MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Direction centrale de la sécurité publique
Direction départementale de la sécurité publique de Seine-et-Marne
Circonscription d'Agglomération de Melun Val de Seine

POLICE NATIONALE

La police nationale vous informe sur les arnaques aux SMS et par internet, qui peuvent vous coûter très cher:

Définition d'une arnaque: escroquerie, vol, tromperie.
But d'une arnaque: obtenir *quelque chose* par une manœuvre frauduleuse (*votre identité, des documents, comme votre Carte Nationale d'Identité, votre permis de conduire, vos références sécurité sociale, C.A.F., Impôt, des informations bancaires, comme vos numéros de comptes, vos codes personnels…)*

Règle n° 1: Toujours se méfier des trop bonnes affaires !!!

La vigilance doit s'exercer particulièrement sur tous les supports téléphoniques et informatiques – **3 mots clés:** *observation – méfiance – prudence -*

Une vigilance particulière est à apporter sur les réseaux sociaux, pourquoi ?
Plus de 16 millions d'utilisateurs actifs sur Snapchat chaque jour en France, 46,5 millions d'utilisateurs actifs sur Facebook par mois… Ces chiffres illustrent l'importance et la démocratisation des réseaux sociaux au sein de la Société.
La crise sanitaire a elle aussi accéléré la dématérialisation et a multiplié les opportunités d'une délinquance qui exploitait déjà le potentiel du numérique

Les escrocs s'adaptent à toutes les évolutions et recherchent donc «leurs potentielles victimes» parmi des réservoirs regroupant un maximum de monde et ils savent aussi «coller» à la réalité économique et sociale du moment afin de mieux vous abuser !
Très récemment encore, leurs messages comportaient de grossières fautes d'orthographe, attention cela peut être beaucoup moins vrai maintenant !!!

Pourquoi reçoit-on ces SMS et mails frauduleux ?

Les raisons sont assez simples, nous communiquons nous-même, suite à diverses sollicitations notre adresse mail et numéro de téléphone !
Qui n'a pas communiqué ces informations à une boutique, à un professionnel de la vente, ou pour un simple jeu !
Vos données personnelles sont alors entrées dans un fichier et vous devenez «clients privilégié» …

Les futures victimes sont aussi approchées par des publicités sur internet, sur les réseaux sociaux, les amenant à divulguer, via des formulaires internet, des données personnelles...

Ce que vous ne savez peut -être pas c'est que de nombreux groupes et chaînes vendent leurs fichiers clients, qui ont une valeur marchande, *avec les éléments que vous avez acceptés de transmettre vous-même* et que régulièrement ces données sont revendues à d'autres professionnels, mais pas que, à un moment donné vos données peuvent tomber dans les mains d'escrocs qui malheureusement utiliseront ces informations pour mieux vous piéger et vous manipuler.

Soyez attentifs, vos enfants peuvent également être impactés de la même manière en utilisant les réseaux sociaux !!!

Conseil : - Créez-vous une adresse internet sans aucune référence à votre nom, prénom, lieu d'habitation, département, que vous communiquerez aux organismes non officiels et garder une adresse «dite officielle», pour les administrations, la banque, les impôts, la CAF…
- Ne communiquez votre numéro portable que lorsque cela est vraiment nécessaire.

Mode opératoire :

Les arnaques par SMS ou internet se présentent toujours de la même manière:
- *un titre vous incite à la consultation*, (attention il peut s'agir aussi d'un organisme de confiance usurpé !)
- *un texte vous invite à corriger une situation* qui n'existe pas, par exemple vous invite à cliquer sur un lien si vous n'êtes pas à l'origine d'une commande...)
- *un texte vous propose une juteuse affaire …(* il peut s'agir de toucher une somme d'argent, affranchir ou recevoir un colis, mettre à jour un compte… ou une multitude d'autres choses)

attention c'est à ce niveau que tout se joue

vous êtes alors invités à cliquer sur un lien ou des renseignements personnels seront demandés (identité, numéro de sécurité sociale, références bancaires, codes d'accès…)

Conseils :

S M S : *Ne jamais répondre au SMS et ne jamais cliquer sur le lien indiqué.*
Relever le numéro d'envoi du message, puis transférer le SMS au 33700, enfin renvoyer à nouveau au 33700 le numéro de transmission relevé, sans aucune autre information.
Le 33700 vous signalera alors la fin de la procédure de signalement.

Mail: *Ne jamais répondre au message et ne jamais cliquer sur le lien indiqué.*
Transféré votre mail *sans aucune autre information à:*
fraude-bretic@interieur.gouv.fr

A l'issue des transmissions, mettre le mail ou le sms à la corbeille et vider cette dernière.
Ces deux services bloquent les numéraux d'appels signalés et exploitent les renseignements transmis.

Conseils généraux:
- Ne jamais cliquer sur un lien ou une pièce jointe sans être certain de la fiabilité de l'expéditeur.
- Si nécessaire, vérifiez l'adresse de l'expéditeur par un autre canal.
- Ne jamais répondre à un mail suspect ou à du chantage, afin de ne pas montrer que vous êtes réceptif au message, ne jamais payer de demande de rançon, mais déposez plainte.

MON QUOTIDIEN NUMÉRIQUE

- Votre départ en vacances approche à grands pas: adoptez les bons réflexes en ligne.
- Les cambrioleurs usent souvent de stratagèmes simples pour identifier leurs victimes sur le web, voici quelques clés pour partir léger:

- N'indiquez pas vos lieux de vacances sur les réseaux sociaux.
- Verrouillez vos comptes et limiter vos accès qu'aux intimes en réglant la visibilité de vos publications en ligne.
- Soyez discrets sur vos biens.
- Évitez de donner des renseignements qui permettent d'identifier votre domicile.

Quelques arnaques en vogue:

Arnaque à la vignette Crit'Air: (mails et / ou sms) Cette dernière est déjà nécessaire dans certaines agglomération mais devrait être obligatoire sur l'ensemble du territoire qu'en 2025. (elle peut se commander sur les sites officiels du style service-public.fr ou certificat-air.gouv.fr mais jamais par SMS.

Arnaque à la carte vitale: (mails et / ou sms) Les mises à jour ou toutes opérations liées à la carte vitale ne se font jamais via sms ou mail.

Arnaque à la location immobilière: Ne jamais effectuer de transfert en cash, via transcach où autre, pour un soit-disant dépôt de garantie, attention si votre interlocuteur ne vous propose que des échanges mails, sans autre élément !!!.
La règle précise de ne rien verser avant la signature d'un bail précis

Nota: La généralisation de l'authentification forte mise en place par les banques a permis la baisse du taux de fraude des paiements internet (- 20%) .
Cependant les menaces évoluent toujours, car les escrocs contournent ces sécurités mises en place, en développant de nouvelles techniques de fraude:

- fraude par manipulation directe des clients

(Attention aux appels téléphoniques ou un escroc se présente comme votre conseiller bancaire – *il peut même connaître son identité et se faire passer pour lui, ou pour un de ses collègues* – et peut par exemple vous solliciter en urgence suite à une soit disant «attaque informatique» et vous soutirer vos codes bancaires, numéros bancaires et diverses informations ou souhaiter mettre à jour vos données personnelles

D'autres scénarios ont cours: le fraudeur peut prétendre devoir bloquer ou annuler dans l'urgence une fraude à la carte bancaire ou au virement sur votre compte et sollicite alors vos codes secrets afin de faire au plus vite soit-disant dans votre intérêt

Toutes ces opérations ne se font jamais par mail, sms ou téléphone. Mais dans les locaux de votre établissement bancaire avec un conseiller bancaire.
Ces appels visent en réalité à contourner les nouveaux dispositifs de sécurité des paiements.

Fréquemment, les escrocs utilisent une technologie qui leur permet de faire apparaître le numéro de téléphone de la banque usurpée et de masquer leur vrai numéro.

Les Français seraient les plus escroqués en Europe

Près d'un Français sur deux se fait tromper par un message l'avertissant d'une bonne nouvelle.

Les arnaques en ligne continuent de guetter les consommateurs européens… et tout particulièrement les Français.

En cause, le perfectionnement notable des techniques employées par les escrocs pour inspirer confiance aux consommateurs. *Ainsi, une grande majorité des sondés affirment être sensibles aux messages d'urgence envoyés par des pirates, qui les convainquent de cliquer sur un lien dans un mail ou un SMS.*

50% avouent se faire avoir par les messages annonçant une bonne nouvelle, généralement de l'ordre d'un remboursement.

Soyez encore plus vigilant

Malgré les recommandations fréquentes émanant des autorités publiques, la majorité des Français ne surveille pas les détails permettant d'établir la véracité d'un message.

Vous êtes nombreux à examiner l'orthographe, mais ce point est de plus en plus rectifié par les escrocs.

Beaucoup moins pensent à vérifier l'adresse mail de laquelle émane le message, il est conseillé de passer sa souris sur le lien afin de vérifier sur quel site Web il renvoie.

Il convient d'être vigilant car de plus en plus de banques refusent de rembourser les victimes, arguant qu'elles ont fait preuve de «négligence».
