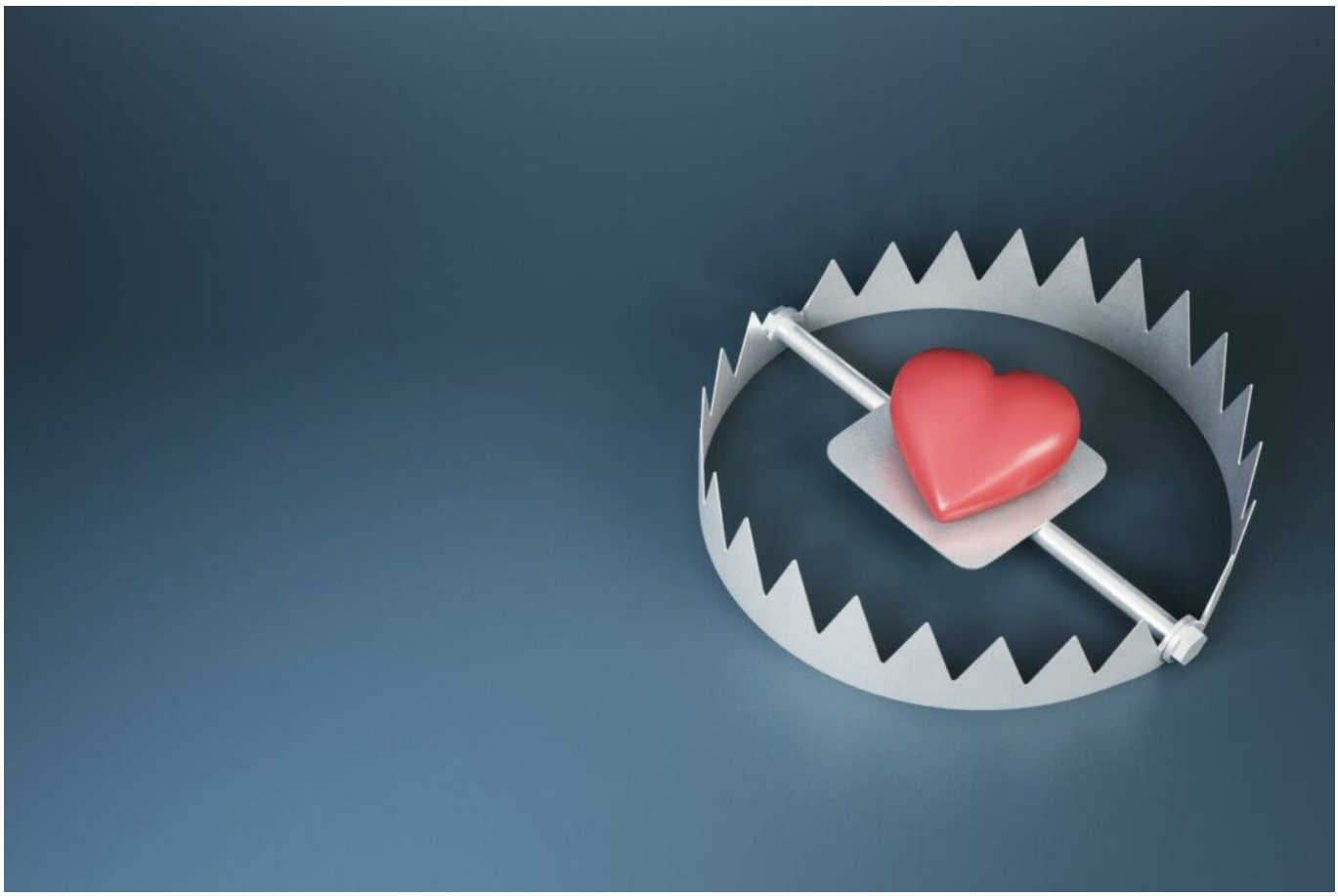
Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

Escroqueries amoureuses, restez vigilants sur les plateformes de rencontre



« 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

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

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 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

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

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 qui pourraient être utilisées à mauvais escient et restez vigilant.

Benoit Grunemwald, expert en cybersécurité chez Eset France

Saint-Valentin : attention aux cyber-arnaques

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

Avec la Saint-Valentin, les amoureux du monde entier s'efforceront de trouver la meilleure façon de témoigner leurs sentiments. Mais en parallèle, les cybercriminels sembleront également être gagnés par l'esprit de cette journée.

« Comme chaque année, le 14 février, les amoureux célèbreront l'amour à travers le monde,explique Hervé Liotaud, vice-président Europe de l'Ouest chez Sailpoint société spécialisée dans gestion des identités et des accès numérique. Mais ce ne sont pas les seuls pour qui ce jour sera une fête. Les cyber-criminels savent aussi en profiter. Arnaques sur les sites de rencontre, ransomwares, usurpation d'identité, piège au colis… Toutes les techniques seront bonnes pour atteindre leur cible. »

La Saint Valentin : proie des hackers

« En principe, il n'est pas surprenant que les cyber-criminels exploitent des évènements spéciaux tels que des vacances ou des fêtes. Une large cible d'attaque s'ouvre toujours pour des pirates lorsque de nombreuses personnes s'intéressent en même temps à un sujet particulier, et deviennent donc vulnérables. La bonne nouvelle est que les consommateurs ne sont pas sans défense contre ce type d'attaque. »

Des attaques ciblées

« Les précédentes Saint-Valentin ont été fortement marquées par le nombre d'attaques de 'credential stuffing' (vol d'identifiants pour accéder à d'autres comptes) sur les sites de rencontre, dans lesquels des comptes utilisateurs ont été compromis. Les criminels créent régulièrement de faux profils d'utilisateurs avec de faux messages romantiques afin de cibler des personnes seules puis les incitent à leur transférer de l'argent. Chaque année, nous voyons aussi se multiplier les faux sites en ligne proposant une fausse liste de cadeaux mais une escroquerie bien réelle. Cette méthode frauduleuse est particulièrement rentable. Or cette année, une grande part des achats de cadeaux s'effectuera en ligne, les sites marchands en ligne sont d'autant plus susceptibles d'être la cible des cyberattaques. »

Comment s'en protéger ?

« Il est évidemment possible d'appliquer des mesures de sécurité pour atténuer les menaces qui pèsent sur la Saint-Valentin pour protéger les utilisateurs et leurs identités digitales contre ces attaques :

Méfiance lors des achats en ligne : il est primordial de ne faire confiance qu'à des fournisseurs connus et vérifiés, et d'accorder une attention particulière à leur professionnalisme. Ceci inclut, par exemple, la vérification du nom de domaine du site – beaucoup d'acteurs malveillants créent des plates-formes usurpant des noms d'enseignes bien connus, mais ajoutent parfois à la fin « .fr.com » au lieu de simplement « .fr ». Pour s'assurer d'un site authentique, il faut éviter de cliquer directement sur un lien de promotion mais plutôt rechercher la boutique en ligne recherchée sur Google.

Des méthodes de paiement complexes doivent aussi éveiller l'attention : si le paiement doit obligatoirement être fait à l'avance, ceci peut remettre en question le sérieux du site. Des conditions générales de vente très mal traduites et une impossibilité d'impression doivent également alerter les consommateurs, et les inciter à ne pas acheter.

Concernant l'usage des sites de rencontres : les utilisateurs doivent limiter leurs visites à des sites

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 novembre 2024

reconnus, et toujours garder à l'esprit que les cyber-criminels les utilisent aussi. En conséquence, lors des communications avec d'autres utilisateurs, il est essentiel de s'assurer qu'ils possèdent un compte valide.

Les informations sensibles doivent rester secrètes : Il est également crucial d'éviter de partager des données personnelles et sensibles en ligne, telles que son adresse, des informations financières ou d'autres données d'identification personnelle. Ce sujet nécessite une attention particulière, car c'est précisément ce type d'informations qui vaut son pesant d'or pour les pirates – si un utilisateur sollicite explicitement ce genre de données, il s'agit d'un important signal d'alerte et toute communication doit être interrompue.

Savoir qui a accès à quoi : Dans le monde de l'entreprises si vous n'avez pas le contrôle ni la visibilité de savoir qui a accès à quoi au sein de votre système d'information …vous êtes en grand danger. Seule une solution de gestion de vos identités peut y remédier. »

« Cette année encore, la Saint Valentin promet d'être une occasion lucrative pour des cyber criminels qui exploiteront le désespoir des personnes seules, tout comme l'envie de faire plaisir des personnes en couple. Les menaces sont tout aussi importantes de part et d'autre. Toutefois, si les utilisateurs sont conscients des dangers et restent attentifs à certains points et signaux d'alerte qui révèlent de potentielles actions frauduleuses, ces attaques resteront vaines et les identités digitales seront saines et sauves. »