

Chère Cliente, Cher Client,

Dans le cadre de notre engagement continu envers votre sécurité, Bank Assafa vous présente ce guide de sensibilisation dédié à l'utilisation sécurisée de notre application Mobile. Ce document regroupe les bonnes pratiques essentielles à adopter pour accéder à vos services bancaires en toute confiance et garantir la protection de vos informations personnelles.

Gestion des éléments d'authentification

- Tout abonné à l'application Mobile dispose d'un identifiant fixe et d'un mot de passe modifiable. Pour accéder à votre espace personnel, vous devez saisir votre identifiant et votre mot de passe.
- Évitez de noter votre mot de passe sur un bout de papier.
- Il est recommandé de changer votre mot de passe de façon régulière à partir de votre espace personnel.
- Il est aussi recommandé de ne pas enregistrer vos éléments d'authentification dans votre mobile.
- Évitez de confier vos éléments d'authentification à un tiers. **Jamais la banque ne vous demandera de communiquer votre identifiant ou votre mot de passe**, par courrier, par e-mail ou par SMS.
- En cas de perte ou d'oubli, vous pouvez effectuer une demande de recalcul dans l'espace dédié. Un nouvel authentifiant vous sera envoyé via le canal de diffusion contractuel.
- Si vous soupçonnez que quelqu'un connaît votre mot de passe, il faut le changer immédiatement.

Accès sécurisé via l'application Mobile

- Ne laissez jamais votre téléphone sans surveillance.
- Déconnectez-vous de votre application Mobile lorsque vous terminez vos transactions.
- Introduisez toujours votre mot de passe en toute discrétion.
- Évitez d'utiliser l'application sur un smartphone autre que le vôtre.

Protection contre les intrusions externes

- Installez un programme antivirus avec pare-feu intégré et veillez particulièrement à le mettre à jour. Ce programme vous prévient de toute tentative d'intrusion et permet de détecter la présence d'un virus ou d'un malware sur votre téléphone.
- Utilisez une version du système d'exploitation authentique et veillez à la maintenir et à la mettre à jour régulièrement.
- N'installez, dans la mesure du possible, sur votre téléphone que des programmes dont l'origine est sûre.

Protection contre les e-mails et SMS trompeurs

- Évitez d'ouvrir des e-mails d'origine inconnue. Faites particulièrement attention aux e-mails contenant des pièces jointes.
- Soyez attentifs aux e-mails ou SMS reçus : des personnes mal intentionnées vont essayer de vous inviter, dans des messages dits de «**Phishing**», à télécharger des données ou à parcourir certains sites web. Ces messages ont souvent pour but de soutirer des informations confidentielles à votre insu.
- Faites attention lorsque vous cliquez sur un lien figurant dans un e-mail. Vérifiez l'adresse dans la barre de navigation : un site frauduleux peut reproduire l'interface de l'application Mobile de la banque.
- Ne divulguez jamais votre mot de passe par e-mail ou par SMS, même si l'expéditeur paraît sérieux. **La banque ne vous demandera en aucun cas des données confidentielles par e-mail ou SMS.**

GLOSSAIRE

Phishing (Hameçonnage)

Technique frauduleuse visant à obtenir des informations confidentielles via tout canal de communication (e-mails, SMS, appels téléphoniques, QR codes, etc.) en se faisant passer pour un organisme de confiance.

Malware

Programme malveillant conçu pour endommager, perturber ou accéder sans autorisation à un système ou un appareil mobile.

Pare-feu (Firewall)

Système de sécurité qui surveille et contrôle le trafic réseau selon des règles prédéfinies pour bloquer les connexions non autorisées.

BESOIN D'AIDE · CONTACTEZ-NOUS

SERVICE CLIENT
05.29.04.04.44

Portail officiel
www.bankassafa.com