

Fléau du phishing bancaire par sms : Sumeria lance la révolution de l'authentification sécurisée sans sms

Face à la hausse constante de la fraude par SMS (ou « smishing »), Sumeria innove une fois de plus pour sécuriser ses clients en lançant l'authentification silencieuse, une solution qui remplace l'envoi de codes d'authentification sensibles par SMS. Une première pour un établissement bancaire dans l'Union Européenne réalisée en collaboration avec Vonage.

Les mécanismes de fraude par SMS : un phénomène en pleine expansion

Bien qu'il soit censé sécuriser les échanges, le SMS est devenu la cible privilégiée des fraudeurs, qui exploitent la confiance de leurs cibles pour détourner leurs données sensibles. Voici les principaux cas recensés :

1. **Usurpation d'identité** : les fraudeurs envoient de faux SMS aux couleurs de la banque ou d'autres organismes pour obtenir les identifiants et mots de passe des victimes.
2. **Code 2FA récupéré par téléphone** : en possession du premier facteur (identifiants), ils appellent la victime en se faisant passer pour un « service fraude » et lui soutirent le code SMS.
3. **Fenêtre sur le phénomène des « mules »** : recrutées via les réseaux sociaux, ces personnes partagent leur code SMS d'accès au compte, ignorant les risques légaux et financiers encourus.

L'authentification silencieuse : une avancée majeure

Depuis octobre, Sumeria a déployé une **méthode d'authentification silencieuse**, fruit d'une collaboration avec la société Vonage en interaction avec les opérateurs téléphoniques :

Validation automatique par opérateur :

- Lors de la création ou vérification de compte, notre partenaire Vonage sollicite les opérateurs téléphoniques pour confirmer la validité de la carte SIM et de l'appareil.
- Sans action requise, l'opérateur certifie que le numéro est bien utilisé par le propriétaire légitime.

Résultat : une sécurité accrue, sans effort client :

- Il n'y a plus de code 2FA à communiquer, neutralisant ainsi la majorité des scénarios d'ingénierie sociale.
- Le parcours de souscription n'est plus interrompu par l'envoi et la saisie d'un code SMS.

Lutte contre la fraude : l'innovation pour tous

Quelques mois après l'appel certifié, Sumeria franchit une nouvelle étape pour protéger ses clients. Selon des estimations, les tentatives de phishing par SMS ont augmenté de 40 %* en 2023, et près de 40 % des Français auraient été exposés à ce type d'attaque. Cette nouvelle innovation s'inscrit dans l'engagement continu de Sumeria à fournir une expérience bancaire plus sûre et plus simple.

“La fraude bancaire est un véritable fléau qui touche ou menace tous les Français. Être toujours à l'avant-garde de la lutte contre ce fléau par l'exploitation rapide et continue des possibilités offertes par les dernières technologies est pour nous un devoir moral autant qu'un choix stratégique de différenciation dans un secteur bancaire où il faut souvent plusieurs années pour mettre en oeuvre une nouvelle technologie” indique Cyril Chiche, Président de Lydia Solutions.

À propos de Lydia Solutions

Fondée en 2011, Lydia Solutions est l'entreprise française derrière les services Lydia (application de paiement et de cagnottes) et Sumeria (application de services bancaires pour les particuliers, notamment un compte courant rémunéré).

Avec ses 250 collaborateurs basés à Paris, Nantes, Bordeaux et Lyon, Lydia Solutions s'est fixée pour mission de changer les codes de la banque avec une approche essentialiste qui vise l'épanouissement de ses clients.

Acteur majeur du secteur de la finance technologique tricolore, listée dans le FT120, l'entreprise est soutenue par des investisseurs internationaux tels que Accel, Tencent, XAnge, New Alpha, Groupe Duval et Founders Future, auprès desquels elle a levé 235 M€.

Éléments presse

presse@lydia-app.com - <https://sumeria.eu/a-propos/presse>

*Rapport Kaspersky sur le spamming et le phishing 2023:

<https://www.kaspersky.com/about/press-releases/kaspersky-reports-phishing-attacks-grow-by-40-percent-in-2023>