

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 ?

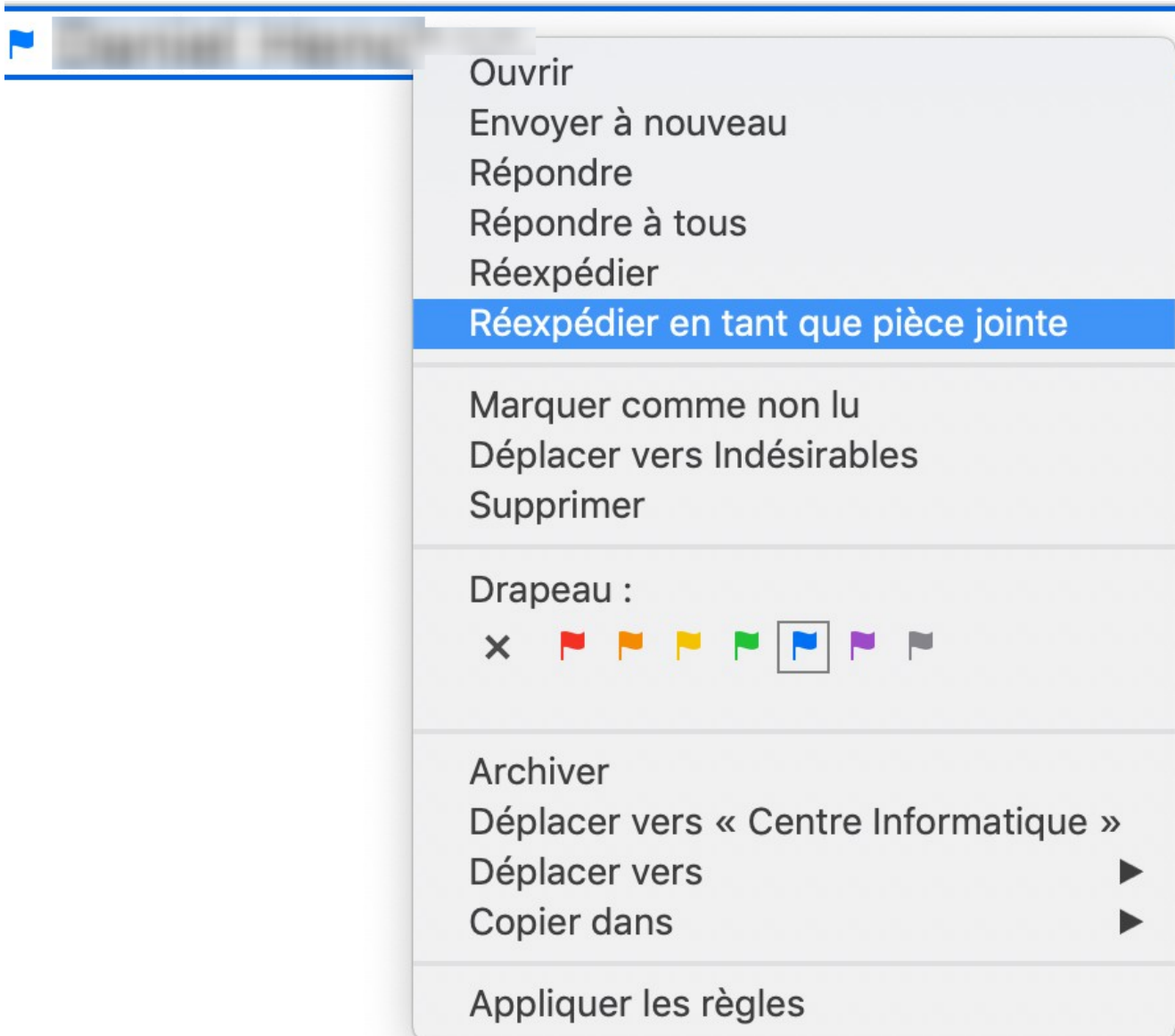
Envoyez une copie du message en tant que pièce jointe au helpdesk (helpdesk@unil.ch) pour que nous puissions adapter nos filtres. (Instructions plus bas)

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.

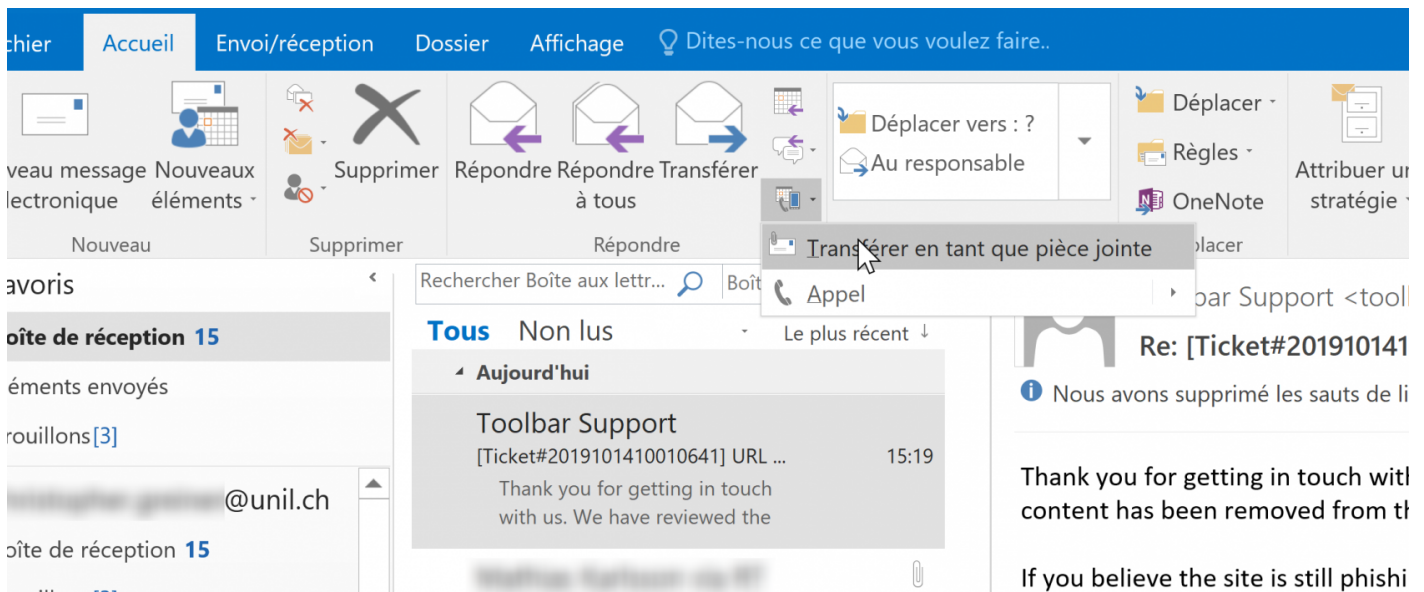
Envoyer une copie du message en pièce jointe sur **Apple Mail**

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**

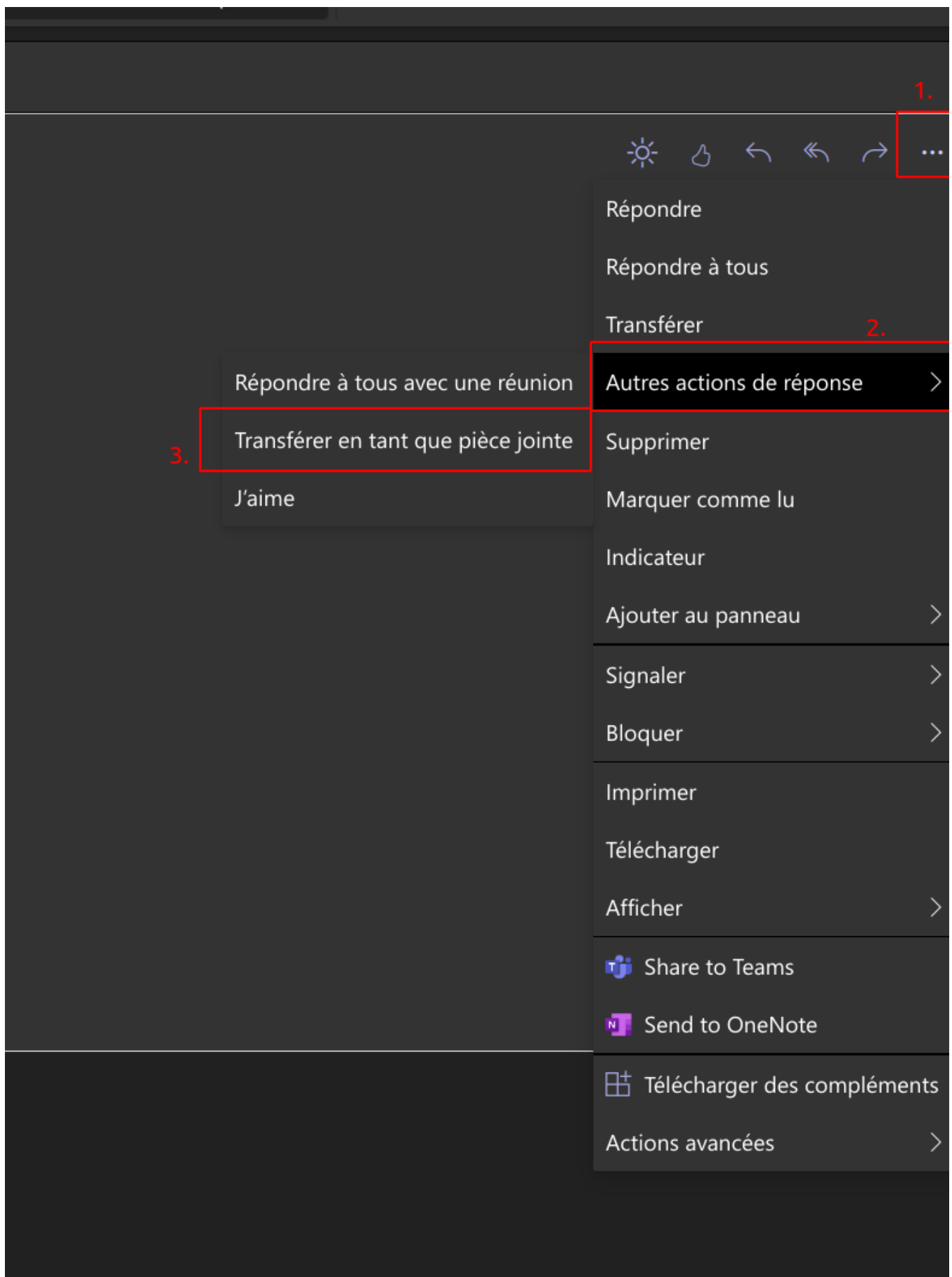
1. Sélectionnez l'email en question
2. Sélectionnez le menu "Accueil" dans le ruban.
3. Dans le menu "Autres actions de réponse", sélectionnez "**Transférer en tant que pièce jointe**"



Outlook Online (outlook.office.com)

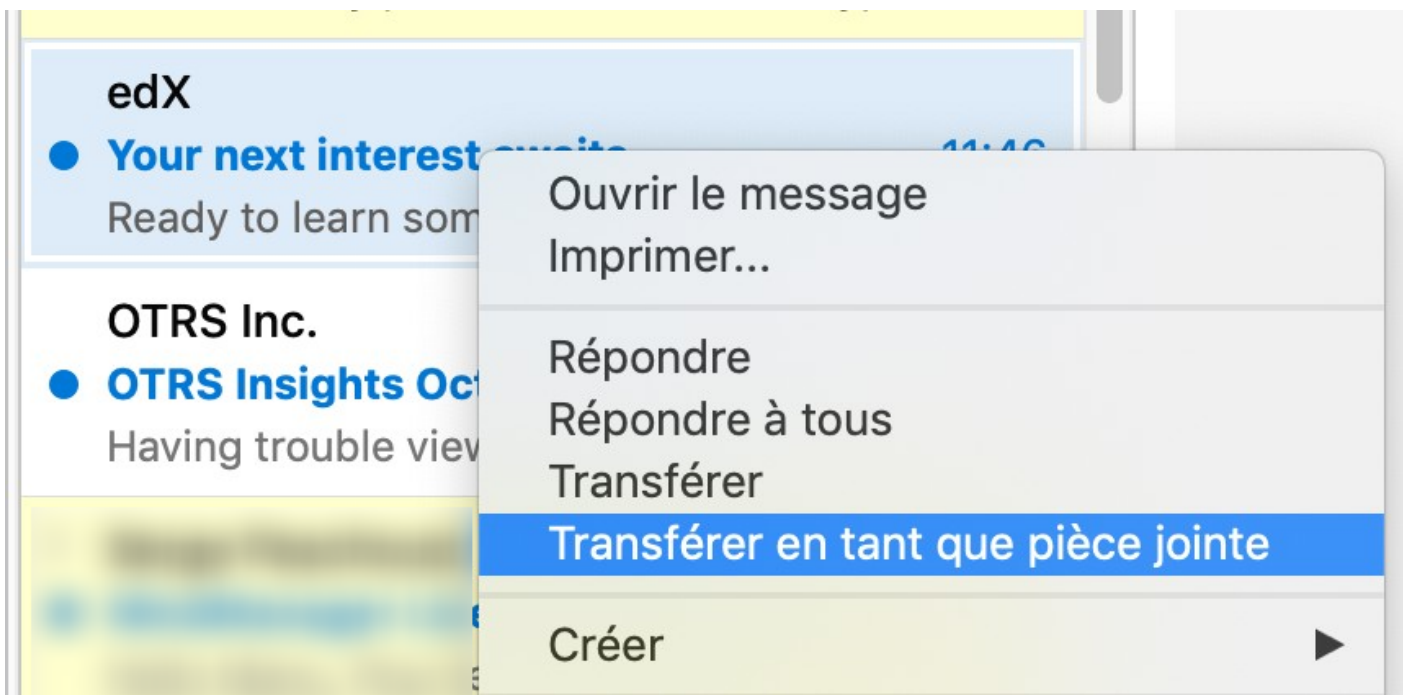
1. Connectez-vous à votre compte sur <https://outlook.office.com>
2. Sélectionnez le spam/phishing
3. Sélectionnez "... " en haut à droite du message
4. Sélectionnez "**Autres actions de réponse**"
5. Sélectionnez "**Transférer en tant que pièce jointe**" et adressez l'email à

helpdesk@unil.ch



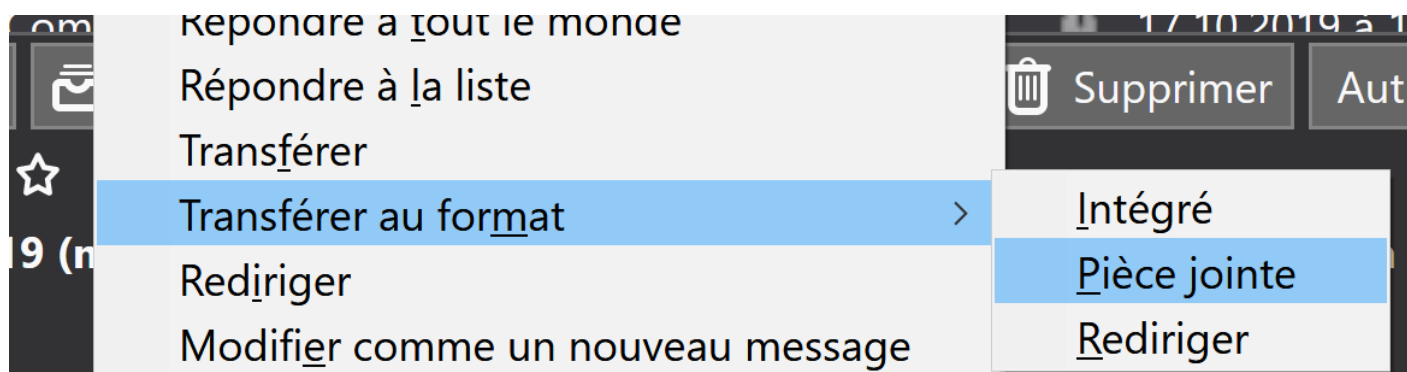
Outlook Mac

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**:

Résultats de la recherche			
Affichage de 1 — 25 éléments sur 41.			
<div>Libérer</div> <div>Supprimer</div>			
<input type="checkbox"/>	De	Destinataire du message	À
<input type="checkbox"/>	"World Bank" <worldbnkfundspayment@gmail.com>	undisclosed-recipient	"World Bank" <worldbnkfundspayment@gmail.com>
<input checked="" type="checkbox"/>	WORLD BANK <worldbnkfundspayment@gmail.com>	undisclosed-recipient	undisclosed-recipient

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*

Bienvenue **cgi**

Options ▼ Ai

Liste sécurisée

Liste de blocage

Langues

Deutsch	[de-de]
English/United States	[en-us]
Español	[es]
Français/France	[fr-fr]
Italiano	[it]
日本語	[ja]
한국어	[ko]
Português/Brasil	[pt-br]
русский язык	[ru]
汉语简体	[zh-cn]
漢語繁體	[zh-tw]

Fermer la session

Les formats suivants sont autorisés :

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

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

Liste sécurisée

[Ajouter à la liste](#)

4 éléments dans la liste

autreexemple.org	
bloquedemail@example.com	
mailbloque@example.com	
otherexample.org	

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

[Afficher la quarantaine du spam](#)

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*

Liste sécurisée

Liste de blocage

Langues

Deutsch	[de-de]
English/United States	[en-us]
Español	[es]
Français/France	[fr-fr]
Italiano	[it]
日本語	[ja]
한국어	[ko]
Português/Brasil	[pt-br]
русский язык	[ru]
汉语简体	[zh-cn]
漢語繁體	[zh-tw]

Fermer la session

Les formats suivants sont autorisés :





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

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

Liste de blocage

[Ajouter à la liste](#)

4 éléments dans la liste

arnaque.com	
scammer.com	
spammer@painintheneck.org	
spammeur@cassepied.org	

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

[Afficher la quarantaine du spam](#)

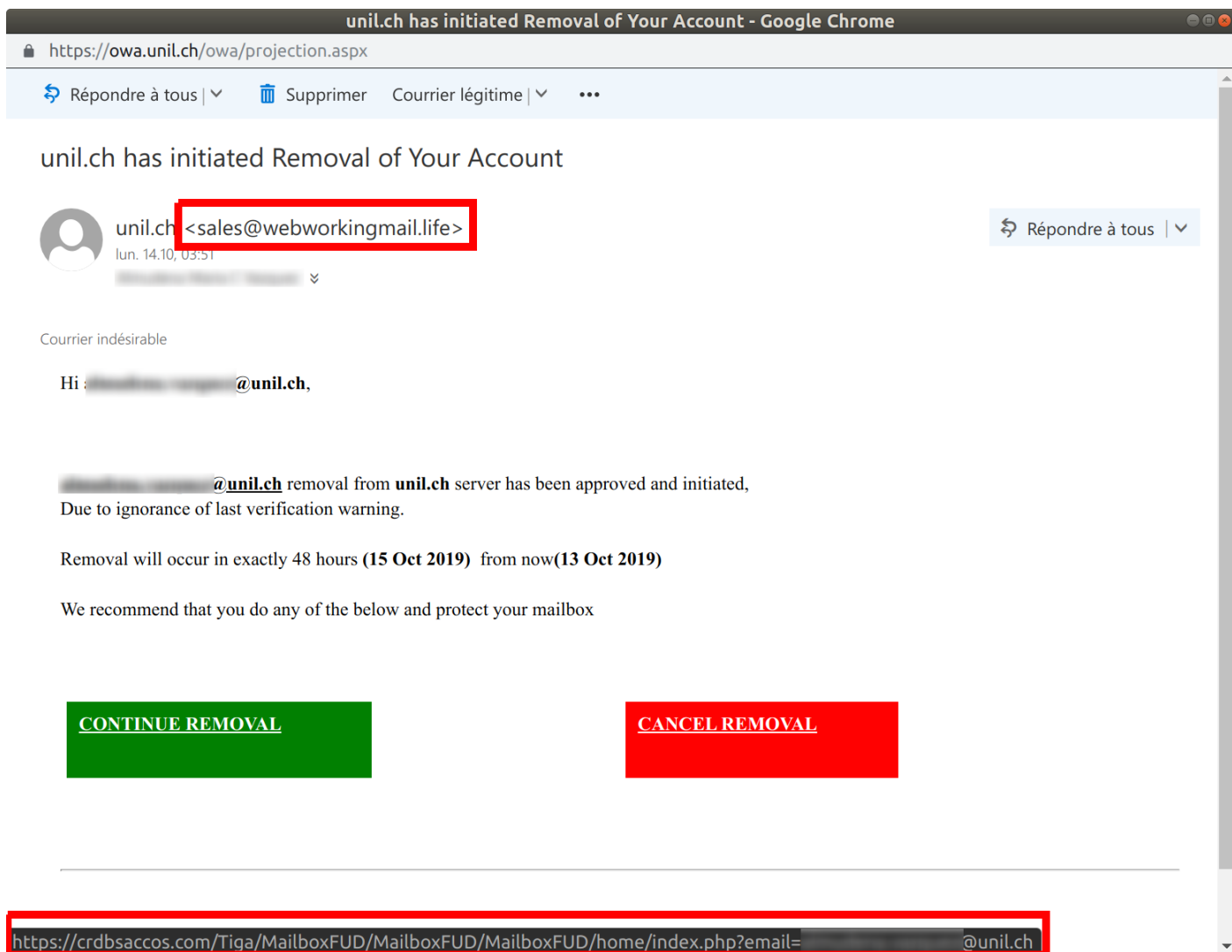
Copyright © 2003-2019 Cisco Systems, Inc. Tous droits réservés. | [Charte sur la vie privée](#)

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.

Révision #33

Créé 15 octobre 2019 13:01:39 par Chr Gr

Mis à jour 14 mars 2024 10:33:35 par Chr Gr