Date de mise à jour : 14/01/2025
Destinataires : Ensemble des utilisateurs

GUIDE DE BONNES PRATIQUES DE SÉCURITÉ

Version finale

Troisième année BUT Informatique

—

Présenté par :

BOUCHAMI Enzo, BOULBAYEM Jaoued,

LOEB Dorian, MAALAL Ines,

VERDILHAN Tom

—

Chargé de Suivi Technique :

M. OLIVIER Gérard

Responsable SAE :

Mme Salou Alexandra

V.A. Productions

amU Aix Marseille Université

Table des matières

1. Pourquoi ce guide ?

Nous avons mis en place des protections techniques robustes sur l'application (chiffrement, pare-feu). Cependant, la sécurité informatique est un travail d'équipe. La technologie protège le serveur, mais c'est vous qui protégez l'accès à votre compte.

Ce document résume les bons réflexes à adopter au quotidien pour garantir la sécurité des données de l'entreprise.

2. Votre mot de passe est votre clé

Votre mot de passe est la seule barrière entre un pirate et les données clients.

- **Complexité :** L'application exige désormais un mot de passe d'au moins 8 caractères avec majuscules, chiffres et symboles. C'est le minimum pour résister aux attaques automatiques.
- **Astuce mémorisation :** Plutôt qu'un mot compliqué, utilisez une "phrase de passe".
  Exemple : "J'aimeLeCafeLeMatin99!" est plus facile à retenir et plus difficile à pirater que "X9!bK2".
- **Usage unique :** N'utilisez jamais votre mot de passe professionnel sur des sites personnels (Facebook, LinkedIn, etc.). Si l'un de ces sites est piraté, votre compte professionnel sera compromis.

3. Sécuriser son accès au quotidien

L'application étant accessible via internet, la vigilance est de mise, surtout en dehors des bureaux.

- **Verrouillage d'écran :** Prenez l'habitude de verrouiller votre session (Windows + L) dès que vous quittez votre poste, même pour une courte pause.
- **Ordinateurs partagés :** Si vous devez exceptionnellement utiliser un ordinateur qui n'est pas le vôtre, utilisez toujours le mode "Navigation Privée" du navigateur et assurez-vous de cliquer sur "Déconnexion" une fois terminé.
- **Connexion en déplacement :** Évitez les réseaux Wi-Fi publics (gares, hôtels, cafés) qui sont souvent peu sécurisés et espionnés. Privilégiez toujours le partage de connexion (4G/5G) de votre téléphone professionnel.

4. Vigilance face aux emails (Phishing)

Les pirates tentent souvent d'imiter les emails de service pour voler vos identifiants.

- **Vérifiez l'expéditeur :** Assurez-vous que les emails de notification (nouveau compte, réinitialisation) proviennent bien de l'adresse officielle de l'entreprise.
- **Méfiez-vous de l'urgence :** Un email vous demandant d'agir très vite ("Votre compte va être supprimé", "Facture impayée") est souvent une tentative d'arnaque. Prenez le temps de vérifier auprès de l'administration avant de cliquer.

5. Protection des données clients

Vous manipulez des informations confidentielles (coordonnées clients, tarifs, factures).

- **Exports de fichiers :** Si vous téléchargez des statistiques ou des listes de clients (Excel/CSV), ces fichiers ne doivent pas sortir de l'environnement professionnel. Ne les copiez pas sur des clés USB personnelles ou des services de stockage en ligne non approuvés.
- **Imports de documents :** Lors de l'envoi de bons de commande signés, vérifiez bien le contenu du fichier avant de l'importer pour éviter les erreurs.

6. Que faire en cas de doute ?

Si vous pensez avoir fait une erreur (clic sur un lien suspect, mot de passe potentiellement connu d'un tiers, perte de matériel) :

1. **Changez immédiatement votre mot de passe** via l'espace "Paramètres".
2. **Prévenez l'administrateur** sans attendre.

Une réaction rapide permet souvent d'éviter ou de limiter les conséquences d'un incident.