LES SPAMS, SCAMS, PHISHINGS ET RANSOMWARES

QUAND LES COURRIERS ÉLECTRONIQUES ET SMS DEVIENNENT UNE MENACE !

SOMMAIRE

LE MAIL : LE COURRIER 2.0

- Avec l'arrivée d'internet et sa démocratisation au début des années 2000, de nouveaux modes de transmission ont bouleversé nos moyens de communication.
- Parmi eux, le mail (ou courriel en français), est sans aucun doute un des plus connus, voire des plus utilisés.
- Cependant, bien que très pratique de part sa facilité d'utilisation et sa rapidité, il n'en demeure pas moins sans dangers !
- Dans ce cours, nous allons aborder ces différentes menaces, les conseils pour les reconnaitre et ne pas en être victime.

PARTIE 1 : LE COURRIER INDÉSIRABLE

Définition :

Le courrier indésirable est le terme générique qui désigne les courriers non sollicités, inutiles ou qui présentent un danger pour l'internaute.

Il se compose de plusieurs types de mails, que nous allons apprendre à différencier.

LE SPAM (OU POURRIEL) : LE FLÉAU DE VOTRE BOITE MAIL !

- **Un spam, c'est quoi ? :**

Lorsque l'on reçoit un courrier indésirable, on a tendance à le qualifier de spam. L'action dite de « spammer » est le fait d'envoyer EN MASSE un message pour qu'il atterrisse dans le plus de messageries possibles (sans le consentement des personnes ciblées). On peut donc en déduire que, tout message indésirable est un spam mais, avec différents niveaux de dangerosité.

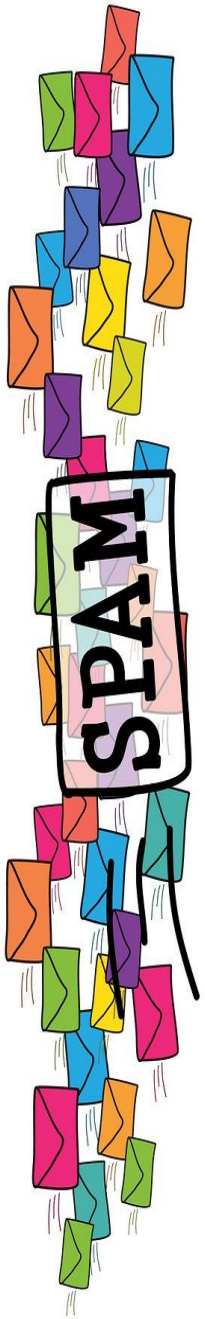
- **Pourquoi est ce que je reçois des spams ?**

Difficile de répondre avec certitude. Cela peut dépendre de plusieurs facteurs.
En général, lorsque vous recevez des spams, c'est parce que vous avez inscrit, (le plus souvent par inadvertance), votre adresse mail sur un ou plusieurs sites peu sécurisés. Mais ce n'est pas la seule raison. Il se peut également que même malgré tous les efforts de l'utilisateur, son mail se retrouve sur une ou plusieurs listes de diffusion (là encore, sans son consentement). On dit même que certaines entreprises en ont fait un juteux business de revente.
Faites donc attention à bien vérifier la réputation du site sur lequel vous inscrivez votre mail !

- **Comment ne plus recevoir de Spams ?**

Là encore, c'est compliqué car, une fois votre adresse mail dans la liste, il n'est pas simple de faire arrêter les envois.
- La première des règles à suivre : Il ne faut JAMAIS OUVRIR UN SPAM ! (en effet, cela à pour action de montrer à l'envoyeur que votre boite est toujours active et les envois automatiques continueront encore plus) ! Il va donc vous falloir apprendre à les repérer et c'est ce que nous allons voir ensuite.
Dès vous avez identifié un spam, placer le directement dans le dossier « courriers indésirables ». TOUS LES CLIENTS DE MESSAGERIE EN ONT UN !
Avec le temps, votre boite mail apprendra à les reconnaitre et les placera d'elle-même dedans. Le dossier étant automatiquement supprimé au bout de 10 ou 30 jours, (selon le réglage) aucune action n'est requise de votre part.

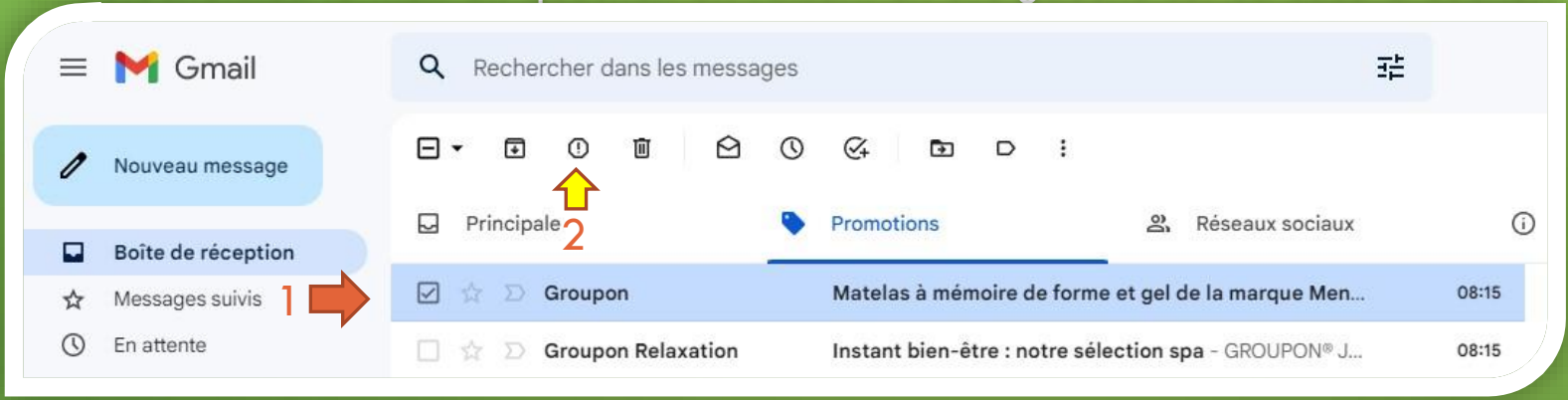
Et enfin, si les mails d'un même utilisateur reviennent sans cesse, sachez que vous avez la possibilité de le mettre directement en liste noir.
Vous ne devriez plus recevoir de message de la dite personne mais… gardez en tête que cette action reste peu efficace.
A savoir : Les spams étant envoyés par des robots automatisés, les adresses changent quasiment tout le temps, d'où la difficulté de les faire stopper.
Si malgré tout, vous continuez d'être submerger de mails indésirables, il vous reste l'option (plus radicale) de créer une nouvelle boite mail.
Mon petit : Si possible, créez vous plusieurs boites mails distinctes (Perso, travail…). Certains fournisseurs d'accès en proposent jusqu'à 5 GRATUITES. Cela évitera qu'une seule et même boite traine partout sur la toile et cela en réduira d'autant plus les infections.



COMMENT METTRE UN MAIL DANS LE COURRIER INDÉSIRABLE ?

La procédure est simple. Elle comporte 2 étapes :

1- Sélectionnez le mail en question en faisant un clic gauche sur sa case à cocher.



2 – Cliquez sur le bouton « Signalez comme spam ». Gmail va alors vous demander une confirmation. Si vous confirmez, cela aura pour effet de déplacer automatiquement le message dans le dossier « courriers indésirables ou spams ».

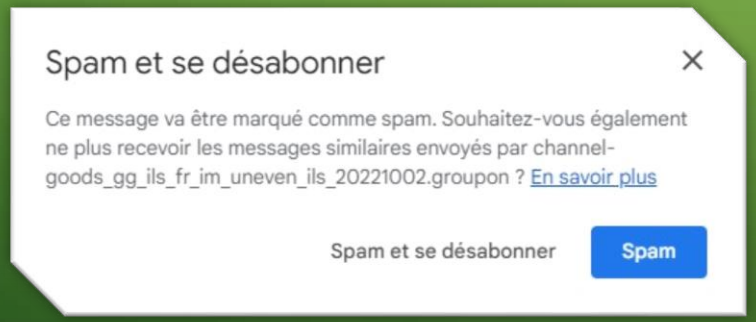


Fig. 1

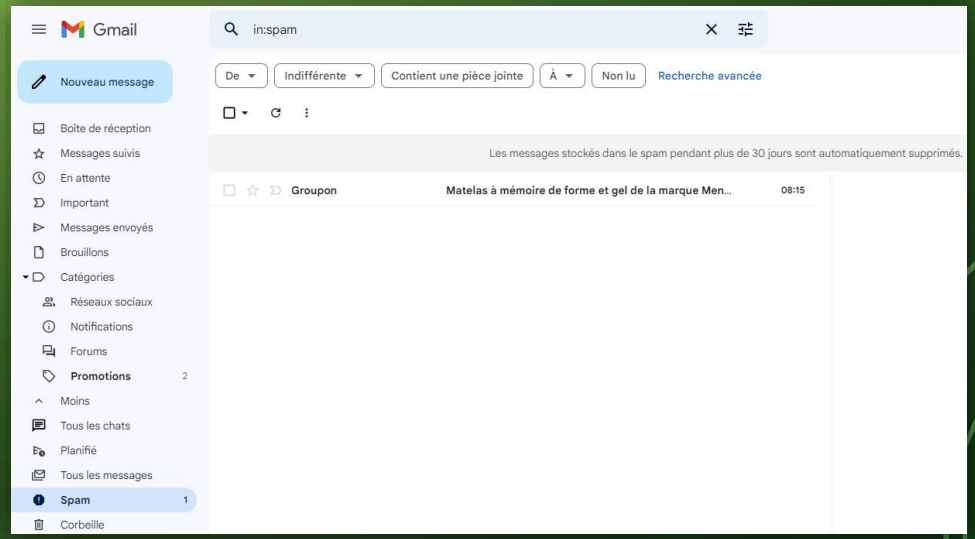
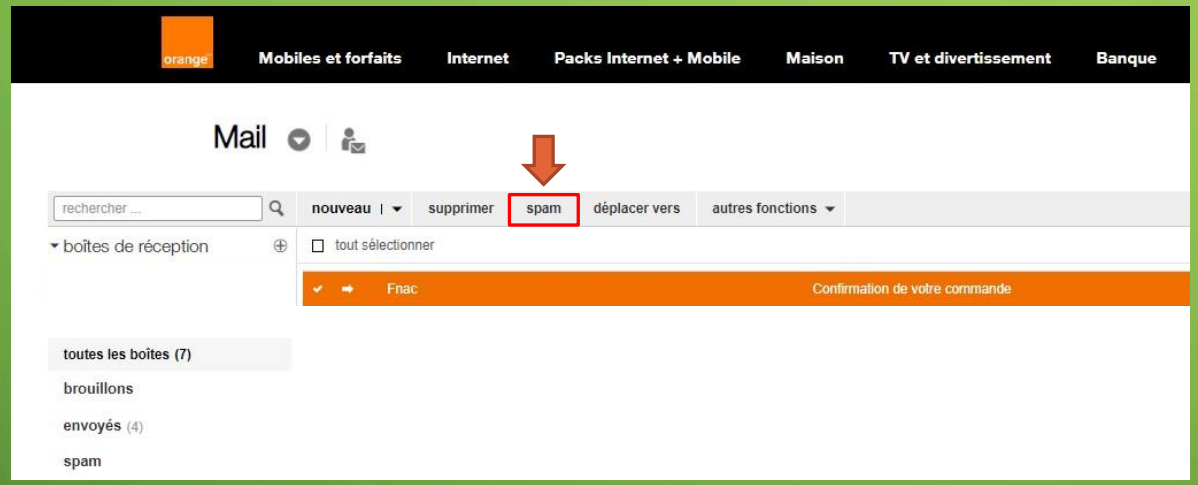


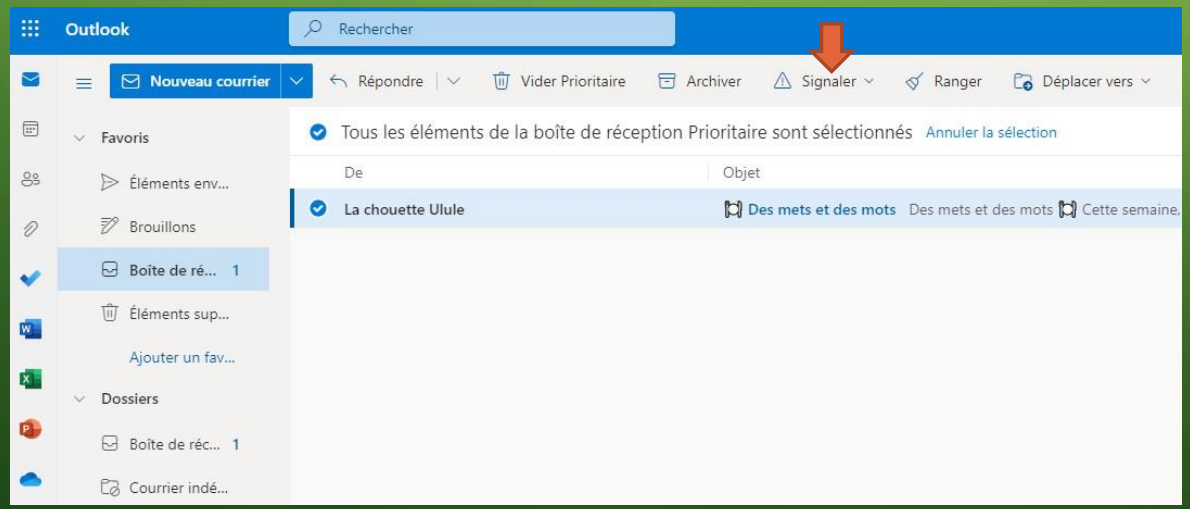
Fig. 2

LES DIFFÉRENTES FORMES DU BOUTON « SPAM »

Nous venons de voir comment mettre en spam un courrier sur Gmail. Cependant, il se peut que (dans le cadre de votre travail ou tout simplement par choix personnel), vous utilisiez un autre client de messagerie. Le principe reste le même mais les boutons peuvent différencier. Voici quelques exemples :



Ici, sur la boite mail Orange, le bouton Spam n'est pas sur forme d'icone mais directement nommé « spam ».



Alors qu'ici, sur Hotmail / Outlook, c'est le bouton signaler qui fait office de mise en spam.
Avec, vous aurez la possibilité :

- Soit de marquer le message comme simple « spam ».
- Soit de le marquer comme étant un « hameçonnage ».

QU'EST CE QU'UN ANTI-SPAM ET COMMENT FONCTIONNE T'IL ?

Nous savons désormais mettre un mail dans le dossier « spam » mais c'est manuel et sur plusieurs dizaines de fichiers, cela pourrait vite devenir fastidieux, et dangereux. C'est pourquoi les sociétés de messageries électroniques intègrent à leurs logiciels une fonction anti-spam automatique.

L'anti-Spam, qu'il vienne d'une boite mail, ou d'un logiciel tierce désigne un algorithme qui va être conçu pour apprendre à votre messagerie à différencier les bons mails, des mauvais.

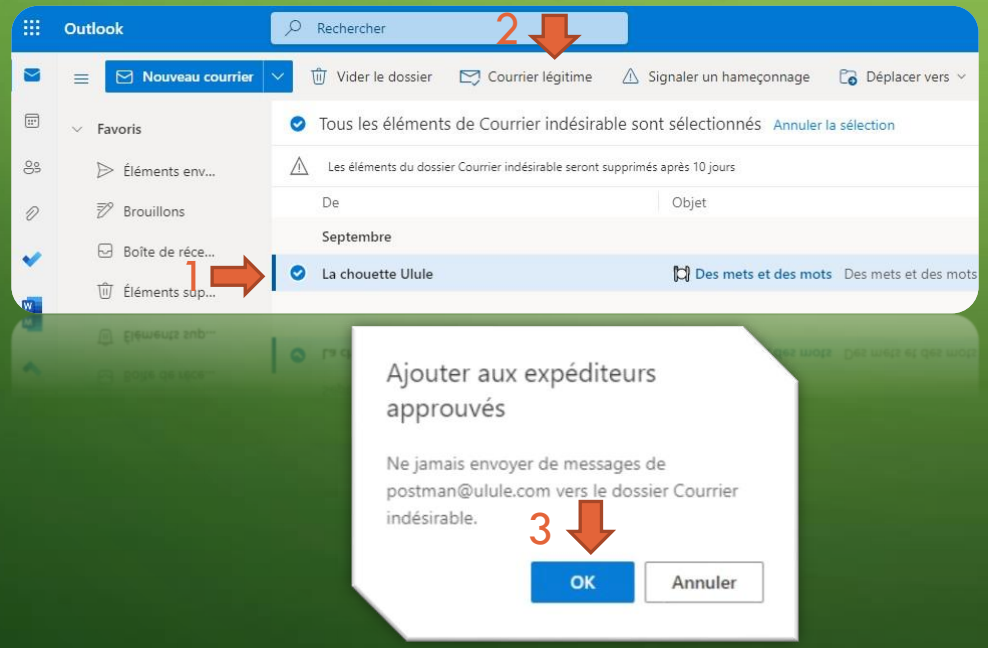
Il va donc analyser le message entrant et, en fonction de son contenu et/ou de son comportement, va le classer :

- Dans la boite de réception, s'il le considère comme étant « sain »
- Dans le dossier « courriers indésirables » s'il le considère comme « suspect ».

La technologie anti-spam n'est cependant pas infaillible. Il se peut que des spams réussissent à passer la barrière et se retrouve dans la « boite de réception » ou à l'inverse, que des mails parfaitement sains et utiles se retrouvent dans le dossier « courriers indésirables ». **Pensez donc à vérifier régulièrement ce dossier pour être sûr de ne pas passer à coté de mails importants !**

Si cela arrive, il va donc falloir que l'on dise à notre boite mail qu'elle a fait une erreur et qu'elle doit retransférer le mail sain dans la boite de réception.

Pour ce faire, nous allons faire l'inverse de la manipulation faite précédemment.



1- Dans le dossier « Courriers indésirables » ou « Spam », sélectionnez le mail que vous souhaitez retransférer.

2 - Cliquez sur le bouton :
« courrier légitime, non-spam
ou déplacer vers boite de réception ».

3 – Acceptez l'ajout de l'expéditeur
à la liste des « approuvés ».

Désormais, le message sera de nouveau considéré comme « sain » par votre boite mail et les prochains ne seront plus classés comme « courriers indésirables ».

PARTIE 2 : PETIT SPAM DEVIENDRA GRAND !

Dans la 1ère partie, nous avons vu ce qu'est un spam.

Maintenant, penchons nous sur les autres menaces liées aux courriers électroniques

Nous allons voir :

- Qu'est ce que le Scam ?
- Qu'est ce qu'un Phishing ?
- Qu'est ce qu'un Ransomware ?

Et, puisque les dangers ne se limitent pas qu'à internet, nous aborderons aussi :

- Les arnaques au téléphone mobile !
- Les coupons P. C. S.

LE SCAM

- **Le Scam, c'est quoi ?**

Le terme Scam ou est un terme générique qui désigne la fraude sur internet. Ici, on ne parle plus de petits spams publicitaires mais bel et bien d'arnaques **(le plus souvent bancaires pour s'enrichir à l'insu de l'utilisateur).**
À L'inverse du rançomware, que l'on abordera plus tard dans cette présentation et, qui lui, est une méthode de vol dite « brute », le Scam va quant à lui utiliser une méthode plus douce mais, tout aussi efficace si on ne sait pas déceler ses pièges à temps.

- **Il existe plusieurs type de scam :**
  Le 4.1.9, Loterie, offre d'emploi, crédit, voiture, sentimental etc etc … le principe est **TOUJOURS LE MEME**. Vous recevez un mail dans lequel on vous informe que vous avez gagné quelque chose et que, pour en bénéficier, vous allez devoir verser une certaine somme d'argent ou, à l'inverse, que vous en avez gagné. **Bien entendu, il ne faut jamais rien donner car vous n'obtiendrez jamais RIEN en retour et vous ne reverrez jamais l'argent qui vous a été versé !!!**

- **Comment reconnaitre le scam ?**

L'avantage du Scam, c'est qu'il est facile à reconnaitre.

- Il vous est envoyé par une personne TOTALEMENT INCONNUE.
- La police d'écriture est différente d'un mail normal.
- La civilité du mail est souvent fausse (Madame au lieu de Monsieur et inversement).
- Le corps du mail est souvent truffé de fautes d'orthographes.
- Une importante somme d'argent est presque toujours demandée ou promise.
- On vous annonce que vous avez participé à un concours et que vous avez gagné un gros lot sans même avoir participé.

Le plus dangereux des scams et sans doute le sentimental car il joue sur le coté affectif et solitaire de certaines personnes en détresse et il peut durer plusieurs MOIS. Attention donc aux relations numériques que vous nouez et SURTOUT, si la personne demande de l'argent pour venir vous rejoindre, ou en prétextant un quelconque ennui financier momentané, REFUSEZ ! **C'est souvent le signe d'une arnaque de haut vol mise en place par des fraudeurs d'autres pays et, une fois versé, l'argent est quasi IMPOSSIBLE à récupérer ! Soyez donc très prudent !**

LE PHISHING : NE MORDEZ PAS A L'HAMEÇON !

- **Le phishing, c'est quoi ?**

De l'anglais Phishing ou en français « hameçonnage », c'est l'action utilisée par le fraudeur ou hacker pour piéger l'utilisateur en se faisant passer pour un organisme connu afin que ce dernier, se sentant en confiance, donne ses coordonnées. On peut aisément le classer parmi les menaces les plus dangereuses parce qu'il repose sur le vol de données personnelles, (qu'elles soient bancaires, de sécurité sociale ou d'autres institutions publiques) dans le but de s'enrichir ou à des fins d'usurpation d'identité.

- **Comment cela fonctionne ?**

Le principe est simple. Le hacker essai de dupliquer, à l'identique ou quasiment la page de l'institution ou de l'entreprise dont il souhaite piéger les utilisateurs. A ceci prêt que, le formulaire qu'il va vous demander de remplir ne va pas renvoyer les informations vers la vraie entreprise mais, directement chez le fraudeur. Ensuite, il n'aura plus qu'à utiliser ces données, sur internet, à votre insu et, comme bon lui semble.

Mais alors, comment puis-je reconnaitre un Phishing ?

Bien qu'il s'avère extrêmement dangereux, il est tout de même relativement simple de reconnaitre un phishing. Partez toujours du principe qu'ABSOLUMENT JAMAIS, une institution bancaire ou administrative ne vous demandera vos identifiants NI MOT DE PASSE ou CODE SECRET QUE CE SOIT PAR MAIL OU PAR TELEPHONE !

- Lorsque vous effectuez un paiement ou que vous communiquez vos coordonnées personnelles sur un formulaire internet, vérifiez TOUJOURS que l'adresse du site commence par HTTPS : ainsi que la présence d'un petit cadenas en bas de page. Ces 2 signes vous assureront de la sécurité du site sur lequel vous inscrivez vos données.

Sachant cela, vous identifierez déjà 98 % des mails frauduleux. Quand vous êtes dans le doute, ne répondez JAMAIS et n'hésitez pas à contacter la dite institution. Elle vous dira de suite, si elle est à l'origine d'un quelconque mail vous étant destiné.

Si vous avez été victime d'un Phishing, faites une analyse complète de votre ordinateur avec un antivirus et anti-malware, CHANGEZ LE MOT DE PASSE DU COMPTE POTENTIELLEMENT COMPROMIS et bien entendu, contactez les autorités !

LE RANSOMWARE OU RANÇONGICIEL

- **Le ransomware, c'est quoi ?**

Dans l'échelle des escroqueries aux mails, là encore, le ransomware est certainement une des plus dangereuse infection !
Comme son nom l'indique, son but va être **de demander une rançon financière** à la personne ou l'institution ciblée.

- **Comment cela fonctionne ?**

Dans un premier temps, comme dans le cas d'un phishing, le hacker vous envoi un mail en l'apparence anodin.
Il va vous être demandé de cliquer sur un lien ou de télécharger un logiciel. Une fois l'action de votre part effectuée, un programme malveillant va totalement bloquer votre ordinateur.
Le hacker va vous promettre de vous restituer vos données car il vous enverra un code pour le débloquer **à la seule condition que vous lui versiez une rançon !**

Surtout, ne payez JAMAIS !

Bien qu'il soit tentant de payer car il va vous dire que vous récupérerez vos données aux plus vite, c'est ABSOLUMENT à PROSCRIRE ! Et ce, pour plusieurs raisons :

- Le vol de données sous couvert de rançon est un délit !

- Rien ne vous assure que vous retrouverez vos données après le paiement ni que la somme d'argent ne sera pas redemandée et / ou augmentée après le premier versement.

- **Que faire si je suis victime d'un ransomware ?**

Une fois encore, **référez en aux autorités compétentes !** Elles seules seront en mesure de vous guider dans la marche à suivre.

Si malgré tout vous avez payé, gardez toutes les preuves possibles, elle vous seront utiles pour les éventuelles procédures qui découleront de votre signalement.

LES ARNAQUES AU TÉLÉPHONE MOBILE

On l'oublie un peu souvent, mais … les arnaques ne se font pas QUE sur internet. Depuis quelques années, les arnaques au téléphones mobile sont de plus en plus nombreuses.

La plus courante réside dans le fait de recevoir un appel (généralement d'un numéro étranger) d'une personne qui, par le biais d'un message alarmant, vous demande de la rappeler.

Si vous le faite, une personne dit quelques mot, raccroche et vous vous apercevez ensuite que vous avez été débité de 1 ou plusieurs euros sur votre facture de téléphone. C'est ce que l'on appelle une arnaque par numéro surtaxé. Prenez donc garde à ne pas décrocher si le numéro vous est totalement inconnu ! Si une personne souhaite vraiment vous contacter, elle laissera un message.

Les SMS aussi sont porteurs d'arnaques. La plus récente étant celle qui vous incite à faire refaire votre carte vitale ou encore ceux qui vous annoncent que vous avez gagné tel ou tel lot ou que votre compte en banque ou Netflix sera clôturé sans action de votre part. Evidemment, c'est un mensonge !

Là encore, il existe des bons gestes pour ne pas se faire avoir :

33700 La plateforme de lutte contre les spams vocaux et sms

- Gardez en tête que, quand c'est trop beaux, c'est à 99,9 % FAUX !
- Ne répondez JAMAIS à un SMS inconnu !
- Ne cliquez sur AUCUN LIEN quel qu'il soit si vous n'êtes pas à 100 % sûr de sa provenance !
- Et surtout n'hésitez pas à transmettre tout SMS ou numéro de téléphone / SMS douteux aux autorités pour qu'elles puissent remonter la filière et faire cesser ces arnaques. Il existe un numéro dédié : le 33700

Mon petit : Si vous êtes harcelé par des appels / SMS incessants, vous avez la possibilité de les bloquer : Soit directement via la liste noire de votre téléphone mobile, soit en vous inscrivant sur la plateforme gouvernementale contre le démarchage abusif : BLOCTEL.

LES COUPONS P. C. S. !

- C'est quoi un coupon PCS ?

Dans l'univers du paiement digital, un nouveau venu a fait son apparition. Le coupon P. C. S. (Prepaid Cash Service Card) ou en français, le service de carte Prépayée.

- Comment ça fonctionne ?

Le processus est simple. Une personne qui a besoin d'argent, va par exemple vous demander 50 €.

Vous vous rendez chez votre buraliste à qui vous faites le paiement. En retour, il vous imprime un ticket muni d'un code et c'est, ce dit code, que vous donnerez au destinataire. Il lui suffira ensuite d'utiliser ce code par internet ou par sms pour recharger sa carte pour récupérer le montant associé au ticket.

- Pourquoi l'arnaque au coupon PCS se multiplie ?

De part sa grande facilité d'obtention et surtout le fait que ce soit intraçable, le coupon PCS est de plus en plus prisé par les fraudeurs.
On dit que les plafonds peuvent être de 500 € / Jour (dans la limite de 1000 € / mois mais si vous validez avec une carte d'identité et votre adresse auprès de l'organisme bancaire, les plafonds peuvent être considérablement augmentés. Dans la limite de 10 000 € ! On comprend donc pourquoi de plus en plus d'arnaqueurs se tournent vers ce nouveau gain d'agent « facile ».

- Quelles sont les arnaques concernées par les coupon PCS ?

Les arnaques les plus courantes qui utilisent le coupon PCS sont bien évidemment les arnaques aux sentiments mais elles ne sont pas les seules. Elles peuvent aussi concerner :

- Les pseudos promesses d'embauches.
- Les achats d'animaux.
- De voitures et/ou de produits Hi-Tech
- Les arnaques à la location...

Une fois le code en poche et le paiement effectué, il est malheureusement impossible de remonter jusqu'à celui qui vous a escroqué ! Ces arnaques étant la plupart du temps montées dans d'autres pays, les autorités auront beaucoup de mal à pouvoir vous aider. Soyez donc vigilants !

En France, il existe de multiples moyens de paiement légaux et traçables donc, si on vous demande un paiement par coupon PCS sur internet, à 99,9 % c'est une arnaque donc là encore REFUSEZ et ne donnez pas suite !

Exemple de


IMPORTANT
IL N EXISTE AUCUN SITE DE VERIFICATION DE COUPON PCS. SI ON VOUS PROPOSE DE VERIFIER VOTRE COUPON, NE LE FAITES SURTOUT PAS !

NOTRE SERVICE CLIENT EST JOIGNABLE SEULEMENT ET UNIQUEMENT AU : 0811 880 200. N UTILISEZ AUCUN AUTRE NUMERO POUR NOUS CONTACTER.

Credit:250.00Eur

1- Rechargez par SMS
Envoyez RECH suivi du code secret:
F8AC29501A
(espace) et les 4 derniers chiffres de votre carte.
EX: RECH A123456789 1234
Numero SMS:
Carte PCS Black:
PCS Infinity :
PCS Chrome :
2-Rechargez sur internet
Espace mon compte
www.pcsmastercard.com

Date de Validite: 16/09/20
No Serie:000018512774

Coupon P. C. S.

PARTIE 3 : LES MAILS FRAUDULEUX A TRAVERS 6 EXEMPLES !

Dans cette 3eme et dernière partie, nous allons mettre en pratique tout ce que nous avons vu dans ce cours, afin que vous puissiez déceler les arnaques d'un premier coup d'œil.

Pour ce faire, voici les faux mails et SMS les plus typiques que vous pourrez être amené à rencontrer. A savoir :

- Un faux scam classique.
- L'arnaque mail à l'assurance maladie.
- 2 faux mails de banque et une fausse facture.
- 2 faux mails de gain à la loterie.
- Les faux SMS.
- L'arnaque à la P. J. , gendarmerie et Interpol.

Le tout accompagné de commentaires explicatifs pour que ce soit plus compréhensible. C'est parti ! ☺

©Sources : Divers sites internet gouvernementaux luttant contre les spams et le phishing.

Toutes les images et captures présentes dans cette présentation sont utilisées dans un but purement pédagogique.

Elles sont gratuites et libres de droits.

EXEMPLE 1: LE SCAM TYPIQUE

Voici un exemple typique de faux mail. Plusieurs choses doivent nous alerter ici :
On nous prévient qu'on va gagner de l'argent, le corps du texte contient des fautes et sa mise en texte hasardeuse.
On nous demande de cliquer sur un lien et 100 % des gens gagnent et tout est gratuit !

Objet : Prêteurs en lice – Vous gagnez

Réduisez vos paiements de prêt immobilier

Les taux d'intérêt grimpentt !
Offrez A Votre Famille La Liberté Financière Qu'elle Mérite

Refinancez Aujourd'hui et ECONOMISEZ
*Rapide et FACILE
*CONFIDENTIEL
*Top 100 des prêteurs
*100 % GRATUIT

FAUX

Inscrivez-vous aujourd'hui ! {LIEN}

Toutes les cartes de crédit sont acceptées

Pour retirer votre nom de notre base de données, veuillez cliquer sur {LIEN} ou utiliser l'un des moyens expliqués ci-dessous.

En vous remerciant.

Appelez le 1-800-279-7310
Ou envoyez un courrier à l'adresse suivante :
1700 E. Elliot Rd. STE3-C4
Tempe, AZ. 85283

EXEMPLE 2 : LE MAIL D'ARNAQUE A L'ASSURANCE MALADIE

Les choses qui doivent nous alerter ici :

- Nom d'expéditeur totalement inconnu et provenance également.
- L'objet nous parle de la sécurité du compte alors que le corps nous informe d'un remboursement.
- Un montant de remboursement nous est communiqué avant même la connexion à notre espace client.

De : E-service Clients BRED <BRED_secureID9593.noreply@zwina.com>
Envoyé : Thursday, October 29, 2020 9:51:42 AM
À : prenom.nom@courriel.fr
Objet : Au sujet de la sécurité de votre compte! #Re-664366

Mail de phishing avec une adresse mail suspecte et un objet de mail alarmiste

Message du 20/10/21 02:10
De : "Group Service" <pimkies@dfyoxc.owler.com>
A :
Copie à :
Objet : Asurance Maladie | Ameli.Fr

FAUX

SÉCURITÉ SOCIALE
l'Assurance Maladie

Bonjour

Votre caisse d'assurance maladie vous informe que vos remboursements de frais à recevoir

Nous vous demandons de mettre à jour vos données pour que votre remboursement soit effectué dans les plus délais.

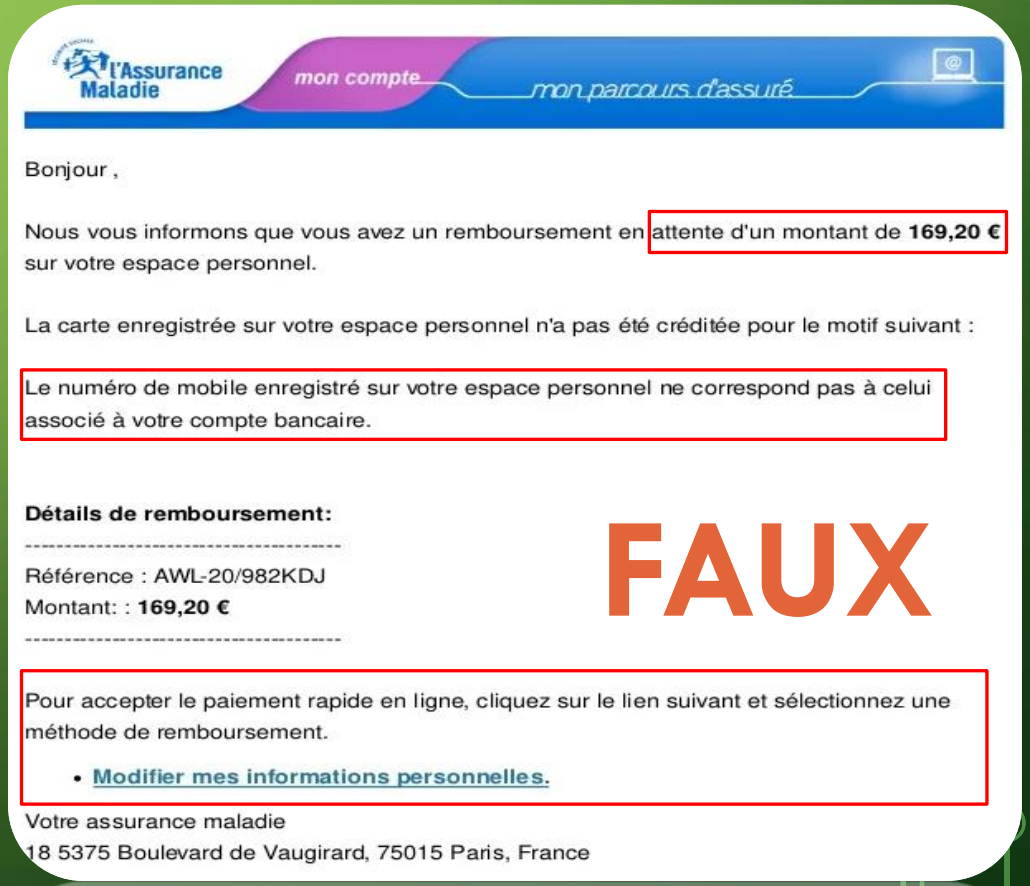
Montant: 249.98 Euro

Référence: Ameli-A8005W

https://www.assure.ameli.fr

Nous vous remercions et nous vours prions agréer nos salutations distingués.

Dans ce second exemple fort bien réalisé, on nous demande de modifier nos informations personnelles pour pouvoir bénéficier d'un remboursement de soins.
Evidemment c'est totalement faux et ce, même si le mail comporte une pseudo « référence » et une « adresse ».
Si vous devez être amené à modifier vos coordonnées, c'est UNIQUEMENT par le biais de votre compte Ameli sécurisé et certainement pas par mail !



l'Assurance Maladie — mon compte — mon parcours d'assuré

Bonjour ,

Nous vous informons que vous avez un remboursement en attente d'un montant de **169,20 €** sur votre espace personnel.

La carte enregistrée sur votre espace personnel n'a pas été créditée pour le motif suivant :

Le numéro de mobile enregistré sur votre espace personnel ne correspond pas à celui associé à votre compte bancaire.

Détails de remboursement:

Référence : AWL-20/982KDJ
Montant: : **169,20 €**

FAUX

Pour accepter le paiement rapide en ligne, cliquez sur le lien suivant et sélectionnez une méthode de remboursement.

- Modifier mes informations personnelles.

Votre assurance maladie
18 5375 Boulevard de Vaugirard, 75015 Paris, France

EXEMPLE 3 : LES FAUX MAILS DE BANQUE ET FAUSSES FACTURES

Dans cet exemple, le faux message est flagrant ! Bien que cette fois encore, la ressemblance est à première vue parfaite, si on a l'œil, on repère de suite la supercherie.

- L'objet « SOCGEN@FRANCE.FR qui semble plus être une adresse mail est incohérente !
- La banque ne vous invitera jamais à consulter ses messages en cliquant sur un lien mais vous demandera de le faire directement sur votre profil client sécurisé !

Exemple d'un mail frauduleux aux couleurs de la Société Générale.

Dans ce mail qui usurpe l'identité d'ING on vous annonce que votre compte a été désactivé et comme d'habitude, on vous demande de cliquer sur un faux lien !
Les banques n'utilisent JAMAIS ce procédé ! contactez immédiatement votre conseillé et transmettez lui le mail frauduleux.

Exemple d'un mail frauduleux aux couleurs d'ING.

En ce qui concerne la fausse facture, ici là encore, tout est faux !
Pour autant, cette arnaque au mail reste cependant très simple à détecter.
Normalement, vous savez si vous avez récemment acheté une télévision à 999 € dans l'enseigne en question ou pas. Donc, si vous n'avez jamais effectué cet achat, c'est que c'est forcément une arnaque.

Dans TOUS LES CAS, N'HESITEZ PAS à transférer SYSTEMATIQUEMENT le mail au service anti fraude du site marchand concerné ! Il se chargera de signaler l'escroquerie aux autorités pour remonter l'origine du phishing et faire cesser ces pratiques.

EXEMPLE 4 : LE PSEUDO GAIN À LA LOTERIE

Dans ces 2 exemples de faux mails à la loterie estampillés « Française des Jeux », plusieurs choses doivent vous alerter :

- La présence d'un coupon réponse, le montant astronomique du gain !
- Les faux textes, logos et signatures qui, le plus souvent pris sur le net constituent une usurpation d'identité
- Et surtout le fait qu'on dise que votre adresse mail a été tirée au sort et que vous devez écrire à un notaire pour recevoir vos gain !

Capture 1 : Message frauduleux aux couleurs du groupe la Française des jeux

Capture 2 : Message frauduleux aux couleurs du jeu EuroMillions – MyMillion

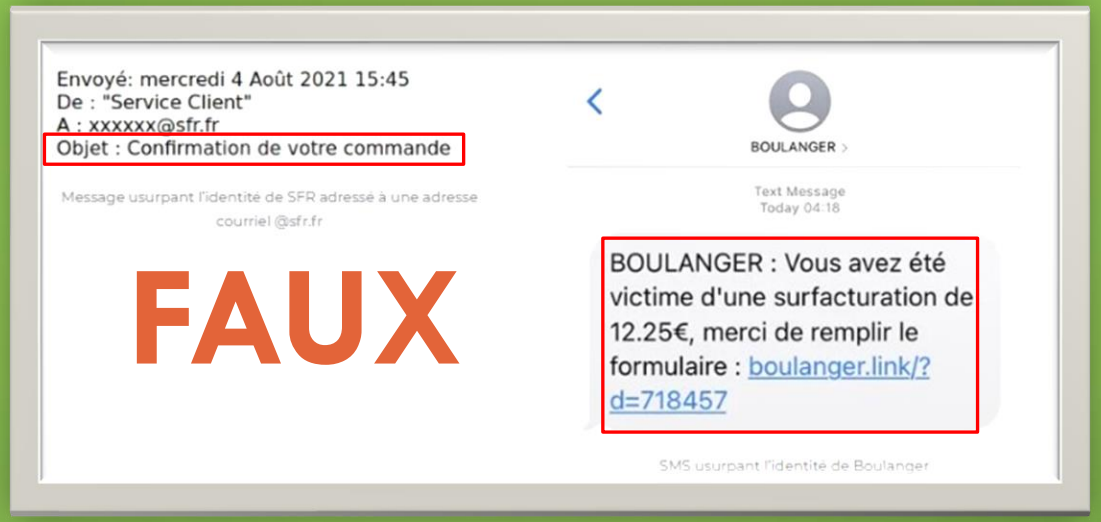
Capture 4 : Faux ticket gagnant aux couleurs du jeu de loterie EuroMillions – MyMillion

Mauvaise mise en forme et gain délirant !

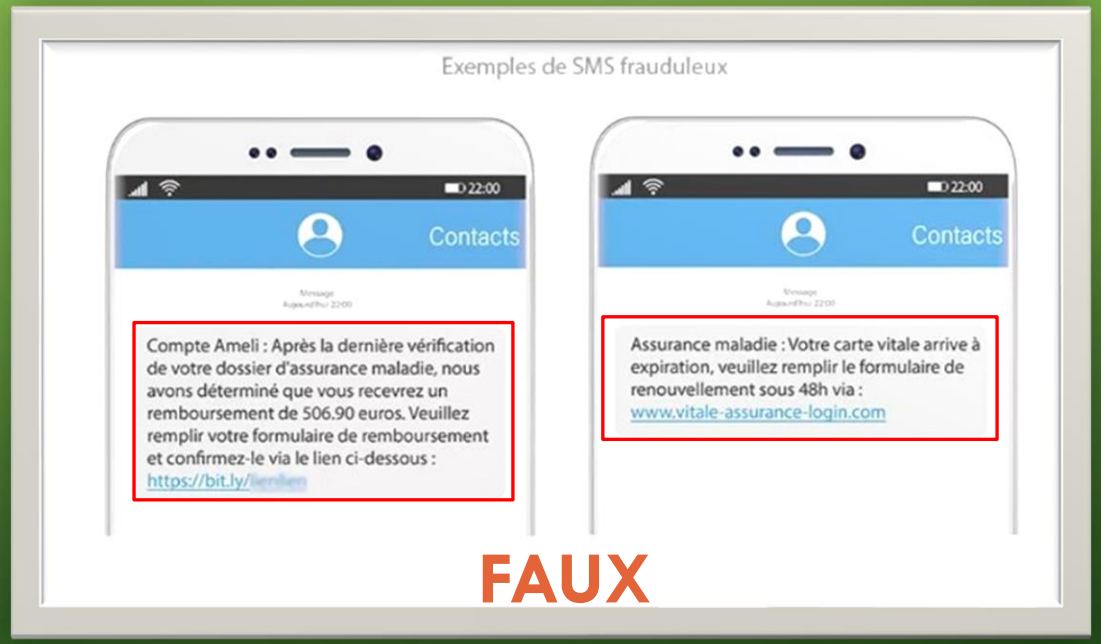
La Française des jeux ne demandera JAMAIS que l'on la contacte par mail ou SMS pour effectuer une remise de gain ! Si vous avez joué et potentiellement gagné, rapprochez vous de votre buraliste chez qui vous avez validé votre ticket ou rendez vous sur FDJ.FR pour plus de renseignements liés à votre compte en ligne ou encore dans un centre officiel de la « Française des Jeux » !

EXEMPLE 5 : LES FAUX SMS

Voici un faux SMS qui se prétend venir de boulanger et qui usurpe également l'identité de SFR !
Là encore, promesse de remboursement contre remplissage de formulaire via un lien totalement hasardeux.



Et ici, encore un au nom d'Ameli qui utilise le même procédé qui consiste à cliquer sur des liens contre promesse de remboursement ou pour refaire votre carte vitale. Encore une fois, TOUT EST FAUX !



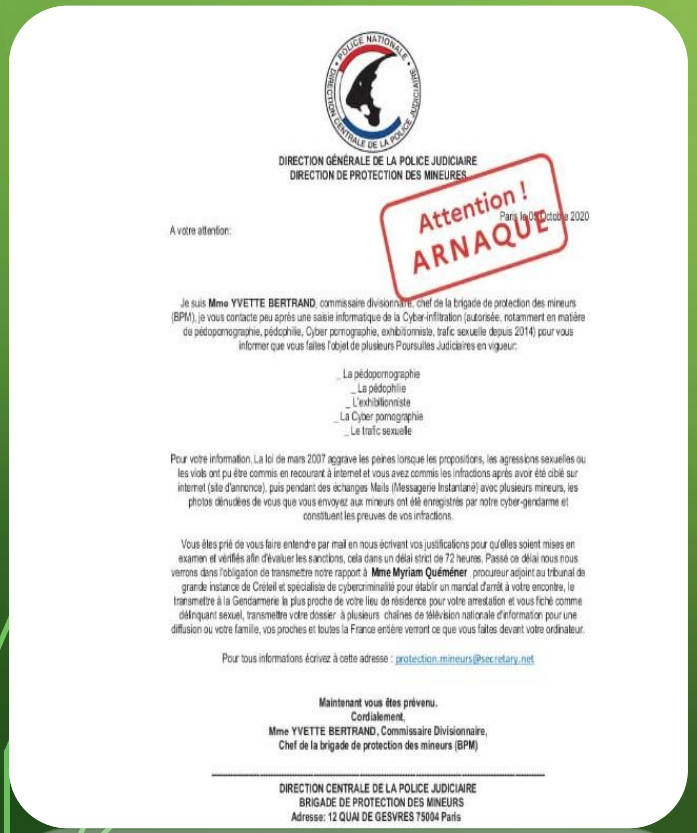
Les enseignes de magasins et les services publics n'utiliseront JAMAIS les mails et/ou SMS pour vous redonner de l'argent ou refaire vos papiers !

Ce sont toujours de FAUX LIENS, qui renvoient vers de fausses adresses mails ou de faux sites internet qui volent vos coordonnées personnelles une fois le faux formulaire rempli !

EXEMPLE 6 : L'ARNAQUE AU NOM DE LA P.J. GENDARMERIE OU INTERPOL !

On termine par la dernière arnaque internet en vogue actuellement mais qui tourne déjà depuis près de 2 ans, le mail alarmiste qui se prétend venir de la Police Judiciaire, de la Gendarmerie Nationale ou même d'Interpol.

Non content de détourner les logos, l'adresse des services des forces de l'ordre et d'usurper l'identité de personnes connues mais plus en activité, ce mail pousse le processus un peu plus loin que les autres puisqu'ici, le but est de vous faire PEUR afin que vous donniez vos coordonnées personnelles et ainsi, pouvoir vous les voler !
Evidemment ce mail est totalement faux ! La police ou la gendarmerie ne vous contactera jamais par mail quel que soit ce qui vous est reproché !
Si vraiment elle devait vous entendre, elle se déplacera chez vous ou vous serez convoqué. Donc ne tombez pas dans le piège. Ne répondez PAS, NE CLIQUEZ PAS SUR LE LIEN ! et … comme les autres, signalez le mail aux autorités !



DIRECTION GÉNÉRALE DE LA POLICE JUDICIAIRE
DIRECTION DE PROTECTION DES MINEURES

Attention ! ARNAQUE

Paris le 02 Octobre 2020

A votre attention:

Je suis **Mme YVETTE BERTRAND**, commissaire divisionnaire, chef de la brigade de protection des mineurs (BPM), je vous contacte peu après une saisie informatique de la Cyber-infiltration (autorisée, notamment en matière de pédopornographie, pédophilie, Cyber pornographie, exhibitionniste, trafic sexuelle depuis 2014) pour vous informer que vous faites l'objet de plusieurs Poursuites Judiciaires en vigueur:

_ La pédopornographie
_ La pédophilie
_ L'exhibitionniste
_ La Cyber pornographie
_ Le trafic sexuelle

Pour votre information, La loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet (site d'annonce), puis pendant des échanges Mails (Messagerie Instantané) avec plusieurs mineurs, les photos dénudées de vous que vous envoyez aux mineurs ont été enregistrés par notre cyber-gendarme et constituent les preuves de vos infractions.

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions, cela dans un délai strict de 72 heures. Passé ce délai nous nous verrons dans l'obligation de transmettre notre rapport à **Mme Myriam Quémêner**, procureur adjoint au tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, le transmettre à la Gendarmerie la plus proche de votre lieu de résidence pour votre arrestation et vous fiché comme délinquant sexuel, transmettre votre dossier à plusieurs chaînes de télévision nationale d'information pour une diffusion ou votre famille, vos proches et toutes la France entière verront ce que vous faites devant votre ordinateur.

Pour tous informations écrivez à cette adresse : protection.mineurs@secretary.net

Maintenant vous êtes prévenu.
Cordialement,
Mme YVETTE BERTRAND, Commissaire Divisionnaire,
Chef de la brigade de protection des mineurs (BPM)

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS
Adresse: 12 QUAI DE GESVRES 75004 Paris

Gendarmerie nationale

DIRECTION GÉNÉRALE DE LA GENDARMERIE

Je suis Mr Christian RODRIGUEZ, directeur général de la gendarmerie nationale. Je vous contacte peu après une saisie informatique de cyber-infiltration (Autorisée, notamment en matière de pédopornographie, Site Pornographique, Cyber pornographie, pour vous informer que vous faites l'objet de plusieurs poursuites judiciaires en vigueur :

* LA PÉDOPORNOGRAPHIE
* SITE PORNOGRAPHIQUE
* CYBER PORNOGRAPHIE
* DÉTOURNEMENT DE MINEURS

FAUX

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications afin qu'elles soient mises en examen et vérifiées de sorte à évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport

À Mme Mélanie BRIARD, substitute du procureur de la République près le tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, et vous serez fiché comme délinquant sexuel. Votre dossier sera également transmis aux médias pour une diffusion où votre famille, vos proches et toute l'Europe entière verront ce que vous faites devant votre ordinateur.

Maintenant vous êtes avertis.

Cordialement,

Directeur général de la gendarmerie nationale.

DIRECTION CENTRALE DE LA GENDARMERIE
BRIGADE DE PROTECTION DES MINEURS
Adresse : 4 rue Claude-Bernard 92130 Issy-les-Moulineaux

Message frauduleux usurpant l'identité de la Gendarmerie Nationale

INTERPOL

CONVOCATION POUR NECESSITE D'UNE ENQUÊTE JUDICIAIRE

DECEMBRE, 2021

ARNAQUE !

ARNAQUE !

ARNAQUE !

ARNAQUE !

LE RÔLE DE L'ANTIVIRUS DES ANTI MALWARES ET DES ANTIPUBS

Beaucoup de gens pensent qu'un antivirus, c'est inutile. Le plus souvent parce que c'est cher mais aussi et surtout, parce qu'ils estiment qu'à la vue de l'utilisation qu'ils font de leur PC, investir dedans, est une dépense superflue. C'EST UNE ERREUR !

La première des choses à comprendre c'est que, lorsque vous connectez votre PC à internet, il devient une porte d'entrée sur le MONDE ENTIER avec ses avantages, mais aussi ses inconvenants.

Aujourd'hui, internet ne nous sert plus seulement à consulter des pages ou écouter de la musique. Nous faisons TOUT avec !

Faire nos courses, consulter nos comptes bancaires, nos dossiers médicaux … etc etc … autant de choses qui font qu'il s'est rendu indispensable mais qu'il a aussi collecté de plus en plus nos données personnelles, chose qui a, du même fait, réveiller l'intérêt de personnes malveillantes qui ont vu en sa sur-utilisation une nouvelle source de profit facile et rapide !

Voilà pourquoi est important d'être bien protéger lorsqu'on surfe sur internet. Assurez vous d'avoir :

- Un antivirus A JOUR (ça vous évitera pas mal de virus, notamment si vous télécharger beaucoup de fichiers. Tous les fabricants de solutions anti-virales du marché offrent des solutions tout en 1 très efficaces).

c'est LA BASE DE LA PROTECTION ! Après, il existe d'autres logiciels complémentaires qui viennent renforcer la sécurité.

- Un anti malware qui lui, surveillera votre trafic internet en arrière plan, vous préviendra des sites frauduleux et bloquera les attaques entrantes avant qu'elle ne vous atteignent.

- Un antipub, qui lui vous bloquera toutes les publicités intempestives non désirées et qui accélérera grandement votre vitesse de navigation.

Des solutions gratuites de très bonne qualité existent. Cependant, si vous le pouvez, préférez un abonnement annuel.

Pour autant, posséder toutes ces protections ne signifie pas qu'internet deviendra 100 % sans danger ! La vigilance reste la règle n°1 !

LES BONS CONSEILS POUR ÉVITER LES ARNAQUES AUX MAILS / SMS :

Tout ce que nous venons d'aborder, peut faire peur. Pourtant, il existe des moyens simples et rapides d'identifier une arnaque aux mails, SMS et de s'en prémunir.
Avant toute chose, dites vous que le 1er rempart contre la fraude, **c'est vous** ! Si vous êtes bien informé sur internet et ses dangers, que vous savez les repérer et les identifier, aucune raison de vous faire arnaquer. Nous allons cependant récapituler quelques principes de base :

- Avant de surfer sur internet, **veillez à toujours avoir votre PC ou votre téléphone à JOUR**. Les pirates se servent des failles de sécurité pour entrer dans les systèmes d'exploitation obsolètes !
- **Ne surfez pas sur internet sans antivirus et là encore, tenez le à jour !** Un antivirus périmé, c'est comme si vous n'en aviez pas ! **ANALYSEZ TOUTE PIECE JOINTE téléchargée !**
- Si vous faites des achats sur internet, **vérifiez que le site marchand à pignon sur rue ! Que l'adresse du site débute par HTTPS et vérifiez la présence du cadenas en bas de page.**
- **Préférez le code virtuel à achat unique à celui de votre carte bancaire !** C'est gratuit et ça évite les arnaques au vol de numéros de carte. (Sur demande auprès de votre banque).

Lorsque vous recevez des mails et/ou sms dont vous n'êtes pas sûr :

Autant que possible, NE L'OUVREZ PAS ! Si vous l'avez fait par inadvertance, vérifiez les noms, objets, orthographe et le phrasé du mail / SMS reçu.

- Ne cliquez sur AUCUN LIEN qui vous semble douteux ! (cela pourrait vous rediriger vers un site frauduleux ou vous installer des logiciels espions et vous voler vos données !).

- S'il est question **d'ARGENT, NE JAMAIS EN ENVOYER ! Si on vous demande un paiement en coupon P. C. S. REFUSEZ !**

N'oubliez pas non plus que :

- LES GAINS DE JEUX NE SONT JAMAIS TRANSMIS PAR MAIL OU PAR SMS !
- L'administration française NE VOUS DEMANDERA JAMAIS DE LUI COMMUNIQUER VOS COORDONNEES BANCAIRES ou MOT DE PASSE, ni de REFAIRE VOS PAPIERS par mail, téléphone fixe ou SMS ! Si vous devez le faire, prenez TOUJOURS CONTACT AVEC LE SERVICE PUBLIC OFFICIEL de votre propre initiative.

- Si vous rencontrez quelqu'un sur internet, **PRENEZ VOTRE TEMPS ! Renseignez vous BIEN sur votre interlocuteur avant d'entreprendre quoi que ce soit !**
- Si on vous demande de l'argent, REFUSEZ ! **À tous les coups, c'est une arnaque !!!**

En enfin : Faites attention à ce que vous postez sur les réseaux sociaux ! Moins vous en dites sur votre vie privée, moins vous serez tracé !

Mon petit ✚ : Afin de renforcer la sécurité de vos comptes et éviter une éventuelle usurpation d'identité, quand c'est possible, activer l'authentification à 2 facteurs. En cas de changement de mot de passe, une demande d'autorisation sera envoyée sur votre téléphone portable, ce qui compliquera fortement la tâche du fraudeur s'il essai prendre possession à distance d'un compte vous appartenant. SURTOUT, N'UTILISEZ JAMAIS UN MEME MOT DE PASSE POUR PLUSIEURS SITES !

Et si malgré tout ces conseils, vous avez tout de même été victime d'une arnaque sur internet, autant que possible, **gardez les preuves !**
N'hésitez pas à faire des captures d'écran et contactez les autorités compétentes.

Liens utiles :

Si vous ou un de vos proches êtes victime de cyber malveillance :

La plateforme de signalement PHAROS : www.internet-signalement.gouv.fr ou https://www.cybermalveillance.gouv.fr/

- Pour signaler tout SMS ou appel frauduleux : le 33700 - Ainsi que https://www.bloctel.gouv.fr/ contre le démarchage téléphonique abusif. (fixe et Mobile).

CONSEILLER NUMÉRIQUE France services

CONSEILLER NUMÉRIQUE France services

FRANCE RELANCE

EDDY QUEMET & *ANNIE BOURTHOUMIEU*

Votre Conseillère numérique France services

vous remercient pour votre attention.

CCAS

Val'Aïgo Communauté de communes

BESSIÈRES