[Prénom][NOM]
[Adresse]
[Code Postal][Ville]
Tél. : 01.23.45.67.89

[Nom Destinataire]
[Adresse Destinataire]
[Code Postal][VILLE]
Paris, le 20/06/2026

Modèles d'e-mails pour rappeler les bonnes pratiques de sécurité informatique

Objet : rappel des bonnes pratiques de sécurité informatique. Bonjour [Nom ou nom de l'équipe], la protection de nos données et de nos systèmes dépend des gestes de chacun. Nous vous proposons un point sur quelques règles simples à appliquer au quotidien. Choisissez des mots de passe longs et différents pour chaque service, et ne les partagez jamais, même avec un collègue. Méfiez-vous des e-mails inattendus : avant de cliquer sur un lien ou d'ouvrir une pièce jointe, vérifiez l'adresse de l'expéditeur et, au moindre doute, transmettez le message au service informatique. Installez sans tarder les mises à jour proposées sur vos ordinateurs et téléphones, car elles corrigent souvent des failles déjà exploitées. Enfin, évitez les réseaux Wi-Fi publics pour consulter des documents sensibles. Un guide complet est disponible ici : [lien vers le guide interne]. Pour toute question, écrivez à [adresse du service informatique]. Merci de votre attention. Cordialement, [Prénom Nom], [poste], [nom de l'entreprise].

Objet : recrudescence des tentatives de phishing, restons vigilants. Bonjour [Nom ou nom de l'équipe], ces derniers jours, nous avons observé une hausse des e-mails frauduleux visant nos collaborateurs. Certains imitent nos fournisseurs ou notre propre direction pour vous pousser à communiquer un mot de passe ou à valider un paiement. Soyez particulièrement attentifs : une faute d'orthographe, une adresse d'expéditeur légèrement modifiée, une demande urgente ou inhabituelle sont autant de signaux d'alerte. Ne cliquez sur aucun lien et ne répondez pas si quelque chose vous semble anormal. Signalez immédiatement le message à [adresse de signalement] : mieux vaut une alerte de trop qu'un clic de trop. Rappelez-vous qu'aucun service interne ne vous demandera jamais votre mot de passe par e-mail. En cas de doute sur un message reçu, contactez directement la personne concernée par un autre canal. Votre réactivité protège toute l'entreprise. Cordialement, [Prénom Nom], service informatique de [nom de l'entreprise], joignable au [numéro de téléphone].

Objet : deux minutes pour sécuriser votre compte. Bonjour [Nom ou nom de l'équipe], ce message demande une seule action concrète de votre part, dès aujourd'hui. Merci de vérifier que l'authentification à deux facteurs est bien activée sur vos comptes professionnels. Cette protection ajoute une étape de validation, par exemple un code reçu sur votre téléphone, qui empêche un intrus de se connecter même s'il connaît votre mot de passe. La procédure d'activation prend moins de cinq minutes et se trouve ici : [lien vers la procédure]. Profitez-en pour remplacer tout mot de passe réutilisé sur plusieurs services par un mot de passe unique. Si vous rencontrez la moindre difficulté, notre équipe vous accompagne : écrivez à [adresse du support] ou appelez le [numéro de téléphone]. Merci de traiter cette demande

avant [date butoir], afin que l'ensemble des comptes soit protégé. Votre coopération compte pour la sécurité de tous. Cordialement, [Prénom Nom], [poste], [nom de l'entreprise].

Objet : sécurité du télétravail, les réflexes à garder. Bonjour [Nom ou nom de l'équipe], travailler à distance offre de la souplesse, à condition de conserver les mêmes exigences de sécurité qu'au bureau. Connectez-vous toujours au [VPN de l'entreprise] avant d'accéder à nos applications et à nos documents : il chiffre vos échanges et les rend illisibles pour un tiers. Sauvegardez vos fichiers importants sur les espaces approuvés, serveurs internes ou cloud validé par l'entreprise, et non sur des supports personnels. Verrouillez votre session dès que vous quittez votre poste, même chez vous, et évitez que des proches utilisent votre matériel professionnel. Méfiez-vous enfin des espaces partagés et des réseaux Wi-Fi de passage. Si vous avez besoin de configurer un de ces outils, le service informatique reste disponible à [adresse e-mail] ou au [numéro de téléphone]. Merci de contribuer à un environnement de travail sûr, où que vous soyez. Cordialement, [Prénom Nom], [poste], [nom de l'entreprise].

Adaptez l'objet, le ton et le destinataire de chaque modèle avant l'envoi, et personnalisez tous les éléments entre crochets.

[Prénom][NOM]

Signature