Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Avignon : la CPME 84 organise un petit-déjeuner sur le thème de la cybersécurité

Le mercredi 24 mai, de 8h à 10h30, vous pourrez participer au petit-déjeuner organisé par la CPME 84, en partenariat avec l'opérateur orange, sur le thème « Cybersécurité : comment protéger ses données ? ».

La CPME 84
La CPME 84 est la première organisation patronale du Vaucluse dédiée spécifiquement aux TPE-PME, commerçants, indépendants et professions libérales du département.

Le sujet
Les enjeux, les menaces et les solutions qui seront évoqués tourneront autour de la nécessité de comprendre le contexte actuel dans les entreprises vis-à-vis des cybermenaces. Il s'agira d'apprendre à identifier les cybermenaces récurrentes pour mieux les appréhender et les éviter. Pareillement, il sera question des réflexes et des actions à mettre en place pour minimiser les risques.

Cet évènement sera animé par Rémy Martin, responsable du développement propme grand sud-est Orange. Cette rencontre sera suivie d'une visite des locaux de l'opérateur historique Orange.

À savoir
De 8h30 à 10h30. 24 mai. Parking gratuit sur site. Avenue de la croix rouge. Avignon. Inscription définitive via l'e-mail contact@cpme84.org . 04 90 14 90 90.

J.G

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

« Une nuit pour hacker » : la compétition en cybersécurité organisée par la CCI de Vaucluse

Le pôle ingénierie informatique du campus de la CCI de Vaucluse organise une capture de drapeau numérique la nuit du 31 mars au 1er avril. Près de 80 joueurs sont attendus.

Au programme de cette nuit pour hacker, deux compétitions se dérouleront en parallèle. Une première épreuve sera organisée pour les amateurs et pour les informaticiens non spécialistes de la cyber, avec présentation, mise en situation et découverte des compétences nécessaires en cybersécurité. Une compétition taillée sur mesure pour les débutants grâce aux apprentis en 2e année de la formation cybersécurité de la CCI qui les accompagneront dans le processus de résolution.

La deuxième épreuve sera destinée aux professionnels déjà rôdés au milieu de la cybersécurité. Le niveau sera relevé et les défis tous inspirés de failles réelles. Osint, reverse, pawn, web, forensics seront de la

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

partie. Les professionnels en cybersécurité pourront lors de cet évènement, rencontrer, discuter et même challenger de potentiels futurs apprentis grâce à cette compétition.

De nombreux goodies seront à remporter, dont un Amiga500 min.

Vendredi 31 mars de 18h à 3h au campus de la CCI de Vaucluse, allée des Fenaisons, Avignon. Inscription en cliquant ici (nombre de places limitées).

J.R.

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

---

Protection des données à caractère personnel en entreprise

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Le samedi 28 janvier prochain aura lieu la journée européenne de la protection des données à caractère personnel. A cette occasion, Alexandre Cogné, expert cyber chez Ping Identity rappelle comment bien protéger ses données au sein d'une entreprise.

« La gestion de nos données personnelles sous-entend automatiquement une notion de consentement mais à quel moment la traiter et comment la faire perdurer ?, interroge Alexandre Cogné, expert cyber chez Ping Identity, société américaine présente dans le monde entier spécialisée dans la cyber-sécurité des entreprises. Pour les entreprises, en interne, la question doit être abordée lors de la signature du contrat de travail. Saviez-vous que les employés placent leurs données personnelles sous la responsabilité de leur employeur ? La gestion des identités au sein même de l'entreprise est alors un problème qui fait l'objet d'une situation dont les bases doivent être claires et connues de tous. »

Les bonnes pratiques RGPD

« Du côté du consommateur, songez au SIAM (Service integration and management). C'est un outil qui permet aux services IT de multiplier les fournisseurs en articulant rendement et efficacité. Les gestionnaires des identités s'appuient sur un profil utilisateur, c'est-à-dire sur une plateforme dont l'utilisateur a déjà accepté les conditions d'utilisation. Mais connaissez-vous suffisamment les bonnes pratiques RGPD ? Les éditeurs sont automatiquement soumis à cette charte lorsque les données ont été saisies. La plupart des éditeurs vont ainsi faire signer cette dernière par la plateforme commerciale pour laquelle ils agissent. En renforçant la sécurité des accès ils contribuent à limiter toute fuite potentielle des données. Savez-vous si la charte a été signé au sein de votre entreprise ? Si ce n'est pas le cas il faudrait alors songer à changer de prestataire. »

La garantie des accès

« Si vous travaillez pour une plateforme de vente en ligne, les failles peuvent être de deux ordres : une vente volontaire des données et une cyberattaque. Êtes-vous en capacité d'apporter à vos utilisateurs toutes les garanties à la circulation de leurs données ? Si vous faites les bons choix, peu importe ! Dans la mesure où un éditeur de solution de gestion des identités va garantir chaque accès de manière très rigoureuse. Il contribuera à sécuriser le dispositif de gestion des données. Aujourd'hui la gestion des identités apporte un certain nombre de garanties en termes de respect des données privées mais connaissez-vous les solutions existantes ? Elles permettent d'identifier les risques, de les gérer et de limiter les fraudes. Les consommateurs et les entreprises en bénéficient vis-à-vis de leurs responsabilités mais aussi sur un aspect financier. »

Alexandre Cogné, expert cyber chez Ping Identity

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Protéger les avocats et les équipes juridiques contre les cyber-risques

Qu'ils fassent partie d'un cabinet d'avocats ou qu'ils soient juristes au sein d'une entreprise, les avocats traitent chaque jour des informations sensibles et sont susceptibles d'être la cible de cyberattaquants.

Les avocats ont des obligations éthiques et légales de protéger les données de leurs clients et de les signaler rapidement aux autorités compétentes ainsi qu'à leurs clients s'ils subissent une violation de données. Ils ont également un rôle essentiel à jouer à la suite d'une violation. Ce seul fait en fait des cibles prisées des cybercriminels.
Quels sont les cyber-risques auxquels les avocats sont alors confrontés ? Et de quelle manière les équipes informatiques et les cabinets d'avocats peuvent-ils protéger leurs clients et leurs organisations ?

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Des informations sensibles
Selon le domaine d'activité et le contexte, les avocats gèrent une grande variété d'informations sensibles et confidentielles. Les clients, les employés et leurs entreprises comptent sur le fait qu'elles restent en sécurité entre leurs mains. Les avocats spécialisés dans l'emploi peuvent traiter les Informations personnelles identifiables (IPI) de leurs clients, notamment les numéros de sécurité sociale, les numéros de permis de conduire, des informations bancaires, les dates de naissance ou encore les dossiers médicaux.

La cybermenace contre les équipes juridiques
Les avocats comprennent bien la valeur de la sécurité des informations. Elle est essentielle à la confidentialité qui rend possible le conseil juridique et la relation avocat-client. Cependant, avec des ressources informatiques parfois limitées, leur traitement d'informations sensibles et les failles de sécurité des logiciels juridiques, les équipes juridiques sont régulièrement sujettes aux cyberattaques.

Des failles de sécurité dans les technologies juridiques
Depuis plusieurs années, la technologie juridique (ou Legal Tech) facilite grandement leur quotidien, de la comptabilité à la facturation en passant par les communications avec les clients et la gestion des documents. La confiance et la confidentialité étant des éléments fondamentaux des pratiques juridiques, il est essentiel de disposer d'une technologie juridique sécurisée. La technologie juridique permet aux organisations de traiter plus rapidement les données, de réduire les erreurs administratives, de créer une transparence dans la facturation et de permettre aux équipes juridiques internationales de collaborer plus efficacement. Les logiciels de découverte électronique (ou eDiscovery) aident les avocats à trouver et à trier les documents et à se concentrer sur des tâches plus importantes.
Dans les grands cabinets d'avocats et les équipes juridiques internes, des professionnels de la sécurité disposant de moyens sont équipés pour gérer la sécurité de l'information et la technologie. Cependant, le fait de disposer de plus de moyens ne se traduit pas nécessairement par une diminution des attaques ou des violations, bien au contraire.

Le manque de temps favorise la praticité au détriment de la sécurité
Peu importe où et comment ils exercent, les avocats ont le devoir de protéger les informations de leurs clients. Cependant, les exigences en matière de productivité et d'heures facturables se heurtent souvent à la sécurité des informations d'une manière qui porte atteinte à la confidentialité. Bien qu'elle ne soit pas à proprement parler une cybermenace externe, la non-conformité comporte un risque important de litiges coûteux ou d'interruptions des activités. Heureusement des solutions existent. Une formation à la sécurité peut aider les avocats et le personnel non-juriste à reconnaître les vecteurs de menace et à instiller l'importance de la sécurité de l'information dans un cabinet axé sur le client.

Ces dernières années, des cyberattaques très médiatisées contre de grands cabinets d'avocats ont mis en évidence la menace omniprésente contre les avocats et les données sensibles. Il devient donc nécessaire de protéger les avocats et les données confidentielles qu'ils traitent au quotidien face aux cybermenaces. L'hygiène des mots de passe, par exemple, contribue grandement à atténuer le risque et l'impact des cybermenaces.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Arnaud De Backer – Channel Sales Manager EMEA – Chez Keeper Security

---

10 conseils pour vous protéger pendant vos vacances contre les cybermenaces

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, méfiez-vous des menaces lorsque vous utilisez un Wi-Fi public pour vous connecter à votre banque en ligne, boutique en ligne ou tout simplement pour vérifier vos e-mails.
Eset, spécialisé dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public, propose un guide pour vous permettre de voyager en toute sécurité et garder ainsi toutes vos données personnelles et vos appareils protégés.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

1. Avant de prendre la route, assurez-vous d'exécuter sur vos appareils une mise à jour complète du système d'exploitation ainsi que des logiciels, et de posséder une solution de sécurité de confiance.

2. Sauvegardez vos données et placez-les dans un endroit sûr. Pensez à déplacer les données sensibles du disque dur de votre ordinateur portable sur un disque dur externe chiffré le temps de vos vacances.

3. Ne laissez jamais vos appareils sans surveillance dans les lieux publics. Activez la fonction antivol de vos appareils pour tracer les appareils volés ou perdus, et au besoin d'effacer les contenus à distance.

4. Mettez un mot de passe fort et activez la fonction 'délai d'inactivité' sur tous vos appareils, que ce soit votre ordinateur portable, votre tablette ou votre téléphone. Retrouvez tous les conseils d'Eset pour un mot de passe efficace en cliquant ici.

5. Dans la mesure du possible, utilisez uniquement des accès internet de confiance. Demandez à votre hôtel ou l'endroit où vous logez le nom de leur Wi-Fi et utilisez exactement le même nom : faites attention aux arnaques qui essaient de ressembler aux Wi-Fi publics en ajoutant le mot « gratuit » au nom de la connexion Wi-Fi.

6. Si l'Internet de votre hôtel vous demande de mettre à jour un logiciel afin de pouvoir vous connecter, déconnectez-vous immédiatement et informez-en la réception.

7. Ne vous connectez pas à des connexions Wi-Fi qui ne sont pas chiffrées avec WPA2. Toutes les normes inférieures à celle-ci ne sont tout simplement pas assez sûres et peuvent être facilement piratées.

8. Si vous devez utiliser le Wi-Fi public pour vous connecter à votre réseau d'entreprise, utilisez toujours votre VPN (réseau virtuel privé).

9. Si ce n'est pas urgent, évitez les banques et boutiques en ligne quand vous utilisez le Wi-Fi public. Sinon, nous vous conseillons d'utiliser le partage de connexion de votre téléphone et de surfer en utilisant internet sur votre téléphone portable.

10. Si vous n'utilisez pas encore d'antivirus de confiance et suspectez votre ordinateur portable d'être infecté, vous pouvez utiliser gratuitement le scanner ESET Online qui ne nécessite aucune installation et peut être utilisé pour détecter et retirer des logiciels malveillants.

CCI Vaucluse : informer sur les risques

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

d’insécurité matérielle et informatique

Ce vendredi 20 mai, la Chambre de commerce et d’industrie (CCI) de Vaucluse organise une réunion d’information en partenariat avec la Gendarmerie Nationale. Ce rendez-vous, adressé aux entreprises de tous secteurs et aux collectivités, aura pour thème ‘L’environnement sécuritaire des entreprises et des collectivités’.

L’objectif de cette réunion est de faire de la prévention concernant les risques d’insécurité matérielle et informatique. Au programme : le principe de base de sécurisation, la protection des bâtiments et de l’environnement, ou encore les principes fondamentaux en matière de lutte contre les cyber-menaces.

Pour s’inscrire à cette réunion gratuite, il suffit de remplir le formulaire en ligne.

Vendredi 20 mai. De 8h30 à 10h30. CCI Vaucluse. 46 cours Jean Jaurès. Avignon.

V.A.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

Scannez avec prudence, les arnaques aux QR codes fleurissent

Les QR codes font fureur et les escrocs l'ont remarqué. « Méfiez-vous de ces petits carrés noirs et blancs », prévient Benoit Grunemwald, expert en cybersécurité chez Eset France.

Les QR codes ont le vent en poupe. Ces modestes carrés existent peut-être depuis 1994, mais ils sont réellement devenus célèbres depuis la crise du Covid-19. Aujourd'hui, vous pouvez les apercevoir partout, les codes étant utilisés pour l'affichage des menus de restaurants jusqu'aux transactions sans contact en passant par des applications de partage de contacts.
Toutefois, comme toute autre technologie courante, l'utilisation généralisée des QR codes a également attiré l'attention des escrocs, à des fins criminelles. Cette tendance a même suscité une alerte de la part

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

du FBI (Federal bureau of investigation) aux États-Unis. Comment les fraudeurs utilisent-ils les codes à des fins illicites ?

Qu'est-ce qu'un QR code et comment fonctionne-t-il ?
Abréviation de 'Quick response', un QR code est un type de code-barres interprétable par une machine instantanément. Un QR code peut contenir jusqu'à 4 296 caractères alphanumériques, ce qui permet un décodage facile par l'appareil photo d'un smartphone.
Les chaînes de texte qui sont codées dans un QR code peuvent contenir une variété de données. L'action déclenchée par la lecture d'un QR code dépend de l'application qui interagit avec ledit code. Les codes peuvent être utilisés pour naviguer vers un site web, télécharger un fichier, ajouter un contact, se connecter à un réseau Wi-Fi et même effectuer des paiements. Les QR codes sont très polyvalents et peuvent être personnalisés pour inclure des logos. Les versions dynamiques des QR codes vous permettent même de modifier le contenu ou l'action à tout moment. Cette polyvalence peut toutefois être une arme à double tranchant.

Comment les QR codes peuvent être exploités ?
Le grand nombre de cas d'utilisation des QR codes (et le potentiel d'utilisation abusive) n'échappe pas aux fraudeurs. Voici comment les cybercriminels peuvent détourner les codes pour voler vos données et votre argent :

1. **Redirection vers un site web malveillant pour voler des informations sensibles :** Les attaques d'hameçonnage ne se propagent pas uniquement par e-mails, des messages instantanés ou des SMS. Tout comme les attaquants peuvent utiliser des publicités malveillantes et d'autres techniques pour vous diriger vers des sites frauduleux, ils peuvent faire de même avec les codes QR.

2. **Téléchargement d'un fichier malveillant sur votre appareil :** De nombreux bars et restaurants utilisent des QR codes pour télécharger un menu au format PDF ou installer une application vous permettant de passer une commande. Les attaquants peuvent facilement falsifier le QR code pour vous inciter à télécharger un fichier PDF malveillant ou une application mobile malveillante.

3. **Déclencher des actions sur votre appareil :** Les QR codes peuvent déclencher des actions directement sur votre appareil, ces actions dépendant de l'application qui les lit. Cependant, il existe certaines actions de base que tout lecteur QR est capable d'interpréter. Il s'agit notamment de la connexion de l'appareil à un réseau Wi-Fi, de l'envoi d'un e-mail ou d'un SMS avec un texte prédéfini, ou de l'enregistrement des informations de contact sur votre appareil. Bien que ces actions ne soient pas malveillantes en soi, elles peuvent être utilisées pour connecter un appareil à un réseau compromis ou envoyer des messages en votre nom.

4. **Détourner un paiement :** La plupart des applications financières permettent aujourd'hui d'effectuer des paiements au moyen de codes QR contenant des données appartenant au destinataire de l'argent. De nombreux magasins vous affichent ces codes pour ainsi faciliter la transaction. Cependant, un attaquant pourrait modifier ce QR avec ses propres données et recevoir des paiements sur son compte. Il pourrait également générer des codes avec des demandes de collecte d'argent pour vous

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

tromper.

5. Voler votre identité : De nombreux QR codes sont utilisés comme certificat pour vérifier vos informations, comme votre carte d'identité ou votre carnet de vaccination. Dans ces cas, les QR codes peuvent contenir des informations aussi sensibles que celles contenues dans votre pièce d'identité ou votre dossier médical, qu'un attaquant pourrait facilement obtenir en scannant le QR code.

Nous avons adopté les QR codes dans notre vie quotidienne. Et comme avec toutes les nouvelles pratiques, il nous faut prendre de nouvelles habitudes pour rester vigilants. Chaque nouvelle technologie amène son lot d'avantages mais aussi de menaces.

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 juillet 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 Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

« 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 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

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 22 juillet 2024

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. »