

Fiche d'information : Comment se protéger contre les escroqueries par e-mail, téléphone, SMS et WhatsApp

Les messages frauduleux ne sont malheureusement pas rares et leur nombre ne cesse d'augmenter. Des membres des Amis de la Nature en ont également été victimes à plusieurs reprises ces derniers temps.

Pour te protéger contre les messages frauduleux, il existe différentes mesures permettant de minimiser le risque.

Nous te présentons ci-dessous les points auxquels tu dois prêter attention en matière de messages frauduleux.

Réduire le nombre de messages frauduleux

Il existe certes des moyens de réduire le nombre de messages frauduleux, mais malheureusement, ceux-ci ne permettent pas de les éviter complètement.

Il reste donc important de faire preuve de prudence et de réagir de manière appropriée face à des messages ou des appels suspects.

Coordonnées publiques

Les escrocs recherchent sur Internet des coordonnées accessibles au public (adresses e-mail et numéros de téléphone) qu'ils peuvent utiliser pour mener leurs escroqueries.

Si ton adresse e-mail ou ton numéro de téléphone apparaît en permanence sur le site web des Amis de la Nature, dans la rubrique « À propos de nous », le risque que tu sois contacté par des escrocs augmente.

Pour éviter ce risque, l'adresse e-mail et le numéro de téléphone ne devraient figurer que dans la confirmation d'inscription à l'activité.

Si cela n'est pas possible, nous te recommandons de remplacer ton adresse e-mail privée par une adresse e-mail des Amis de la Nature. Si tu ne disposes pas encore d'une adresse e-mail des Amis de la Nature, nous pouvons t'en créer une. Il est également possible de configurer un transfert vers ton adresse e-mail privée.

Tu devrais supprimer ton numéro de téléphone privé du site web des Amis de la Nature. Le premier contact devrait alors s'effectuer via l'adresse e-mail.

Filtre anti-spam

Les filtres anti-spam peuvent détecter automatiquement les messages et les appels suspects grâce à différentes caractéristiques. Selon l'application utilisée, ceux-ci sont soit bloqués directement, soit marqués comme spam, soit déplacés vers un dossier distinct.

Filtre anti-spam pour les e-mails

Un filtre anti-spam peut être activé dans la plupart des clients de messagerie. Pour Microsoft Outlook, voici la procédure à suivre : [Filtre anti-spam d'Outlook](#)

Si tu utilises une adresse e-mail « Naturfreunde », tu peux éventuellement configurer d'autres filtres : [Filtre anti-spam Hostpoint](#)

Filtre anti-spam téléphonique

Pour les appels, il est possible d'activer un filtre anti-spam dans les paramètres de la plupart des smartphones modernes. Sur les appareils Android, ce paramètre s'intitule « Identification de l'appelant et protection anti-spam ».

Chez les opérateurs de télécommunications suisses, il est possible d'activer des filtres anti-spam supplémentaires. Pour Swisscom, voici le guide à suivre : [Filtre anti-spam Swisscom](#)

Filtre anti-spam pour SMS

Pour les SMS, un filtre anti-spam peut être activé dans les paramètres de l'application, sous « Paramètres des messages -> Sécurité et confidentialité -> Protection anti-spam ».

Filtre anti-spam WhatsApp

WhatsApp propose différentes fonctionnalités de protection contre les messages indésirables. Dans « Paramètres -> Confidentialité -> Avancé », vous pouvez activer la fonction « Bloquer les messages provenant de comptes inconnus ». Celle-ci bloque les messages provenant de comptes inconnus qui envoient un grand nombre de messages.

Reconnaître les messages frauduleux

Les messages frauduleux ne sont souvent pas reconnaissables comme tels au premier coup d'œil. C'est pourquoi il est important de prendre le temps de les examiner attentivement. Si tu n'es pas sûr qu'un message soit frauduleux, demande plutôt conseil à quelqu'un avant d'y répondre. Quatre yeux valent mieux que deux!

Numéro de téléphone inconnu

Si tu reçois un message ou un appel provenant d'un numéro de téléphone que tu ne connais pas, tu dois toujours faire preuve de prudence.

Prends l'habitude d'enregistrer les numéros de téléphone que tu connais et de bloquer ceux qui t'envoient des spams.

Adresse e-mail de l'expéditeur

Cette arnaque fonctionne ainsi : tu reçois un e-mail provenant d'une adresse qui semble aussi fiable que possible. Il suffit de changer une seule lettre pour que l'adresse soit à peine reconnaissable, tout en étant pourtant différente.

Par exemple, les deux adresses e-mail suivantes sont différentes (dans l'une d'elles, le «l» minuscule a été remplacé par un «I» majuscule):

- heinz.vogt@naturfreunde-kloten.ch
- heinz.vogt@naturfreunde-kloten.ch

Fautes d'orthographe et style

Ces escroqueries reposent généralement davantage sur la quantité que sur la qualité et présentent souvent des caractéristiques similaires :

- Fautes d'orthographe
- Orthographe inhabituelle (ß au lieu de ss)
- C'est urgent
- Il n'est pas possible de téléphoner
- Il s'agit d'argent

Comment réagir correctement lorsqu'on reçoit un message frauduleux

Un message frauduleux n'est pas forcément dangereux en soi. Cependant, les fraudeurs tentent souvent, par le biais de ce contact, de vous inciter à divulguer des informations personnelles, à effectuer un virement bancaire ou à ouvrir des fichiers malveillants.

Si vous pensez qu'un message est suspect:

- Ne répondez pas au message
- Ne cliquez sur aucun lien
- N'ouvrez aucun fichier
- N'effectuez aucun virement bancaire

Réagir correctement lorsqu'on s'en est rendu compte trop tard

Même en faisant preuve de prudence, il peut arriver que l'on se rende compte trop tard d'une escroquerie. Il est alors important d'agir le plus rapidement possible afin de limiter les dégâts.

Les démarches à effectuer dépendent de ce qui s'est passé exactement.

- Mot de passe saisi -> Modifier le mot de passe
- Coordonnées de la carte bancaire saisies -> Bloquer la carte
- Virement effectué -> Informer la banque
- Fichier ouvert -> Vérifier si l'appareil est infecté par un logiciel malveillant

Si tu as des questions ou des doutes, tu peux à tout moment contacter
support@naturfreunde.ch.