Antispam et sécurité messagerie

La messagerie de l'UNIL est équipée d'un filtre, réglable, qui analyse les messages entrants dans le but de déterminer s'ils contiennent des contenus dangereux (malware, virus, phishing) ou s'il s'agit de messages indésirables (spam), auquel cas ils sont mis en quarantaine.

Doc publique

Documentation publique du service

Doc publique

Antispam à l'UNIL

Le filtre anti-virus et anti-spam de l'UNIL

Nous utilisons Cisco Email Security pour scanner les emails arrivant et quittant le réseau de l'UNIL. Ce service va analyser les mails et mettre les mails détectés comme spam ou phishing dans votre quarantaine, et bloquer les pièces jointes malveillantes.

En cas de résultat positif de cette analyse, le message subit des modifications dont le marquage du sujet qui permet alors à chacun de le classer ou de le détruire aisément (avec un filtre automatique par exemple). Les messages reconnus comme spam seront mis en quarantaine, ne polluant ainsi plus du tout la boîte aux lettres personnelle.

Cisco Email Security repose sur plusieurs couches de protection et de détection, parmi lesquels

- listes noires/blanches
- de multiples filtres antispam
- un anti-virus
- un filtre analysant les pièces jointes pour des menaces connues
- un filtre "graymail" détectant les mails de marketing, de réseaux sociaux, etc
- des filtres manuels
- un filtre basé sur les menaces récentes détectées par Cisco
- etc.

Que fait le filtre anti-spam?

Dans le filtre anti-spam, le mail est soumis à une batterie de tests détectant des phrases ou des tournures souvent utilisées par les spammeurs, les URLs suspicieuses, ainsi qu'une analyse de la réputation du serveur de messagerie de l'expéditeur.

Chaque test attribue une note au message. A la sortie, le message est considéré comme du spam si la somme des notes dépasse un certain seuil. Des lignes indiquant les résultats de ces tests sont ajoutées dans l'entête du message. Ces lignes sont reconnaissables par leur libellé "**IronPort-**" ou "**X-IronPort-**". Si le seuil est dépassé, il y deux options:

1. Le seuil est dépassé et Cisco Email Security suspecte que le message est un spam: le message **{Suspected Spam?}** est inséré dans le sujet et le message est distribué normalement.
2. Le seuil est largement dépassé, indiquant que Cisco est sûr que le message est un spam: le message **{Spam?}** est inséré dans le sujet et le message est mis dans la quarantaine de l'utilisateur.

Pour voir sa quarantaine, il faut se connecter sur https://spam.unil.ch avec ses identifiants UNIL.

Que fait le filtre anti-virus?

Lorsqu'un message arrive dans Cisco Email Security, l'anti-virus Sophos effectue son analyse et, selon le résultat de l'analyse, va distribuer le courriel, ajouter un avertissement dans le sujet du message (**[WARNING:**), ou mettre le message en quarantaine.

La mise en quarantaine

Plutôt que recevoir dans sa boîte aux lettres les messages marqués comme spam, Cisco va conserver ces emails dans une quarantaine pendant 30 jours puis éliminés. Vous recevrez un email hebdomadaire si un ou plusieurs emails qui vous sont destinés ont fini dans votre quarantaine.

Contrairement à MailCleaner, il n'est pas possible de modifier la fréquence d'envoi du rapport de quarantaine, ni de configurer Cisco pour envoyer tous les messages, spam y compris, sur sa boîte plutôt que la quarantaine. Nous estimons que le filtrage amélioré offert par Cisco rend cela superflu.

Les messages mis en quarantaine peuvent être à tout moment consultés et éventuellement retirés de la quarantaine via l'interface web accessible à l'adresse https://spam.unil.ch Pour y accéder, il faut s'authentifier avec son nom d'utilisateur et mot de passe habituels (les mêmes que pour la messagerie). Dans la liste affichée des messages mis en quarantaine, vous pouvez libérer un message si besoin, c'est-à-dire de demander à Cisco Email Security de déposer tout de même le message dans sa boîte aux lettres. **ATTENTION:** les messages libérés vont souvent être mis dans le dossier **Courrier indésirable!** Il est également possible de gérer ses listes sécurisée et de blocage, qui sont des listes blanches et noires personnelles.

Le filtre anti-spam peut-il se tromper?

Si les tests qu'effectue le filtre anti-spam étaient systématiquement efficaces, le problème du spam serait définitivement réglé. Dans la réalité, bien que le taux de succès soit élevé, il faut prendre des dispositions pour traiter les erreurs possibles du système qui sont de deux types:

Les "faux positifs"

C'est le cas où un message légitime est marqué à tort comme spam. Il ne faut donc pas oublier de consulter régulièrement le rapport hebdomadaire envoyé par Cisco Email Security afin d'y déceler les éventuels faux positifs. Contactez le helpdesk en donnant les détails de l'email qui a été faussement bloqué avec ses entêtes en suivant la marche à suivre ici.

Les "faux négatifs"

C'est le cas où un spam déjoue les filtres de Cisco Email Security et parvient dans votre boîte aux lettres sans être marqué.

Afin d'améliorer l'efficacité de Cisco Email Security, il est utile de signaler ces erreurs en renvoyant ces messages au helpdesk avec ses entêtes en suivant la marche à suivre ici.

Doc publique

FAQ

J'ai reçu un spam ou un phishing dans ma boîte qui n'a pas été détecté par l'antispam, que dois-je faire ?

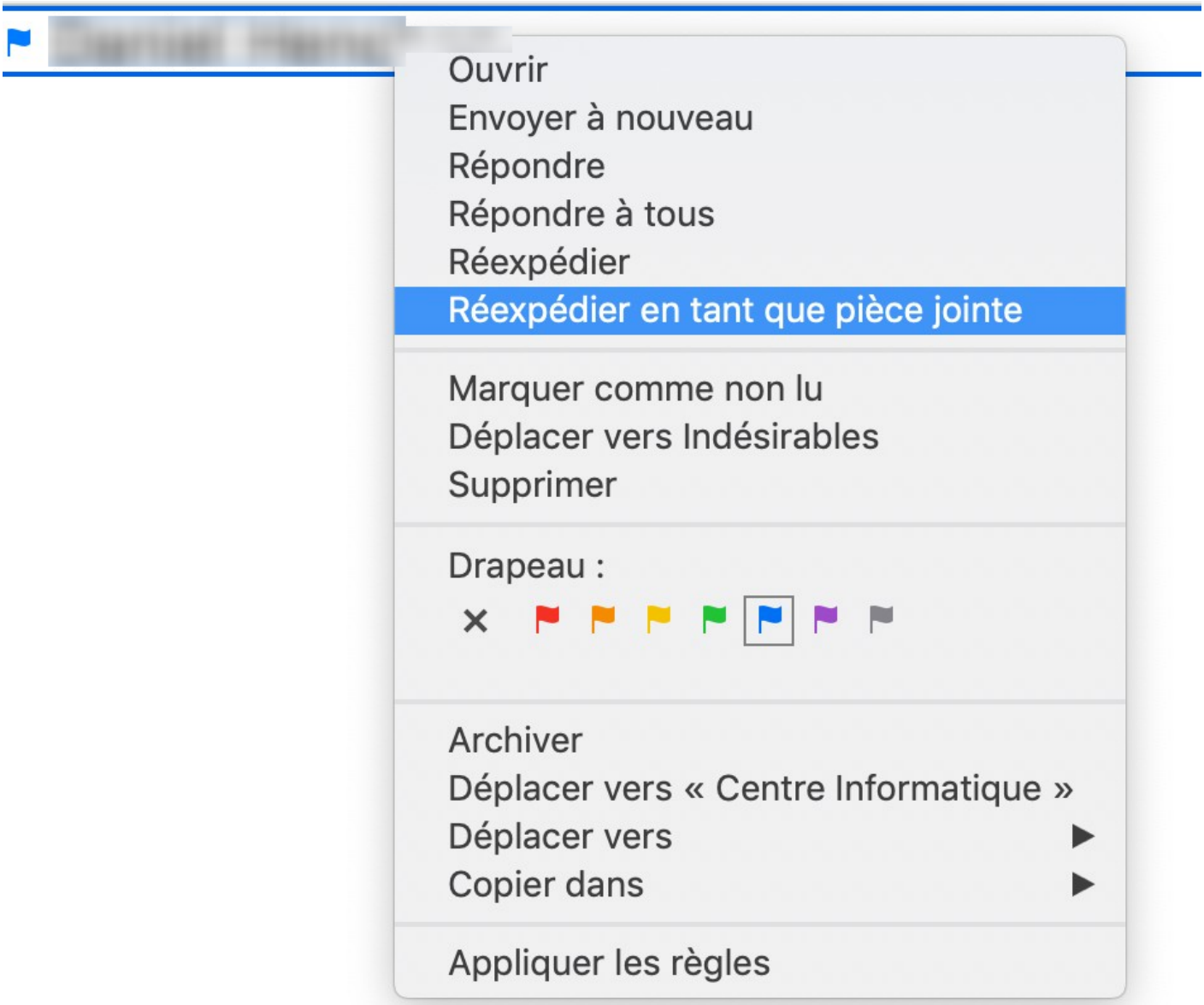
Envoyez une copie du message en tant que pièce jointe au helpdesk (helpdesk@unil.ch) pour que nous puissions adapter nos filtres. (Instructions plus bas)

J'ai reçu un mail légitime mais avec {Suspect Spam?} dans le sujet ou qui a fini dans ma quarantaine, que dois-je faire ?

Envoyez une copie du message en tant que pièce jointe au helpdesk (helpdesk@unil.ch) pour que nous puissions adapter nos filtres.

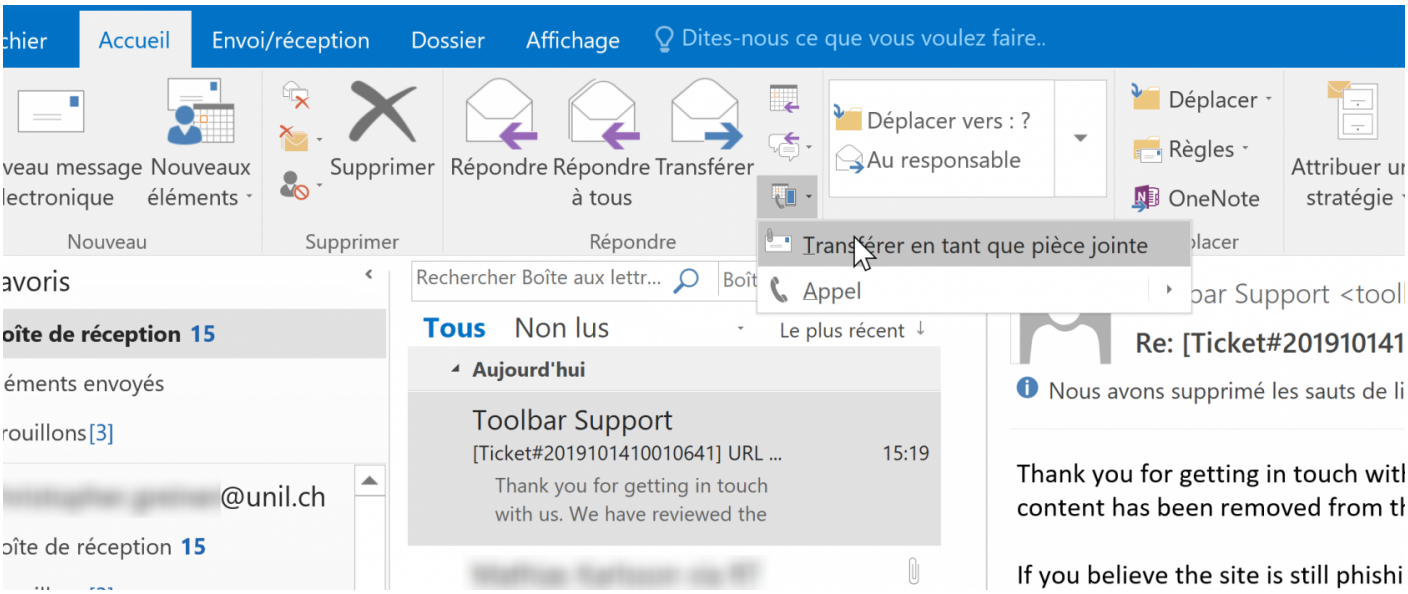
Envoyer une copie du message en pièce jointe sur **Apple Mail**

1. Sélectionnez l’email en question
2. Clic droit, ou Pomme + clic.
3. Sélectionnez “**Réexpédier en tant que pièce jointe**"



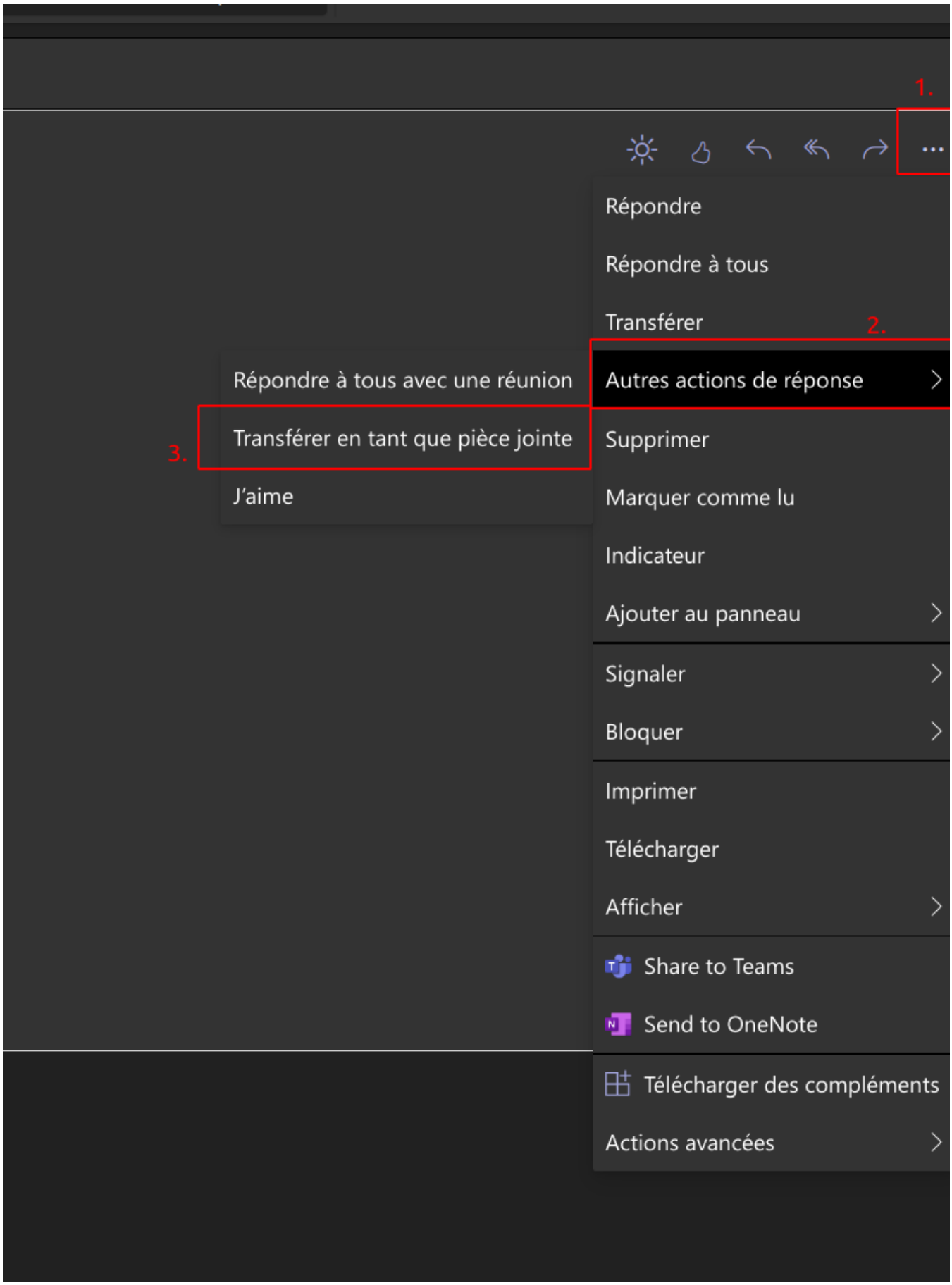
Envoyer une copie du message en pièce jointe sur **Outlook PC**

1. Sélectionnez l’email en question
2. Sélectionnez le menu "Accueil" dans le ruban.
3. Dans le menu “Autres actions de réponse", sélectionnez "**Transférer en tant que pièce jointe**"



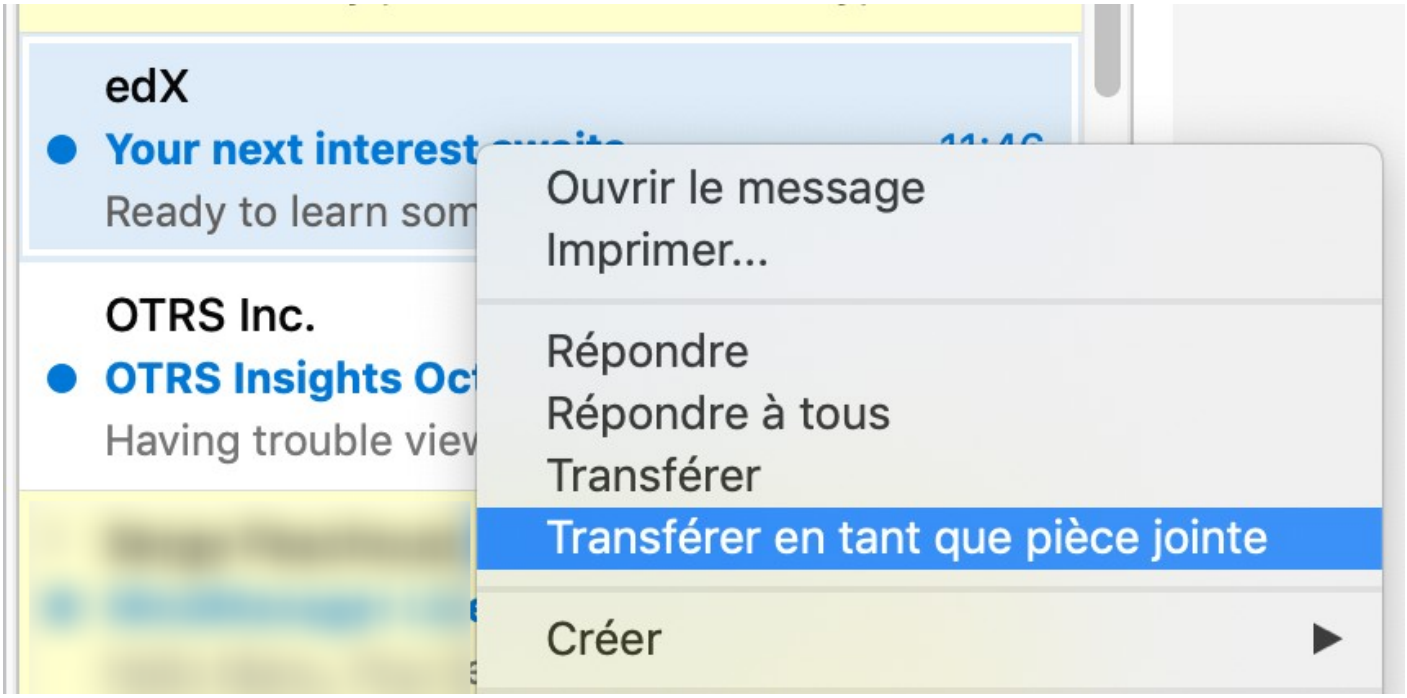
Outlook Online (outlook.office.com)

1. Connectez-vous à votre compte sur https://outlook.office.com
2. Sélectionnez le spam/phishing
3. Sélectionnez "**...**" en haut à droite du message
4. Sélectionnez "**Autres actions de réponse**"
5. Sélectionnez "**Transférer en tant que pièce jointe**" et adressez l'email à **helpdesk@unil.ch**



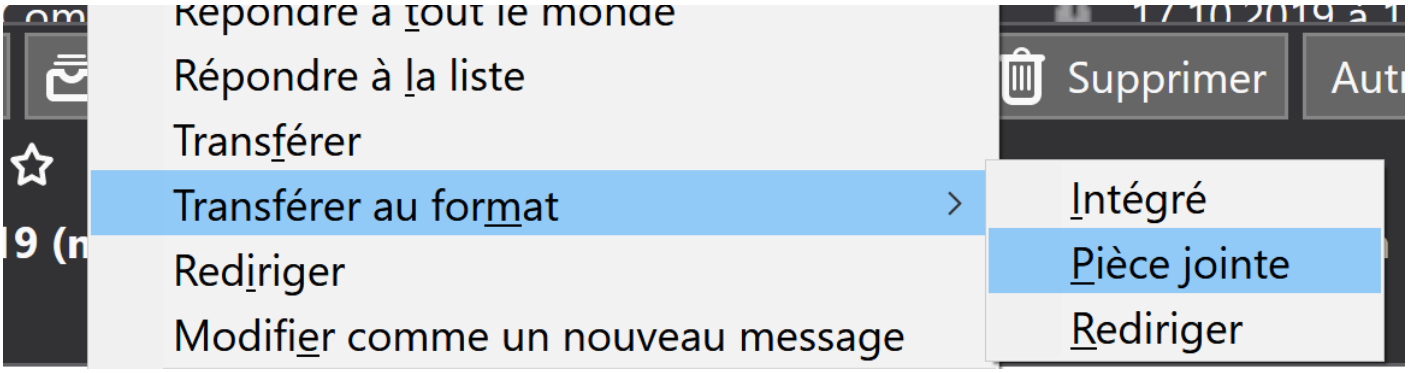
Outlook Mac

Clic droit sur le message --> Transférer en tant que pièce jointe.



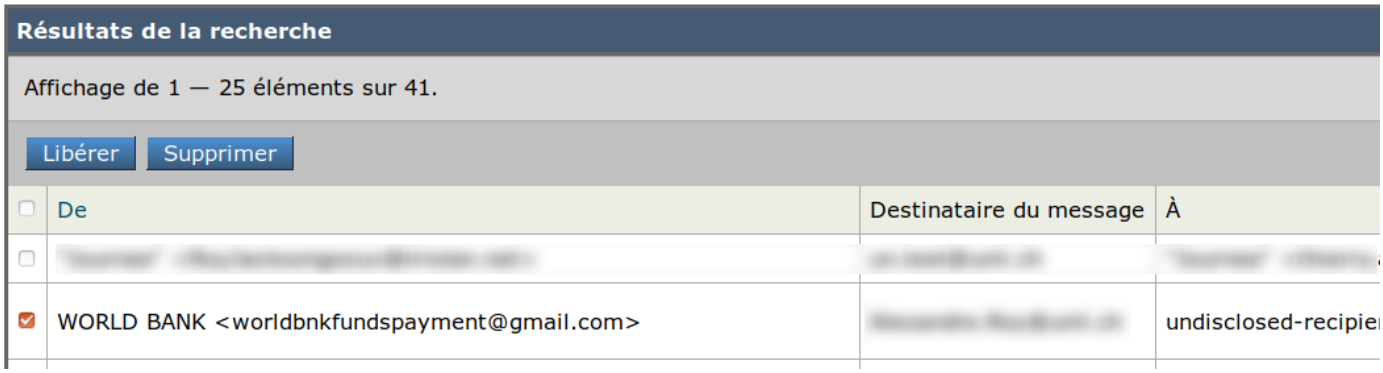
Envoyer une copie du message en pièce jointe sur **Thunderbird**

Clic droit sur le message --> Transférer au format --> Pièce jointe.



Un email légitime a été détecté comme spam, quoi dois-je faire?

Nous vous conseillons de soumettre le cas au helpdesk pour que nous puissions adapter nos filtres. Pour libérer un message faussement retenu dans la quarantaine, il faut vous connecter sur https://spam.unil.ch, sélectionner le message en question et cliquer sur le bouton **libérer**:



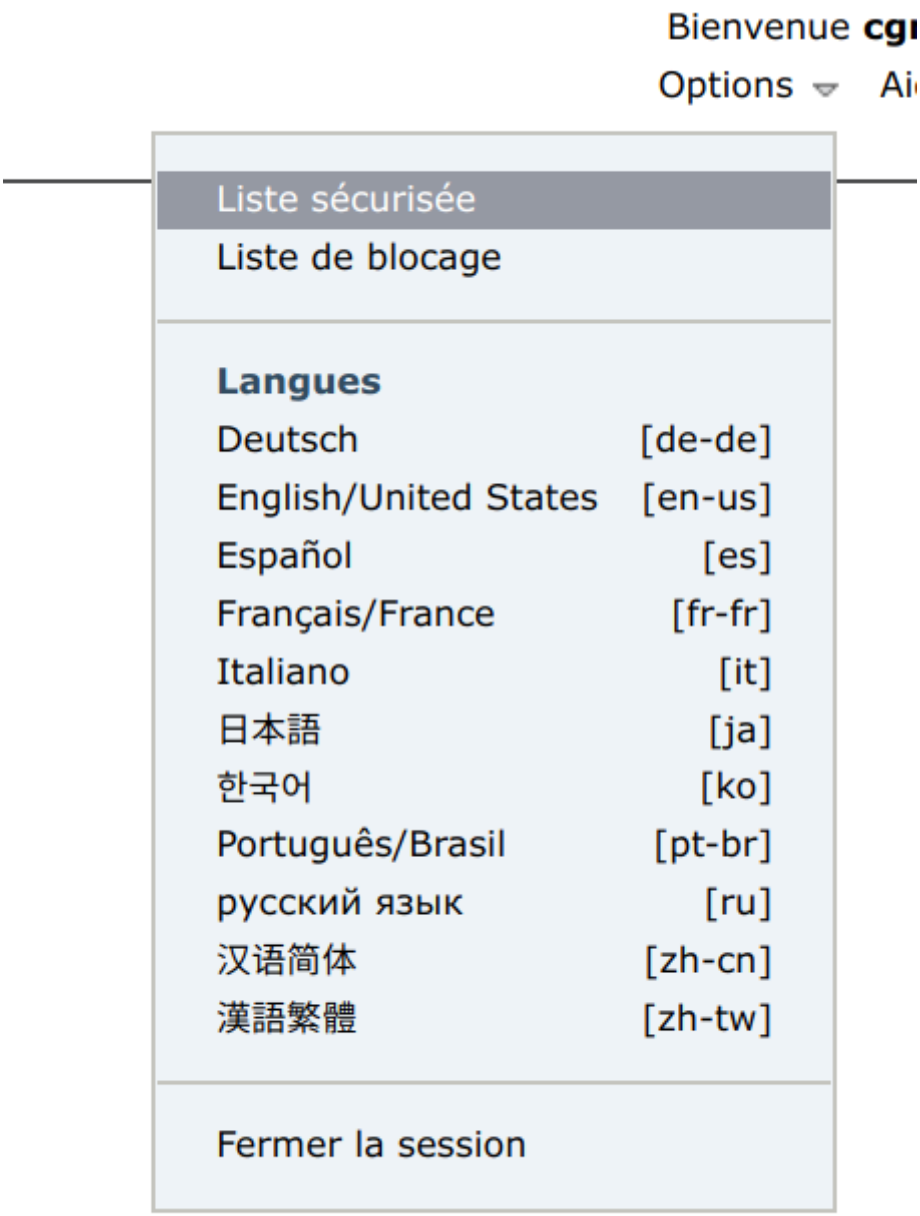
ATTENTION: les messages libérés vont souvent être mis dans le dossier **Courrier indésirable!** Vous pouvez ajouter l'adresse, ou le domaine à votre liste blanche si c'est un problème récurrent.

Comment utiliser ma liste sécurisée?

La liste blanche s'appelle maintenant la liste sécurisée. Chaque utilisateur de la messagerie UNIL a sa propre quarantaine, avec sa propre liste sécurisée.

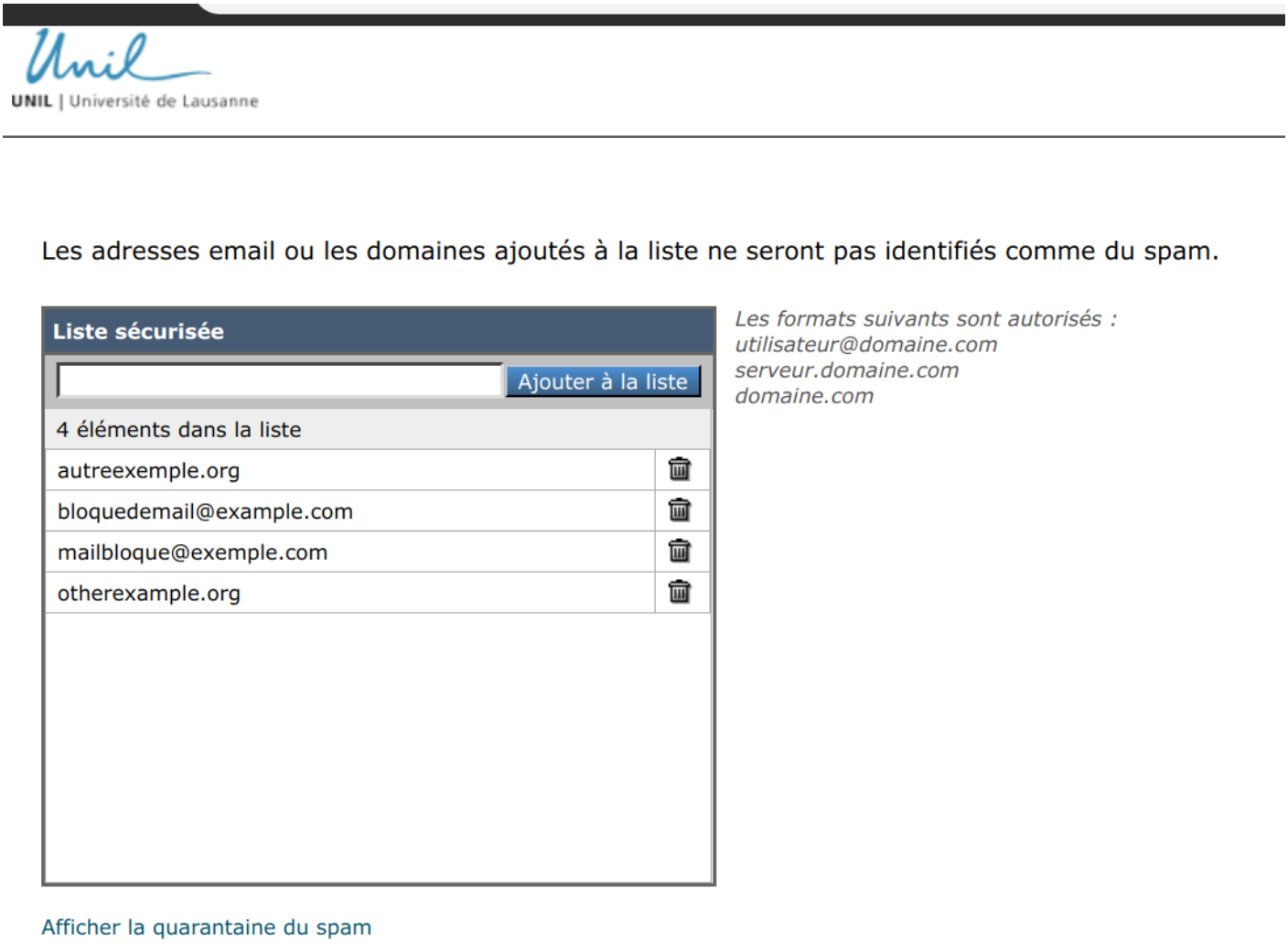
Pour y accéder, il faut se connecter à https://spam.unil.ch avec son username et mot de passe UNIL.

Dans le menu option, en-haut à droite, sélectionnez *Liste sécurisée*



Les formats suivants sont autorisés :

- utilisateur@domaine.com
- serveur.domaine.com
- domaine.com



Comment utiliser ma liste de blocage?

La liste noire s'appelle maintenant la liste de blocage. Chaque utilisateur de la messagerie UNIL a sa propre quarantaine, avec sa propre liste de blocage.

Pour y accéder, Il faut se connecter à https://spam.unil.ch avec son username et mot de passe UNIL.

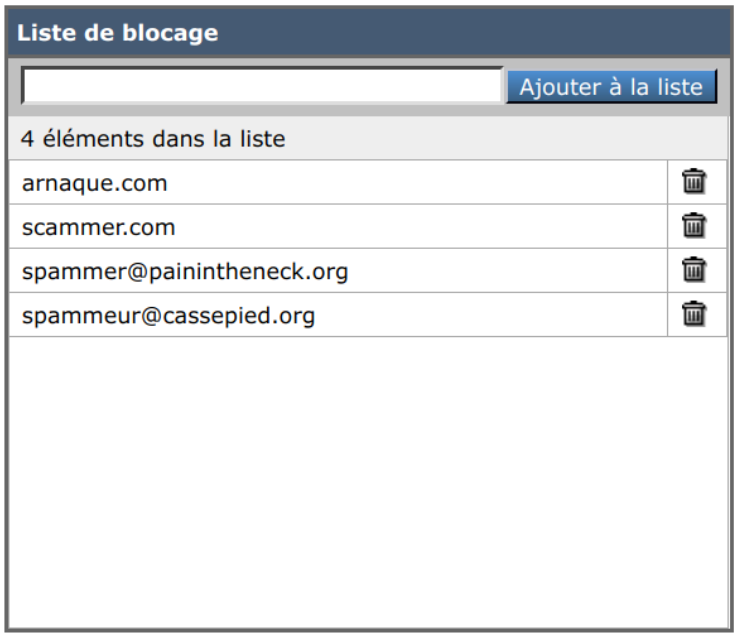
Dans le menu option, en haut à droite, sélectionnez *Liste de blocage*

Les formats suivants sont autorisés :

- utilisateur@domaine.com
- serveur.domaine.com
- domaine.com

UNIL | Université de Lausanne

Les adresses email ou les domaines ajoutés à la liste seront toujours identifiés comme du spam.



Les formats suivants sont autorisés :
utilisateur@domaine.com
serveur.domaine.com
domaine.com

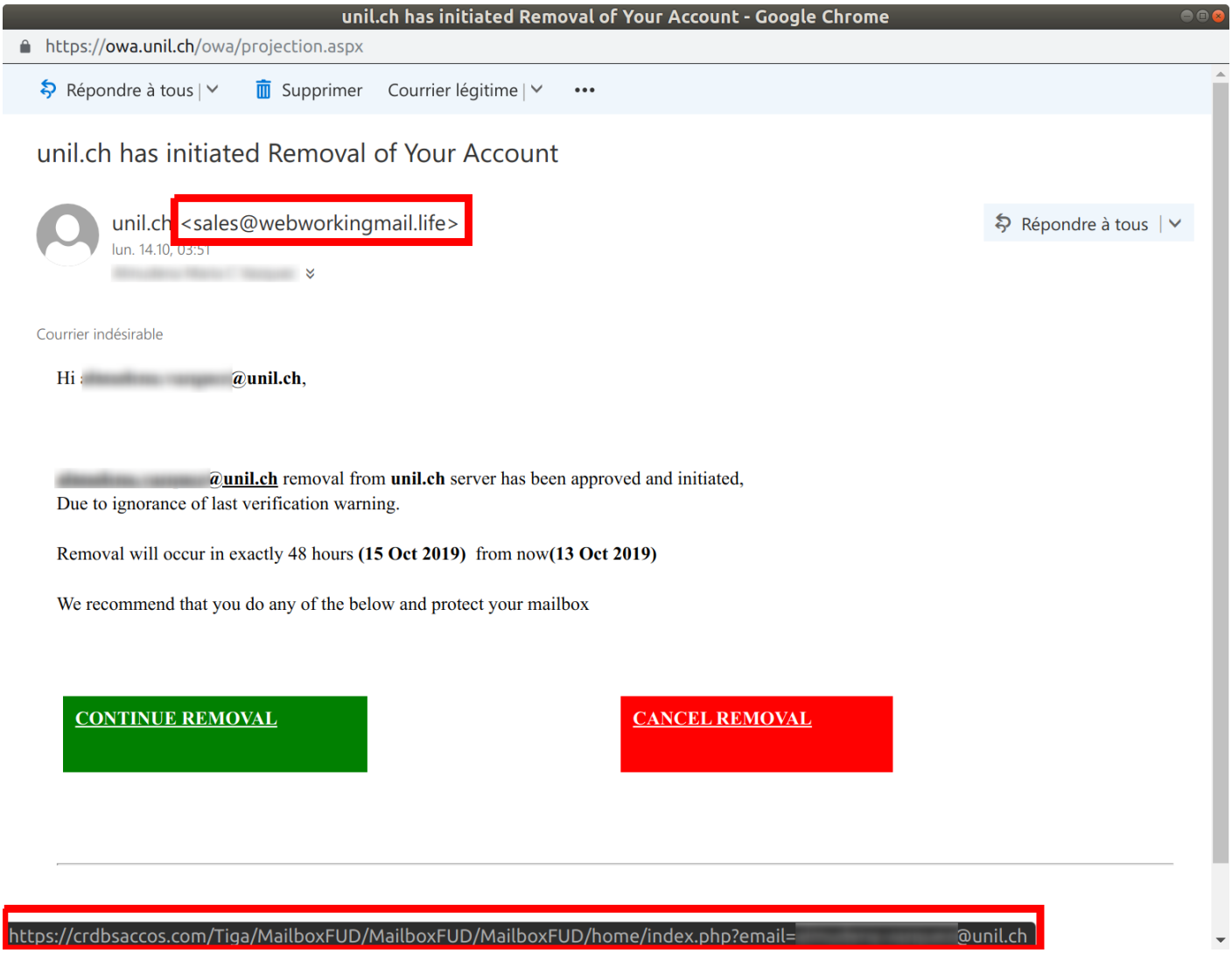
Afficher la quarantaine du spam

J'ai reçu un email, mais je ne suis pas sûr qu'il soit légitime

Quelques réflexes de base:

- Vérifiez bien l'adresse d'expédition. Sur mobile, cela peut être caché et il faut dérouler un menu pour voir l'adresse d'expédition complète
- Vérifiez bien les éventuels liens contenus dans les messages.
- Est-ce que le but du message vous paraît légitime? Un recteur ne va pas vous demander d'acheter des cartes iTunes en urgence par exemple et le Centre Informatique ne va pas vous demander d'effectuer en urgence une action pour revalider votre boîte/augmenter votre quota.

Exemple d'un email de phishing, avec en rouge la véritable adresse email de l'expéditeur, ainsi que les liens "CONTINUE REMOVAL" et "CANCEL REMOVAL" pointant vers un domaine malicieux:



Le helpdesk se tient à votre disposition pour analyser le contenu de tout message suspicieux.

Je n'ai pas reçu un mail qui m'a été envoyé, que dois-je faire? J'ai envoyé un mail qui n'est jamais arrivé, que dois-je faire?

Premier réflexe, allez voir dans votre quarantaine en vous loguant sur https://spam.unil.ch et voir si l'email en question ne s'est pas fait détecter comme spam. Si vous ne trouvez toujours pas l'email, vous pouvez contacter le helpdesk avec un **maximum d'informations: adresses de l'expéditeur et de destination, date et heure approximative** ou tout autre information pouvant nous aider à trouver la trace de l'envoi.

Je reçois systématiquement des emails d'une même origine et je souhaite que cela s'arrête.

Si c'est une liste de diffusion "légitime", il faut se désabonner. Si cela provient d'une origine plus douteuse, vous pouvez ajouter l'adresse, ou le domaine à votre liste de blocage.

Qu'est-ce qu'un phishing?

Vous trouverez beaucoup d'information sur le phishing, ainsi que d'autres arnaques en ligne sur le site https://ibarry.ch.

J'ai cliqué sur un lien dans un email de phishing et j'ai entré mon mot de passe. Que dois-je faire?

Il faut que vous changiez votre mot de passe tout de suite en vous rendant sur https://www.unil.ch/ci/pass.

Je reçois régulièrement des emails de ma propre adresse, est-ce que mon compte est compromis?

Le "spoofing" d'email est l'envoi d'email avec une adresse d'expédition forgée.

Il est fréquent que les spams et les phishings utilisent cette technique du spoofing afin de cacher l'origine du message au destinataire.

Doc publique

Eviter le phishing

Qu'est-ce que le phishing ?

Le **phishing**, traduit en français par "hameçonnage", est une méthode frauduleuse utilisée par des pirates informatiques pour voler vos données personnelles (par ex: nom d'utilisateur, mot de passe, date de naissance, numéro de carte de crédit) afin de pouvoir ensuite usurper votre identité électronique.

Une tentative de phishing se présente généralement sous forme d'un e-mail:

- qui prétend provenir d'un émetteur de confiance, comme une banque, une administration ou une entreprise
- qui utilise généralement le prétexte d'un contrôle de vos informations (menaçant même de fermer votre compte si vous ne répondez pas)
- et qui vous demande de communiquer votre nom d'utilisateur, mot de passe, numéro de carte de crédit, etc. soit par e-mail, soit en suivant un lien vers un formulaire sur un faux site web, imitant le véritable site.

Une fois en possession de vos données personnelles, les pirates peuvent accéder à vos données et usurper votre identité pour toutes sortes d'opération frauduleuses.

Comment l'éviter ?

Il faut savoir qu'aucune banque, administration ou entreprise ne vous demandera jamais par e-mail vos données personnelles. Si vous recevez un message vous demandant ce type d'information, il faut donc:

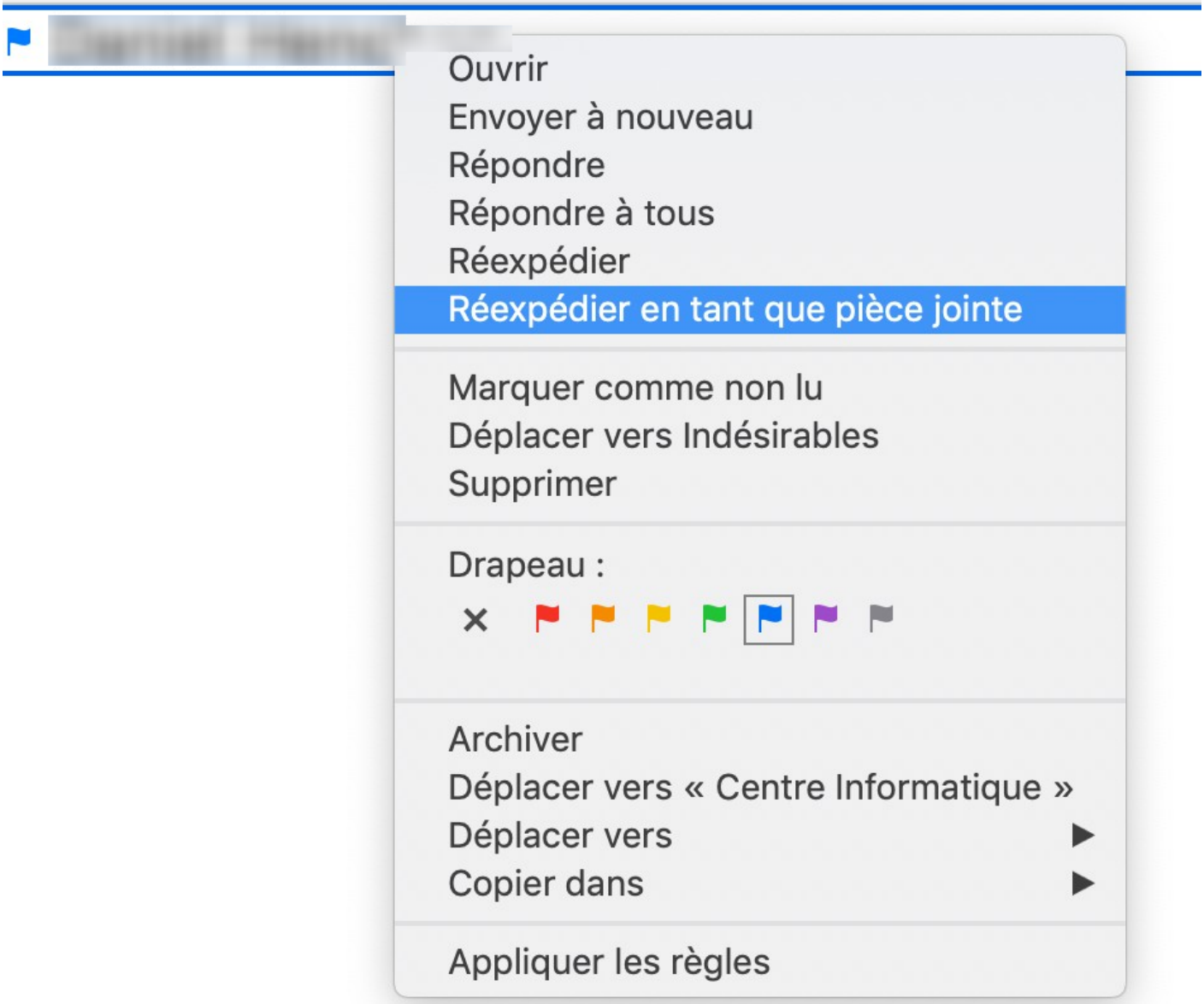
- ne jamais cliquer sur les liens contenus dans ces messages
- ne jamais répondre à ces messages

transmettre pour information ce message au Help desk du Ci (helpdesk@unil.ch), en incluant l'en-tête complet, afin de nous permettre de rechercher l'émetteur du message

Apple Mail

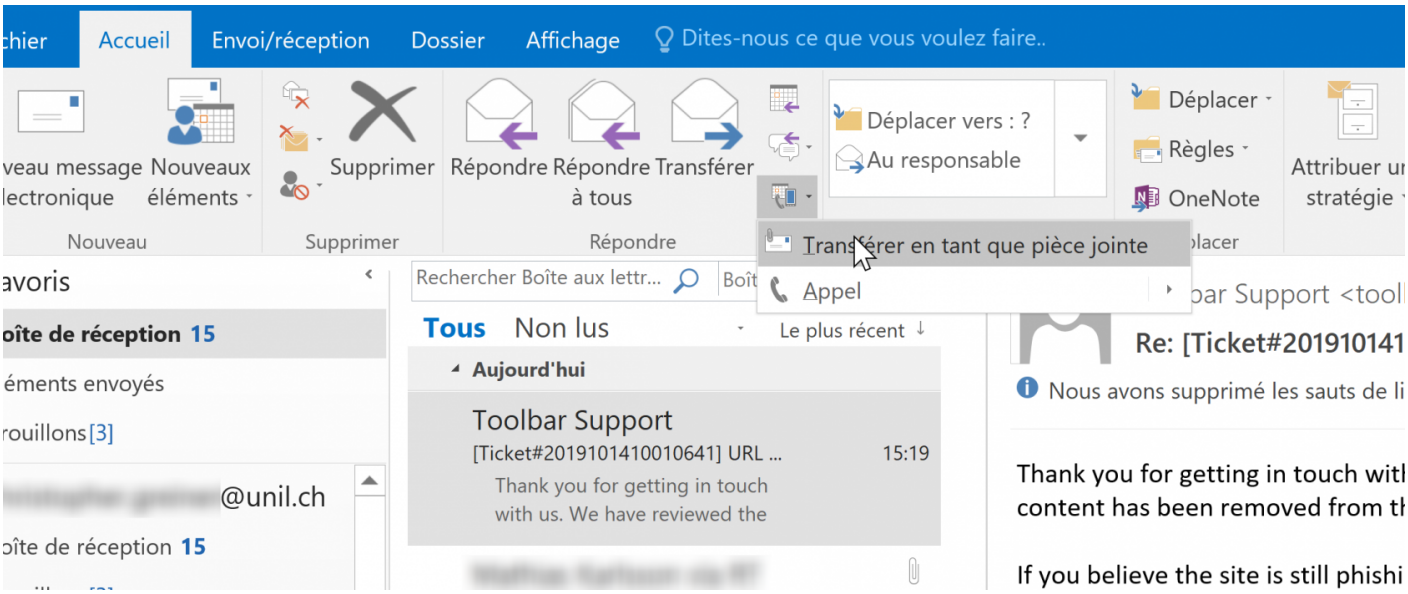
1. Sélectionnez l’email frauduleux

2. Clic droit, ou Pomme + clic.
3. Sélectionnez “**Réexpédier en tant que pièce jointe**"



Outlook PC

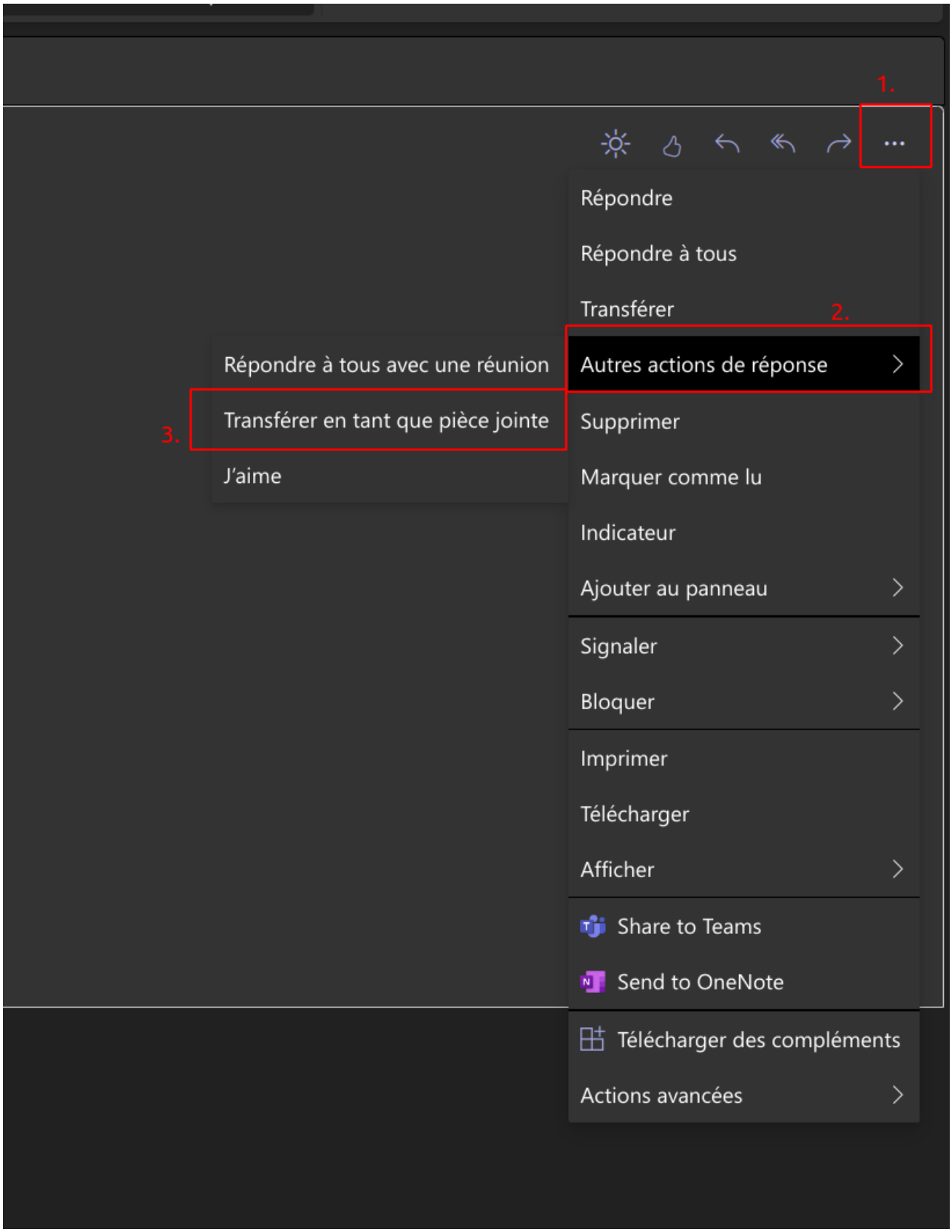
1. Sélectionnez l’email frauduleux
2. Sélectionnez le menu "Accueil" dans le ruban.
3. Dans le menu “Autres actions de réponse", sélectionnez "**Transférer en tant que pièce jointe**"



Outlook Online (outlook.office.com)

Il n'est pas possible de réexpédier un email en tant que pièce jointe. Il faut nous transmettre les entêtes du message en suivant la marche à suivre ci-dessous:

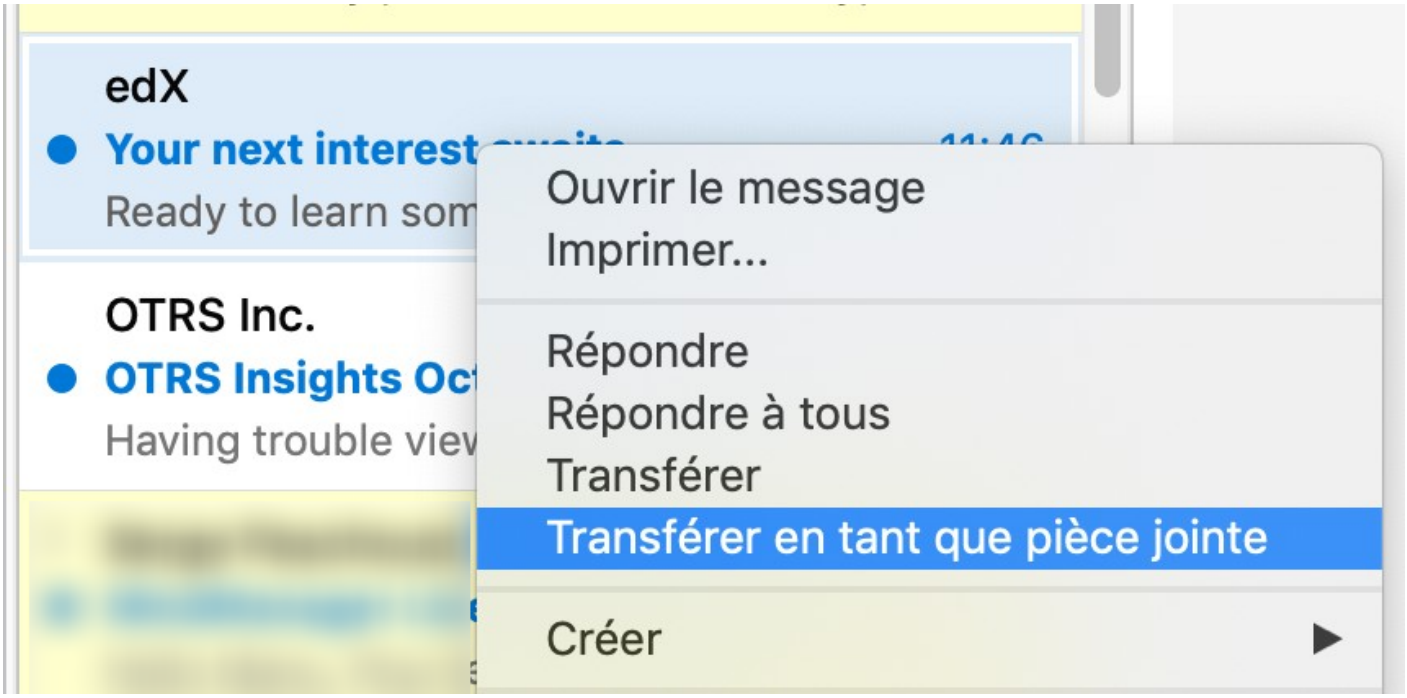
1. Connectez-vous à votre compte sur https://outlook.office.com
2. Sélectionnez le spam/phishing
3. Sélectionnez "..." en haut à droite du message
4. Sélectionnez "Autres actions de réponse"
5. Sélectionnez "Transférer en tant que pièce jointe" et adressez l'email à helpdesk@unil.ch



Finalement, vous pouvez supprimer l'email frauduleux.

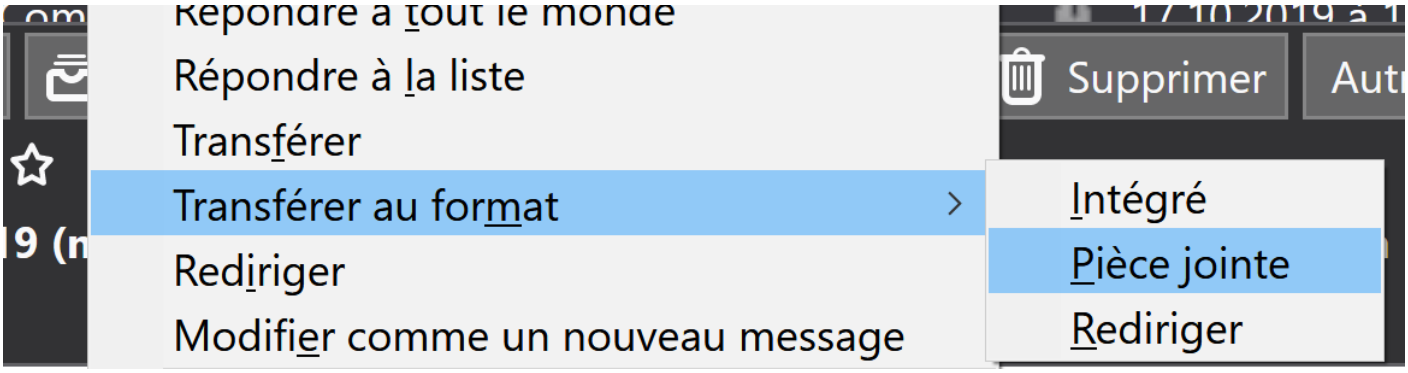
Outlook Mac

Clic droit sur le message --> Transférer en tant que pièce jointe.



Thunderbird

Clic droit sur le message --> Transférer au format --> Pièce jointe.



Si des pirates utilisent cette technique, c'est qu'elle fonctionne encore auprès de certains utilisateurs naïfs. Les messages et les contrefaçons de sites web utilisés sont parfois très bien imités. Vous pouvez même recevoir un message qui semble provenir de l'UNIL (par exemple du help desk ou du centre informatique), donc faites attention. Si vous voulez accéder à un site proposé dans un lien, mais que vous n'êtes pas certain que le message provient d'un émetteur fiable, ne cliquez pas sur ce lien. Tapez plutôt l'adresse de ce lien manuellement dans votre navigateur web.

Et si cela se produit accidentellement avec votre compte utilisateur UNIL

Si accidentellement vous vous laissez abuser par une tentative de phishing,
changez votre mot de passe immédiatement:

1. aller sur https://id.unil.ch/pass
2. suivre les instructions.

Si vous n'êtes pas certain de savoir comment faire, appelez notre service de help desk:
021 692 22 11 (de 8h à 17h) ou par email helpdesk@unil.ch.