بنك المغرب
BANK AL-MAGHRIB

POUR UN USAGE SÉCURISÉ DES SERVICES BANCAIRES EN LIGNE

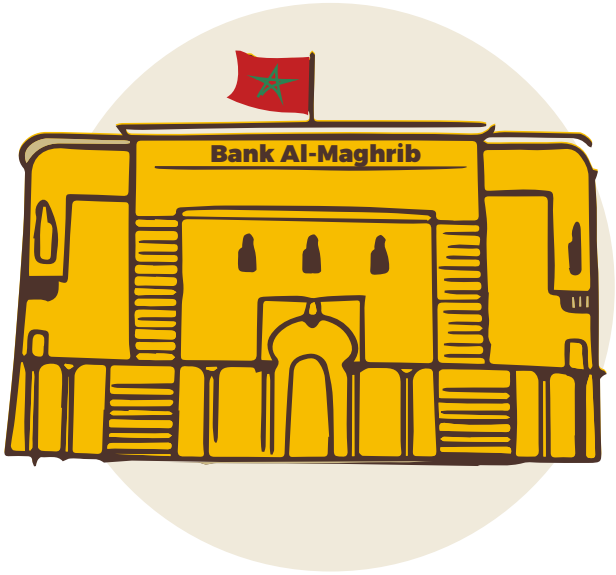
INFOS UTILES

Dans le cadre de sa mission de protection de la clientèle bancaire, Bank Al-Maghrib met ce guide à la disposition des usagers des services bancaires digitaux.

L'utilisation des services bancaires en ligne présente de nombreux avantages pour les clients :

- Commodité ;
- Rapidité ;
- Facilité d'usage.

Pour promouvoir un usage sécurisé des services offerts en ligne, il est indispensable d'adopter quelques bons réflexes à l'effet d'en maîtriser les risques.



1 Qu'est-ce qu'un service bancaire en ligne ou digital

Les services bancaires digitaux (ou numériques, ou en ligne) comprennent un large éventail de services financiers offerts via des plateformes ou applications accessibles sur ordinateur ou téléphone

Les usagers peuvent réaliser un ensemble d'opérations à distance sans contrainte de déplacement physique dans une agence bancaire ou un point de vente

2 Quelles sont les principales opérations bancaires réalisées en ligne ?

Les principales opérations proposées sur les applications web ou mobile des établissements bancaires et de paiement sont :

1 CONSULTATIONS

Comptes (solde, historique des opérations)

Cartes bancaires associées au compte et la possibilité d'en modifier certains paramètres

Crédits en cours

Simulation de nouveaux crédits

Offres de la banque (produits, packages…) et de la grille tarifaire appliquée par l'établissement bancaire

2 DEMANDES

L'édition du RIB

La demande de chéquier

L'assistance et le conseil en ligne

Le dépôt de réclamations

La souscription à des services en ligne pour l'ouverture de compte ou la demande de crédit

3 TRANSACTIONS

La réalisation d'opérations de virement

La recharge de cartes prépayées

Le paiement de factures, de taxes et autres frais (téléphonie, eau, électricité, autoroute, vignette…)

La gestion du portefeuille titres

Le transfert d'argent et la mise à disposition de fonds

3 Comment accéder aux services bancaires digitaux ?

L'accès se fait à distance à travers un un ordinateur, une tablette ou un smartphone connecté à internet

L'accès nécessite au préalable la disposition d'un compte utilisateur fourni par l'etablissement bancaire du client ainsi que d'un mot de passe. Pour cela, l'usager :

- Se connecte à l'application web ou mobile, installée sur l'appareil d'accès ou accessible en ligne.
- Saisit son nom d'utilisateur et son mot de passe pour accéder aux fonctionnalités applicatives
- Suit les instructions pour réaliser l'opération choisie

4 Quels sont les bons gestes pour un usage sécurisé des applications web et mobile ?

L'usage sécurisé des services bancaires en ligne nécessite une sécurisation de :

1. L'APPAREIL D'ACCÈS

- Mettez à jour vos systèmes et antivirus sur ordinateur, tablette, mobile et scannez-les régulièrement
- En cas de perte ou de vol de l'appareil d'accès, le déclarer immédiatement à votre banque pour bloquer l'accès au compte et procéder au changement immédiat du mot de passe d'accès

2. L'APPLICATION UTILISÉE

- Assurez-vous de l'authenticité de l'application mobile avant son téléchargement et son installation sur votre appareil mobile
- Sécurisez l'accès lorsqu'il s'effectue par WIFI en redoublant de vigilance lors de l'utilisation des connexions publiques.
- S'assurer de l'authenticité du portail web, en étant vigilant notamment dans le cas ou des données personnelles sont demandées (en particulier les coordonnées bancaires)

En cas de doute sur l'authenticité, vérifier l'existence de mentions légales sur le site, de numéro de tél permettant d'entrer en contact avec des personnes, s'enquérir de la e-réputation en tapant le nom du site associé au terme « arnaque », se poser la question sur la cohérence de la demande.

Dans de nombreux cas, certains sites frauduleux parviennent à imiter parfaitement des sites, notamment de banques, et vous demande de saisir vos coordonnées bancaires, notamment dans le cadre d'une campagne de mise à jour des informations de la clientèle

3. LA CARTE SIM

- Protégez votre carte SIM contre toute tentative frauduleuse de récupération de vos informations personnelles
- Protégez le code de votre carte SIM et surveillez son éventuelle modification
- En cas de perte ou de vol de votre carte SIM, le déclarer immédiatement à votre banque pour bloquer l'accès au compte de l'application web et mobile
- La protection de votre carte SIM est essentielle, car dans le cadre d'une transaction en ligne, elle empêchera un fraudeur qui a pu se procurer les coordonnées de votre carte bancaire, de recevoir le code sécurisé de sa banque, permettant le paiement effectif de la transaction

4. LE COMPTE D'ACCÈS

- Choisissez un mot de passe robuste pour le compte d'accès à l'application web ou mobile, difficile à déchiffrer (combinaison de caractères alphanumériques et caractères spéciaux). Changez-le immédiatement en cas de doute sur sa confidentialité
- Tapez vos identifiants (nom utilisateur et mot de passe) à l'abri des regards indiscrets lors de toute utilisation de l'application mobile ou web
- Mémorisez votre compte d'accès à votre application web ou mobile (nom utilisateur et mot de passe) et ne pas l'inscrire sur un support pouvant facilement être subtilisé
- Ne pas enregistrer par défaut vos données d'identification saisies lors de la connexion à l'application mobile ou web
- Votre compte d'accès est strictement personnel ; ne jamais le communiquer à autrui quelle que soit la raison
- Protégez votre compte d'accès contre toute tentative frauduleuse de récupération de vos informations personnelles

Faites attention aux tentatives de récupérations de vos données personnelles quand vous recevez des SMS sur vos smartphones vous incitant à cliquer sur un lien et à envoyer vos informations d'identification, vos informations bancaires et vos données privées

Se méfier des appels lorsqu'une personne se présente comme salarié de votre banque en vous demandant de lui communiquer vos données bancaires, sous prétexte de mise à jour, d'annuler une opération, de vous protéger d'une fraude,...

Redoubler de vigilance lorsque l'objet de l'appel est une offre alléchante qui ne peut être refusée et que la décision doit être immédiate, ou encore un cadeau ou autre gain

5. L'OPÉRATION EN LIGNE SOUHAITÉE

- Déconnectez-vous systématiquement de l'application après chaque utilisation
- Lors de l'exécution des opérations sur l'application mobile ou web, assurez-vous de l'utilisation du mécanisme d'authentification renforcée [1]
- Vérifiez régulièrement le relevé de vos opérations réalisées sur votre compte bancaire pour informer votre banque en cas d'anomalie
- Effacez votre historique de navigation et les cookies[2] après la réalisation d'une opération bancaire en ligne

1 L'authentification renforcée signifie que deux facteurs au moins sont confirmés par le client parmi les trois suivantes :

la possession
du terminal d'accès (par le client)

la connaissance
du mot de passe par le client

l'identification
du client par empreinte digitale ou tout autre moyen

Dans une grande majorité des cas, l'authentification forte nécessite l'ouverture de l'application mobile de banque en ligne et la saisie d'un code d'identification et d'un mot de passe (ou le contrôle de l'empreinte digitale) sur un téléphone préalablement enregistré par la banque. Cette méthode est plus forte que celle qui consiste à l'envoi d'un OTP via SMS sur le téléphone portable, qui ne remplit qu'un seul des deux critères s'il n'est pas associé à la confirmation d'un mot de passe. Cette authentification renforcée peut également s'opérer via des dispositifs mis en place par des partenaires de la banque tel le système de tiers de confiance national.

2

Un « cookie » est un fichier de données stocké sur le navigateur ou sur le disque dur de votre ordinateur ou de votre appareil mobile lors de la consultation d'une page Web. Les cookies sont utilisés aux fins de la collecte de données relatives à votre appareil et à vos interactions sur le site Web (par exemple, type de navigateur utilisé, système d'exploitation, adresse IP…)

Un site internet qui utilise des cookies faisant appel à des données personnelles doit recueillir le consentement de l'internaute avant le dépôt de ces cookies. De même qu'il doit préciser la finalité de l'utilisation des cookies et expliquer à l'internaute les moyens de s'y opposer Ce consentement s'opère en général via un clic sur un bouton d'invitation à l'acceptation de l'utilisation des cookies.

Pour toute information complémentaire ou demande de précision :

080 200 11 11

accueil@bkam.ma