Fiche-conseils

LES BONNES PRATIQUES D'HYGIÈNE E-MAIL

Comme dans une boîte aux lettres physique, des courriers officiels, suivis de commande ou de livraison, publicités, arnaques, et bien d'autres choses encore, s'accumulent dans les boîtes aux lettres électroniques. Gérer son courrier électronique (e-mail) est donc tout aussi important que de gérer son courrier papier. Cependant, l'e-mail a pour particularité d'être accessible en ligne, avec tous les défis que cela comporte, notamment en terme de sécurisation des échanges et de protection des données personnelles. De bonnes pratiques dites d'hygiène e-mail sont donc à adopter tant au niveau de la boîte réceptionnant les courriers électroniques que de l'adresse e-mail.

Protéger et sécuriser son adresse e-mail professionnelle

Votre institution ou votre établissement vous a attribué une adresse e-mail. À ce titre, vous la-le représenter en plus de votre propre personne. Une utilisation responsable est donc primordiale pour, notamment, crédibiliser vos échanges et maintenir une bonne image de vous-même et de votre employeur mais également protéger votre vie privée et la sécurité de l'institution ou de l'établissement dont vous dépendez.

À faire

Choisir un mot de passe fort et unique

Le mot de passe de votre boîte e-mail professionnelle doit être complexe (mélange de lettres, chiffres et symboles), unique et régulièrement changé.

sécurisation des informations, réduction des risques de piratage

Conseil !

Si l'option est proposée et disponible sur votre boîte e-mail, activez l'authentification à deux facteurs (2FA) pour un niveau de sécurité supplémentaire.

Signaler tout e-mail suspect

Si un e-mail vous semble suspect ou frauduleux, signalez-le à votre service informatique, voire au service CSIRT (csirt@restena.lu) de la Fondation Restena. Signalez-le au moindre doute, même si cela vous semble inutile. Seules les personnes responsables de la sécurité pourront juger de la pertinence de l'information.

De même, si vous recevez un e-mail d'une institution/entreprise/banque connue et que vous n'êtes pas sûr-e de sa légitimité, renseignez-vous auprès de cette institution par d'autres moyens de communication (par téléphone par exemple) ou en visitant son site officiel.

amélioration des filtres de sécurité anti-spam et anti-phishing

Le saviez-vous ?

Signaler des emails suspects est une démarche responsable qui aide non seulement à protéger votre propre sécurité en ligne, mais aussi à préserver celle de l'ensemble de la communauté de la recherche et de l'éducation.

À ne pas faire

Stocker son mot de passe 'en clair'

Ne notez pas en clair sur un calepin, ni sur un post-it, et n'enregistrez pas non plus vos mots de passe dans un document texte ou tableur de votre ordinateur ou smartphone.

compromission de compte, violation de la vie privée

Conseil !

Gérez vos mots de passe avec un gestionnaire de mots de passe. La plateforme d'identification *open source* Passbolt, par exemple, est développée au Luxembourg.

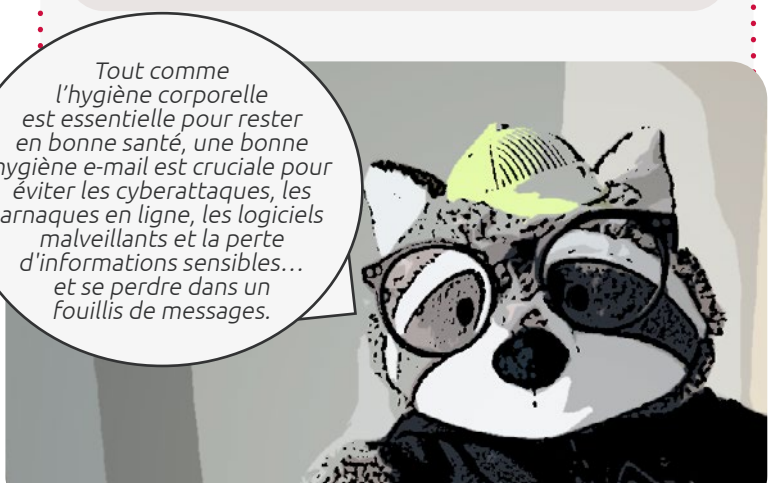
Ouvrir des pièces jointes et liens suspects

Méfiez-vous des e-mails provenant de sources inconnues ou inhabituelles. L'expéditeur vous est inconnu, le sujet de l'e-mail est alarmant, et/ou vous recevez une pièce jointe inattendue ? Ne cliquez pas sur des liens non sollicités et n'ouvrez pas les pièces jointes.

tentative de phishing, virus

Conseil !

Vous avez un doute sur un e-mail ? Signalez-le comme e-mail suspect puis supprimez-le sans attendre.



Respecter la confidentialité des informations transmises

Avant de partager toute information confidentielle ou sensible, assurez-vous que des mesures de sécurité supplémentaire, telles que le chiffrement (PGP/GPG, S/MIME), sont implémentées sur votre boîte e-mail. Pour cela, renseignez-vous auprès de votre service informatique.

Dans le cas contraire, ou si vous ne connaissez pas le degré de sécurisation de votre boîte e-mail, préférez des outils de partage sécurisés.

confidentialité des données, communication sécurisée, intégrité des informations échangées

Le saviez-vous ?

FileSender, le service de partage de fichiers volumineux de Restena dispose de l'option "chiffrement à connaissance zéro".

Sécuriser les connexions à distance

Pour une sécurisation optimale des échanges électroniques, le protocole cryptographique TLS doit être activé tant sur les serveurs que sur le client de messagerie. Bien que la sécurisation du serveur de messagerie relève de la responsabilité du fournisseur de services, vous pouvez manuellement activer le TLS dans votre programme client tant pour les e-mails entrants que sortants.

protection des données sensibles, minimisation des risques de cyberattaques

Utiliser son adresse à des fins privées ou personnelles

Votre adresse e-mail professionnelle doit être réservée aux communications liées à votre activité professionnelle. Consultez et suivez la politique de votre établissement concernant son utilisation. L'usage des informations confidentielles et les pratiques autorisées en ligne sont généralement listés et partagés dans une charte informatique.

Dans tous les cas, ne l'utilisez ni pour vous inscrire à des services non professionnels (réseaux sociaux, portails privés) ni sur des forums ou des plateformes publiques/ privées.

fuite/ violation de données, compromission de l'adresse, spam, tentative de phishing

Conseil !

Distinguez clairement votre adresse professionnelle de votre adresse privée.

Le **protocole TLS** (ou *Transport Layer Security*) crypte l'échange d'informations de connexion (code d'accès) et la réception et l'envoi d'e-mails entre un client de messagerie (boîte e-mail) et des serveurs de messagerie.

Grâce à lui, les échanges envoyés par et reçus sur son adresse e-mail sont protégés.

L'authentification à deux facteurs est une méthode d'authentification nécessitant deux preuves d'identité distinctes.

Au mot de passe s'ajoute un facteur d'authentification supplémentaire : code unique envoyé par e-mail ou SMS, application d'authentification, clé physique ou donnée biométrique.

Le **chiffrement** convertit les données d'un format lisible à un format codé. Les données ne peuvent être lues que par la ou les personnes détenant la bonne clé de chiffrement.

Des données chiffrées interceptées par une personne non autorisée sont illisibles et inexploitables. Dans les messageries électroniques, les **protocoles informatiques PGP/GPG, S/MIME** assurent cette protection.

Protéger et sécuriser sa boîte aux lettres électronique

En plus d'une adresse e-mail, votre employeur vous met à disposition une boîte aux lettres électronique. À ce titre, il est garant de sa sécurité. Il a notamment pour responsabilité de protéger l'infrastructure technique où sont hébergées les boîtes e-mail. Ce premier niveau de sécurité n'est pourtant pas suffisant, chaque personne individuellement a un rôle à jouer pour la protection de sa propre boîte e-mail.

À faire

Organiser sa boîte aux lettres

Si vous recevez quotidiennement un grand volume d'e-mails, une organisation rigoureuse est essentielle. Sans structure claire, vous risquez de perdre la vue d'ensemble de vos e-mails, entraînant retard dans le traitement des messages voire perte d'e-mails importants. Utilisez des dossiers et des filtres pour organiser vos e-mails, et classez-les régulièrement.

contrôle de sa boîte de réception, gestion et suivi des projets améliorés

Supprimer les e-mails inutiles

Les e-mails non pertinents sont à supprimer régulièrement. Ils contiennent de nombreuses données, potentiellement sensibles, qui pourraient être 'volées' en cas de compromission de la boîte e-mail.

limitation des risques de fuites de données

Archiver régulièrement les e-mails

Archivez régulièrement les e-mails que vous souhaitez conserver mais qui ne s'avèrent pas opportun de conserver dans la boîte de réception.

allègement de l'espace disponible sans suppression de messages

Maintenir à jour son profil utilisateur

Les informations du profil utilisateur associées à une adresse e-mail sont cruciales. Au-delà des configurations techniques, elles sont indispensables en cas de perte d'accès à votre boîte e-mail. La vérification et la mise à jour de ces informations doivent donc être réalisées régulièrement.

efficacité et rapidité du support en cas de besoin d'assistance

Le saviez-vous ?

Un article du Règlement général sur la protection des données (RGPD) exige que les données personnelles soient exactes et, si nécessaire, tenues à jour, et que toutes les mesures raisonnables soient prises pour supprimer ou rectifier rapidement les données inexactes.

À ne pas faire

Envoyer des fichiers volumineux

Pour garder votre boîte de réception légère et éviter les problèmes de taille limite pour les envois, l'envoi de pièces jointes volumineuses par e-mail est déconseillé.

surcharge de l'espace disponible, envoi impossible de fichiers dépassant les tailles autorisées

Conseil !

Utilisez des services de transfert de fichiers volumineux, comme le (Restena) FileSender.

Utiliser la boîte mail comme espace de stockage et/ou sauvegarde

Votre boîte de réception doit être dédiée aux e-mails. Ce n'est pas un endroit pour stocker, voire sauvegarder à long-terme, des documents ou des fichiers volumineux.

surcharge de l'espace disponible, fuites de données en cas de compromission

Conseil !

- Utilisez une sauvegarde locale ou une sauvegarde *cloud* pour stocker et conserver vos informations importantes. Veillez cependant à consulter et respecter la politique de votre institution à cet égard.
- Si cela est possible et autorisé, envisagez une protection supplémentaire comme le cryptage des données stockées.

Conserver des données sensibles

Les informations personnelles, financières ou confidentielles (mots de passe, numéros de carte de crédit, dossiers médicaux ou scolaires, etc.) ne devraient pas être conservées dans une boîte mail sans protection appropriée de type PGP/GPG, S/MIME.

fuites de données en cas de compromission

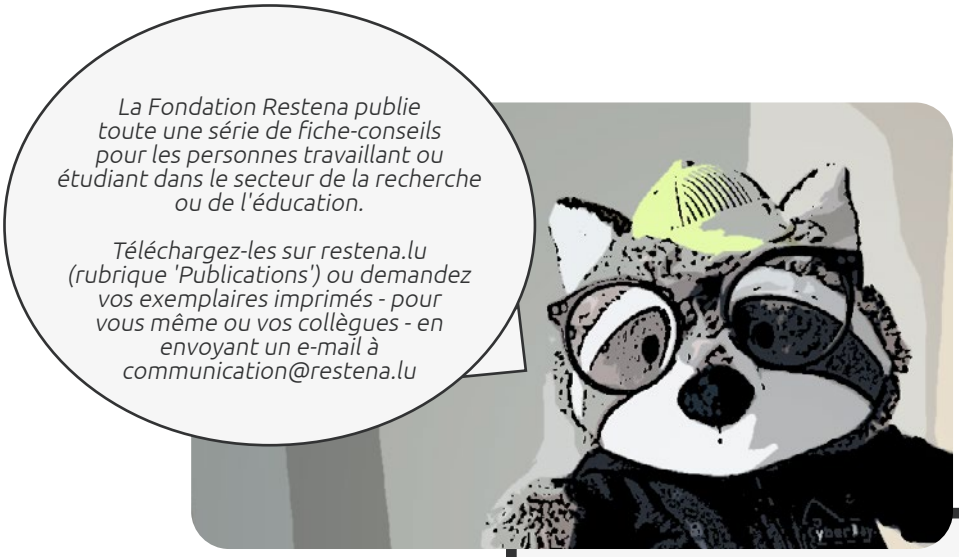
Conseil !

Déplacez/archivez tout e-mail contenant des données sensibles hors de votre boîte aux lettres si cette dernière n'est pas cryptée à l'aide des protocoles PGP ou S/MIME.

Votre messagerie professionnelle est gérée par Restena ?

• Vérifiez et maintenez à jour les informations de votre profil utilisateur, telles que vos données signalétiques (adresse postale, etc.). Pour cela, connectez-vous à l'outil de « Gestion de compte en ligne » à l'adresse account.restena.lu

• L'utilisation du protocole TLS version 1.2 ou supérieure est obligatoire pour toute connexion aux serveurs de messagerie de Restena. Les clients de messagerie que vous utilisez doivent donc impérativement être conformes à cette exigence de sécurité pour pouvoir réceptionner et envoyer des e-mails.



À (RE)DÉCOUVRIR DANS LA MÊME SÉRIE...

• 'Choisir son mot de passe avec soin'
• 'Les messages spam & phishing'
• 'D'une cyberattaque à la saisie des données'
• 'Les attaques d'ingénierie sociale'
• 'Sauvegarder ses données sans risque'

LU ET APPROUVÉ PAR HEX

Offre de services

La Fondation Restena propose un service d'hébergement de messagerie électronique sécurisé, performant et de haute disponibilité et gère la messagerie électronique professionnelle pour les enseignant(e)s au Luxembourg.

Pour plus d'informations sur ces services, rendez-vous sur restena.lu/fr/service/hebergement-e-mail et restena.lu/fr/service/messagerie-educationlu

Co-funded by the European Union

Cette fiche-conseils est l'une des activités de sensibilisation mises en place dans le cadre du projet européen LuCySe4RE, financé par le programme Digital Europe de l'Union européenne (DIGITAL) dans le cadre de la convention de subvention n° 101127864.

restena
réseau · sécurité · .lu