بنك المغرب
BANK AL-MAGHRIB

معلومات مفيدة

من أجل استخدام آمن للخدمات البنكية عبر الأنترنت

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