus à jour**
 - **Pas de mot de passe dans un fichier texte**
 - **Sauvegarde personnelle des documents importants**
 - **Signalement des anomalies au support sans délai**
-

14.5. Comportements à risque à corriger

Mauvaise pratique	Risque
Utiliser le même mot de passe partout	Compromission en cascade
Ignorer les messages d'alerte	Incident non détecté
Connecter sa clé USB perso	Infection possible
Cliquer sur tout ce qui arrive par mail	Ransomware probable
Télécharger un logiciel depuis un blog	Logiciel espion intégré
Prêter son badge ou compte	Piste d'audit faussée

14.6. Moyens pédagogiques et sensibilisation

Formats recommandés :

- Sessions de formation courtes (15 à 30 min)
- Campagnes de phishing simulées
- Affiches/mémos en salles de pause
- Vidéos explicatives (ANSSI, CNIL)
- Boîte mail dédiée aux signalements
- Journée cybersécurité annuelle

Publics à cibler :

- Nouveaux arrivants
- Utilisateurs métiers sensibles (RH, finance)

- Responsables d'équipes
 - Télétravailleurs
-

14.7. Rôle de l'AIS dans la diffusion de la sécurité

L'AIS agit comme **réfèrent technique ET éducatif** :

- Explique les politiques internes de sécurité (PSSI, RGPD...)
 - Met en place des restrictions techniques ET les accompagne d'explications
 - Élabore des guides utilisateurs sécurisés
 - Anime des ateliers pratiques (ex : MFA, boîte mail piégée...)
-

14.8. Intégration des règles de sécurité dans les outils et procédures

- **GPO (Group Policy)** : désactiver supports USB, verrouillage auto, politique mot de passe
 - **Filtrage Web / DNS** : blocage des sites malveillants
 - **Pare-feux utilisateurs** : port 445 bloqué, règles sortantes strictes
 - **Postes utilisateurs verrouillés** après 10 min d'inactivité
 - **VPN obligatoire** hors site
 - **Accès AD** limités au strict nécessaire (PoLP)
-

14.9. Conformité avec la réglementation française

RGPD :

- Minimisation des données
- Consentement explicite
- Conservation limitée dans le temps
- Sécurité technique ET organisationnelle

CNIL :

- Guide des bonnes pratiques utilisateurs
- Charte informatique recommandée
- Délégué à la protection des données (DPO)

ANSSI :

- Guide d'hygiène informatique (42 règles)
- Recommandations sur la sensibilisation

- Responsabilité partagée entre DSI, RH, sécurité
-

14.10. Activités pratiques et évaluation

Projets :

- Création d'un mémo cybersécurité à destination des collègues
- Animation d'un atelier MFA ou gestion des mots de passe
- Simulation d'une attaque par phishing avec débriefing
- Élaboration d'une mini-formation interne (PPT ou vidéo)

Évaluations :

- QCM sur les règles de sécurité
- Présentation d'un plan de sensibilisation pour un service
- Création d'un kit cybersécurité à distribuer aux utilisateurs