Les arnaques
Questions / Réponses

Présentation du problème

Vous recevez régulièrement des messages dans votre messagerie qui peuvent être :

- Sérieux
- Des spams publicitaires
- Des arnaques

On peut aussi recevoir des arnaques sur son Smartphone.

Nous allons voir dans ce document les différents types d'arnaques que vous pouvez recevoir.

Voir le sommaire page suivante.

Sommaire

1 Les différents types d'arnaques

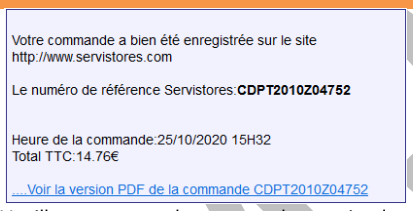
1.1 Faux message

Vérifiez systématiquement les pièces jointes à vos emails. Une pièce jointe de type EXE ou Dll est évidement très dangereuse. Il peut en être de même depuis un fichier Docc ou Pps qui peut cacher des macros en langage Basic.

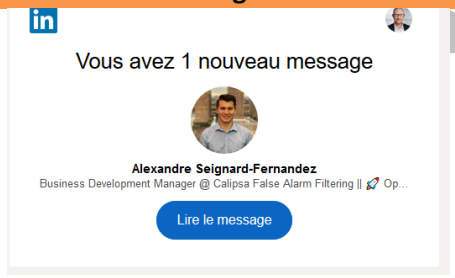
1.1.1 Ampoules gratuites et faux message CA

1.Vous pensez recevoir 5 ampoules gratuites mais immédiatement après un clique de souris sur ce message, vous avez des fenêtres d'alerte, si vous êtes bien protégé. Ces sites sont dangereux et ils se multiplient.

2.Une commande jamais passée → Un clique de souris → Alarme immédiate

ATTENTION DANGER	Fausse commande	Une partie du texte
	 Veuillez noter que la commande est simplement enregistrée. Elle ne sera traitée par Servistores qu'après réception/validation du paiement. Si vous n'effectuez pas le paiement ou si ce dernier est refusé, la commande sera ignorée	.Une fois votre paiement effectué, vous recevrez un second mail, pour vous informer de la bonne réception de votre paiement par Servistores. Attention, pour éviter d'être considéré comme du spam, ce mail ne sera envoyé qu'après un délai de 15 minutes, à compter à partir de la réception du paiement. Bla bla bla à suivre avec liens dangereux
Ci-joint un fuax message re_u évidement un Dimanche matin afin que le CA ne soit pas joignable. **La ccéder à mon espacemène évidement à un faux sire du crédir agricoke, parfairtement immité.** **ON ?E REJOINT JAMAIS UNE BANQUE DEPUIS UN LIEN SUR UN MESSAGE.** **En cas de doute, appelez votre banque par téléphone.**		J'ai reçu, un message d'un vendeur que je ne connaissais pas, proposant une Webcam à un bon prix. Lorsque je me suis connecté, de nombreuses fenêtres se sont ouvertes avec un bruit alarmant. J'au éteint le Pc sans fermer Windows. J'ai subi ce genre de choses une fois par semaine en fécrier. Avat c'était une fois pas an…

1.1.2 Faux message Linkdin

Faux message Linkdin		
	Il faut très vite éteindre. Si le problème n'est pas résolu au redémarrage. 1. Fermez au plus vite les fenêtres avec ALT F4. 2. Lancez votre antivirus en mode total.	3. Lancez RogueKiller en scan total et supprimez les malwares trouvés Lancez Malware bytes. Supprimer esl malwares si besoin est. Redémarrez. En principe plus de problème. Une heure de perdue.

1.2 Arnaques en ligne

1.2.1 Black Friday : attention aux arnaques en ligne !

https://www.service-public.fr/particuliers/actualites/A15326

1.3 Arnaque deopuis son Smartphone

Question

Je reçois un appel téléphonique de ma banque (c'est bien son numéro qui s'affiche), me précuisant que mon compte ou ma carte bleue a été piratée. On vous proposera par exemple de changer de carte bleue?

Réponse

Pas de panique. C'est une arnaque. Sachez donc qu'il existe des logiciels permettant de falsifier le numéro appelant sur votre Smartphone, pour vous faire croire qu'il s'agit d'une société précise, de la gendarmerie, d'une banque ou autres…Les pirates ont de l'imagination et du savoir faire.

Comment réagir aux propositions ?

Si cela se passe pendant le week-end l'arnaque est presque certaine.

Si c'est une banque, par exemple, n'acceptez rien d'autre qu'un rendez-vous. Demandez quel est le nom du conseiller. Au mieux déplacez-vous à la banque pour mettre les choses au clair et au pire, rappelez la banque par téléphone et demandez à être mis en relation avec votre conseillé habituel.

En résumé

Même si le bon numéro s'affiche sur votre Smartphone, ne rien traiter pouvant engager une sécurité quelconque, surtout pendant un week-end. Demandez le nom de la personne appelante et choisissez de prendre rendez-vou.s

1.4 Arnaque à la carte bancaire

Question

Ma carte bancaire a été piratée. Je constate des dépenses vers des personnes que je ne connais pas ?

Réponse

Dés lors que vous constatez des dépenses anormales, faites opposition à votre carte, soit par téléphone, soit sur le site Internet de la banque ou en vous déplaçant. Changez immédiatement de carte bleue avec un nouveau numéro et un nouveau code à 4 chiffres.

Avant que cela ne vous arrive :

Regardez la procédure à appliquer pour faire opposition à votre carte bancaire. Notez cette procédure pour pouvoir agir vite, si besoin est.

Refusez toujours de laisser votre numéro de carte bancaire sur les sites d'achat. Il est important de refuser que votre numéro de carte reste pour des achats futurs, ce que proposent des sites comme Amazon.

1.5 Usurpation d'identité

Question

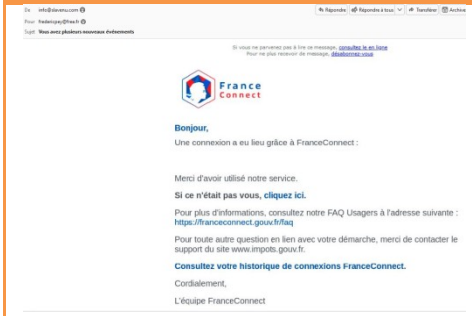
Que faire en cas d'usurpation d'identité ?

Réponse

Voici la réponse de la CNIL :

https://www.cnil.fr/comment-reagir-face-une-usurpation-didentite

1.6 Arnaque sur FranceConnect

Le texte de l'arnaque	Comment reconnaître ce faux ?	Que faire ?
	1. L'adresse du receveur (destinataire) n'est pas la vôtre 2. L'adresse de l'expéditeur n'est pas France Connect 3. Le lien est toujours le même et il couvre tout le fichier email. C'est donc une image et non un texte.	1. Ne pas répondre. 2. Copier le lien dans un traitement de texte. 3. Signaler ce lien, si possible en copiant le fichier source de l'email. 4. Pour cela installer l'extension SignalSpam dans Thunderbird.

1.7 Usurpation de RIB -

1.7.1 Le principe

Ce type d'arnaque peut se produire lorsque votre compte email ou celui d'un artisan est piraté et pisté.

1. Vous avez fait faire des travaux à un artisan.
2. Pour payer ces travaux vous recevez le Rib de l'artisan par email.
3. Les pirates changent le Rib, pour un compte temporaire crée par eux.
4. Votre paiement sera versé sur ce faux compte.
5. Trop tard pour réagir, la banque ne remboursera pas car vous êtes responsable du virement.

En résumé

On ne communique jamais le RIB par email. Si c'est le vas, vérifiez oralement en contactant l'artisan (ou la personne par téléphone).

1.8 Nouveau type d'arnaque : Le QR Code

Ne jamais photographier un QR Code sans se poser de question sur sa sécurité.

Que Choisir vous met en garde et vous signale les QR Codes à éviter :

https://www.quechoisir.org/actualite-arnaque-mefiez-vous-des-qr-codes-n113198/?at_medium=email&at_emailtype=retention&at_campaign=nlh20231115

1.9 SMS ou message faux colis

Question

Les SMS annonçant un faux colis sont-ils dangereux ?

Réponse

OUI si vous vos connectez sur le lien qu'il contient ou sur le numéro de téléphone proposé . VOUS DEVEZ SUPPRIMER CES SMS SANS RIEN FAIRE D'AUTRE.

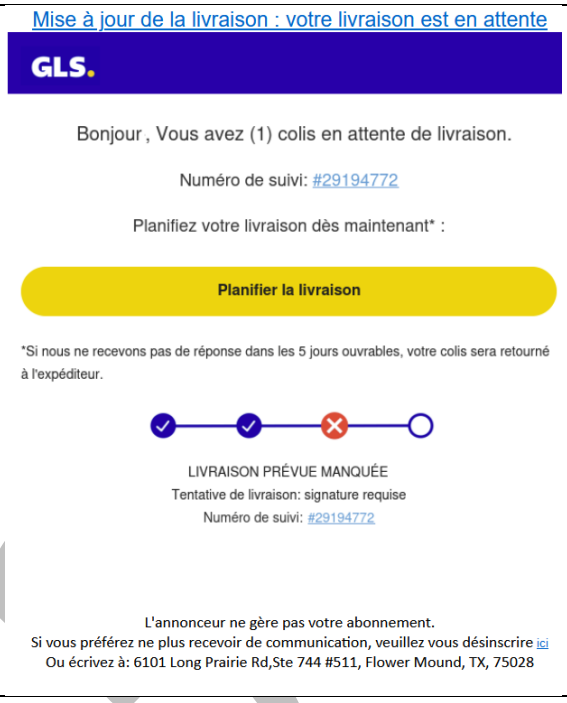
Voici une analyse de Que Choisir à ce sujet :

https://www.quechoisir.org/actualite-arnaque-au-colis-ce-sms-cache-un-redoutable-virus-qui-copie-votre-application-bancaire-n90690/?utm_medium=email&utm_source=nlh&utm_campaign=nlh210428&at_medium=email&at_emailtype=retention&at_campaign=nlh210428

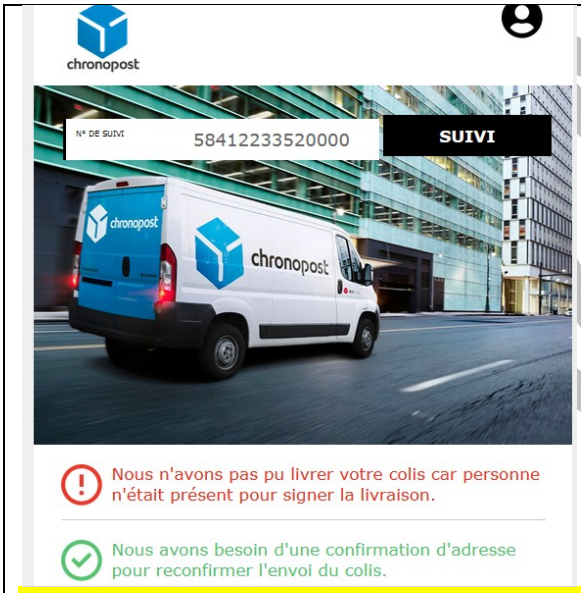
Exemple :

Encore une arnaque :
Comment les repérer :
1°) Lire l'adresse de l'expéditeur.
2°) Réception avec destinataires cachés, car vous n'êtes pas le seul à recevoir cet e-mail.
3°) Le lien est douteux (je l'ai uniquement copié dans un traitement de texte. Pas question de l'ouvrir.
4°) Le lien est sur tout le message et non pas uniquement sur les boutons. Il ne s'agit donc pas d'un texte, mais de l'image d'un texte
Toujours vérifier ces critères en as de doute

Ce que dit le site gouvernemental sur les arnaques :
Voilà les conseils donnés par le site gouvernemental.
https://www.economie.gouv.fr/entreprises/comment-lutter-contre-spams



Lisez cet article qui met en garde et propose des solutions



Ce message est une arnaque

Avis de Norton :

AVERTISSEMENT

1.9.1.1 Evaluation Norton

L'évaluation Norton est réalisée par le système d'analyse automatique de NortonLifeLock. En savoir plus.

1.9.1.2 Rapport de menace

Il s'agit d'une page web dangereuse connue. Il est fortement recommandé de ne **PAS** visiter cette page.

Cliquez ici pour envoyer une contestation

1.9.1.3 Consultez un site. Nous l'évaluons.

1.10 Main mise sur votre PC

1.11 Usurpation carte d'identité

Question

Quelle est la durée de validité de ma carte d'identité ?

Réponse

Si votre carte d'identité est assez récente, la durée de validité est affichée au dos. Dans le cas contraire consultez ce document du service public :

https://www.service-public.fr/particuliers/vosdroits/F35005

1.12 Usurpation carte vitale

Voici un message de l'assurance maladie que je vous transmets :

ATTENTION AUX MESSAGES FRAUDULEUX **es tentatives de fraude à distance se multiplient** et les méthodes employées par les fraudeurs sont de plus en plus élaborées. L'Assurance Maladie **vous met en garde** contre les appels, courriels et SMS frauduleux. Ces tentatives d'hameçonnage (phishing) augmentent, notamment sur la commande de carte Vitale. **Soyez vigilants face à ce risque !** Le discours employé par le fraudeur est souvent très réaliste. Il cherchera à vous mettre en confiance et insistera sur le caractère urgent de sa démarche.	**QUELQUES REGLES CONCERNANT LA CARTE VITALE** Elle est gratuite. En cas de **perte, vol ou dysfonctionnement**, vous devez effectuer une déclaration dans votre compte ameli. Sa commande ou son renouvellement s'effectue sur votre compte ameli ou sur l'application compte ameli. **Important :** L'Assurance Maladie **ne vous demandera jamais** la transmission par mail ou SMS de vos coordonnées bancaires complètes **ni** de vos informations personnelles. **Bon à savoir** : Retrouvez tous nos conseils et exemples pour reconnaitre les appels, emails et SMS frauduleux en cliquant ici. Si vous recevez un SMS frauduleux, signalez-le sur le site **33700.fr** ou en envoyant un **SMS au 33 700**. Ce service d'alerte fera bloquer l'émetteur du message. Cordialement, Votre correspondant de l'Assurance Maladie

MORALITE : ON NE SE CONNERCTE JAMAIS A UN LIEN RECU PAR E-MAIL

1.12.1 Autre arnaque

Arnaque carte vitale	Attention	A faire absolument
	Les mots « nouvelle carte vitale répétés 3 fois. Le site proposé est dangereux. Ne pas se connecter	Téléchargez l'application Site Advisor de McAfee. Installez cette application sur vos navigateurs. Vous serez prévenu des arnaques en allant sur le site.

1.13 Les adresses e-mail dangereuses

Ne répondez jamais aux adresses de ce type

Copier le lien (bouton droit), sans jamais l'ouvrir. Il sera facile de constater que c'est un faux, en le plaçant simplement dans un traitement de texte, par un copier/Coller.

Si possible, faites un signalement sur les sites suivants :

https://www.signal-spam.fr/

https://www.signal-arnaques.com/scam/add

https://www.internet-signalement.gouv.fr/PharosS1/

1.14 Arnaque à l'assurance maladie

Attention vous recevez uun message comme celui-ci-dessous, vous demandant de vous connecter à votre compte.

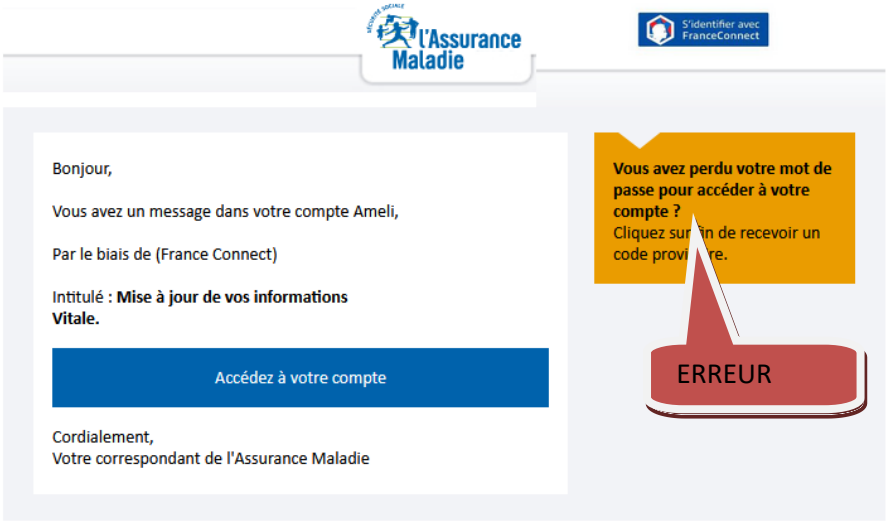
Il vous propose de vérifier vos coordonnée (Nom, prénom,, e-mail et mot de passe)

En remplissant cette soit disant vérification vous ouvrez la porte à l'arnaque.

Voius devez toujours :

1. Vérifier l'adresse de l'expéditeur.
2. Vérifier le lien proposé sur les deux sites suivants :

Norton / https://safeweb.norton.com/ et Virustotal : https://www.virustotal.com/gui/home/upload



ATTENTION

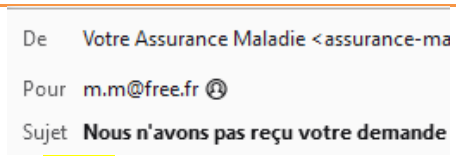
VirusTotal ou Norton

Peuvent vous dire que les sites ne sont pas dangereux.

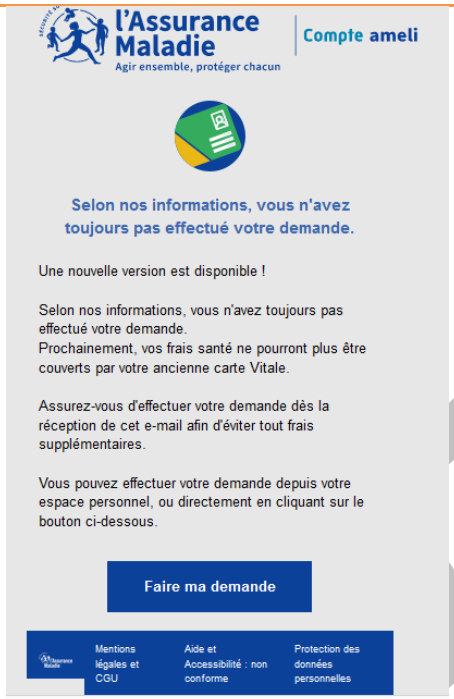
Le lien en effet peut ne pas être dangereux, mais les informations, que vous, vous allez laisser, peuvent être piratées, si le site est un faux.

Connectez-vous toujours depuis vos favoris ou vos marque-pages, pour être certain d'être sur le bon site.

Comment voir l'arnaque ?



Le POUR n'est pas pour vous personnellement.
L'adresse m.m@free.fr est une fausse adresse générique, très souvent utilisée dans les arnaques.
Le document ci-joint semble réel. Si vous regardez le lien qui se trouve sous le bouton, nous ne sommes pas da,s ameli.fr.
Pour voir le lien, du bouton droit de la souris, cliquez sur Copier le lien. Puis collez ce lien dans un traitement de texte, sans l'ouvrir.
https://r.wolueas.fr/?id=GICHNYBHSQ ← Faux lien



1.15 Arnaque au permis de conduire

Vous avez des copies de permis de conduire ou de carte d'identité :

Sur votre PC cryptez ces images à l'aide de Glary Utilities par exemple . En effet un « rogue » installé à votre insu sur votre PC, peut pirater ces fichiers . Pour éviter cela, passez régulièrement,t votre antivirus, malwarebytes er Rogue-Killer surtout si vois êtes allé sur des sites inconnus quel-qu'il soient.

Si vous vois faites vler ces documents sur papiier, bous devez immédaitement vous rendre) la police ou à la gendarmerie pour faire une déclaration de vol ou de perte. C'est indispensable pour les incidents en justice qui peuvent en découdre.

1.16 Arnaque à la plaque d'immatriculation de votre véhicule

Cette article vient d'un site, certainement celui qui est signalé à la fin de l'article.

1.16.1 Immatriculation "doublettes", comment réagir ?

« Doublettes » (P.V. reçus à cause de quelqu'un qui utilise frauduleusement Une plaque minéralogique identique à la vôtre).

La solution pour éviter les ennuis :

Vous êtes victime de « Doublettes » - Surtout ne prenez pas à la légère le «PV ». Cela peut vous mettre dans des situations catastrophiques. Réagissez très vite! En suivant la procédure indiquée ci-dessous.

Je cite le site indiqué ci-dessous

1.16.2 1ère étape :

Réunir toutes les preuves justifiant qu'il n'était pas possible que vous soyez sur les lieux au moment de l'infraction. (Travail, achats, Rendez-vous.)

Si vous avez été flashé, rien de plus simple, demandez le cliché. L'adresse

Du service photographies est indiquée au dos de la contravention.

1.16.3 2ème étape :

Une fois toutes les preuves réunies ; Allez déposer plainte à la Gendarmerie la plus proche pour « Usurpation de plaques d'immatriculation » Code NATINF 25123. Demandez un récépissé et une copie de la plainte.

1.16.4 3ème étape

Passez à votre Préfecture avec la copie de la plainte et demandez une nouvelle immatriculation. C'est impératif sinon, vous serez toujours embêté.

1.16.5 4ème étape :

Remplissez correctement la requête en exonération, joignez copie du récépissé de la plainte, copie de tous les justificatifs et envoyez le tout en recommandé avec accusé de réception à l'Officier du Ministère Public dont L'adresse figure sur la contravention. Logiquement, vous n'aurez plus de problème.

Cette procédure est l'œuvre de l'ANDEVI, association de défenses des victimes de P. V. établis de façon injuste. Voici l'adresse de leur blog :

http://www.andevi.info/article-doublettes-l-andevi-vous-donne-la-solution-84127238.html

Contacts : A.N.D.E.V.I : 02.51.63.57.74 ou 06.69.53.01.08

www.andevi.info

Email: andevi@sfr.fr

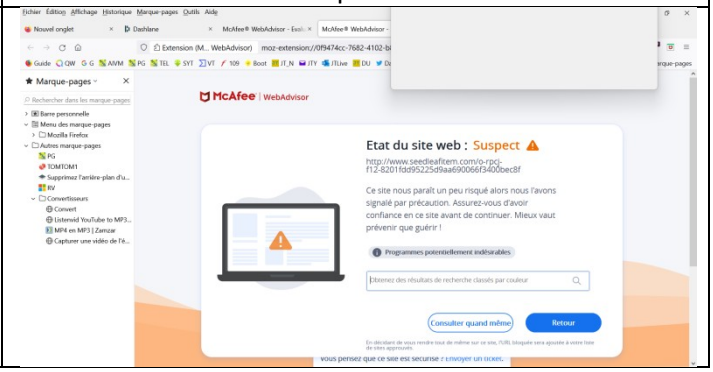
1.17 Arnaque à la carte bancaire

https://www.quechoisir.org/actualite-fraudes-a-la-carte-bancaire-en-hausse-mais-pas-mieux-remboursees-n93040/?utm_medium=email&utm_source=nlh&utm_campaign=nlh210713&at_medium=email&at_emailtype=retention&at_campaign=nlh210713

1.18 Arnaque au compteur Linky

https://www.quechoisir.org/actualite-compteur-linky-arnaque-a-la-mise-a-jour-n92976/?utm_medium=email&utm_source=nlh&utm_campaign=nlh210713&at_medium=email&at_emailtype=retention&at_campaign=nlh210713

1.19 Arnaque Amazon

La fausse PUB Amazon	McAfee Web Advisor vous prévient.
On vous offre un cadeau. Vous avez été choisi … une photo avec un beau sapin de Noël	

1.20 WhatsApp : des méthodes douteuses

https://www.quechoisir.org/billet-du-president-whatsapp-une-alerte-europeenne-lancee-n93104/?utm_medium=email&utm_source=nlh&utm_campaign=nlh210713&at_medium=email&at_emailtype=retention&at_campaign=nlh210713

Question

Que dit le fondateur de Telegram ?

Réponse

« Restez loin de WhatsApp » pour éviter de voir votre téléphone être piraté », prévient le fondateur de Telegram.

A lire cet article :

https://mobiles.developpez.com/actu/337428/-Restez-loin-de-WhatsApp-pour-eviter-de-voir-votre-telephone-etre-pirate-previent-le-fondateur-de-Telegram-qui-estime-que-WhatsApp-est-un-outil-de-surveillance-depuis-13-ans/

1.21 Arnaque au bitcoin

DOSSIER SPECIAL: Le dernier investissement de Xavier Niel **Xavier Niel** viens avec un nouvel investissement secret qui permet de rendre des centaines de personnes riches en France. La semaine dernière, il est apparu sur Quotidien et a annoncé une nouvelle "échappatoire richesse" qui, selon lui, peut transformer qui ce soit en millionnaire dans 3-4 mois. Niel pousse chacun en France à profiter de cette opportunité incroyable avant que les grandes banques ne la ferment définitivement. **ENCORE PLUS** Et bien sûr, quelques minutes après la fin de l'interview, BNP Paribas a appelé pour stopper la diffusion de l'interview de Niel- il était déjà trop tard. Yann Barthès **LeMonde.fr**	***Le journal le Monde n'a rien à voir avec cette arnaque que j'ai reçue 3 fois sur des adresses différentes.***

2 Les menaces

2.1 Arnaque et menace sur mon PC

Votre PC est menacé de tomber en panne.

Trés forte musique inquiétante et un numéro de téléphone d'appel en urgence.

2.1.1 Comment réagir efficacement ?

Question

Tout d'un coup, une musique très inquiétante retentie et un numéro de téléphone s'affiche. Je dois immédiatement appeler ce numéro pour régler le problème. Dans le cas contraire je risque le blocage de mon PC ?

Réponse

Quel est le problème	Que faire immédiatement ?	Ensuite…
Une rançon vous sera demandée pour réparer votre PC. **Votre adresse IP vient d'être attaquée, vous devez réagir très vite, mais certainement pas en appelant le n° de téléphone proposé.** **Vous devez éteindre en force votre PC. Sur un fixe, couper le courant. Sur un portable appuyez longuement sur le bouton Marche/Arrêt.** **Il ne faut pas que Windows se referme normalement**	En coupant le courant sans que Windows se referme proprement en enregistrant sa session. Vous avez pu éviter que le malware s'installe. Il ne faut pas attendre et pas essayer de répondre au numéro de téléphone du pirate qui vous agresse. Vous devez réagir de cette façon immédiatement.	1. Eteignez votre box et attendez une minute. 2. Rallumez la box, elle se réinitialisée et le pirate et son malware auront disparu. 3. Rallumez votre PC normalement. ***En principe, tout va bien si vous n'avez pas trop attendu pour réagir.***

Plus votre réaction a été immédiate et moins vous risquez de voir votre PC bloqué. Si c'est le cas Windows devra peut-être réinitialisé. Au pire certains de vos documents seront cryptés.

Par prudence : Tous vos documents importants doivent absolument être sauvegardés sur un disque externe ou sur des clés USB. La double-sauvegarde est indispensable.

2.2 Arnaque OneDrive

Question

Je reçois une menace de fermeture du OneDrive associé à mon compte outook.com.

Réponse

Ne répondez pas, car le but est de connaitre votre mot de passe.

2.1 Menaces et accusations

Question

Je reçois des menaces (ou accuusation), m'accusant de pédophilie. Que faire ?

Réponse

Rien. Des milliers de personnes reçoivent ce type d'ignominie chaque semaine.

Surtout ne jamais répondre à ces accusations ou menaces. Surtout ne payez jamais les rançons pour, soit disant, vous oublier. Vous ne risquez rien en supprimant purement et simplement ce type de message. La seule chose utile à faire, est de copier le fichier source de ce message et de communiquer ce fichier source à un site comme signal-spam → https://www.signal-spam.fr/

Depuis Thunderbird c'est très facile. Il suffit de faire menu Autres → Afficher la source, puis du bouton droit Cliquez sur « Tout sélectionner ». Et enfin du bouton droit « Copier ». Il vous suffit de recoller (bouton droit Coller) ce fichier source dans l'espace correspondant du site Signal-spam.

2.2 Message de la gendarmerie ou ministère de la justice (accusation)

Souvent en pièce jointe !

2.2.1 Exemple de message

DIRECTION GÉNÉRALE DE LA GENDARMERIE

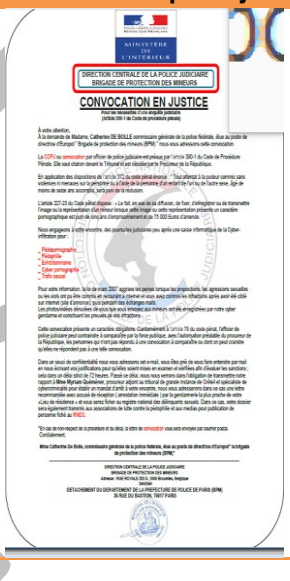
Après une saisie informatique de cyber-infiltration dans votre serveur, vous faites l'objet de
Plusieurs poursuites judiciaires en vigueur notamment en matière :
** PÉDOPORNOGRAPHIE*
** SITE PORNOGRAPHIQUE*
** CYBER PORNOGRAPHIE*
Pour votre information, La loi n° 125 de mars 2007 aggrave les peines lorsque les propositions, les
Agressions sexuelles ou les viols ont pu être commis en recours à l'internet et vous aviez bel et bien
Commis des infractions à usage pornographie envers mineur sur des sites privés.
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 auprès du tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre égard, le transmettre à la gendarmerie la plus proche de votre lieu de résidence pour votre arrestation à comparaître et vous serez fiché comme délinquant sexuel.
En attente de votre justificatif pour l'ouverture du PV (Procès-Verbal).
Maintenant vous êtes avertis.
Mr Christian RODRIGUEZ Directeur général de la gendarmerie nationale. DIRECTION CENTRALE DE LA GENDARMERIE BRIGADE DE PROTECTION

2.2.2 Les erreurs commises dans ce message

1. Envoyé à « undisclosed recipients » ce qui prouve que vous n'êtes pas seul à le recevoir.
2. Les menaces présentes dans le texte.

3. L'envoi depuis une adresse outlook.com : brigademineursprotection@outlook.com ce qui n'a pas de sens. Les gendarmeries n'utilisent pas d'adresse sur outlook.com.
4. Une faute d'orthographe, ce qui n'est plus un critère décisif.
5. Ecriture centrée ce qui n'a pas de sens dans un courrier administratif.

En copiant le fichier source de cet email, vous pouvez détecter l'adresse IP de l'envoi de l'expédition. L'expéditeur a pu cependant se cacher derrière un VPN. Cela peut être utile si vous souhaitez vous-même porter plainte contre ce type de message.

Le message reçu	La pièce jointe
• **Nous vous prions de prendre connaissance de votre Convocation en pièce jointe et nous recontacter dans les plus brefs délais, faute de quoi, nous nous verrons dans l'obligation de procéder à votre interpellation …** • ***(B.P.M)*** • ***Gendarmerie Nationale***	

2.3 Menaces de mort

Question

Vous recevez un e-mail avec menace de mort, si vous ne versez pas une certaine somme d'argent. Que faire ??

Réponse

Pas de panique. Ne pas se laisser impressionner. « Que choisir » vous informe et vous répond. Voici le lien :
https://www.quechoisir.org/actualite-arnaque-et-maintenant-le-faux-tueur-a-gages-n110334/?at_medium=email&at_emailtype=retention&at_campaign=nlh20230906

3 Arnaques aux banques

3.1 Les précautions à prendre

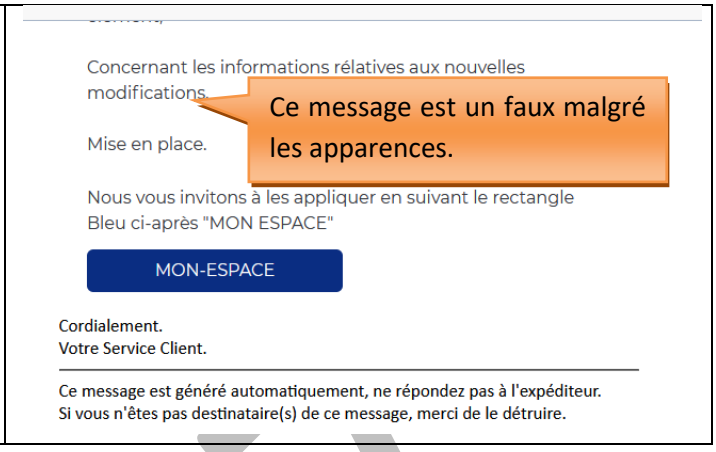
Les précautions à prendre. Comment se protéger. Les recours
Voici le document sur le site gouvernemental :
https://www.economie.gouv.fr/particuliers/protection-usurpation-identite?xtor=ES-39-[BI_342_20231114]-20231114-[https://www.economie.gouv.fr/particuliers/protection-usurpation-identite]#

3.2 Banque Postale

Arnaque 1

Voici un message qui semble anodin..
Le bouton bleu même sur un site d'aspect identique à celui de la banque postale, mais ce site est un faux, une imitation parfaite.

1. On ne se connecte jamais depuis un lien d'un e-mail
2. En cas de doute, on vérifie les liens du bouton droit avec un copier / coller dans un traitement de texte, afin de voir et vérifier le lien en question.
3. On ne se connecte à sa banque que depuis ces favoris ou marque-pages.



Autre arnaque

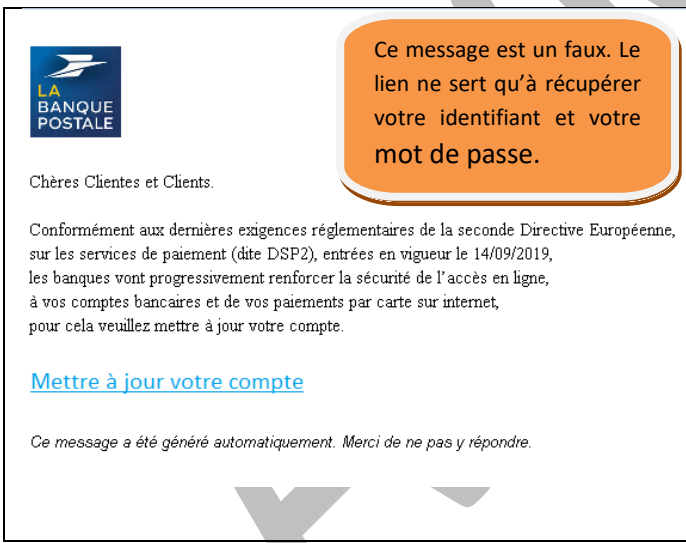
Les arnaques « Au colis sont incessantes aussi bien sous Windows que sur les Smartphone. Ne répondez jamais, ne vous connectez pas si vous n'avez aucun colis en attente.

Méfiez-vous aussi des documents qui, soit disant, vous attendent dans les e-documents de votre banque. Il faut accéder à votre banque, uniquement par le lien URL que vous avez stocké vous-même, dans vos favoris ou marque-pages. Ne vous connectez jamais depuis un lien venant d'un email.

Pour tester un lien, ouvrez un traitement de texte. Faites un clic droit sur le lien, puis « Copier le lien », recollez ce lien dans un traitement de texte sans l'ouvrir, il sera alors bien lisible et sans connexion il est sans danger.

Cela permet de vérifier son authenticité.

Arnaque 1



Arnaque 2. Googhle vous pirate vos photos et veut vous les revendre sous forme d'album !

Arnaque 3

Arnaque 3	Arnauqe	A véifier et faire,
#Cher(e) #client(e), Ce e-mail fait l'objet d'une recommandation indispensable concernant la sécurisation de vos opérations et de vos données personnelles. Veuillez vous connecter en cliquant sur **MA BANQUE** et suivez les	Ce type d'arnaque est très courant sur toutes les banques, J'ia reçu un message encore beaucoup plus crédible sur la sécurisation des comptes du Crédit Agricole,,Ces messahes ne proviennent pas de votre banques,	1. Vérifier l'adresse de l'expéditeur (elle ne correspond pas à la banque). 2. Vérifiez si vous êtes le seul destinataire. Là aussi, dans le cas contraire c'est un faux 3. Dans tous les cas : On n'utilise jamais un lien provenant d'un e-mail, 4 . **Le message vous arrive sur une**

différentes étapes "**activer le CertCode**" Ayez s'il vous plait votre téléphone mobile et votre boite de réception e-mail à votre portée avant d'entamer la procédure. *En ignorant cet avis vous vous exposez à une interdiction temporaire de toutes vos opérations de débit.* Nous vous remercions de votre confiance... Message sécurisé **La Banque Postale** tous droits réservés		**autre adresse que celle que vvous avez laissé à la ba,que** Remarque : vous pouvez vérifier le lien de la façon suivante : Cliquez bouton droit sur le lien → Copier le lien.. Ouvrez le Wordpad ou le bloc-notes. Coller le lien sans l'ouvrir. Il apparaît alors dans sa réalité. Si ce n'est pas le lien classique sur votre banque c'est un faux, pour essayer de copier votre identifiant et votre mot de passe, En aucun cas vpous ne devez ouverir ce lien

Banque__Assurances.

Dans le cadre de la directive européenne relative aux services de paiement 2 (DSP2)1, le niveau de sécurité de l'accès à votre **Espace client banque postale** et de vos opérations de paiement en ligne a été renforcé.

Prochainement, la confirmation de votre identité ne sera plus possible avec le code reçu par SMS.

Vous pouvez bien évidemment gérer vos comptes depuis votre mobile ou votre tablette, en cliquant sur **:https://www.labanquepostale.fr : PARAMÈTRES** et suivre les instructions

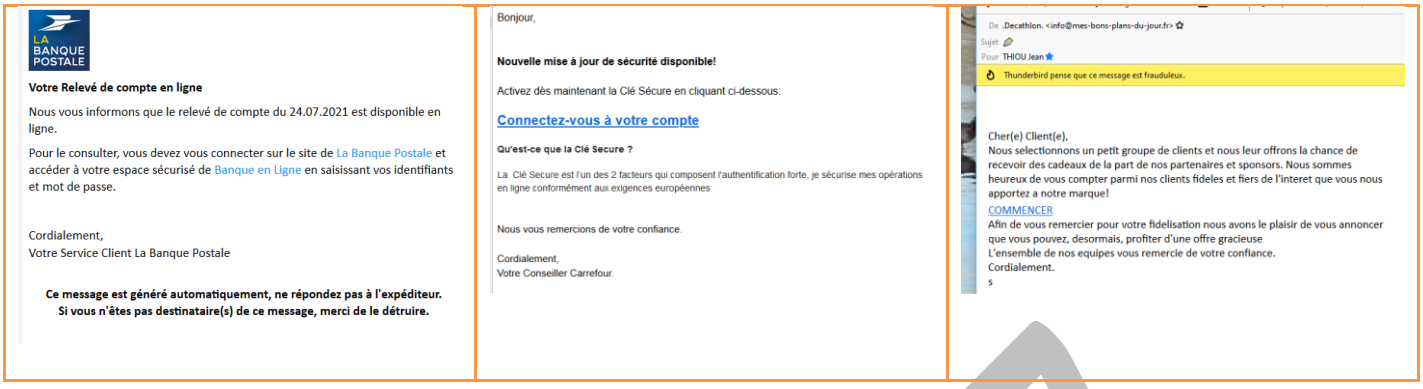
Vous devrez obligatoirement vous authentifier avec la fonctionnalité de Certicode plus une solution simple et rapide, vous permet de réaliser des opérations bancaires plus facilement et sans délai d'attente.

PS : En ignorant cet avis vous vous exposez à une interdiction temporaire de toutes vos opérations de débit.

Très Cordialement
La Banque Postale

Arnaque 4

Un faux de la banque postale	Arnaque Carrefour	Anaque Decathlon



LA BANQUE POSTALE

Votre Relevé de compte en ligne

Nous vous informons que le relevé de compte du 24.07.2021 est disponible en ligne.

Pour le consulter, vous devez vous connecter sur le site de La Banque Postale et accéder à votre espace sécurisé de Banque en Ligne en saisissant vos identifiants et mot de passe.

Cordialement,
Votre Service Client La Banque Postale

Ce message est généré automatiquement, ne répondez pas à l'expéditeur.
Si vous n'êtes pas destinataire(s) de ce message, merci de le détruire.

Bonjour,

Nouvelle mise à jour de sécurité disponible!

Activez dès maintenant la Clé Sécure en cliquant ci-dessous:

Connectez-vous à votre compte

Qu'est-ce que la Clé Secure ?

La Clé Secure est l'un des 2 facteurs qui composent l'authentification forte, je sécurise mes opérations en ligne conformément aux exigences européennes.

Nous vous remercions de votre confiance.

Cordialement,
Votre Conseiller Carrefour.

De :Decathlon. <info@mes-bons-plans-du-jour.fr>
Sujet
Pour THIOU Jean
Thunderbird pense que ce message est frauduleux.

Cher(e) Client(e),
Nous selectionnons un petit groupe de clients et nous leur offrons la chance de recevoir des cadeaux de la part de nos partenaires et sponsors. Nous sommes heureux de vous compter parmi nos clients fideles et fiers de l'interet que vous nous apportez a notre marque!
COMMENCER
Afin de vous remercier pour votre fidelisation nous avons le plaisir de vous annoncer que vous pouvez, desormais, profiter d'une offre gracieuse
L'ensemble de nos equipes vous remercie de votre confiance.
Cordialement.
s

Arnaque 5

LA BANQUE POSTALE

Chères Clientes et Clients.

Conformément aux dernières exigences réglementaires de la seconde Directive Eu sur les services de paiement (dite DSP2), entrées en vigueur le 14/09/2019, les banques vont progressivement renforcer la sécurité de l'accès en ligne, à vos comptes bancaires et de vos paiements par carte sur internet, pour cela veuillez mettre à jour votre compte.

Mettre à jour votre compte

Attention :

Ne faites jamais confiance à ce genre de texte.
On n'ouvre jamais un lien depuis un email.
On va sur le site et l'on recherche directement les liens.

3.3 Arnaque au Crédit Lyonnais

N'activez JAMAIS les liens qui vous sont proposés. Consultez vos banques deuis vos propres liesn que vous avez pu placer dans les marque-page ou les favoris.

3.3.1 Nouvelle carte ou remboursement frauduleux

https://www.service-public.fr/particuliers/actualites/A15364?xtor=EPR-100

3.3.2 Deux autres fraudes

Cher (e) Client(e),
Le 23/12/2021, vous avez reçu un nouveau prélèvement instantané d'un montant de 867,06 euros en provenance de E-Market Online sous la référence 07458458599758100217399 89.
Nous vous invitons a bien vouloir prendre connaissance de ce message qui es si important. Grace à votre identifiant LCL muni de votre mot de passe.
Pour consulter votre solde et le détail des opérations, rendez-vous dans votre Espace Client :
Se Connecter

Depuis votre application LCL, vous pouvez également accéder à ce service en vous rendant dans votre "Accueil".

LCL vous remercie de votre confiance.

LCL BANQUE ET ASSURANCE

Chère Cliente, Cher Client,

Merci de nous aider à rendre vos opérations bancaires encore plus sécurisées.

Votre conseiller vous invite à activer gratuitement votre nouveau service d'uthentification forte **«LCL- Appareil de Confiance»** pour sécuriser vos transactions bancaires.

Cliquez sur le lien sécurisé ci-dessous pour commencer le processus d'installation:

https://lcl.fr/monespace/appareildeconfiance/activation

Nous vous remercions de votre confiance.
LCL - Banque et assurance
Ce message a été généré automatiquement. Merci de ne pas y répondre.

3.4 Arnaque au Crédit Agricole :

Toute une banque pour vous

Bonjour

Vous avez un urgent message de votre conseiller régionale CA a lire au plus vite.

Merci d'en prendre connaissance en accédant tout simplement au document "en fichier joins". .

Merci,

Votre conseiller

3.5 Arnaque à la caisse d'épargne

CEPAC CAISSE EPARGNE
Une obligation qui s'applique a tous les clients

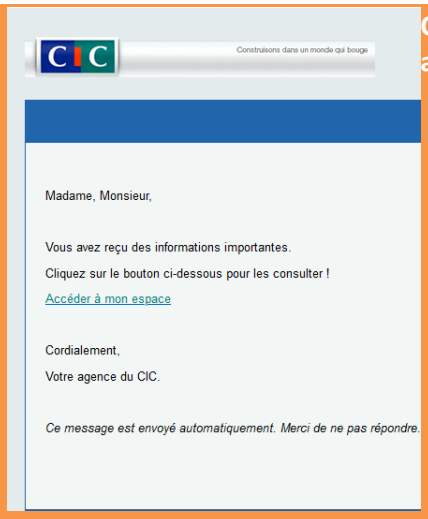
Vous avez une (1) notification disponible,

Nouveau mécanisme sur notre plateforme, l'ancien sera obsolète d'ici quelques jours.
Activez dès maintenant le service de (Sécurité forte) en vous rendant sur le lien ci-dessous

J'Active mon nouveau Secur'Pass

Siège social : 1 place de la Gare 75001 Paris. 437 642 531 RCS Paris. Société coopérative à capital variable. Établissement de crédit. Société de courtage d'assurances. Immatriculée à l'ORIAS sous le 07 008 967
Afin de contribuer au respect de l'environnement, merci de n'imprimer ce mail qu'en cas de nécessité.

3.6 Arnaque au CIC



Ce qui est nouceau dans c ette arnaque.

1. **Le lien n'est pas sur l'image, mais c'est un vrai lien sur une phrase, comme le ferrez une banque.**
2. **En bas du message, toutes les précisions habituelles données par les banques, (non lisible sur cette image jointe)**

1. **Afficher le source du message –on yrouve cette rubrique dna s le meuinui de Thiunderbird**
2. **A partir du source → Bouton droit sélectionnez tout.**
3. **Bouton droit → Copier**
4. **Ouvrir Signals-pam.com et se connecter.**
5. **Collez le fichier source**
6. **Le signalement est terminé**

3.7 Arnaque à la Société Générale

3.7.1 Faux problème de réglementation

SOCIETE GENERALE

Cher(e) Client(e)

Afin de respecter la réglementation mise en œuvre et destinée à sécuriser davantage vos opérations en ligne,
Nous mettons en place un moyen plus simple
Appelé **S.E.C.U.R-I.P.A.S.S**. Vous pouvez l'activer dès maintenant via le lien ci-dessous :

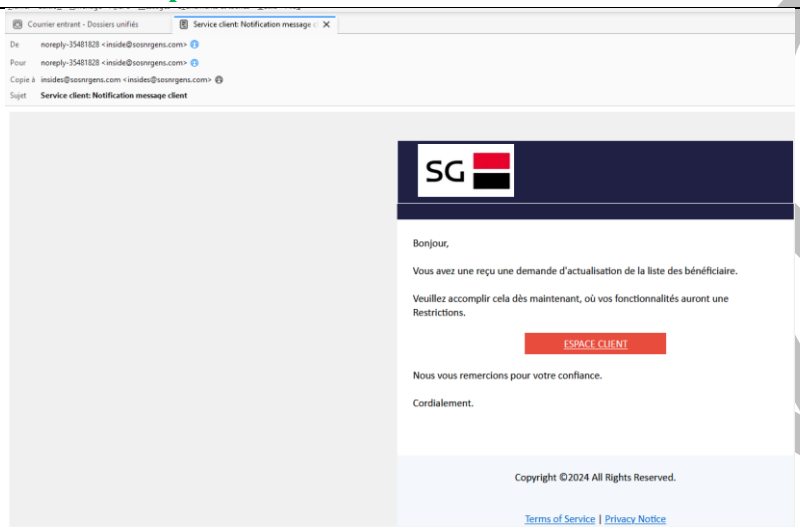
CLIQUEZ ICI

Ps : en ignorant cet avis vous vous exposez à une interdiction temporaire de toutes vos opérations

L'ensemble de nos équipes vous remercie pour votre confiance

On n'utilise jamais un lien venant d'un message. Tout lien doit être vérifié en haut de son navigateur, avant son utilisation. Utilisez toujours mes liens que vois avec sauvegardés (donc vérifiés) dans vos favoris ou vos marque- pages..

3.7.2 Faux problème de liste des bénéficiaires



1. « De » n'a rien à voir avec une banque, « Pour » n'est pas pour vous.
2. Le lien ne va pas vers une banque.
3. Une faute d'orthographe au dernier mot

3.7.3 Soit disant problème de téléphone

Nouveau type d'arnaque	Attention	La bétise à faire
	• La fausse adresse de l'expéditeur est difficile a détecter car elle ressemble étrangement à la vraie. • L'adresse du destinataire n'est pas là votre, mais celle d'un groupe. • Le sujet est évidemment faux, si vous n'avez pas changé de numéro de téléphone	• Se connecter depuis le bouton en rouge, sur un site qui imite la banque en question • En cas de doute, vous devez appeler directement votre banque par téléphone, ou vous présenter sur son lieu habituel, ou vous connecter depuis le lien sûr, que vous avez placé dans vos favoris (ou marque-pages)

3.8 Arnaque à la banque de France

Chèr (e) Client (e)

Sécures'Code est un service gratuit mis à disposition de tous les clients titulaires d'un compte bancaire sur le territoire français
C'est une authentification dite forte car elle requiert deux facteurs d'authentification sur les trois existants pour confirmer tous vos paiements.
Pour l'activation de ce service, vous devez obligatoirement valider un formulaire d'adhésion dans la base de données globale de la **BanqueDeFrance.fr.**

Ce service est obligatoire et vous est offert gratuitement par votre BANQUE.

Pour activer ce service cliquez sur : Activation Sécures'Code

Service Clients
Merci de votre confiance,
Banque-France.fr
Tous droits réservés ®2022

Il ne faut JAMAIS se connecter à ce type de lien Vous devez passer directement par votre banque.

4 Arnaques et piratage de votre Smartphone. Faux message

4.1 Le faux message téléphonique.

1. Vous recevez un coup de téléphone qui semble provenir de votre banque car c'est son numéro qui s'affiche.
2. Le conseiller bancaire en question, vous prévient que votre compte bancaire a é té piraté.
3. Il vous propose un nouveau compte pour régler le problème.
4. Vous avez tout perdu.

En résumé

Il faut raccrocher poliment et contacter immédiatement sa banque sur place ou par téléphone en appelant le vrai numéro. En général, les banques vous informent, sur ce qu'elles font et ne le font pas par téléphone ou par email

4.2 Tout savoir sur les appels frauduleux

Voici une mise en garde du service public, avec des types d'appels et des signalements possibles.
https://www.service-public.fr/particuliers/actualites/A17208?xtor=EPR-100

4.3 Le démarchage abusif.

Question

Comment lutter contre le démarchage abusif ?

Réponse

Réponse du service public (en particulier, Les arnaques à la rénovation).
https://www.service-public.fr/particuliers/actualites/A17228
ou encore ce lien ;
https://www.service-public.fr/particuliers/vosdroits/F33267

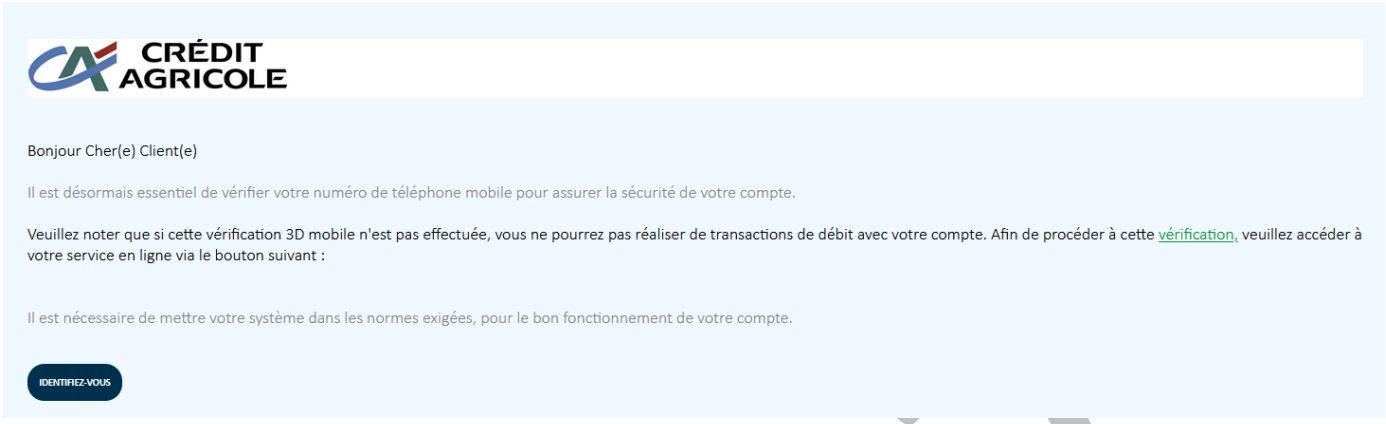
4.4 Le piratage de votre Smarphone

Soyez prudent. Le piratage d'un smartphone est plus simple que celui d'un PC. Soyez très prudent.
Voici les recommandations de Dashlane à ce sujet :
https://www.dashlane.com/fr/blog/comment-savoir-si-votre-telephone-a-ete-pirate

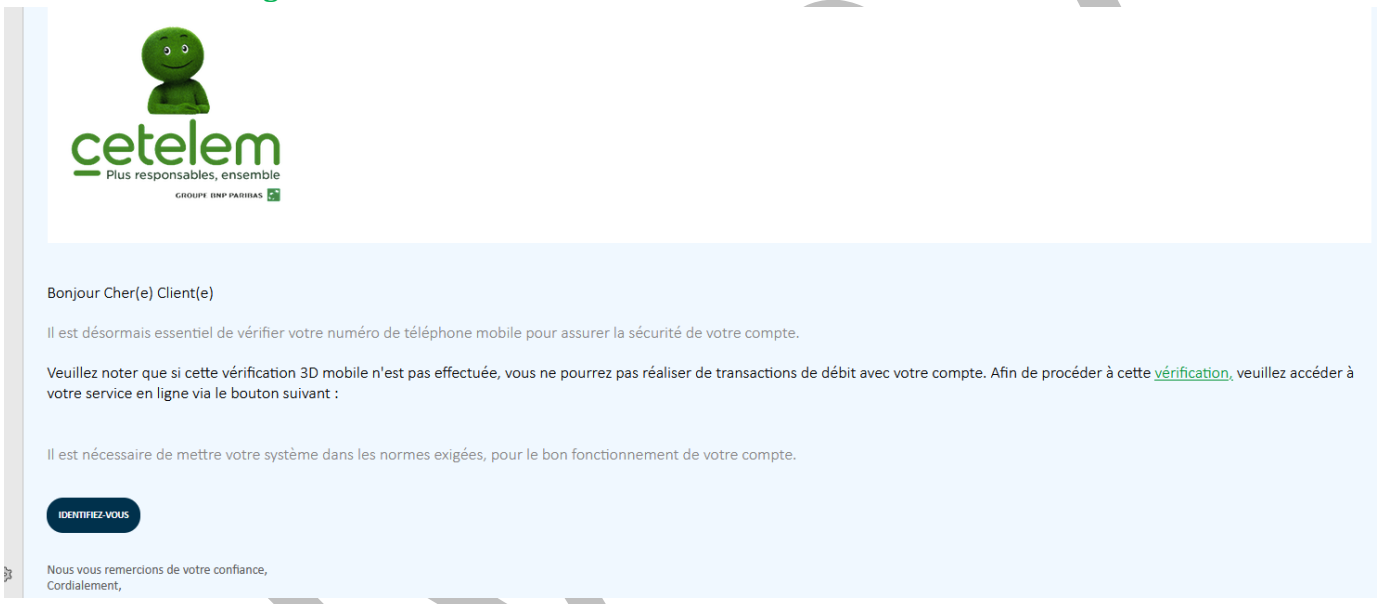
4.5 Le type d'arnaque du moment, presque identique pour 3 banques

Cette arnaque a pour but de pirater votre Smartphone :

4.5.1 Le crédit agricole



4.5.2 Autre message.



Usurpation d'une banque. Beaucoup sont visées avec ce même type de message. Surtout ne pas cliquer.
ON N'OUVRE JAMAIS UN LIEN SUR UN MESSAGE PROVENANT (soit disant) D'UNE BANQUE

4.5.3 Une nouvelle banque attaquée par cette arnaque

5 Comment se protéger -Comment réagir

5.1 Compte e-mail – Réseaux sociaux

Question

Existe-t-il des dangers particuliers sur vos comptes E-mail ou sur les réseaux sociaux?

Réponse

OUI. Utilisez le lien précédent. https://www.service-public.fr/particuliers/vosdroits/N31138

Liens détaillés sur ces sujets

- Ransomware ou rançongiciel
- Piratage d'une messagerie électronique (mail, réseaux sociaux...)
- Phishing (hameçonnage)
- Fraude liée à un achat sur internet
- Fraude liée à une location sur internet
- Chantage / Menaces lors d'une relation amoureuse ou amicale sur internet

5.2 La banque de France vous informe sur les arnaques

5.2.1 Vidéo :

https://youtu.be/pluU4cSJdbE

5.2.2 Document :

https://particuliers.banque-france.fr/info-banque-assurance/arnaques-les-bons-reflexes/les-arnaques-aux-moyens-de-paiement#

5.3 Les conseils de la DGCCRF

Direction générale de la concurrence, de la consommation et de la répression des fraudes)

https://www.economie.gouv.fr/achats-fin-annee-conseils-consommateurs-black-friday-noel

5.4 Les co Conseil de la Caisse d'épargne

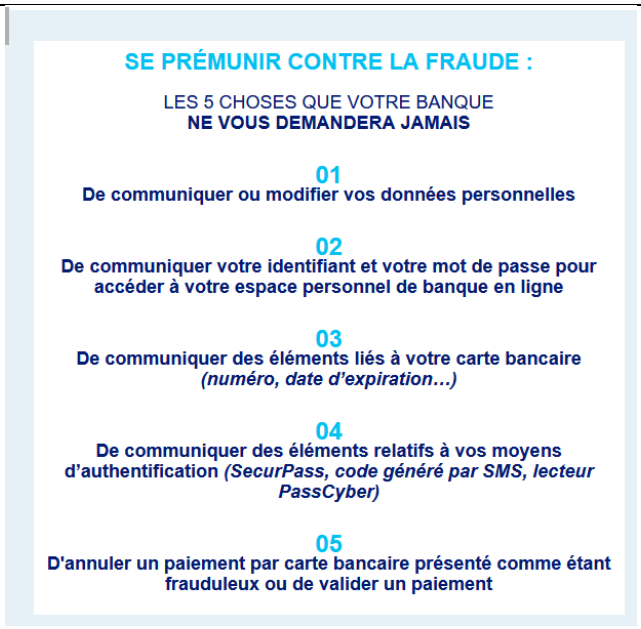
9 exemples différents sont décrits, après avoir géré les cookies, évidement.

https://www.caisse-epargne.fr/loire-centre/votre-banque/securite/

5.5 Conseils de la banque populaire.

Je cite :

➤ Ne cliquez jamais sur les liens contenus dans des SMS ou emails de provenance douteuse.
➤ Ne répondez jamais à un email vous demandant vos coordonnées bancaires ou vous alertant sur une fraude ou une urgence particulière.
➤ Composez vos codes confidentiels à l'abri des regards.
➤ Vérifiez régulièrement vos relevés de comptes ainsi que la liste des bénéficiaires de virements enregistrés dans votre espace personnel de banque en ligne.
➤ N'enregistrez aucune donnée personnelle sur votre ordinateur ni sur votre téléphone portable.
➤ Installez un anti-virus sur vos équipements informatiques et pensez à effectuer les mises à jour régulièrement.
➤ Utilisez des mots de passe différents et changez-les régulièrement.
➤ Ne communiquez jamais vos données personnelles à qui que ce soit.



5.6 Info sur les arnaques à la carte bancaire

Question

Avez-vous des informations sur les fraudes à la carte bancaire ?

Réponse

https://www.quechoisir.org/actualite-fraudes-a-la-carte-bancaire-en-hausse-mais-pas-mieux-remboursees-n93040/?utm_medium=email&utm_source=nlh&utm_campaign=nlh210713&at_medium=email&at_emailtype=retention&at_campaign=nlh210713

5.7 Les critères à retenir.

1. L'ordure qui vous envoie ce message n'a pas une adresse officielle.
2. Vous n'apparaissez pas dans l'adresse du destinataire, ce qui prouve que beaucoup de gens reçoivent ce message en copie cachée.
3. Le lien pour répondre n'a rein d'officiel.

5.8 Les précautions à prendre.

Du bouton droit de la souris cliquez sur le lien pour le copier. Surtout ne pas l'utiliser. Ouvrez-le » bloc-notes ou le Wordpad ou uu traitement de texte et coller ce lien si vous voulez savoir à quoi il ressemble.

Ne répondez jamais.

Si vous souhaitez lire la pièce jointe, il est important de l'enregistrer dans vos téléchargements sans l'ouvrir. Vérifiez avec votre antivirus ou avec Malwarebytes qu'elle ne contient pas de virus afin de l'ouvrir en tourte tranquillité.

Si vous le souhaitez, faites un rapport sur le site https://www.signal-spam.fr/

Question

Existe-t-il un document de prévention, permettant de se prémunir contre les arnaques ?

Réponse

Oui en 16 fiches. Contre les arnaques et les méthodes frauduleuses. Ce document des services publics est à télécharger sur ce lien : https://www.economie.gouv.fr/files/files/2022/Guide-TF-actualise-1907.pdf?v=1658841542

Ce guide identifie notamment des arnaques massivement utilisées récemment :

- Arnaques au compte personnel de formation (CPF) ;
- Escroquerie à l'encaissement de chèque (représente 284 millions d'euros au premier semestre 2021 d'après l'observatoire de la sécurité des moyens de paiement) ;
- Usurpation d'identité (en forte hausse).

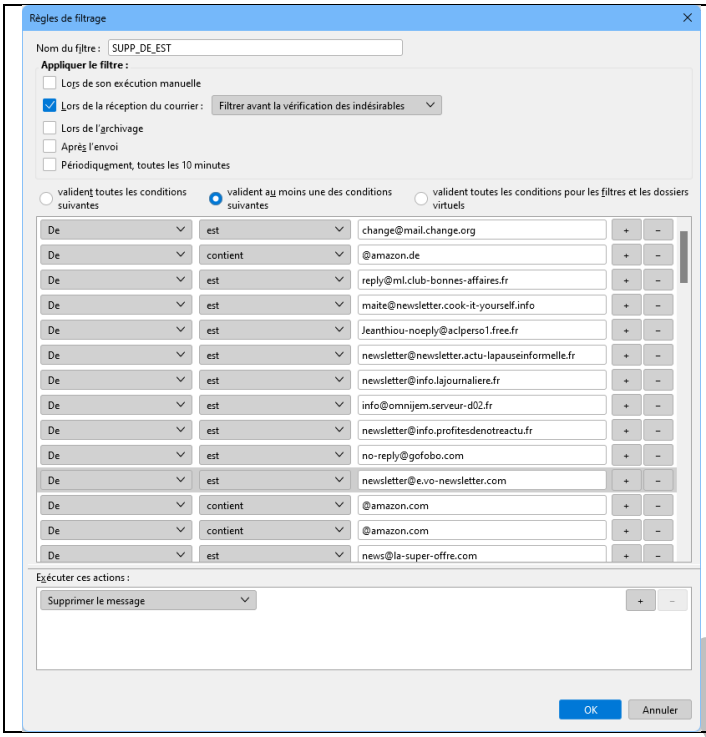
5.8.1 Que Choisir vous informe

https://www.quechoisir.org/actualite-arnaque-tentative-de-phishing-dans-les-boites-aux-lettres-n102748/?at_medium=email&at_emailtype=retention&at_campaign=nlh20220914

5.8.2 Vous avez détecté un message dangereux

Envoyez le fichier source du message au site https://www.signal-spam.fr/

5.9 Filtrage des adresses e-mails depuis Thunderbird



Question

Comment filtrer ces adresses dans Thunderbird ?

Réponse

Vous recevez un message que vous sentez être une arnaque.

Vous pouvez filtrer l'adresse de l'expéditeur.

Menu → Outils Filtres des messages .

Une fenêtre s'ouvre → Cliquez sur le bouton nouveau, si vous n' »avez pas de filtre existant.

La fenêtre ci-jointe s'ouvre.

Comme vous le voyer ici, programmez la suppression systématique des e-mails envoyés par ces adresses pourries.

Le signe plus, vous permet d'ajouter d'autres adresses dans le même filtre.

Le nom du filtre que j'ai donné se trouve en haut ç gauche de cette fenêtre (SUPP_DE_EST).

(Voir à la fin des news, la rubrique messagerie pour plus de détails)

6 Signaler un spam - une arnaque

Question

Comment signaler une arnaque ?

Réponse

Utilisez ce lien officiel :

https://www.service-public.fr/particuliers/vosdroits/N31138

6.1 Signaler un spam ou une arnaque par e-mail.

Question

A quoi sert signal-spam et comment l'utiliser ?

Réponse

Vous en avez assez de recevoir des messages non sollicités, sur votre adresse e-mail. Certains sont manifestement des arnaques (au colis par exemple ou des changements sur votre compte bancaire. Alors il est bon de faire un signalement.

Il ya encore quelques temps, il fallait se rendre sur le site de signal-spam, rentrer son nom et so mot de passe. C'est maintenant beaucoup plus simple. 2 clics suffisent

6.2 Comment procéder ?

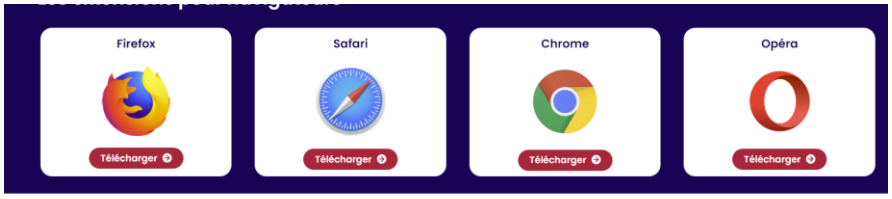
Question

J'ai constaté des changements pour le site signal-spam.fr. Comment faire pour signaler un spam ou une arnaque depuis un message e-mail ?

Réponse

Effectivement le signalement se fait maintenant depuis une extension depuis votre navigateur ou votre messagerie, quel qu'il soit (Firefox, Chrome, Safari ou Edge en ce qui concerne le navigateur ou Thunderbird, Outlook en ce qui concerne la messagerie. Pour installer cette extension :

1. Rendez-vous sur le site https://www.signal-spam.fr/
2. Descendez dans l'écran d'accueil. Voici les extensions qui apparaissent :



3. Sélectionner l'extension à télécharger (à vous de choisir, une pu plusieurs extensions. Personnellement j'ai choisi celles de Firefox et de Thunderbird.
4. Pour Firefox, une nouvelle version sera téléchargée.
5. Pour Thunderbird une extension nommée signal_spam-4.1.6-tb.xpi

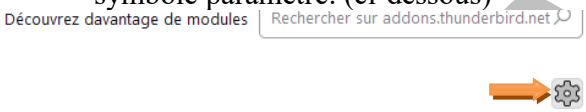
6.3 .Comment installer cette extension dans Thunderbird ?

Question

J'ai trouvé une extension sous forme de fichier signal_spam-4.1.6-tb.xpi. Comment installer cette extension

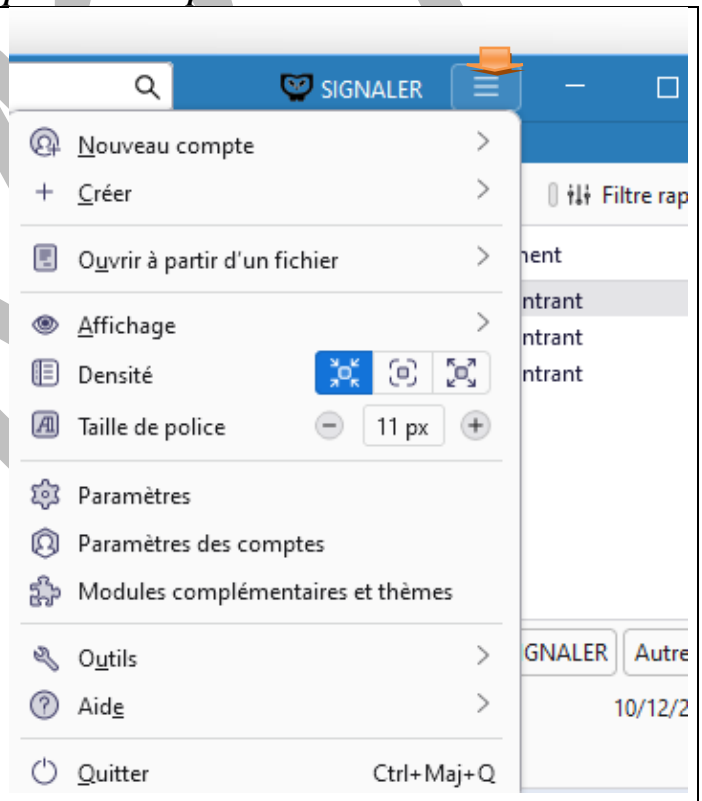
Réponse

6. Ouvrez Thunderbird. Cliquez sur le menu en haut à gauche (3 barres horizontales) → Modules complémentaires
7. Dans la fenêtre qui s'ouvre, cliquez sur le symbole paramètre. (ci-dessous)

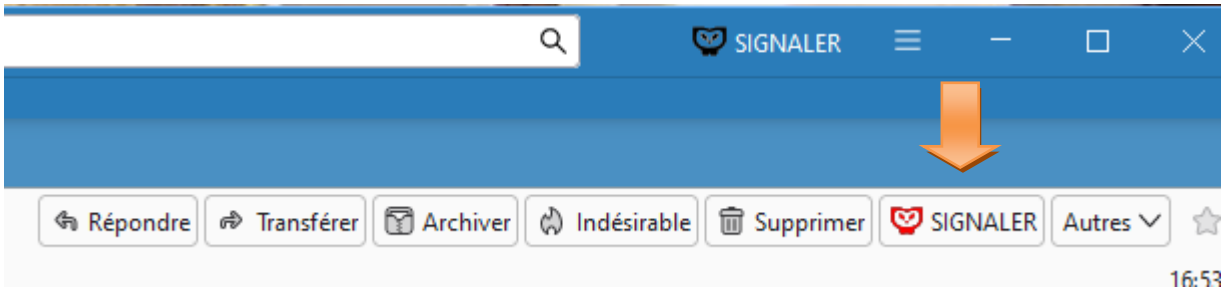


8. Sélectionnez « Installez un module depuis un fichier »
9. Une nouvelle fentre s'ouvre avec un bouton parcourir permettant d'aller chercher le fichier XPI téléchargé.
10. Il ne reste plus qu'à activer cette extension et à la paramétrer.

Personnellement j'ai évité de la mettre en un seul clic car le bouton de « Signal-spam » et juste à côté du bouton « Supprimer » et une erreur est vite arrivée.
Je dois donc cliquer une fois sur le bouton « Signal-spaml » qui ouvre un bouton « Signaler » pour un deuxième clic.
Le message est signalé et il est automatiquement effacé



Voici les boutons que vous verrez en haut à droite de vos messages lorsque vous les ouvrez en lecture.



6.4 Que se passe-t-il pour Firefox avec Signal-spam ?

Un nouveau setup de Firefox est téléchargé. Vous pouvez l'installer. Si Firefox est déjà installé sur votre PC, une simple mise à jour sera faite contenant l'extension Signal-spam.

Question

Pourquoi ne pas utiliser le site officiel de signalement, pour signaler les spams et les arnaques.

Réponse

Voici le lien officiel : https://www.internet-signalement.gouv.fr/PharosS1/

Vous devez, sur ce site, passer 10 mn pour fournir les renseignements à compléter, en 4 temps. Mais il en manque un : le fichier source du message de l'arnaque, qui est le seul vraiment utile. Mais ce site officiel le refuse même en pièce jointe. C'est stupide car « le fichier source » contient de nombreux renseignements tels que les adresses IP. Signal-spam le fait en deux clics.

Ci-dessous, voici les 4 étapes du site officiel (bon courage) :