بنك المغرب
BANK AL-MAGHRIB

POUR UN USAGE SÉCURISÉ DES SERVICES BANCAIRES EN LIGNE

INFOS UTILES

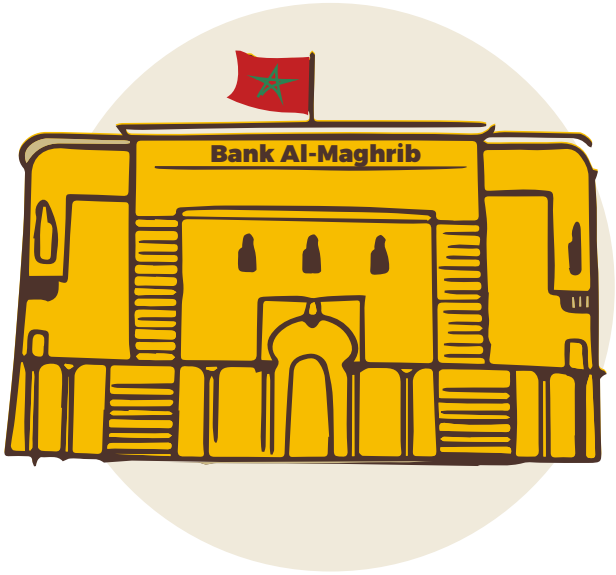
© Bank Al-Maghrib - Mars 2023

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

بنك المغرب
BANK AL-MAGHRIB

معلومات مفيدة

من أجل استخدام آمن للخدمات البنكية عبر الأنترنت

© بنك المغرب - مارس 2023

في إطار مهمته المتعلقة بحماية زبناء البنوك، يضع بنك المغرب هذا الدليل رهن إشارة مستعملي الخدمات البنكية الرقمية.

يوفر استعمال الخدمات البنكية الإلكترونية عدة مزايا بالنسبة للزبناء:

- التيسير والإتاحة؛
- السرعة؛
- سهولة الاستعمال.

وتشجيعا للاستخدام الآمن للخدمات المقدمة عبر الإنترنت، من الضروري اعتماد بعض ردود الأفعال الجيدة من أجل التحكم في مخاطرها.

1 ما هي الخدمة البنكية عبر الإنترنت أو الرقمية

تشمل الخدمات البنكية الإلكترونية (الرقمية أو عبر الانترنت) باقة واسعة من الخدمات المالية المقدمة بواسطة منصات أو تطبيقات يمكن الولوج إليها عبر الحاسوب الآلي أو الهاتف النقال

يمكن للزبناء القيام بعمليات متعددة عن بعد دون تحمل إكراهات التنقل إلى وكالة بنكية أو إحدى نقاط البيع

2. ماهي العمليات البنكية الرئيسية المنجزة عبر الأنترنت

العمليات الرئيسية المقدمة على تطبيقات الانترنت والهاتف النقال للمؤسسات البنكية ومؤسسات الأداء هي كالتالي:

1 استشارات

الحسابات (الرصيد، تواريخ العمليات المنجزة)

البطاقات البنكية المرتبطة بالحساب وإمكانية تغيير بعض المعايير

القروض الجارية

محاكاة قروض جديدة

عروض البنك (المنتجات، الباقات....) والتسعيرة المطبقة من طرف المؤسسة البنكية

2 طلبات

طباعة بيان التعريف البنكي

طلب دفتر الشيكات

المساعدة والمشورة عبر الانترنت

إيداع الشكايات

الانخراط في خدمات إلكترونية من أجل فتح الحساب أو طلبات القروض

3 المعاملات

إنجاز عمليات تحويل

تعبئة البطاقات مسبوقة الدفع

تسديد الفواتير والرسوم والمصاريف الأخرى (الهاتف والماء والكهرباء والطريق السيار، والضريبة على السيارات...)

تدبير محفظة السندات

تحويل الأموال ووضعها رهن الإشارة

3 كيفية يتم الولوج إلى الخدمات البنكية الرقمية

يتم الولوج عن بعد من خلال الحاسوب الآلي أو اللوحة الإلكترونية أو الهاتف الذكي المتصل بالإنترنت

يتطلب الولوج بداية التوفر على حساب مستخدم مقدم من المؤسسة البنكية للزبون وكذا على كلمة السر. ولهذه الغاية، يتعين على المستخدم:

- تسجيل الدخول إلى التطبيق الشبكي أو النقال، الموجود على جهاز الولوج أو الذي يمكن الولوج إليه عبر الانترنت
- كتابة اسم المستخدم وكلمة السر للولوج إلى ميزات التطبيق
- تتبع التوجيهات لإنجاز العملية المختارة

4 ما هي أفضل الإجراءات من أجل استخدام آمن لتطبيقات الانترنت والهاتف النقال

يتطلب الاستعمال الآمن للخدمات البنكية على الانترنيت تأمين ما يلي :

1. جهاز الولوج

تحيين الأنظمة والبرمجيات المضادة للفيروسات على الحاسوب، الجهاز اللوحي والجوال مع فحصها بانتظام

في حالة ضياع أو سرقة جهاز الولوج، يجب إشعار البنك الخاص بك فوريا بذلك من أجل حظر الولوج إلى الحساب وتغيير الرقم السري

2. التطبيقات المستخدمة

التحقق من صحة موثوقية التطبيقات قبل تنزيلها وثبيتها على الهاتف المحمول

تأمين الولوج عندما يتم عبر الشبكات اللاسلكية (WIFI) عبر تعزيز اليقظة عند استخدام الشبكات العمومية

التأكد من موثوقية موقع الإنترنت، مع توخي الحذر بشكل خاص في حالة طلب المعطيات الشخصية (خصوصا البيانات البنكية)

وفي حالة الشك في موثوقية الموقع، يجب التأكد من وجود إشعارات قانونية فيه ورقم هاتف يخول الاتصال بالأشخاص، والاستفسار عن السمعة الإلكترونية عبر كتابة اسم الموقع متبوعا بمصطلح «احتيال»، والتساؤل حول ملاءمة الطلب.

في العديد من الحالات، تتمكن بعض المواقع الاحتيالية من تقليد المواقع الأصلية، لاسيما مواقع البنوك عبر طلب إدخال بياناتكم البنكية، وذلك عبر ادعاء إجراء تحيين معلومات الزبناء.

3. بطاقة SIM

- حماية بطاقة وحدة التعريف المشترك (SIM) من أي محاولة احتيال لسرقة معلوماتك الشخصية
- حماية الرقم السري ومراقبة أي محاولة لتغييره
- في حالة ضياع أو سرقة بطاقة SIM الخاصة بك، يجب الإعلان عن ذلك فوريا للبنك من أجل حضر الولوج للحساب والتطبيقات على الانترنيت والهاتف النقال
- تعد حماية بطاقة وحدة تعريف المشترك (SIM) أمرا ضروريا، لأنه يمكن في إطار معاملة بنكية من منع محتال تحصل على بياناتكم البنكية، من التوصل بالرقم السري للبنك الذي يمكن من الأداء الفعلي للمعاملة.

4. حساب الولوج

- اختيار كلمة سر قوية وصعبة الاختراق (خليط من الحروف الأبجدية الرقمية والرموز الخاصة). يجب تغييره فوريا في حالة الشك بخصوص سريته
- إدخال بيانات الاعتماد الخاصة بك (اسم المستخدم وكلمة المرور) بعيدًا عن أعين المتطفلين أثناء استخدام تطبيقات الانترنت والهاتف النقال
- تذكر حساب الولوج لتطبيقاتكم على الانترنت والهاتف النقال (اسم المستخدم وكلمة السر) ولا يجب تسجيله على أي دعامة سهلة الاختراق
- لا يجب تسجيل بيانات الاعتماد الخاصة بك عند إدخالها في تطبيقات الانترنت والهاتف النقال
- يعتبر حساب الولوج شخصيا، لا يجب مشاركته مع الغير مهما كان السبب
- حماية حساب الولوج من أي محاولة احتيال لسرقة معلوماتك الشخصية

يجب الاحتياط من محاولات سرقة المعطيات الشخصية عند تلقي رسائل SMS على الهواتف الذكية تدعوكم للضغط على رابط أو إدخال بيانات الاعتماد والمعلومات البنكية أو البيانات الخاصة

الحذر من المكالمات الهاتفية لاسيما عندما يقدم الشخص نفسه كموظف في البنك الخاص بك، بحجة تحيين المعلومات أو إلغاء عملية ما أو حمايتك من الاحتيال، وما إلى ذلك.

مضاعفة اليقظة عندما يكون هدف المكالمة هو عرض جذاب يصعب رفضه ويجب أن يكون القرار فوريا أو هدية أو أي مكسب آخر

5. العمليات اللازم إجراؤها على الانترنيت

- تسجيل الخروج من التطبيق بشكل منتظم بعد كل استعمال
- التأكد من استخدام آلية معززة عند إنجاز العمليات على تطبيقات الانترنت والهاتف النقال
- التأكد بشكل منتظم من كشوفات العمليات المنجزة على حسابكم البنكي لإشعار بنككم في حال حدوث شيء غير طبيعي
- مسح تاريخ التصفح وملفات الارتباط بعد إنجاز أي عملية بنكية عبر الانترنيت

1 يتطلب التوثيق الإلكتروني المعزز توفر عاملين على الأقل من الفئات الثلاث التالية:

ملكية جهاز الولوج
(بالنسبة للزبون)

معرفة الرقم السري
(من قبل الزبون)

التعرف على الزبون
(عبر بصمة الإصبع أو وسيلة أخرى)

في أغلب الحالات، يتطلب التوثيق الإلكتروني القوي فتح تطبيق الهاتف النقال للبنك على الانترنيت وإدخال كلمة السر(أو بصمة الإصبع) على هاتف جوال مسجل مسبقا من قبل من المؤسسة البنكية. تحل هذه الطريقة محل عملية إرسال OTP عبر SMS إلى الهاتف النقال، التي تستوفي معيارا واحدا فقط من المعيارين إن لم يكن مرتبطا بتأكيد كلمة السر. يمكن إجراء هذا التعرف المعزز كذلك عبر منظومات وضعها شركاء البنك مثل نظام الطرف الثالث للثقة الوطني.

2

ملفات تعريف الارتباط هي ملفات بيانات مخزنة على مستعرض الويب أو على القرص الصلب للحاسوب أو الهاتف النقال خلال تصفح الانترنت. وتستعمل ملفات تعريف الارتباط من أجل جمع المعطيات المسجلة في أجهزتكم بالإضافة للتفاعلات على صفحات الويب (على سبيل المثال نوع المتصفح المستعمل ونظام التشغيل وعنوان IP)...

يجب أن يحصل أي موقع إلكتروني يستعمل ملفات تعريف الارتباط لجمع المعطيات الشخصية، على موافقة مسبقة من قبل المستخدمين قبل استخدامها. كما يجب تحديد الغرض من استخدامها وتفسير كيفيات الاعتراض عليها للمستخدمين. تتم هذه الموافقة عموما عبر النقر على زر يدعوكم لقبول استخدام ملفات تعريف الارتباط.

للحصول على أية معلومة اضافية، يمكنكم الاتصال ببنك المغرب:

080 200 11 11

accueil@bkam.ma