Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Arnaques & fraudes : comment agir avec Service-Public.fr

Des pratiques commerciales mensongères, trompeuses ou arnaques, visant particuliers et entreprises, deviennent de plus en plus régulières. Comment réagir face aux arnaques ? Comment se protéger ? Service-Public.fr vous livre ses conseils.

Assurance maladie : se protéger des escroqueries et des messages frauduleux

Courriers électroniques, SMS, appels téléphoniques… les tentatives de fraudes peuvent se présenter sous différentes formes. Comment reconnaître des sollicitations malveillantes ? L'Assurance maladie rappelle les conseils essentiels en matière de sécurité. En savoir plus

Déposer une plainte à distance avec Visioplainte

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Le dispositif de Visioplainte, expérimenté par le ministère de l'Intérieur dans les départements de la Sarthe et des Yvelines, va progressivement être étendu au reste de la France. Déjà opérationnel dans la Sarthe, il permet aux victimes d'infractions de porter plainte sans avoir à se déplacer en commissariat ou en gendarmerie. Renseignez-vous ici.

Se renseigner avant de choisir vos partenaires et prestataires, consulter le Bulletin officiel des annonces civiles et commerciales (Démarche en ligne)

Depuis 2008 le Bulletin officiel des annonces civiles et commerciales (Bodacc) permet de consulter gratuitement en ligne les annonces parues, qui publie les actes enregistrés au registre du commerce et des sociétés (RCS) : ventes et cessions, immatriculations et créations d'établissement, modifications et radiations de personnes physiques ou morales inscrites au registre du commerce et des sociétés (RCS), procédures collectives, procédures de conciliation, procédures de rétablissement professionnel et avis de dépôt des comptes des sociétés.

Des conseils pratiques pour éviter de se faire arnaquer par des réparateurs professionnels

Une panne d'électricité chez vous, une fuite d'eau, ou encore des clés oubliées à l'intérieur de votre logement : de nombreuses situations peuvent vous amener à faire appel en urgence à un dépanneur ; et celui-ci est susceptible d'abuser de votre situation de détresse. La direction générale de la concurrence, de la consommation et de la répression des fraudes a publié une série de recommandations pour que chacun puisse se prémunir contre les professionnels malintentionnés. Lire la suite

SignalConso : une application mobile pour le site qui protège les consommateurs

Prix non affiché, promotion non appliquée, retard de livraison, clauses abusives, difficulté à se faire rembourser… Vous pourrez désormais signaler ces litiges sur la nouvelle application mobile de SignalConso, alors que la plateforme enregistre son 500 000e signalement. Service-Public.fr vous rappelle le mode d'emploi de ce dispositif. Se renseigner

Chantage / Menaces lors d'une relation amoureuse ou amicale sur internet

Si une personne rencontrée sur internet vous réclame de l'argent, vous pouvez porter plainte ou signaler cette situation. Vos recours dépendent du motif de cette demande d'argent.

Il peut s'agir d'une menace de diffusion d'informations compromettantes (chantage). Votre contact peut aussi chercher à vous convaincre en mentant sur le motif et en envoyant des faux documents. En savoir plus

Escroquerie

L'escroquerie consiste pour l'escroc à obtenir un bien, un service ou de l'argent par une tromperie (manœuvres frauduleuses…) s'il est démontré que l'auteur des faits a eu l'intention de tromper sa victime. Si vous êtes victime, vous pouvez déposer plainte à la police ou en gendarmerie ou par courrier

Ecrit par le 22 juillet 2024

auprès du procureur. Pour certaines escroqueries commises sur Internet, vous pouvez porter plainte en ligne en utilisant le téléservice THESEE. Nous vous présentons les informations à connaître. En savoir plus ici.

Fraude à la carte bancaire

En consultant vos comptes, si vous constatez qu'un paiement suspect a été réalisé avec votre carte bancaire, vous devez d'abord faire opposition sur votre carte au plus vite. Il est également conseillé de déclarer la fraude aux forces de l'ordre (police ou gendarmerie). Vous devez ensuite contacter votre banque pour vous faire rembourser la somme concernée. Se renseigner

Signaler une fraude à la carte bancaire (Perceval) (Démarche en ligne)

Ce service permet de signaler une fraude à la carte bancaire si vous remplissez les conditions suivantes :

- Vous êtes toujours en possession de votre carte bancaire
- Vous n'êtes pas à l'origine des achats en ligne
- Vous avez déjà fait opposition à la carte auprès de votre banque

Accéder à la démarche en ligne

Pré-plainte en ligne (Démarche en ligne)

Permet d'effectuer une pré-déclaration en ligne pour une atteinte aux biens (vol ou escroquerie par exemple) ou certains faits à caractère discriminatoire par un auteur inconnu.

Après la pré-déclaration en ligne, vous devez prendre rendez-vous au commissariat ou à la brigade de gendarmerie de votre choix pour signer la plainte. Accéder à la démarche

---

Les 11 arnaques aux applications de paiement à connaître

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Qu'il s'agisse de partager l'addition après une soirée ou d'envoyer de l'argent pour un cadeau, nous sommes de plus en plus nombreux à faire confiance aux applications de paiement comme Lydia, Cash App ou encore PayPal. C'est un moyen rapide et transparent d'effectuer des transactions financières. Les deux principales fonctions de ces applications étant de payer les autres et d'être payé. Deux actions particulièrement sensibles aux cyberattaques. Elles offrent ainsi quelques dispositifs de sécurité particuliers pour vous protéger comme le chiffrement, les verrous de sécurités, les notifications ou encore les désactivations de paiement à distance. Mais malheureusement, cela ne suffit pas vous pourriez subir l'une de ces 11 arnaques courantes :

· **Un faux service d'assistance :** Les escrocs des applications de paiement profitent souvent des utilisateurs en se faisant passer pour le service d'assistance. Or, ces services d'assistances ne vous demanderont jamais de fournir votre code d'accès ou votre code PIN, d'envoyer un paiement, de faire un achat, de télécharger une application pour un « accès à distance », ou d'effectuer une transaction « test » de quelque nature que ce soit. Si vous recevez un message qui semble provenir du support d'une application aller directement dans l'application pour le contacter, sans répondre au message.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

· **Des offres alléchantes :** L'une des arnaques les plus populaires est celle des escrocs qui proposent des biens ou des services coûteux – mais fictifs – en échange d'un paiement. Les paiements d'applications sont instantanés et ne peuvent généralement pas être annulés. N'oubliez pas que si quelque chose semble trop beau pour être vrai, il s'agit probablement d'une escroquerie.

· **Des dépôts aléatoires :** Un dépôt d'argent aléatoire est souvent utilisé pour endormir les utilisateurs et leur donner un sentiment de confiance envers les escrocs. Cependant, les escrocs peuvent vous envoyer un paiement « par accident » et vous demander de leur renvoyer le montant du paiement. Le montant que vous leur renvoyez provient des fonds de votre compte. Ces escrocs contestent le paiement auprès de leur banque ou de leur carte de crédit après que vous avez renvoyé les fonds. Cela signifie qu'ils seront remboursés à la fois par vous et par leur banque.

· **Un gain fictif :** Vous pouvez être contacté pour réclamer de fabuleux prix en espèces. Mais pour recevoir le prix, ils doivent d'abord envoyer de l'argent. Les applications de paiement ne demandent pas à leurs utilisateurs de payer pour les concours ou les promotions, donc les demandes d'envoi d'argent pour réclamer un prix sont probablement frauduleuses.

· **Une demande de numéro de sécurité sociale :** En général, il est préférable de ne communiquer votre numéro de sécurité sociale qu'à des sources de confiance et vous devriez éviter de communiquer des informations d'identité importantes aux demandeurs sur n'importe quelle application.

· **Des aides gouvernementales :** Certains escrocs peuvent promettre de l'argent sous la forme d'une subvention gouvernementale ou d'un programme d'aide. Mais toute demande d'informations financières est un signe révélateur d'une escroquerie.

· **Les « cash flippers » :** Les escrocs peuvent prétendre être en mesure de « retourner » les fonds des utilisateurs afin de gagner plus d'argent. L'escroquerie au cash flipping est conçue pour prendre l'argent des utilisateurs sans jamais leur donner de retour sur investissement.

· **De faux remboursements :** Si vous vendez quelque chose sur un marché en ligne, un escroc peut vous contacter en prétendant qu'il est intéressé par l'article et qu'il effectuera un paiement via une applications de paiement – sauf que vous ne recevrez pas l'argent et qu'il prétendra avoir envoyé le paiement plusieurs fois. Il exigera le remboursement de votre propre argent pour un article qu'il n'a jamais payé.

· **Une fausse histoire d'amour :** Si vous rencontrez quelqu'un sur une application de rencontre ou un réseau social et qu'il vous demande de lui envoyer de l'argent via une application de paiement, soyez extrêmement prudent. Si une personne que vous n'avez pas rencontrée en personne prétend avoir des intentions romantiques et vous demande de l'argent, soyez méfiant.

· **Un e-mail de phishing :** Les équipes de l'application ne vous demanderont jamais de fournir des informations de connexion ou n'utiliseront pas un langage menaçant dans leurs messages. Si vous recevez ce qui semble être un e-mail de phishing, vous devez contacter le support via l'application.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

· **De fausses alertes de sécurité :** Certains escrocs peuvent envoyer un e-mail frauduleux prétendant que votre compte a été compromis et que vos informations personnelles ont été divulguées. Les escrocs incluent souvent des liens vers de faux sites Web dans les e-mails qui vous invitent à modifier vos identifiants de connexion, mais cette astuce peut en fait voler vos informations de connexion existantes.

Vous l'aurez compris il existe de nombreuses manière d'accéder à vos données via les applications de paiement, assurez-vous d'en être conscient et d'avoir les bons réflexes.

Bastien Bobe, directeur technique Europe continentale chez Lookout