Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

La gendarmerie de Bollène recherche les victimes d'une escroquerie

Suite aux interpellations de plusieurs ressortissants irlandais abordant les automobilistes, la gendarmerie nationale de Vaucluse alerte sur une série d'escroquerie et lance un appel à témoin.

Les gendarmes de Bollène viennent de procéder aux interpellations de plusieurs ressortissants irlandais suspectés de commettre des escroqueries dans la région, voire sur le territoire national.

Les escrocs opèrent de manière à ce que des automobilistes (aire de repos, sorties d'autoroute, bord de route) leur viennent en aide en faisant croire à une panne d'essence ou un autre mobile… Ces derniers indiquent alors ne plus avoir d'argent liquide pour se rendre chez eux en Irlande.

« Ils demandent alors à leur victime de retirer une forte somme d'argent et en remboursement ils procèdent à un virement bancaire, explique la gendarmerie de Vaucluse. Ce virement est fait devant la victime mais avec une application fictive. Ensuite, les protagonistes suivent la victime au distributeur de billets et se font remettre la somme. Mais plusieurs heures, voire quelques jours plus tard, la victime s'aperçoit que le virement n'a jamais été réalisé et comprend qu'elle a été victime d'une escroquerie… »

La gendarmerie nationale lance donc un appel à témoins pour retrouver les témoins et les victimes de l'escroquerie ou de sa tentative, en vue de compléter les investigations utiles pour confondre les

Les Petites Affiches de Vaucluse depuis 1839

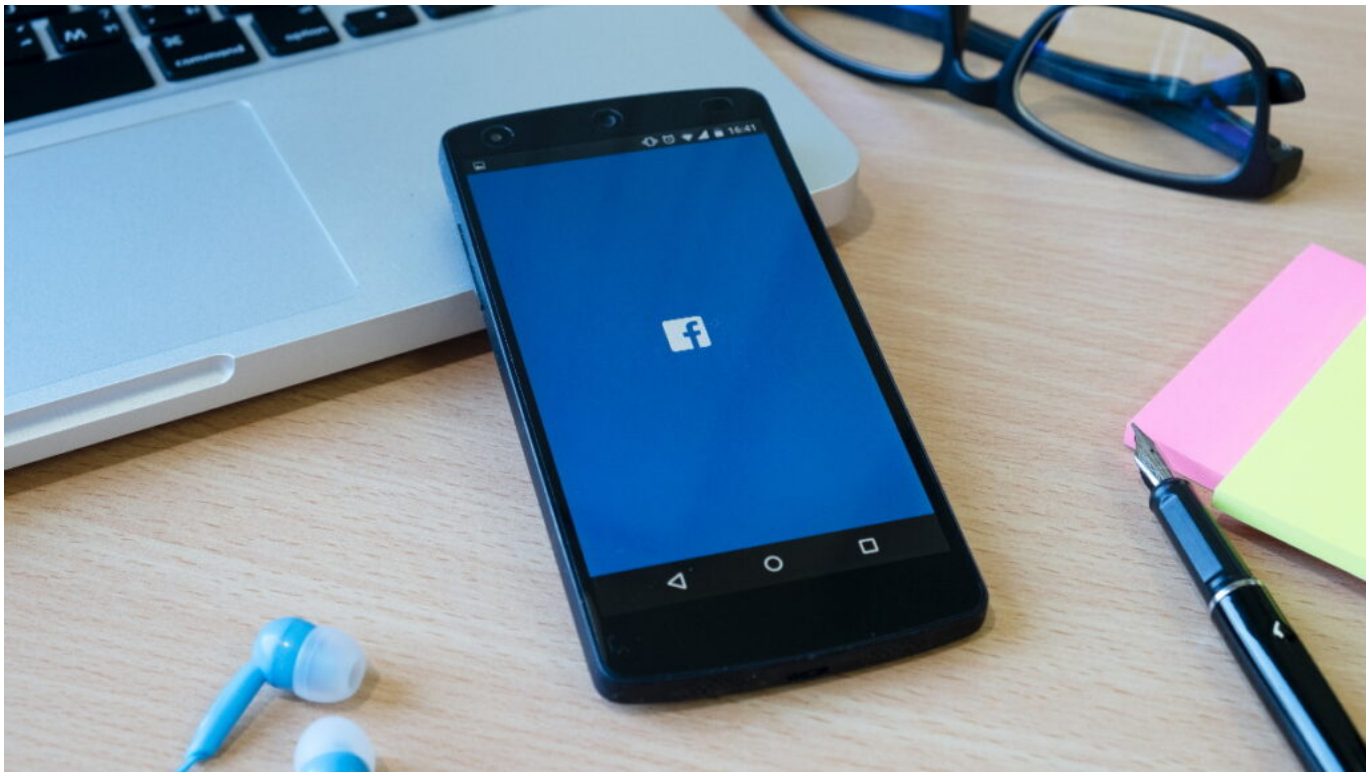
Ecrit par le 23 juillet 2024

auteurs…

Brigade de gendarmerie de Bollène : 04 90 30 10 28

Rosalie Ricard-stagiaire

Escroqueries sur Facebook Marketplace : comment les identifier et les éviter ?



Pour assurer la sécurité de vos informations personnelles et financières en ligne, il est important de connaître – que vous achetiez ou vendiez – les signes suspects à surveiller sur Facebook Marketplace et de savoir comment vous protéger contre les escroqueries.

Facebook Marketplace est rapidement devenu un lieu de prédilection pour vendre ou acheter des objets d'occasion localement. Le fait que les acheteurs et les vendeurs puissent acheter des biens et

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

communiquer facilement au sein de l'application Facebook a permis à l'adoption de Facebook Marketplace de monter en flèche.

Comment identifier une escroquerie sur Facebook Marketplace

Si la plupart des utilisateurs de Marketplace sont des acheteurs et des vendeurs de confiance, des personnes malintentionnées peuvent également profiter du site pour faire tomber les gens dans des escroqueries. Voici quelques signes clés qui peuvent indiquer que vous communiquez avec un escroc :

- Trop beau pour être vrai : les acheteurs doivent se méfier de toute annonce proposant un prix extrêmement bas pour un objet de valeur. De même, les vendeurs doivent se méfier des acheteurs potentiels qui proposent un prix supérieur à celui demandé.
- L'urgence artificielle : les escrocs utilisent souvent l'illusion de l'urgence pour inciter les acheteurs ou les vendeurs à conclure des transactions moins que légitimes.
- Demandes de paiement étranges : Facebook recommande aux acheteurs d'éviter les ventes ou les transactions qui exigent que vous payiez avec des cartes-cadeaux. Il est également recommandé de vérifier la qualité et l'état de l'objet acheté avant d'échanger de l'argent ou des informations personnelles de quelque nature que ce soit.
- Photos suspectes : s'il n'y a qu'une seule photo d'un article provenant du site où il a été acheté à l'origine et aucune photo actuelle de l'article dans son état réel, il faut se méfier du fait que l'article n'existe peut-être pas, ou qu'il n'existe peut-être pas dans la qualité promise.

Les 6 escroqueries courantes sur la Marketplace Facebook

- Articles contrefaits : l'une des escroqueries les plus courantes sur Facebook Marketplace consiste à mettre en vente des articles contrefaits ou endommagés. Il est conseillé de toujours examiner attentivement le profil du vendeur et de lire les commentaires des clients avant d'acheter un article sur Facebook Marketplace, et d'obtenir autant d'informations que possible sur le produit avant de l'acheter afin de s'assurer qu'il est légitime.
- Fausses annonces : bien souvent, les escrocs exigent un paiement anticipé pour ensuite se retirer de l'affaire ou disparaître et vous n'obtenez jamais l'article acheté.
- Fraude immobilière : les escrocs peuvent publier des photos de maisons ou d'appartements dont ils ne sont pas propriétaires et les « vendre » ou les « louer » à l'improviste à des acheteurs qui ne se doutent de rien. Facebook conseille de ne pas envoyer d'acompte pour des biens de grande valeur (y compris pour la location d'un appartement) sans s'être assuré au préalable qu'il s'agit bien d'un bien réel.
- Trop-perçu : les utilisateurs frauduleux envoient souvent plus d'argent que ce que vous avez demandé, pour ensuite exiger le remboursement du « trop-perçu ». Lorsque vous essayez de déposer le chèque, il est sans provision et vous ne recevez donc aucun paiement. Si un acheteur envoie un trop-perçu, le vendeur peut refuser les fonds et demander à l'acheteur d'envoyer un autre paiement avec le solde correct.
- Profils suspects : vous devez pouvoir consulter ses évaluations et avis, ses autres annonces et

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

son activité sur le marché. Si l'utilisateur n'est pas originaire de la région ou si son profil est vide, c'est peut-être le signe qu'il n'est pas celui qu'il prétend être.
- Hameçonnage pour obtenir des informations personnelles : les escroqueries par hameçonnage sur Facebook Marketplace ont pour but de voler vos données et informations personnelles. L'escroc peut vous demander un code ou un numéro de téléphone pour compléter un code de vérification à deux facteurs sur un système de messagerie non sécurisé. Ce code peut être lié à une autre application qui lui permet de voler votre numéro de téléphone portable et vos informations de compte, ce qui lui donne un accès complet à d'autres comptes qu'il souhaite utiliser.

Comment signaler une escroquerie ?

Pour signaler un vendeur frauduleux à Facebook, accédez à la Marketplace et cliquez sur l'article. Sélectionnez le nom du vendeur sur la page de l'annonce et cliquez sur « Signaler ». Vous pourrez ainsi signaler le vendeur en fonction du type d'escroquerie qu'il a commise ou tentée de commettre. Pour signaler un acheteur frauduleux, cliquez sur les messages échangés entre vous et l'acheteur potentiel puis sélectionnez l'option « Signaler l'acheteur ». Suivez la procédure indiquée pour signaler l'acheteur frauduleux à Facebook et faire en sorte que d'autres personnes ne soient pas victimes de cette escroquerie.

Ce que vous pouvez faire pour éviter les escroqueries sur Facebook Marketplace

La meilleure façon d'éviter les problèmes est de rester vigilant et de connaître les arnaques courantes sur Facebook Marketplace. Sachez reconnaître les signaux d'alarme et suivez toujours les meilleures pratiques pour vendre et acheter en toute sécurité. Si vous utilisez des méthodes de paiement sûres, si vous vérifiez l'authenticité des produits et si vous refusez les offres ou les demandes suspectes, vous aurez beaucoup plus de chances de rester en sécurité.

Si vous êtes tout de même victime d'une escroquerie, il est possible d'avertir le prestataire de services de paiement que vous avez utilisé pour lui signaler l'escroquerie et demander un remboursement par l'intermédiaire de son service de protection contre la fraude. Facebook Marketplace est une plateforme qui peut être très utile, mais à utiliser toujours de manière avertie !

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

Bastien Bobe, Directeur technique EMEA chez Lookout.

Attention aux arnaques téléphoniques aux faux agents de la Banque de France

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

La Banque de France alerte le public sur des tentatives d'escroqueries téléphoniques utilisant frauduleusement son nom et son numéro de téléphone.

Les escrocs prétendent appartenir au personnel de la Banque de France (souvent le service des fraudes) et demandent aux personnes contactées d'annuler des opérations prétendument frauduleuses en se connectant à leur espace personnel de leur banque. En réalité, les personnes procèdent à la validation d'opérations au profit des escrocs. Ces escrocs sont d'autant plus crédibles qu'ils parviennent à afficher, sur l'écran du téléphone de la personne contactée, le véritable numéro de la Banque de France et qu'ils détiennent des informations personnelles de leur victime, notamment ses coordonnées bancaires.

> « La Banque de France ne sollicite jamais la communication de coordonnées bancaires, d'informations personnelles ou la validation/annulation d'une opération bancaire. »

Que faire si vous êtes victime ?

1. Contactez votre banque ! Signalez-lui rapidement les opérations frauduleuses, au plus tard dans les 13 mois de la date du débit. Ce délai est plus court* lorsque l'établissement du bénéficiaire du paiement se situe en dehors de l'Union Européenne ou de l'Espace Économique Européen. Pour rappel : votre banque

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

doit rembourser la somme débitée. En cas de désaccord, la charge de la preuve appartient à la banque. Pour refuser de vous rembourser, la banque doit démontrer que vous avez été particulièrement négligent dans la conservation de vos données bancaires.

2. Déposez plainte : www.pre-plainte-en-ligne.gouv.fr

3. Enfin, vous pouvez contacter INFO ESCROQUERIES au 0 805 805 817 (appel gratuit du lundi au vendredi de 9h à 18h30) et/ou faire un signalement sur www.internet-signalement.gouv.fr.

L.G.

** Le délai est alors ramené à 70 jours (le contrat carte peut prévoir un délai plus long, ne pouvant dépasser 120 jours).*

Vignette Crit'Air : attention aux escroqueries à la vente à Avignon

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

La vignette Crit'Air est actuellement au cœur d'une vague d'arnaques. Face à cela, la préfecture de Vaucluse appelle à se méfier des intermédiaires et des sites frauduleux.

La vignette Crit'Air, qui permet de classer les véhicules en fonction de leurs émissions polluantes en particules fines et oxydes d'azote, est au cœur d'une vague d'arnaques. Certains citoyens déboursent bien plus que nécessaire pour obtenir ce certificat, en passant par des « faux sites administratifs », qui font payer un service d'aide à la démarche d'achat de la vignette Crit'Air, alors que les utilisateurs ne sont pas informés qu'ils naviguent sur un site à but lucratif.

A lire aussi : « Vignette Crit'Air : qui et comment circuler sur Avignon ? »

Deux modes opératoires ont été relevés :

- La création de sites frauduleux référencés dans les moteurs de recherche internet où les victimes sont amenées à renseigner leurs coordonnées bancaires ;
- Des campagnes d'hameçonnage par sms ou par mails suivis d'appels téléphoniques dans le but d'obtenir les coordonnées bancaires des victimes.

Des mises en scène prolongent parfois l'escroquerie. La victime est alors contactée par de faux banquiers ou conseillers financiers qui, sous prétexte d'annuler le virement frauduleux, se font révéler des informations bancaires.

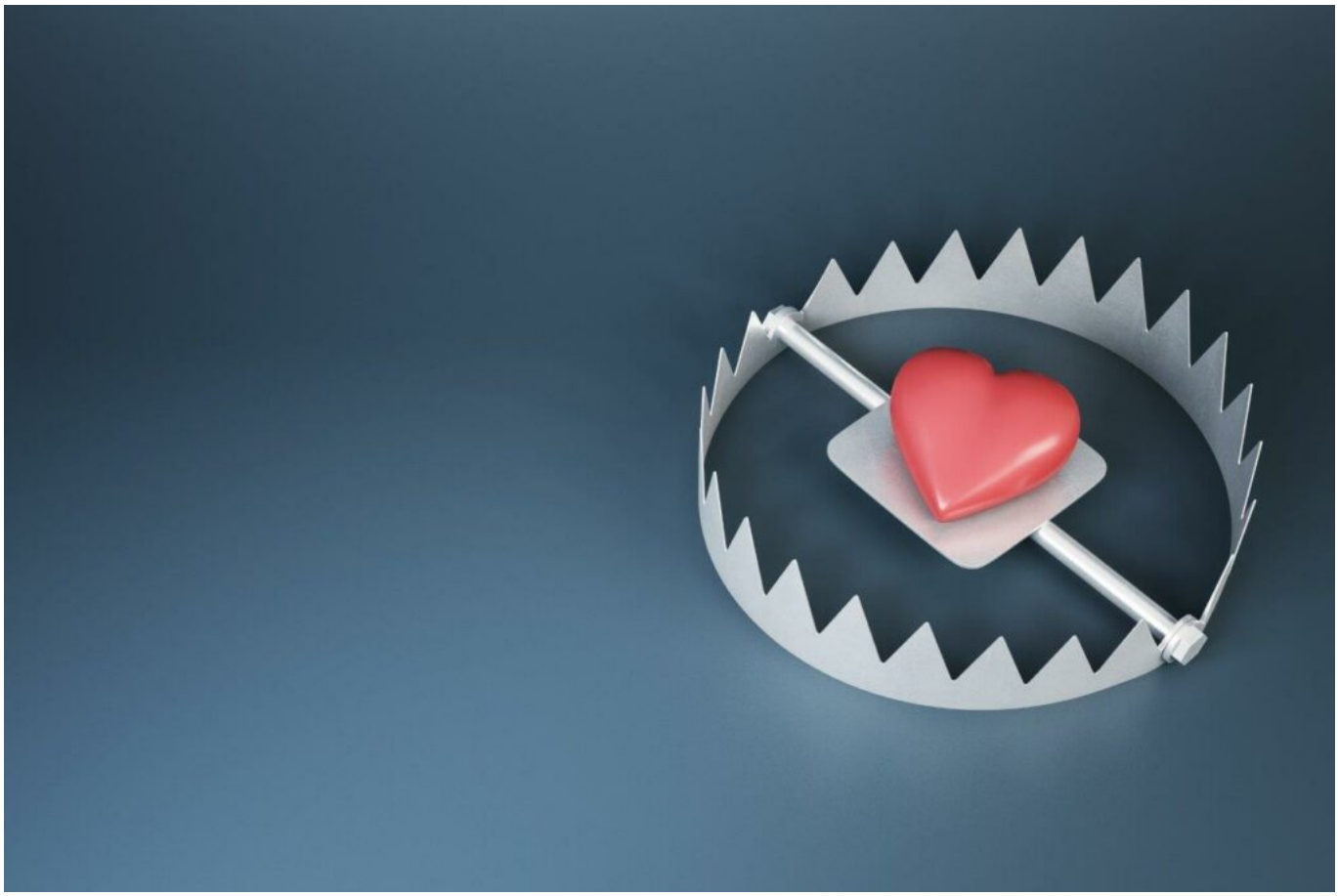
A lire aussi : « Grand Avignon : la vignette Crit'Air a encore un peu de chemin à faire »

Face à ces escroqueries, la préfecture de Vaucluse appelle à la prudence face aux intermédiaires et sites frauduleux. Pour rappel, le seul et unique site officiel de la vignette Crit'Air est certificat-air.gouv.fr.

Escroqueries amoureuses, restez vigilants sur les plateformes de rencontre

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024



« Êtes-vous sur Tinder ? Avec 75 millions d'utilisateurs actifs mensuels, vous pourriez y rencontrer la bonne personne. Mais il existe aussi des pièges dont vous devez vous méfier : ils ont pour noms catfishing, sextorsion, hameçonnage et autres pratiques utilisées par des escrocs… », prévient Benoit Grunemwald, expert en cybersécurité chez Eset France.

Sur les plateformes de rencontre vous pouvez trouver l'âme sœur, comme des personnes mal intentionnées. C'est ce que nous avons pu voir récemment dans le documentaire diffusé sur Netflix, Tinder Swindler, qui raconte l'histoire de plusieurs femmes arnaquées par le même homme. Cet individu bien réel dispose d'un profil avec plusieurs photos, ainsi que des comptes de médias sociaux liés. Cet 'arnacœur' a réussi à extorquer 10 millions de dollars après avoir trompé ses victimes et les avoir incitées à financer son style de vie luxueux. Il ne s'agit pas d'un cas isolé. À l'instar de cet homme, de nombreuses personnes profitent de la solitude des autres et de leur désir de rencontrer leur moitié pour les arnaquer. Petit tour des pièges à éviter.

Données personnelles et vol d'identité : c'est l'arnaque de base. En général, ces profils utilisent des images qui semblent provenir directement du catalogue d'une agence de mannequins ou, à l'opposé, ils utilisent des images d'amateurs, floues et suggestives. Dans les deux cas, les escrocs tentent de vous faire 'swiper' vers la droite. Lorsque vous le faites, ils ne perdent pas de temps. Sous prétexte qu'ils « ne

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

passent pas beaucoup de temps sur Tinder », ils vous demanderont votre numéro de téléphone pour se connecter sur WhatsApp et « apprendre à mieux vous connaître ». À ce stade, vous transmettez déjà des informations personnelles. Il est maintenant beaucoup plus facile pour l'escroc de trouver vos profils de médias sociaux, de voler vos photos et collecter vos données.

Catfishing : les 'catfishers' sont de vraies personnes qui créent de fausses personnalités à l'aide d'informations personnelles volées, généralement à une personne qu'ils ont déjà escroquée. Cela peut sembler inoffensif, mais le catfishing peut causer beaucoup de soucis et durer des mois ou des années. Sachez que les arnaques de catfishing peuvent également impliquer de l'extorsion, et qu'elles peuvent être utilisées pour voler vos informations personnelles, vous envoyer des logiciels malveillants ou même mener des activités d'espionnage.

Sextorsion : les 'nudes' (photos de nus) et le 'sexting' (messages, photos ou vidéos à caractère sexuellement explicite), deux activités aussi populaires que risquées, font de vous une cible facile dont les escrocs peuvent profiter. La victime de sextorsion souffre et s'angoisse, ayant déjà conduit des victimes à mettre fin à leurs jours. Les escrocs sont très conscients de l'impact vicieux que l'exposition peut avoir sur vous, et ils en profitent. Par mesure de sécurité, Tinder ne permet pas aux utilisateurs de partager des photos, mais une fois que vous êtes sorti de son écosystème et que vous commencez à envoyer des SMS sur une autre application, vous pouvez devenir une proie facile pour un maître chanteur. En échange du maintien de la confidentialité de vos photos, on vous demandera une rançon que vous paierez très probablement. Ne vous laissez pas intimider et faites appel à un tiers pour vous aider.

Hameçonnage : en étant sur Tinder, vous êtes également vulnérable aux différents malwares et aux attaques d'hameçonnage. Vous pouvez facilement être amené à ouvrir un lien que vous ne devriez pas ou à donner un code de vérification aléatoire qui permettra à l'escroc d'accéder à vos comptes bancaires. Les premiers échanges passés, vous décidiez de vous rencontrer. Votre contact vous envoie le lien d'un spectacle et vous demande d'acheter les billets parce que sa carte ne fonctionne pas pour les achats en ligne, vous remplissez les détails de votre carte de crédit. Mais en réalité, vous venez de saisir vos coordonnées bancaires sur un faux site Web. Pendant ce temps, votre rendez-vous vous a soudainement disparu…

Escroquerie financière romantique : cette escroquerie est la plus difficile à détecter. Les escroqueries financières liées à la romance existent depuis toujours, mais l'ère numérique permet aux escrocs d'atteindre des sommets. Ne pensez pas qu'ils cherchent à nous extorquer des millions, ils prennent ici et là des sommes modiques. Mise bout à bout, elles leur assurent un revenu. Leur force de persuasion leur permet de soutirer des sommes à de nombreuses victimes, quand celle-ci ne peut plus payer, l'arnaqueur disparait, laissant la victime dans une grande souffrance.

Voici les principales techniques utilisées sur les applications de rencontres. Pour se prémunir, il existe quelques étapes faciles à suivre. D'abord et avant tout, ne sortez pas des applications de rencontre pour aller vers d'autres messageries. Vous resterez ainsi dans un environnement plus sûr où vous pourrez facilement signaler un escroc, ce qui vous protégera, vous et les autres utilisateurs. Si vous décidez de déplacer la conversation vers une autre application, comme WhatsApp, n'envoyez pas de photos de vous

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

qui pourraient être utilisées à mauvais escient et restez vigilant.

Benoit Grunemwald, expert en cybersécurité chez Eset France

Vaucluse : l'Assurance maladie lance une alerte au SMS frauduleux

La Caisse primaire d'assurance maladie (CPAM) de Vaucluse met en garde ses assurés sociaux sur l'envoi depuis quelques jours de sms frauduleux aux assurés Vauclusiens.
Semblant provenir de l'Assurance Maladie ou du site ameli.fr, ce message vous annonce la disponibilité

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 juillet 2024

d'une nouvelle carte Vitale. Ce SMS vous invite à remplir un formulaire avec vos informations personnelles, voire de carte bancaire, pour régler des frais d'expédition pour recevoir votre nouvelle carte Vitale.
« Attention, vous êtes fort probablement face à une tentative d'hameçonnage qui usurpe l'identité de l'Assurance Maladie, précise la CPAM 84. L'objectif des cybercriminels est de dérober vos informations personnelles ou bancaires pour en faire un usage frauduleux.

Exemple de SMS frauduleux.

Escroquerie en ligne
« Attention, ce sont des escroqueries en ligne, vous ne devez pas y répondre ni cliquer sur le lien », insiste la Caisse primaire d'assurance maladie de Vaucluse qui rappelle que « l'Assurance Maladie ne demande jamais la communication d'éléments personnels (informations médicales, numéro de sécurité sociale ou coordonnées bancaires) par SMS. »
« Soyez vigilant, poursuit la CPAM. Cette technique d'escroquerie en ligne est très utilisée. Les escrocs cherchent à obtenir des informations confidentielles afin de s'en
servir. »

Pour plus d'informations sur ce piratage et savoir comment vous en protéger : consultez les conseils sur le site cybermalveillance.gouv.fr

Pour signaler un contenu illicite : connectez-vous sur le portail officiel de signalement de contenus illicites Internet-signalement.gouv.fr