# Les applications de banque mobile (Mobile banking)

**Plus de la moitié des transactions de banque en ligne sont effectuées à l'aide d'un smartphone ou d'une tablette, la plupart du temps via une application mobile proposée par l'institut financier du client. La banque mobile présente une foule d'avantages, mais recèle aussi nombre de dangers.**

**Voici comment utiliser votre application de banque mobile en toute sécurité :**

- Protégez votre dispositif mobile à l'aide de nos « 5 règles pour votre sécurité numérique » (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) . La sécurité de vos opérations de banque mobile passe avant tout par un dispositif sain et sécurisé.
- Pour les paiements avec votre appli de banque mobile, préférez la fonction demande plutôt que la fonction envoi, surtout pour les gros montants. Ainsi, en cas de faute de frappe, etc., ce n'est pas l'argent qui arrivera au mauvais destinataire, mais la demande de virement.
- À l'instar de toutes vos applications, votre appli de banque mobile doit impérativement être téléchargée depuis un store officiel.
- N'installez que les applications dont vous avez vraiment besoin et désinstallez toutes celles que vous n'utilisez pas ou plus.
- Limitez les droits d'accès de toutes vos applications au strict minimum.
- En mobilité, assurez-vous de toujours connecter votre dispositif à un réseau fiable.
- En cas de perte, verrouillez immédiatement votre dispositif. Si vous souhaitez le revendre ou le mettre au rebut, veillez à réinitialiser votre appareil avant de vous en débarrasser.

**Risques et avantages des applications de banque en ligne**

Smartphones et tablettes sont de (petits) ordinateurs et présentent par conséquent les mêmes risques : perte ou vol de données, attaques de malwares, accès non autorisés etc. Leur caractère mobile les expose par ailleurs à d'autres dangers, comme la perte ou le vol.

En contrepartie, ils offrent tous les avantages liés à la mobilité et à leur encombrement réduit. Mais l'utilisation d'une application de banque mobile présente un autre intérêt non négligeable : **contrairement à l'e-banking classique via navigateur, le client de l'institut financier dispose d'un programme spécialement conçu et donc dûment sécurisé pour la gestion numérique des opérations bancaires.**

Leur utilisation décharge donc l'utilisateur conscient des risques de sécurité de toute une série de tâches fastidieuses telles que la saisie manuelle de l'adresse de la banque dans le navigateur et la vérification de la connexion sécurisée. En effet, contrairement au navigateur, l'application de banque mobile exécute automatique ces opérations en arrière-plan, minimisant ainsi les dangers représentés par les fautes de frappe ou le phishing – en supposant que l'utilisateur s'en tienne effectivement à quelques règles de base.

# Utiliser une application de banque mobile en toute sécurité

**Assurer une protection de base**

Il importe en premier lieu de réduire au minimum les risques liés à l'utilisation d'un appareil mobile. Commencez donc par appliquer, pour vos dispositifs mobiles aussi, nos « 5 règles pour votre sécurité numérique » (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) . En particulier, assurez-vous que le verrouillage automatique de l'écran est activé (code d'accès, mot de passe, empreinte digitale ou reconnaissance faciale).

La vigilance est d'autant plus de mise dès lors qu'il s'agit de smartphones et de tablettes. En particulier, il convient de ne jamais laisser votre dispositif sans surveillance. Veillez également à ne communiquer à personne vos codes PIN, codes à usage unique et mots de passe, de les taper à l'abri des regards et de toujours les masquer lors de la saisie. Soyez prudent lorsque vous ouvrez courriels, pièces jointes, messages reçus via des services de messagerie (comme WhatsApp par ex.), ou des MMS. Sachez que les maliciels peuvent également se transmettre via MMS ou WhatsApp. Ne cliquez jamais sur des liens inconnus et effacez immédiatement les messages provenant d'expéditeurs inconnus. Vérifiez les numéros que vous ne connaissez pas avant de les rappeler.

**Vérifier la provenance de l'application**

N'installez que les applications dont vous avez vraiment besoin et assurez-vous qu'elles proviennent de sources sûres, c'est-à-dire des stores officiels (p. ex. Apple App Store ou Google Play Store).

Méfiez-vous des applications ayant un indice de réputation faible ou des recommandations anonymes. Renseignez-vous avant d'installer une appli si vous ne connaissez pas le fournisseur.

Vérifiez de temps en temps les applications que vous utilisez effectivement et désinstallez les applis obsolètes et celles dont vous n'avez plus besoin – toute application superflue représente une faille de sécurité potentielle.

Si votre application de banque mobile vous donne des messages d'erreur ou fonctionne de manière inhabituelle, avertissez-en immédiatement votre institut financier (https://www.ebas.ch/fr/partenaires/) .

**Limiter les droits d'accès**

De nombreuses applis accordent sans raison apparente des droits d'accès illimités. Les applications ne nécessitent pas toutes d'accéder par exemple à la position géographique, au répertoire des contacts ou au statut du téléphone. Lorsque vous accordez tel ou tel droit d'accès, réfléchissez s'il est vraiment nécessaire au fonctionnement de l'application et désactivez tous les droits superflus.

**Vérifier l'opérateur de réseau mobile**

Votre smartphone ou votre tablette peuvent établir une connexion avec votre institut financier ou d'autres dispositif et ce, de différentes manières. Lorsque vous êtes en mobilité, votre dispositif se connecte à différents réseaux wifi pour accéder à Internet. De votre côté, il est important de contrôler leur fiabilité : les fournisseurs peu crédibles de réseaux wifi « gratuits » sont en effet susceptibles de dévier le flux de données échangées par votre application bancaire vers un faux serveur pour voler vos identifiants de connexion.

Sachez enfin qu'il existe pour les appareils Android une application pare-feu servant à surveiller et à sécuriser les connexions actives. Le problème ne se pose pas pour les appareils sous iOS (iPhone / iPad) dans la mesure où ils ne prévoient pas cette possibilité.

**Traiter de manière adéquate les cas de perte, revente et mise au rebut**

Dans le cas où votre smartphone ou votre tablette tombe entre de mauvaises mains, c'est l'ensemble de vos données ou de vos identifiants de connexion qui risquent d'être volés et abusivement utilisés.

Différentes applications permettent de verrouiller à distance les dispositifs perdus ou volés et de supprimer les données qui y sont stockées pour qu'elles ne soient plus accessibles. Une fois votre dispositif verrouillé, il convient de prendre contact avec votre opérateur de téléphonie mobile pour désactiver votre carte SIM.

Si vous ne voulez pas que vos données finissent entre de mauvaises mains après avoir vendu ou jeté votre dispositif, assurez-vous qu'elles ont bien été supprimées de manière irréversible. Pour savoir comment procéder, vous pouvez par exemple consulter le site Internet d'Apple (https://support.apple.com/de-de/HT201274) ou de SRF (https://www.srf.ch/sendungen/kassensturz-espresso/services/handy-daten-sicher-loeschen-so-funktioniert-s) . N'oubliez pas non plus de retirer la carte SIM et de la détruire si vous ne souhaitez plus l'utiliser.

*Par « Mobile Banking » on entend l'exécution de transactions bancaires au moyen d'appareils mobiles tels que les smartphones ou tablettes.*

*Le client peut ainsi accéder aux services d'e-banking grâce à son navigateur mobile ou, comme c'est de plus en plus souvent le cas, via des applications mobiles dédiées.*

***Mémento :*** *Download (PDF) (https://www.ebas.ch/wp-content/uploads/2019/10/mobilebankingSKP_fr.pdf)*