L'ECONOMISTE

Le Cercle des Experts

Fuite des données de cartes bancaires au Maroc: Décrypter la réalité

Par Hicham FAIK | Edition N°:6979 Le 27/03/2025 |

Hicham Faik est un expert international en cybersécurité et confiance numérique reconnu avec plus de 25 ans d'expérience. Certifié CISSP, CISM, ISO27001/27005…
Hicham Faik a occupé des postes stratégiques dans les secteurs de l'énergie, l'assurance et la banque. Il a mis en œuvre la stratégie globale de cybersécurité d'un grand groupe bancaire de 2017 à 2022.
En 2023, il fonde CybrForge, entreprise spécialisée en cybersécurité

■ Retour sur les faits: de l'alerte à la clarification

En mars 2025, une alerte lancée par la startup Cypherleak a suscité une vive inquiétude au Maroc, suite à la diffusion d'informations sur une fuite massive présumée de données bancaires sur le Dark Web. Selon cette alerte, plus de 31.000 numéros de cartes marocaines circulaient clandestinement, dont 5.523 encore valides, potentiellement exploitables pour des fraudes.

L'information, relayée rapidement par les médias et les réseaux sociaux, a généré confusion et inquiétude parmi les utilisateurs des systèmes de paiement électronique au Maroc. Toutefois, des précisions ultérieures ont montré que ces données provenaient principalement de fuites anciennes et non d'un piratage récent des banques marocaines. Comment cette confusion est-elle survenue, et quelles leçons en tirer pour mieux comprendre le phénomène mondial de la fraude à la carte bancaire?

Cette annonce, jugée alarmiste par certains observateurs, a immédiatement capté l'attention des médias, alimentant une perception de menace directe contre les banques marocaines. Face à l'émoi suscité, cette startup a publié le 20 mars un communiqué additionnel pour rectifier son propos initial, expliquant qu'il ne s'agissait en réalité pas d'une fuite récente mais d'une compilation historique de données volées à travers divers canaux et périodes. Cette clarification essentielle a permis de mieux contextualiser l'événement, soulignant qu'aucune compromission active des systèmes bancaires marocains n'avait eu lieu à ce moment précis.

■ Le piège de l'information mal contextualisée

L'affaire de fuite des numéros de cartes bancaires a révélé les risques liés à la diffusion rapide et non vérifiée d'informations sensibles. L'effet d'annonce initial a provoqué une panique injustifiée, fragilisant momentanément la confiance envers les systèmes de paiement électronique.

Une communication responsable, claire et contextualisée s'impose donc désormais comme une nécessité absolue, surtout dans les questions sensibles de sécurité financière.

L'affaire de fuite des numéros de cartes bancaires a révélé les risques liés à la diffusion rapide et non vérifiée d'informations sensibles. Une communication responsable, claire et contextualisée s'impose donc désormais comme une nécessité absolue, surtout dans les questions sensibles de sécurité financière (Ph. Privée)

■ Un phénomène mondial, le Maroc loin d'être un cas isolé

Selon le Data Breach Investigations Report de Verizon (2024), plus de 90% des données bancaires compromises à l'échelle mondiale proviennent d'attaques indirectes, ciblant des utilisateurs finaux ou des commerçants en ligne, et non directement les banques elles-mêmes. En 2023 seulement, Verizon recensait plus de 5.000 fuites de données confirmées impliquant des informations de paiement, avec 37% de ces cas dans le commerce de détail. Europol souligne également l'existence d'un marché noir international dynamique, où des millions de numéros de cartes circulent constamment, alimentés par les mêmes techniques observées au Maroc.

Ces statistiques mondiales permettent de relativiser l'événement marocain: loin d'être exceptionnel, il illustre une tendance globale à laquelle aucun pays n'échappe.

Ainsi, la fuite de données personnelles et confidentielles représente aujourd'hui un défi planétaire qui dépasse largement le seul cadre bancaire. Partout dans le monde, les entreprises, les administrations et les citoyens sont confrontés à cette menace constante, nécessitant une sensibilisation accrue et une vigilance permanente à tous les niveaux.

■ Sécurité bancaire au Maroc: robustesse et axes d'amélioration

Les banques marocaines appliquent rigoureusement les normes internationales (PCI DSS), ainsi que les directives de sécurité de Bank Al-Maghrib et de la DGSSI, et respectent scrupuleusement les lois nationales (loi 05/20 et loi 09/08). Elles disposent de mécanismes performants pour détecter rapidement et neutraliser les risques liés aux données compromises. Toutefois, une plus grande réactivité et une meilleure communication proactive, notamment en direction des commerçants, pourraient encore renforcer cette robustesse.

Origines des fuites des données bancaires

Trois méthodes principales expliquent la compromission des données bancaires, elles restent universelles et nécessitent une vigilance continue:

- ✓ **Phishing (hameçonnage):** Courriels et SMS frauduleux incitant les victimes à divulguer leurs informations personnelles.
- ✓ **Maliciels (info-stealers):** Virus informatiques volant discrètement les données bancaires depuis les appareils infectés (près de 26 millions d'appareils infectés entre 2022-2024 selon Kaspersky).
- ✓ • **Web skimming (Magecart):** Techniques de piratage des formulaires de paiement en ligne représentant 57% des vols de données bancaires en ligne selon Verizon.

■ Vers une cybersécurité collective

Il est important de souligner que les banques marocaines déploient en permanence des efforts considérables, en recourant aux technologies les plus avancées, pour sécuriser les transactions et protéger efficacement leurs clients contre les menaces cybernétiques. Pour réduire davantage les risques de fraude, une communication transparente, des pratiques de sécurité rigoureuses et une vigilance accrue à tous les niveaux restent indispensables.

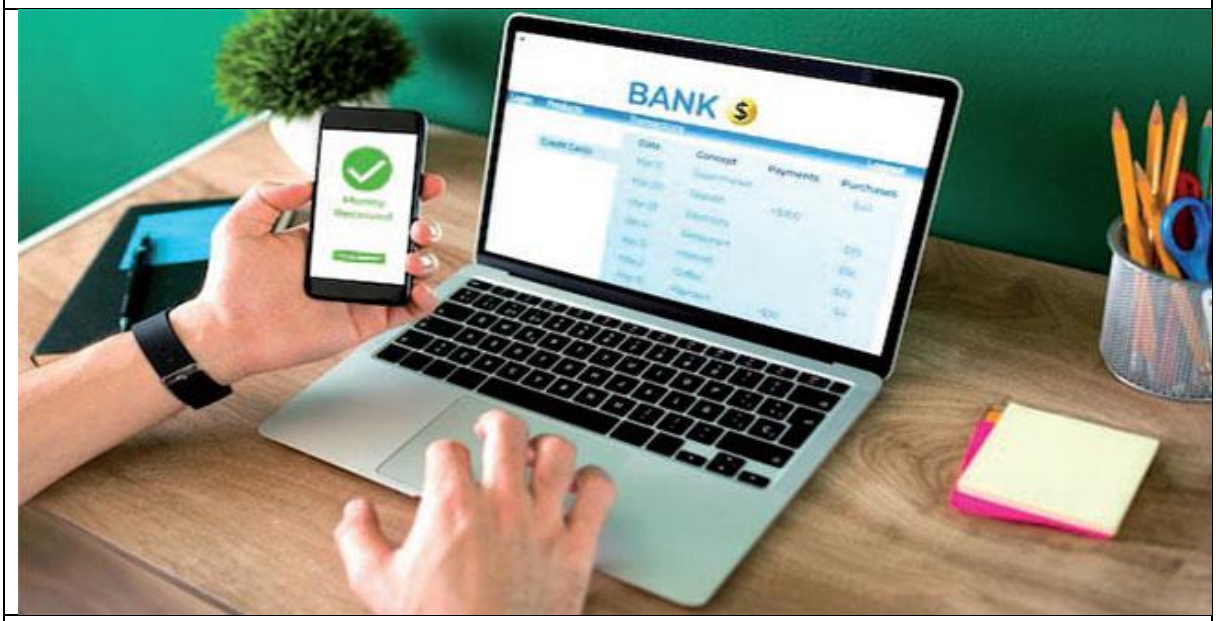
La cybersécurité est ainsi une responsabilité collective et permanente impliquant banques, commerçants, médias et consommateurs. En adoptant ensemble une posture proactive, chacun peut contribuer à préserver durablement la confiance envers les systèmes de paiement modernes.

Propositions et perspectives pour les banques

Pour mieux anticiper et gérer les fraudes, plusieurs mesures innovantes pourraient être adoptées:

- ✓ Développer des systèmes permettant aux banques de notifier immédiatement les commerçants lors de transactions potentiellement frauduleuses, afin d'avertir discrètement les clients concernés.
- ✓ Encourager l'utilisation systématique des cartes virtuelles temporaires pour les transactions en ligne.
- ✓ Généraliser l'authentification multi-factorielle mobile (Push-to-authenticate) des paiements sensibles via les applications mobiles bancaires.
- ✓ Contrôle dynamique et personnalisé des cartes en permettant aux utilisateurs de bloquer temporairement certaines opérations à risque (achats en ligne, internationaux).
- ✓ Mettre en place des services bancaires automatisés pour surveiller en continu et alerter rapidement les clients en cas de fuite de leurs informations.

Recommandations pratiques



Les détenteurs de cartes doivent adopter des pratiques sécurisées simples pour mieux se protéger:

- ✓ Vérifier régulièrement vos relevés bancaires et signaler immédiatement toute anomalie
- ✓ Ne jamais communiquer vos informations bancaires (numéros de carte, CVV, codes PIN)
- ✓ Utiliser exclusivement des sites web sécurisés (HTTPS) pour les achats en ligne
- ✓ Activer systématiquement les dispositifs d'authentification forte proposés par votre banque
- ✓ Faire opposition immédiatement auprès de votre banque en cas de suspicion de fraude
- ✓ Tenir à jour vos appareils électroniques (antivirus, mises à jour logicielles régulières).