ZIMPERIUM®
ADVANCED MOBILE SECURITY

Pourquoi les pirates informatiques adorent votre application bancaire mobile

Le mobile change notre façon de faire des opérations bancaires.

En janvier 2021, il y a plus de 4,32 milliards d'utilisateurs d'internet mobile dans le monde, ce qui représente 59,5 % de la population mondiale. Et en avril 2020, plus de 70 % des clients des quatre plus grandes banques américaines utilisaient des applications bancaires mobiles, contre 63 % un an auparavant. Ce bond peut être attribué à la fermeture de plusieurs agences bancaires pour éviter la propagation du virus COVID-19.

Aujourd'hui, le mobile est la norme de facto. En d'autres termes, si votre stratégie numérique ne tient pas compte du mobile, vous êtes à côté de la plaque.

Environ trois Américains sur quatre **(76 %)** ont utilisé l'application mobile de leur banque principale au cours de l'année écoulée pour leurs opérations bancaires quotidiennes, comme le dépôt de chèques ou la consultation de relevés et de soldes de comptes, selon l'enquête hebdomadaire sur la confiance des consommateurs réalisée par Ipsos et Forbes Advisor aux États-Unis.

Qu'il s'agisse de banque de détail, de banque d'entreprise ou de banque commerciale, votre application de banque mobile est votre nouvelle banque !

Les services bancaires mobiles représentent l'avenir en raison de la commodité indéniable qu'ils offrent dans l'ère post-pandémique définie par la nouvelle économie à faible coût. Selon la recherche anti-fraude de RSA, la présence d'une application mobile est désormais l'une des **3 principales conditions** à remplir pour choisir une banque. Malheureusement, la même étude indique que les capacités de protection contre la fraude d'une banque arrivent en avant-dernière position dans ce choix. Les consommateurs privilégieront toujours la commodité à la sécurité. Mais pour les institutions bancaires, les applications mobiles présentent également un risque numérique massif qui ne peut être ignoré.

La banque mobile fonctionne à travers les générations

97 % des milléniaux ont indiqué qu'ils utilisaient les services bancaires mobiles.

91 % des membres de la génération X et 79 % des baby-boomers ont également déclaré avoir perçu les avantages de ces services.

Source : https://www.businessinsider.com/mobile-banking-market-trends

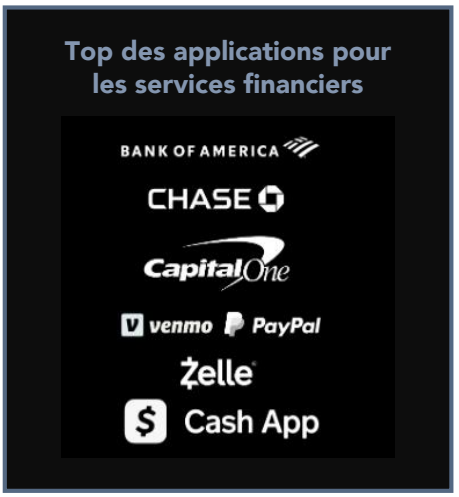
La banque mobile est un secteur d'activité important.

Le secteur bancaire a été carrément au centre de l'évolution du mobile. À l'ère post-pandémique, les applications bancaires mobiles sont devenues la norme de facto en matière de services bancaires. Les consommateurs veulent davantage de fonctions en libre-service et une expérience utilisateur personnalisée dans les applications mobiles. Mais cette expérience personnalisée nécessite de plus en plus d'informations PII. Un smartphone moyen possède plus de 90 applications, et environ 10 % de ces applications sont liées à la gestion de votre santé financière.

La banque mobile est une cible importante.

Malheureusement, l'adoption enthousiaste de la banque mobile par le marché a fait des applications et des utilisateurs des cibles attrayantes pour les cybercriminels. Regardez les statistiques ci-dessous:

- Les transactions frauduleuses par téléphone mobile ont augmenté de 600 % au cours des cinq dernières années
- 1 attaque frauduleuse sur 20 est due à un logiciel malveillant mobile
- Augmentation de 50 % des logiciels malveillants bancaires d'une année à l'autre
- 44 % des fraudes se produisent dans les applications mobiles



Le simple volume des transactions mobiles a déjà atteint une masse critique, où le gain potentiel pour les cybercriminels fait des attaques contre les applications bancaires mobiles une priorité. Aujourd'hui, les utilisateurs de smartphones se connectent en moyenne 30 fois par mois à leur application bancaire mobile.

Au fur et à mesure que les fonctionnalités et les capacités des services bancaires mobiles se développent, l'activité bancaire mobile continuera d'augmenter, et la surface correspondante que les cybercriminels peuvent attaquer augmentera également. Mais la réalité est que les applications bancaires mobiles sont déjà confrontées à un risque sans précédent.

Les développeurs de services bancaires mobiles se heurtent à des obstacles importants.

Les banques sont très soucieuses de la sécurité. Comment se peut-il que le secteur bancaire, modèle de sécurité, ait du mal à assurer la sécurité des applications mobiles ? Le fait est que la demande des clients en matière de services bancaires mobiles dépasse de loin la capacité du secteur à fournir une sécurité à toute épreuve dans un écosystème de dispositifs mobiles en évolution rapide.

En d'autres termes, les développeurs d'applications mobiles sont confrontés à une pression importante exercée par trois forces différentes et concurrentes sur le marché. Premièrement, la demande des clients (et la pression concurrentielle des applications mobiles des autres banques) est intense. Les clients continuent de montrer un appétit considérable pour l'expansion de leur utilisation des services bancaires mobiles. Pour suivre le rythme des clients, les développeurs se concentrent souvent sur les fonctionnalités plutôt que sur la sécurité.

De plus, à mesure que les échéances se rapprochent, les raccourcis de développement deviennent plus attrayants, et les développeurs utiliseront un code non approuvé et ouvert pour les fonctions mobiles. Il y a plus de 26 millions de développeurs d'applications mobiles dans le monde, et la plupart d'entre eux ne sont ni orientés ni incités vers un code sécurisé. Ils sont incités à construire plus rapidement.

Deuxièmement, les plateformes mobiles se disputent la domination du marché. Les développeurs doivent donc soit travailler avec une connaissance limitée des plateformes sous-jacentes, soit devenir des spécialistes d'un sous-ensemble étroit et particulier de plateformes.

Le développement d'applications, le stockage cloud et d'autres frameworks de développement modulaires évoluent constamment et obligent les développeurs à se tenir au courant des meilleures pratiques. Cette fragmentation crée un environnement idéal pour les erreurs de sécurité.

Troisièmement, il y a la réalité de la façon dont les consommateurs utilisent leurs appareils mobiles. Les enquêtes montrent systématiquement que les consommateurs de services bancaires mobiles accordent une valeur à la sécurité en principe. Malgré cela, les consommateurs ne donnent pas toujours la priorité à la sécurité en pratique. Nous avons noté dans une section précédente, par exemple, que certains consommateurs ne suivent pas les pratiques de sécurité essentielles telles que l'utilisation de mots de passe ou la mise à jour vers le dernier système d'exploitation. Cette mauvaise pratique exacerbe toutes les vulnérabilités que les développeurs autorisent par inadvertance dans leurs applications bancaires.

Les applications bancaires mobiles fonctionnent dans un environnement de zéro confiance.

Aujourd'hui, les applications mobiles sont exécutées sur des appareils dont l'intégrité ne peut pas faire l'objet d'une confiance implicite. Chaque appareil mobile a un profil d'utilisation et une position de risque uniques. Bien que cette liste ne soit en aucun cas exhaustive, considérez les cibles suivantes pour les cybercriminels :

- **Appareils compromis et à risque :** Les appareils mobiles eux-mêmes peuvent être entièrement compromis ou risqués en raison de la vulnérabilité des systèmes d'exploitation, des micrologiciels et des paramètres.
- **WiFis malveillants / Rogue :** Les réseaux non sécurisés essaient d'écouter les conversations et les transactions pour voler des informations confidentielles.
- **Applications malveillantes :** D'autres applications malveillantes qui ciblent et exploitent les applications bancaires sur l'appareil pour commettre une fraude. Ces applications utilisent une combinaison de tactiques de phishing, d'abus de permission et de superposition d'écran pour extraire les informations nécessaires à une activité frauduleuse.

Tous ces vecteurs et techniques de menace visent à accéder aux éléments suivants :

- **Informations d'identification.** Les attaquants peuvent chercher à obtenir les informations d'identification bancaires mobiles des utilisateurs pour accéder à leurs comptes et commettre des vols.
- **Données personnelles.** Les cybercriminels se concentrent sur les données clients à forte valeur potentielle, telles que les numéros de sécurité sociale, les dates de naissance et d'autres informations sensibles.
- **Données du titulaire de la carte.** Les attaques de services bancaires mobiles peuvent chercher à recueillir des données spécifiques à la carte, telles que les numéros de carte, les informations sur la date d'expiration et les données CVV.

Les cybercriminels savent que les applications bancaires mobiles sont une cible facile et présentent un énorme potentiel. Cette notion est à l'origine de centaines de chevaux de Troie bancaires mobiles, et des variantes plus sophistiquées n'ont cessé d'apparaître au cours des quinze dernières années.

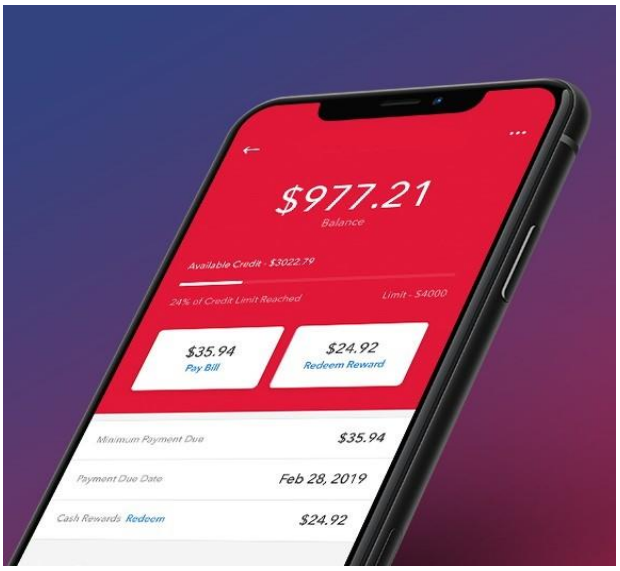
Pourquoi les approches traditionnelles de la fraude rencontrent des difficultés.

Analyse des transactions de confiance : Aujourd'hui, la plupart des plateformes de lutte contre la fraude sont principalement axées sur l'analyse des transactions pour identifier les transactions frauduleuses. Mais la recherche anti-fraude de RSA indique que la majorité des fraudes se produisent lorsqu'un **nouvel appareil** est impliqué. Aujourd'hui, le consommateur moyen remplace son appareil mobile tous les 24 mois, ce qui fait des nouveaux appareils un sujet de préoccupation pour les ouvertures de comptes existants et nouveaux. La connaissance de la position à risque d'un appareil mobile est limitée, voire inexistante.

Nouveau modèle d'interaction : Les appareils mobiles et la pandémie de COVID ont complètement changé la façon dont les consommateurs interagissent avec les banques. Les consommateurs veulent faire de plus en plus de choses dans l'application mobile et profiter également d'une expérience personnalisée. Mais l'infrastructure sous-jacente actuelle de prévention contre la fraude n'a pas encore été adaptée et rattrapée les appareils et applications mobiles.

Confiance implicite : La plupart des banques font implicitement confiance aux transactions des clients et se concentrent sur l'efficacité de leur exécution. Elles n'interviennent pas ou ne remettent pas en question la transaction car elles s'inquiètent d'une mauvaise expérience utilisateur et de la responsabilité associée à ces décisions.

Les services bancaires mobiles ont une influence considérable.



Compte tenu de l'incroyable élan qui a propulsé les services bancaires mobiles vers une position dominante sur le marché, il n'est pas surprenant que les grandes banques soient également des leaders dans ce domaine. L'importance de l'expérience mobile se retrouve dans toute l'organisation de la banque.

Les banques qui visent à atteindre ou à maintenir une position de leader en exploitant l'énorme potentiel que représente la banque mobile doivent surmonter les obstacles à la sécurité de la banque mobile. C'est devenu, en fait, une mission. Zimperium rend cela possible.

Zimperium renforce la sécurité des applications bancaires mobiles pour les banques et leurs clients.

Zimperium fournit une solution puissante avec laquelle les applications bancaires mobiles peuvent **évaluer** la position de risque d'un appareil mobile et se **défendre** en temps réel. Cette capacité d'attestation de l'appareil en temps réel permet aux applications mobiles de déterminer si des fonctions doivent être désactivées ou si des transactions doivent être examinées plus en détail. Les informations sur les risques liés aux appareils sont une pièce essentielle qui manque à la plupart des algorithmes de fraude actuels, qui reposent essentiellement sur l'analyse des transactions. Les informations fournies par la solution sont également mises à la disposition des équipes chargées des fraudes, des risques et de la conformité, afin de leur donner une visibilité qui leur permettra d'affiner leurs stratégies de lutte contre la fraude et la criminalité financière sur le canal mobile.

Cette capacité d'**attestation des appareils** s'appelle zDefend™ et peut être facilement intégrée à n'importe quelle application iOS ou Android. La nature modulaire du kit de développement logiciel (SDK) permet aux développeurs d'intégrer rapidement et sans difficulté le principal moteur de détection mobile basé sur l'apprentissage automatique, Zimperium z9™, directement au sein des applications bancaires mobiles. z9 permet à l'application de déterminer si l'appareil sur lequel elle fonctionne est compromis, s'il est connecté à un réseau non sécurisé et même si des applications malveillantes comme BankBot sont présentes sur l'appareil. Lorsqu'un appareil est attaqué, zDefend informe l'application pour qu'elle lance des alertes et des actions de réduction des risques afin d'atténuer l'impact. zDefend est entièrement configurable par les développeurs d'applications, qui peuvent choisir la mesure corrective à appliquer, par exemple établir un VPN, demander une authentification supplémentaire, augmenter les scores de fraude ou demander à l'utilisateur d'effectuer sa transaction d'une autre manière.

Le SDK zDefend permet aux banques de fournir des applications iOS et Android auto-protégées et de mettre en œuvre des workflows basés sur les risques au sein de l'application. Les développeurs intègrent le moteur z9 dans les applications à l'aide d'un SDK facile à mettre en œuvre qui fonctionne avec les plateformes de développement natives et hybrides. Les développeurs peuvent consacrer plus de temps au développement sans se soucier de la sécurité.

Principaux avantages liés à la fraude

Visibilité

Le moteur de détection basé sur l'apprentissage automatique sur l'appareil permet aux applications de recueillir des données télémétriques sur les attaques et les menaces connues et zero-day, et de les partager avec les équipes chargées des risques et des fraudes. Les informations couvrent les vecteurs de dispositifs, de réseaux, de logiciels malveillants et de phishing. Ces informations sont essentielles pour que les politiques de lutte contre la fraude et les investissements futurs tiennent compte des risques réels.

Prévention contre la fraude en temps réel sur les appareils

Selon le rapport trimestriel de RSA sur la fraude, 44 % des fraudes ont eu lieu sur des applications mobiles au quatrième trimestre 2020. La détection sur l'appareil permet aux apps bancaires de répondre immédiatement aux menaces sur l'appareil lorsque l'intégrité d'une transaction ou de l'app elle-même est menacée. Le moteur z9 avancé peut détecter les faux appareils, les logiciels malveillants bancaires, les techniques avancées de rooting/jailbreak et d'autres techniques sophistiquées de vol d'informations d'identification et de données. En outre, le SDK permet à l'application de limiter de manière proactive ce que l'utilisateur peut faire en fonction du moment où le risque franchit un certain seuil en raison de changements dans le dispositif, le réseau ou les vecteurs de phishing.

Un meilleur filtrage des clients

Les informations sur les risques liées à l'appareil permettent aux équipes chargées de la fraude et des risques d'établir des profils de risque plus précis pour les titulaires de comptes. Cela permettra aux banques de développer des listes de surveillance de nouvelle génération afin de maximiser l'efficacité opérationnelle. Étant donné que les organismes bancaires traitent avec des millions de clients potentiels, cette télémétrie les aidera à prioriser leur activité de contrôle contre ceux qui présentent la menace la plus importante.

Suivi continu des transactions

Le contrôle continu de la fraude consiste à surveiller en permanence toutes les actions effectuées sur un compte bancaire, et pas seulement la connexion initiale et les transactions financières qui en découlent, comme les paiements et les transferts de fonds. Le suivi continu de la fraude porte sur toutes les activités et tous les événements, qu'ils soient monétaires ou non monétaires.

zDefend fournit une protection globale des applications mobiles contre les cyberattaques. Une fois la sécurité intégrée aux applications bancaires mobiles, les banques peuvent se concentrer sur les innovations qui raviront les clients, les fidéliseront et exploiteront tout le potentiel des services bancaires mobiles.

Création d'applications intelligentes d'autodéfense

La plupart des entreprises ont commencé à sécuriser leurs applications mobiles. Mais la plupart s'arrêtent à des solutions d'obscurcissement ou d'analyse de base qui ne suffisent pas à contrer les techniques d'exploitation sophistiquées d'aujourd'hui. Pour mieux comprendre le niveau de sécurité de votre application, contactez-nous à l'adresse info@zimperium.com et demandez une évaluation GRATUITE des risques. Nous aidons les entreprises à comprendre leur exposition et à sécuriser leurs applications mobiles.

ZIMPERIUM®