Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 17 avril 2025

Escroquerie bancaire par spoofing téléphonique : la cour de cassation dédouane le client

Maître Lionel Fouquet nous rappelle que dans une décision du 23 octobre 2024 (pourvoi n° 23-16.267), la Cour de cassation vient préciser de nouvelles règles dans les relations banque / client lorsque celui-ci est victime de spoofing* téléphonique.

Pour mémoire, le spoofing est une escroquerie malheureusement très courante : un faux conseiller bancaire parvient lors d'un appel téléphonique à convaincre une personne de lui remettre ses codes d'accès ou effectuer un virement à son profit.

La Cour indique :

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 17 avril 2025

« Après avoir exactement énoncé qu'il incombe au prestataire de services de paiement de rapporter la preuve d'une négligence grave de son client, l'arrêt constate que le numéro d'appel apparaissant sur le téléphone portable de M. [J] s'était affiché comme étant celui de Mme [Y], sa conseillère BNP et retient qu'il croyait être en relation avec une salariée de la banque lors du réenregistrement et nouvelle validation qu'elle sollicitait de bénéficiaires de virement sur son compte qu'il connaissait et qu'il a cru valider l'opération litigieuse sur son application dont la banque assurait qu'il s'agissait d'une opération sécurisée. Il ajoute que le mode opératoire par l'utilisation du « spoofing » a mis M. [J] en confiance et a diminué sa vigilance, inférieure, face à un appel téléphonique émanant prétendument de sa banque pour lui faire part du piratage de son compte, à celle d'une personne réceptionnant un courriel, laquelle aurait pu disposer de davantage de temps pour s'apercevoir d'éventuelles anomalies révélatrices de son origine frauduleuse. »

Après avoir rappelé qu'il appartient à la banque de prouver la négligence grave de son client, la Cour considère donc que le client qui se fait piéger au téléphone par un faux conseiller bancaire ne peut se voir reprocher par sa banque d'avoir commis une négligence grave. Il a donc le droit d'être remboursé par sa banque des virements frauduleux.

*** Qu'est-ce que le spoofing ?**
Le spoofing regroupe l'ensemble des cyberattaques qui consiste dans le vol de l'identité électronique telle que l'adresse mail, le nom de domaine ou l'adresse IP; et a pour but, le plus souvent, d'obtenir des informations bancaires et confidentielles.

---

5 conseils pour voyager en toute sécurité cet été

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 17 avril 2025

Les vacances d'été font de vous la proie idéale des hackers. Évitez cette fâcheuse situation grâce à ces 5 conseils de cybersécurité.

Les voyages d'été approchent et vous planifiez vos vacances bien méritées ? De simples actions telles que l'utilisation du Wi-Fi public dans les aéroports, les hôtels ou les lieux touristiques peuvent rendre vos appareils vulnérables au piratage et compromettre votre cyber-identité. Pour vous aider à protéger votre identité, vos données financières, vos documents sensibles et vos mots de passe, voici 5 bonnes pratiques en matière de cybersécurité à adopter cet été.

1. Limitez les messages sur les réseaux sociaux qui mentionnent votre destination

Les posts sur les réseaux sociaux sont devenus l'activité préférée des voyageurs. Cependant, il peut être dangereux de publier des messages pendant que vous voyagez et de divulguer votre position exacte alors que vous êtes encore sur place. Une fois que votre position est exposée publiquement, n'importe quel acteur malveillant peut vous prendre pour cible. Bien que cela puisse sembler improbable en tant que touriste, les locaux qui connaissent mieux votre environnement auront plus de facilité à vous localiser que vous ne le pensez. Si vous êtes toujours tenté de publier, attendez d'avoir déménagé dans une nouvelle destination ou mieux encore, le moment où vous serez rentré chez vous.

2. Évitez les réseaux Wi-Fi publics

Bien qu'il puisse être difficile de trouver un réseau Wi-Fi fiable lors d'un voyage, il vaut mieux être en sécurité que dangereusement connecté aux réseaux Wi-Fi publics. Les attaquants peuvent utiliser ce que

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 17 avril 2025

l'on appelle une attaque de type « man-in-the-middle » (MITM) lorsque votre appareil est connecté à un réseau Wi-Fi public, ce qui permet aux hackers d'accéder à votre navigateur ou à votre application et de récupérer vos données stockées. En règle générale, les réseaux Wi-Fi publics doivent toujours être évités.

3. Envisagez d'utiliser un VPN

Lorsque vous voyagez, l'utilisation d'un réseau privé virtuel (VPN) vous permet de rester protégé lorsque vous vous connectez depuis n'importe quel endroit. Non seulement un VPN vous permet d'éviter la limite de bande passante, mais il protège également votre identité en ligne et sécurise votre connexion depuis n'importe quel endroit, même si vous vous trouvez sur un tout autre continent.

4. Téléchargez les documents importants pour les sauvegarder

Voyager vers des destinations et des attractions touristiques nouvelles et inconnues peut être chaotique, ce qui augmente le risque de vol ou d'égarement d'effets personnels importants (passeports, visas, dossiers médicaux, etc.). En téléchargeant des copies de ces documents importants contenant des informations très sensibles vers un gestionnaire de mots de passe sécurisé, vous disposerez de copies numériques de sauvegarde en cas de perte ou de vol.

5. Partagez en toute sécurité des informations d'urgence avec une source de confiance

Pendant vos vacances, renforcez votre sécurité en partageant des informations importantes avec des membres de votre famille ou des amis de confiance, afin qu'ils puissent y accéder en cas d'urgence. Utilisez un service chiffré pour partager en toute sécurité des informations d'assurance ou des documents d'identité, comme votre passeport, pour une durée limitée. Ainsi, en cas d'urgence médicale ou autre, il pourra vous aider sans que des informations sensibles soient exposées par mail, SMS ou messagerie, même à l'autre bout du monde.

Arnaud De Backer, Channel Sales Manager EMEA, Chez Keeper Security.