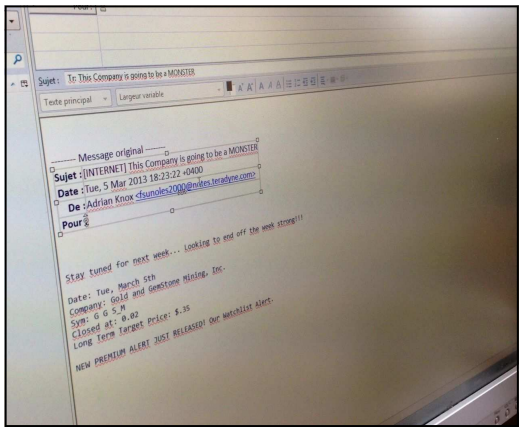
Se méfier des escroqueries les plus courantes via les messageries

Le SPAM *Envoi massif de «Courriers électroniques indésirables »*

Ces courriers sont pour la plupart des messages de type publicitaire.

Comment s'en prémunir ?

Il ne faut jamais répondre à ce type de message car cela indique à l'expéditeur que l'adresse électronique est valide.
Il est conseillé d'utiliser des logiciels permettant de supprimer automatiquement des messages.
De plus amples informations sont disponibles sur le site : www.signal-spam.fr



Si vous êtes victime

- *Déposez plainte au commissariat ou à la gendarmerie la plus proche en faisant usage de la pré-plainte en ligne https://www.pre-plainte-en-ligne.gouv.fr*
- *Munissez-vous de tous les renseignements permettant d'identifier l'escroc (références du transfert d'argent effectué, références de la ou les personnes contactées (adresse de messagerie, pseudo, copie des courriels...).*

POUR SIGNALER UN COURRIEL OU UN SITE INTERNET D'ESCROQUERIES
www.internet-signalement.gouv.fr

Gendarmerie nationale

POLICE NATIONALE

SAP ALIAS

Vous pouvez être victime de malveillances sur internet

Vous utilisez votre ordinateur connecté à internet pour :

- *Consulter des messages,*
- *Naviguer sur des pages web,*
- *Faire du commerce électronique ou acheter des produits sur des sites en lignes .*

Des personnes mal intentionnées peuvent réaliser des escroqueries en utilisant soit des failles techniques soit en abusant de la crédulité des victimes.

Quelques conseils pour se prémunir des escroqueries les plus courantes

LES ESCROQUERIES VIA LES MESSAGERIES

- *Mettre à jour votre système régulièrement*
- *Utiliser un anti-virus régulièrement mis à jour,*
- *Activer le pare-feu de votre sytème.*
- *Se méfier des offres trop alléchantes,*
- *Ne conclure aucun achat important sans rencontrer le vendeur, ni avoir vu ou essayé le bien*
- *Privilégier des sites connus (solutions de paiement en ligne) avant d'effectuer un transfert de fonds ou un virement bancaire à l'étranger,*
- *Évitez les paiements par mandats cash et autres paiements en espèces sur les sites de petites annonces,*
- *S 'assurer qu'il s'agit d'une adresse sécurisée (vérifier la présence du «s» dans l'adresse https:// et la présence d'un cadenas en bas ou en haut de la page sécurisée),*
- *Vérifier son «panier» et le prix du produit avant de confirmer ses achats.*

A savoir

Depuis la loi « sécurité quotidienne » du 15 novembre 2001, la responsabilité du titulaire d'une carte de crédit n'est pas engagée si la carte a été contrefaite ou si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de la carte.

LES ESCROQUERIES AU PAIEMENT PAR CARTE BANCAIRE

- *Ne pas laisser traîner votre carte bancaire à la vue d'autres personnes, ni la laisser dans votre voiture ou tout autre lieu sans protection.*
- *Après chaque achat, penser à reprendre votre carte bancaire.*
- *Ne jetez pas vos tickets de caisse sans les détruire totalement, votre numéro de carte bancaire y figure.*
- *Ne jamais communiquer votre numéro confidentiel de carte bancaire à une tierce personne.*
- *Ne donnez jamais votre numéro de cryptogramme (numéro inscrit au verso de votre carte bancaire, dans l'encart signature, servant aux achats par Internet).*
- *Ne pas laisser le numéro de code secret avec votre carte bancaire.*
- *Votre carte bancaire doit porter votre signature au dos.*
- *Si un message vous demande de rappeler tel numéro, ne le composez pas. Aucune banque ne demande de renseignements par courriers électroniques ou téléphone. Dans le doute, contactez votre banque.*

Se méfier des escroqueries les plus courantes via les messageries

Le PHISHING *Technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes via un site web* ***factice*** *copie conforme du site original.*

Comment s'en prémunir ?

Ne cliquez pas directement sur le lien contenu dans le mail, mais saisissez vous-même l'adresse URL d'accès au service.

Assurez-vous que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par https et qu'un petit cadenas est affiché dans la barre d'état au bas de votre fenêtre.

Le SCAM *Vous recevez un mail d'un richissime étranger. Il dit avoir besoin de votre aide pour récupérer sa fortune bloquée à l'étranger.*

Objectif ?

Vous amener à verser de l'argent (parfois des centaines de milliers d'euros) pour payer des frais de dossiers imaginaires en vous faisant miroiter une partie du pactole.

Comment faire ?

Ne répondez en aucun cas à ces messages et détruire directement ce mail.