

[Prénom] [NOM]

[Adresse]

[CP & Ville]

Tél. : 01.23.45.67.89

[Prénom] [NOM]

[Adresse]

[CP & Ville]

Paris, le 02/04/2025

Exemple 1 : Rappel général des bonnes pratiques

Objet : Rappel important : adoptez les bonnes pratiques de sécurité informatique

Bonjour [Nom/équipe],

La sécurité informatique est une priorité pour [nom de l'entreprise]. Afin de protéger nos données et nos systèmes contre les cybermenaces, nous souhaitons vous rappeler quelques bonnes pratiques essentielles à appliquer au quotidien :

- Mots de passe sécurisés : Utilisez des mots de passe complexes et uniques pour chaque compte. Changez-les régulièrement et évitez de les partager.

Attention aux emails suspects : Ne cliquez jamais sur des liens ou pièces jointes provenant d'expéditeurs inconnus. En cas de doute, contactez l'équipe informatique. Mise à jour des appareils : Assurez-vous que vos appareils (ordinateurs, téléphones) disposent des dernières mises à jour de sécurité.

Utilisation des réseaux publics : Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés pour des activités sensibles.

Pour en savoir plus, nous avons mis à votre disposition un guide détaillé : [\[lien vers le guide\]](#).

Merci de votre vigilance et de votre engagement à respecter ces pratiques. Si vous avez des questions ou besoin d'assistance, n'hésitez pas à contacter [équipe informatique, adresse email ou numéro de téléphone]. Cordialement,

[Prénom Nom]

[Poste]

[Nom de l'entreprise]

[Adresse email]

[Numéro de téléphone]

Exemple 2 : Rappel ciblé avec un appel à l'action immédiat

Objet : Protégez vos données : rappel des règles de cybersécurité

Bonjour [Nom/équipe],

La sécurité de nos données et de nos systèmes est l'affaire de tous. Nous avons récemment constaté une augmentation des menaces comme le phishing et les tentatives de piratage. C'est pourquoi nous vous rappelons quelques actions simples mais cruciales :

Vérifiez les emails : Si un email semble suspect (orthographe, adresse de l'expéditeur, demande inhabituelle), ne cliquez sur rien et signalez-le immédiatement à [équipe informatique].

Sauvegardez régulièrement : Assurez-vous que vos fichiers importants sont sauvegardés dans des espaces sécurisés (serveurs internes ou cloud approuvé).

Utilisez un VPN : Lorsque vous travaillez à distance, connectez-vous toujours via le VPN de l'entreprise pour protéger vos échanges.

Bloquez les accès non autorisés : Verrouillez votre poste de travail lorsque vous vous absentez.

Action immédiate : Merci de prendre quelques minutes pour vérifier vos mots de passe et activer l'authentification à deux facteurs sur vos comptes, si ce n'est pas encore fait.

Votre collaboration est essentielle pour garantir un environnement sécurisé pour tous. Si vous avez besoin d'aide pour appliquer ces recommandations, contactez-nous à [adresse email] ou [numéro de téléphone].

Merci pour votre vigilance. Ensemble, renforçons notre cybersécurité !

Cordialement,

[Prénom Nom]

[Poste]

[Nom de l'entreprise]

[Adresse email]

[Numéro de téléphone]

[Prénom] [NOM]

Signature