Sécuriser ma messagerie

Pourquoi sécuriser mon accès à la messagerie ?

Le service de messagerie nationale est un service interne au sein du Ministère. L'infrastructure qui héberge les données est gérée et maîtrisée par une équipe nationale. Celle-ci définit les règles de sécurité et les met en place sur cette infrastructure. Elle maîtrise et administre les applications et équipements nécessaires permettant d'assurer une protection optimale des données hébergées.

Chaque utilisateur de ce service participe également activement à la sécurité de ce service en appliquant des règles de bonnes hygiène informatique dans ses usages quotidiens, professionnels comme personnels. En permettant l'accès à son compte de messagerie à une tierce personne mal intentionnée, celle-ci peut corrompre et impacter la qualité du service de messagerie mais aussi accéder à des données personnelles.

Comment sécuriser mon compte de messagerie ?

7 règles facilement applicables permettent de sécuriser votre compte de messagerie professionnel :

1. Utilisez des mots de passe solides

Un mot de passe doit comporter 12 caractères mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux. Il ne doit pas être noté sur un papier, ni stocké de manière non sécurisée (fichier texte, navigateur…). Ayez autant de mots de passe différents que de comptes. Les mots de passe doivent être renouvelés au minimum tous les trois ans.

2. Méfiez-vous des messages inattendus

Au moindre doute sur un message, ne l'ouvrez pas, ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe : il peut vous piéger pour dérober des informations confidentielles ou installer un virus. En cas de doute, il est possible de vérifier un document ou un courriel en le déposant sur le service en ligne « Je Clique ou Pas » de l'ANSSI : https://jecliqueoupas.cyber.gouv.fr

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service à compétence nationale rattaché au secrétariat général de la Défense et de la Sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Elle définit notamment les règles en matière de sécurité des systèmes informatiques.

L'hameçonnage ou le phishing consiste à obtenir du destinataire d'un mail, d'apparence légitime, qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion afin de lui dérober de l'argent ou d'accéder à des données de l'organisation pour les utiliser à des fins malveillantes. Il s'agit de l'un des principaux vecteurs de la cybercriminalité. Lorsque vous recevez un mail douteux, vérifiez l'adresse du destinataire et alertez votre dispositif d'assistance académique.

3. N'installez aucun logiciel dont l'origine n'est pas garantie

Un logiciel ou un module additionnel (plug-in) téléchargé depuis un site non-officiel peut contenir des virus et installer des logiciels malveillants comme des dérobeurs de mots de passe (stealers). La plupart des cas d'usurpation d'identité actuels sont causés par des vols de mots de passe réalisés par ce type de logiciel. En milieu professionnel, demandez l'avis de votre dispositif d'assistance académique avant d'installer un logiciel ou un module additionnel sur votre matériel.

4. Appliquez les mises à jour de sécurité sur tous vos appareils (ordinateurs, tablettes, téléphones…) dès qu'elles vous sont proposées

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des personnes malveillantes pour dérober vos données ou vos mots de passe, voire pour détruire vos données. Les mises à jour de sécurité de vos équipements professionnels sont généralement gérées directement par les services techniques académiques ou de votre collectivité de rattachement. Sur vos équipements mobiles, la fonctionnalité de mise à jour du système est disponible dans la rubrique « paramètres ».

5. Protégez vos données professionnelles

Pour éviter toute perte de données, veillez à utiliser exclusivement les lecteurs réseaux (serveurs bureautiques) qui bénéficient de sauvegardes automatisées. Ne stockez pas de données professionnelles sur un espace qui n'est pas géré et maîtrisé par votre organisation comme, par exemple, google drive.

6. Séparez vos usages personnels et professionnels

Ne mélangez pas votre messagerie professionnelle et personnelle et utilisez des mots de passe différents. Ne vous envoyez pas de messages d'une messagerie professionnelle à une messagerie personnelle et inversement. Ne branchez pas de support USB dont l'origine n'est pas parfaitement fiable (une clé peut être piégée pour « aspirer » vos données une fois branchée sur votre matériel).

7. Évitez les réseaux Wifi publics ou inconnus

Privilégiez la connexion à un réseau Wifi connu ou le partage de connexion avec votre téléphone. Évitez les réseaux Wifi publics ou inconnus qui sont souvent mal sécurisés et peuvent être contrôlés ou usurpés par des personnes malveillantes. Si vous n'avez d'autre choix que d'utiliser un Wifi public, veillez à ne jamais y réaliser d'opérations sensibles (ou utilisez le réseau privé virtuel – VPN – fourni par votre organisation).

Mes données sont-elles protégées ?

L'infrastructure nationale sécurise vos données de manière rigoureuse. Les serveurs sont protégés par des pare-feu et des systèmes de détection d'intrusion. Les données sont chiffrées et des sauvegardes automatisées assurent leur intégrité. Les accès aux données sont contrôlés et surveillés pour prévenir toute tentative d'intrusion ou d'accès non autorisé.

Plusieurs structures ministérielles ont pour mission de protéger les données :

1. Le Centre d'Opération Sécurité (SOC) gère la sécurité du réseau et de la messagerie, contrôle et analyse chaque événement ;
2. Le Bureau de la Sécurité Numérique et Centre Opérationnel de la Sécurité des Systèmes d'Information Ministériels est responsable de prévenir et d'apporter une réponse rapide et adaptée à tout incident de sécurité ;
3. La mission nationale en charge du service de messagerie administre les systèmes de sécurité de l'infrastructure hébergeant les comptes de messagerie et supervise cette infrastructure.

La sécurité de l'infrastructure peut être résumée en deux grandes parties :

- Sécurité active: au niveau des mails, au niveau des connexions, traitement des événements (direct ou différé), application des nouvelles règles de sécurité

- Sécurité passive: suivi des failles de sécurité, au niveau des équipements, création de ressources pour assurer cette sécurité active, suivi des événements

La sécurité doit également respecter certains critères :

- Redondance d'équipement, de flux : mise en place d'une infrastructure de secours ;
- Sauvegarde des équipements et des mails ;
- Stockage résilient, durable ;
- Plan de continuité et de reprise d'activité permettant d'assurer le service même en cas d'incident.

Comment gérer les spams ?

Un spam est un message électronique non sollicité et souvent envoyé en masse à un grand nombre de destinataires. Ces messages sont généralement envoyés à des fins publicitaires, de promotion de produits ou services, ou pour des tentatives de fraude.

Un système de repérage des spams est mis en place sur l'infrastructure réseau nationale hébergeant les serveurs de messagerie. Lorsqu'une adresse mail d'expéditeur apparaît suspicieuse, le système bloque cette adresse mail et place les mails en quarantaine. Les mails ne sont donc pas transmis aux destinataires.

Vous recevez régulièrement une notification automatique de mise en quarantaine. Cette notification liste les mails qui vous étaient destinés et qui ont été placés en quarantaine. Vous avez alors la possibilité de libérer le mail pour le recevoir ou de confirmer qu'il s'agit d'un spam et le supprimer définitivement de la quarantaine. Pour en savoir, vous pouvez consulter le **tutoriel** de gestion de spam.

Comment bloquer une adresse mail ou la déclarer comme adresse de confiance ?

Lorsque vous recevez la notification de quarantaine, vous pouvez décider d'intégrer l'adresse mail d'un expéditeur dans votre liste blanche ou votre liste noire:

- La liste blanche recense l'ensemble des adresses mail que vous estimez être des adresses mail de confiance, les mails en provenance de cette adresse mail ne seront alors plus bloqués par le système antispam.
- La liste noire recense l'ensemble des adresses mail que vous jugez indésirables, les mails en provenance de cette adresse mail seront alors systématiquement bloqués par le système antispam.

Comme indiqué précédemment, vous cliquez sur le lien « vos messages en quarantaine ». Si l'un des expéditeurs présents dans la liste vous apparaît comme un expéditeur de confiance, vous cochez la case correspondante au mail qu'il a envoyé et dans le menu déroulant, vous sélectionnez « Libérer et ajouter à la liste sécurisée ».

Pour ajouter une adresse mail en liste noire et la définir ainsi comme définitivement indésirable, vous cliquez sur le lien « vous messages en quarantaine ». En haut à droite de la page qui apparaît, vous passez votre souris sur « Options » et sélectionnez « Liste de blocage ».

Dans la fenêtre qui apparaît, un champ vous permet de saisir l'adresse de l'expéditeur que vous jugez indésirable et de l'ajouter à votre liste noire.

Vous ne recevrez alors plus de mail en provenance de cet expéditeur.

Vous pouvez à tout moment revoir votre liste blanche et votre liste noire.

Pour cela, vous cliquez sur « vos messages en quarantaine » dans la notification reçue. Sur la page qui apparaît, vous passez votre souris sur « Options » en haut à droite de la page.

Pour consulter et retirer une adresse mail de votre liste blanche, vous sélectionnez « Liste sécurisée ». La corbeille présente à droite de l'adresse mail permet de la retirer de la liste.

Pour gérer votre liste noire, vous sélectionnez « Liste de blocage ».

Pour aller plus loin

Les institutions mettent à votre disposition des sites permettant de s'informer et de comprendre les enjeux liés à la sécurité des systèmes d'information. Il est conseillé de les consulter régulièrement.
cybermalveillance.gouv.fr publie de nombreuses ressources :

- Les 10 mesures essentielles pour assurer votre cybersécurité
- Pourquoi et comment bien gérer ses mots de passe
- La sécurité sur les réseaux sociaux
- Apprendre à séparer ses usages pro-perso

Des parcours de formation vous sont également proposés :

PIX.fr propose des modules sur la sécurité des données et des usages numériques : https://pix.fr

M@gistère dispose d'un module de sensibilisation : SensCyber Agir pour contribuer à ma sécurité numérique et celle de mon organisation : https://magistere.education.fr/dgesco/course/view.php?id=2646

Un MOOC (Formation en ligne) conçu et mis à disposition par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) permet de se former au risque cyber et aux réflexes à avoir au quotidien et en cas de crise. Il est disponible à l'adresse suivante secnumacademie.gouv.fr.

Révision #2
Créé 20 août 2025 09:05:03 par Debreczeni Jules
Mis à jour 26 août 2025 13:32:34 par Debreczeni Jules