



VIVRE À SCHWEIGHOUSE



Comment reconnaître un mail frauduleux

Tout comme les escroqueries par téléphone, les escroqueries par mail sont nombreuses. Ces mails qui vous demandent des renseignements, de payer une facture, vous rembourser, vous proposer un emploi, des bons plans... Voici quelques points de vigilance, nous vous proposons des astuces pour essayer de démasquer ces mails frauduleux.

Recherche de l'expéditeur

Une adresse mail se compose : d'un nom de contact, d'un arobase "@" et d'un nom de domaine (entreprise ou fournisseur). Il ne faut pas confondre le nom de l'expéditeur et l'adresse mail de l'expéditeur. Même si le nom de votre correspondant ressemble à une connaissance ou un organisme, il faut vérifier le mail. Si le nom de contact possède les mots "gouv.fr" avant l'arobase (@), il s'agit d'un mail frauduleux. Cependant, si tout semble correct, cela ne signifie pas que le mail n'est pas frauduleux.

Le corps du message

- Le mail est arrivé dans le dossier spams
- Vous ne connaissez pas l'expéditeur, sa demande vous paraît bizarre
- L'objet du mail est vague ou contient votre adresse e-mail
- Le mail contient des fautes d'orthographe ou de grammaire
- Le mail arrive de manière inattendue. On vous propose un emploi alors que vous n'avez fait aucune demande, gagné quelque chose alors que vous ne jouez jamais, devez payer pour quelque chose que vous avez gagné...
- On vous demande de répondre en urgence (une sommation de payer, un remboursement, un ami en difficulté...)
- On vous demande d'effectuer un paiement (placement, crypto, Western Union...)
- On vous demande de transmettre par mail ou par SMS : des mots de passe, numéro de CB ou code envoyé par la banque, un numéro de compte bancaire...
- On vous demande de cliquer sur un lien hypertexte ou scanner un QR code pour accéder à un site ou pour remplir un formulaire. Dans ce cas, il faudra vérifier s'il s'agit du vrai site officiel, pas d'un site cloné
- On essaie d'éveiller votre curiosité avec des phrases du style : « Regardez ce que j'ai lu sur vous... » ou « Est-ce bien vous sur cette photo ? »

En cas de doute, une question, vous pouvez contacter la gendarmerie de Haguenau par téléphone au 03 88 07 41 00, par mail à bta.haguenau@gendarmerie.interieur.gouv.fr ou par chat avec un gendarme de la brigade numérique 24H/24 sur <https://www.gendarmerie.interieur.gouv.fr/Brigade-numerique>

L'adjudant RISCH Grégory
Gendarmerie de HAGUENAU



Nos conseils

- Ne jamais cliquer sur un lien, cherchez vous-même le site officiel sur le web ou appelez l'organisme qui vous a envoyé le mail
- Ne jamais transmettre des informations bancaires (comptes, mots de passe, CB...) par mail ou SMS. Votre banque vous connaît, ils connaissent ses informations
- Ne jamais payer en cryptomonnaie, Western Union, PCS...
- En cas de doute, contactez l'expéditeur en cherchant vous-même ses coordonnées
- Vous décelez un mail frauduleux. Signalez-le à : www.internet-signalement.gouv.fr
- Vous vous rendez compte trop tard. Faites une analyse anti-virus, prévenez votre banque ou autre organisme, changez votre mot de passe
- Un mail qui arrive sans être le résultat d'une action de votre part mérite votre attention. Cela vaut aussi pour la réception de SMS alléchants
- En cas de dépôt de plainte, n'effacez pas les mails originaux ou les SMS. Notez les heures et les numéros de téléphone reçus. Gardez un maximum de renseignements, les enquêteurs en auront besoin

