Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 27 juillet 2024

Besoin d'une vignette Crit'Air ? Méfiez-vous des arnaques !

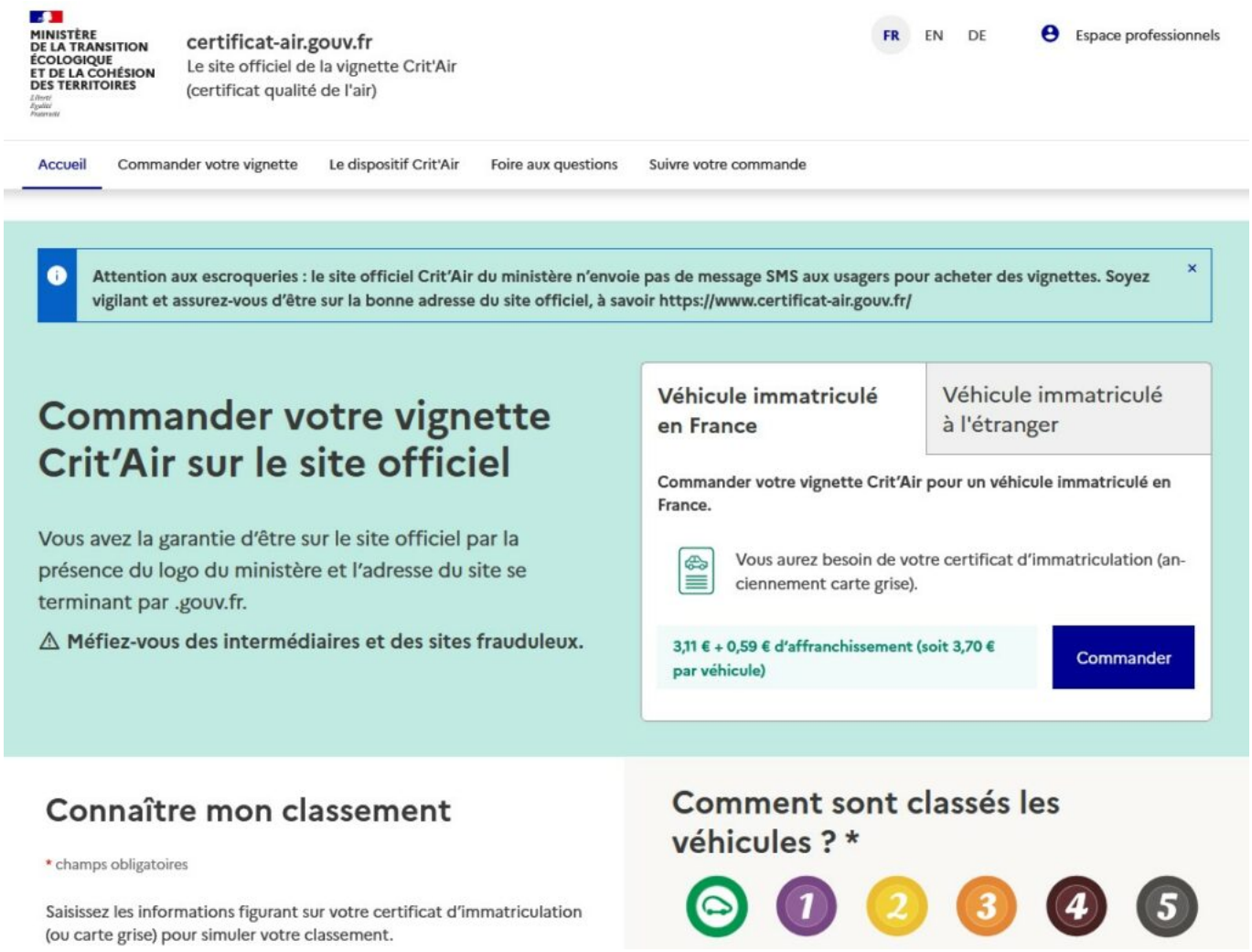
« Soyez sur vos gardes lors de l'achat de votre vignette Crit'Air », conseille Benoit Grunemwald, expert en cybersécurité chez Eset France.

Si vous conduisez votre propre véhicule dans certaines régions de France à certaines périodes, vous devrez acheter une vignette spéciale indiquant le taux d'émission d'une automobile, appelée *Crit'Air*, sous peine de recevoir une amende du gouvernement français. Des programmes similaires existent déjà au Royaume-Uni avec la zone à faibles émissions du centre de Londres, et la vignette qui prouve que vous avez payé est bien moins chère que l'amende.

Une recherche rapide sur Google vous permettra de trouver le site qui fournit les vignettes Crit'Air, ainsi que de nombreux autres sites indiquant que les vignettes sont obligatoires pour tous les véhicules entrant dans certaines régions de France. En accédant au site officiel de l'organisation (voir visuel si-dessous), qui est disponible en français, en anglais et en allemand, vous trouverez des informations sur le programme et le formulaire à compléter.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 27 juillet 2024



Attention au faux site Internet se faisant passer pour des sites officiels.

Ce site n'est absolument pas illicite ou illégitime, bien au contraire. Le problème réside plutôt dans le fait qu'il est extrêmement facile de créer un faux site, d'en faire la promotion et, grâce à des tactiques de référencement astucieuses, de le faire remonter dans le classement de Google. En fait, cette menace n'est pas que théorique et de nombreuses personnes ont rapporté avoir été arnaquées lors de l'achat de leur vignette Crit'Air sur des sites qui prétendaient représenter le gouvernement français

Pour compliquer encore les choses, la quantité de données demandées par le site légitime est plutôt importante, surtout pour un site dont vous n'avez peut-être jamais entendu parler, et qui plus est dans une autre langue.

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

Les vacanciers pressés de remplir un nouveau formulaire et disposant de peu d'endroits pour en vérifier

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 27 juillet 2024

l'authenticité pourraient finir par perdre leur argent ou leurs données. Les escrocs pourraient utiliser habilement cette tactique, surtout lorsque les gens peuvent considérer la vignette comme un désagrément mineur, mais nécessaire, avant de partir en vacances.

Méfiez-vous des imitations

Le site Web authentique indique : « Vous avez la garantie d'être sur le site officiel par la présence du logo du ministère et l'adresse du site se terminant par gouv.fr. Méfiez vous des intermédiaires et des sites frauduleux » Mais malheureusement, rien n'empêche un cybercriminel de copier le logo gouvernement et de changer le libellé pour l'adapter à n'importe quel préfixe qu'il choisit d'utiliser pour son faux site ? Ou d'utiliser des noms de domaine ressemblant www.certificat-air.gouv.fr.example.com ou des URL s'apparentant à exemple.com/www.certificat-air.gouv.fr, qui paraissent donc semblables à un site légitime aux yeux de personnes moins sensibilisées ou attentives ? Ou plus simplement encore, de supprimer ce petit bout de texte du site factice ?

Adobe-stock

En d'autres termes, en tant qu'escroc, il n'est pas nécessaire que vous réussissiez à tromper toutes les victimes possibles pour que votre site vous rapporte de l'argent rapidement et presque gratuitement. En outre, les informations sensibles sont souvent vendues sur le Dark web et d'autres canaux illicites et vous devez également être conscient des attaques secondaires par courrier électronique de phishing si vous avez rempli un formulaire potentiellement frauduleux.

Encore une fois, le problème ne réside pas dans le site Web de Crit'Air, mais dans le fait que les cybercriminels continuent de copier des sites authentiques et de diriger les gens vers des sites

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 27 juillet 2024

frauduleux afin de leur voler leurs données personnelles et précieuses qui se trouvent juste sous leurs doigts. De plus, les personnes qui ont utilisé ces sites frauduleux pour obtenir ce qu'ils croient être une licence légitime pourraient être passibles d'une amende en France, même si elles ignoraient qu'il s'agit d'une escroquerie.

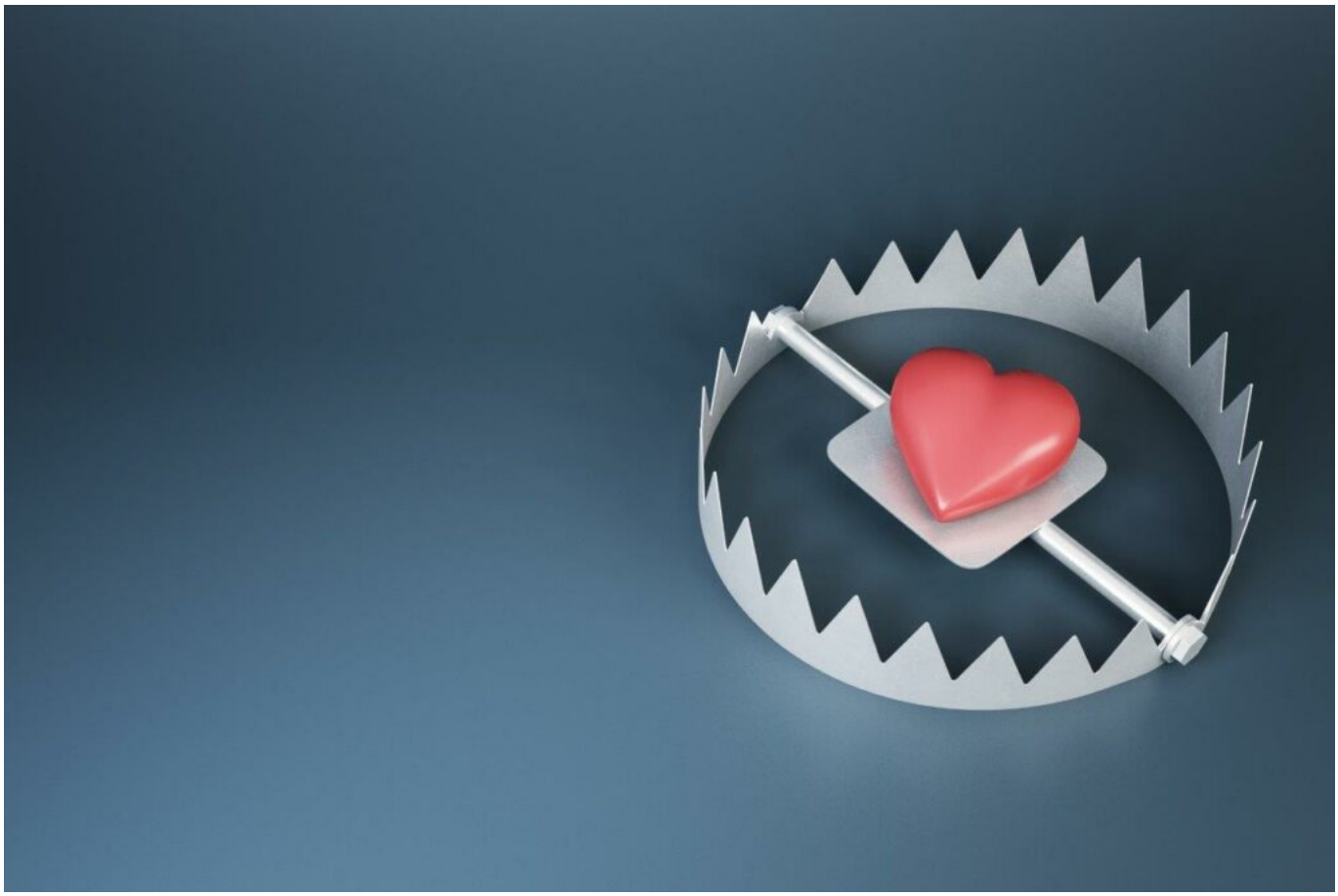
Comment obtenir votre vignette Crit'Air en toute sécurité ?
Comme les cybercriminels saisissent la moindre occasion de voler des données et de l'argent, vous devez être très prudent avant de soumettre vos informations personnelles et financières sur un site Web, surtout si vous visitez un site Web pour la première fois. Dans ce cas précis, il est probablement préférable de taper l'URL à la main, et de veiller à la taper correctement : *certificat-air.gouv.fr*.

Benoit Grunemwald, expert en cybersécurité chez Eset France

Escroqueries amoureuses, restez vigilants sur les plateformes de rencontre

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 27 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 27 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 27 juillet 2024

qui pourraient être utilisées à mauvais escient et restez vigilant.

Benoit Grunemwald, expert en cybersécurité chez Eset France