

أمن الخدمات المصرفية للشركات عبر الإنترنت

كيف نحافظ على أمانك؟

تم تصميم منصّة الخدمات المصرفية للشركات عبر الإنترنت من بنك بيبلوس لحماية معلوماتك وخصوصيتك. فيما يلي بعض إجراءات الأمان التي نحرض على اتخاذها:

مستويات عالية من التشفير

جميع المعلومات المتبادلة بين حاسوبك و خادم الويب الخاصّ ببنك بيبلوس تخضع لعامل الأمان من خلال التشفير. يحوّل التشفير المعلومات إلى نموذج غير قابل للقراءة أثناء انتقالها عبر الإنترنت، كما وتستويج بوابة الخدمات المصرفية للشركات عبر الإنترنت أعلى المعايير الدولية. وفقاً لذلك، يجب أن يكون لديك متصفّح يدعم تشفير 128 بت للوصول إلى النظام.

تسجيل دخول آمن

بالإضافة إلى اسم المستخدم وكلمة المرور الخاصين بك، يطلب نظام الخدمات المصرفية للشركات عبر الإنترنت منك اختيار صورة سرّية. بالنسبة إلى جميع عمليات تسجيل الدخول اللاحقة، بمجرد إدخال مكوّن اسم المستخدم الخاصّ ببيانات اعتماد تسجيل الدخول، سيتولّى موقعنا تعريفك به من خلال إظهار الصورة السرية نفسها للتحقق منها. تُثبت الصورة أنك بلغت الموقع الإلكتروني لبنك بيبلوس وأنها ليست صورة زائفة تحاول خداعك لإفشاء معلوماتك الشخصية. بعد ذلك، سيطلب منك إنهاء إدخال بيانات اعتمادك لتسجيل الدخول من خلال تزويدنا بكلمة المرور الخاصّة بك من أجل إتاحة وصولك إلى النظام.

حماية كلمة المرور

لتعزيز حمايتك، سيطلب نظامنا منك بشكل دوريّ تغيير كلمة المرور الخاصّة بك. أثناء تغيير كلمة المرور، سيظهر لك ما إذا كانت كلمة المرور الجديدة ضعيفة أم متوسطة القوة أم قوية. يصعب على المزوّر تخمين كلمات المرور القوية. يُرجى عدم الكشف عن كلمة المرور الخاصّة بك لأيّ شخص، ونوصي بشدّة بحفظها في ذاكرتك بدلاً من كتابتها حيث قد يجدها آخرون.

تسجيل الخروج التلقائي

عليك دائماً تسجيل الخروج من الخدمات المصرفية للشركات عبر الإنترنت عند الانتهاء. إذا نسيت ذلك، سيتولّى نظامنا تسجيل خروجك تلقائياً بعد فترة زمنية.

حماية خصوصيتك

من أجل مساعدتنا في تثبيت حماية معلوماتك الشخصية، قد تُطلب منك إعادة إدخال بيانات اعتماد تسجيل الدخول الخاصّة بك قبل ولوج الصفحات التي تتضمنّ عنوانك و/أو رقم هاتفك و/أو بيانات اعتمادك لتسجيل الدخول. يؤديّ تقديم بيانات الاعتماد هذه إلى تثبيت هويتك، ما يضمن أنك الوحيد الذي يمكنه رؤية المعلومات الحسّاسة وتعديلها.

الحماية من الاحتيال

لحمايتك من المعاملات الاحتيالية، قد تُطلب منك أيضاً إعادة إدخال بيانات اعتماد تسجيل الدخول الخاصّة بك أثناء إجراء أيّ معاملة يتخلّلها نقل أموال إلى خارج البنك (على سبيل المثال، دفع فاتورة أو تحويل إلى حساب خارجي).

كيف يمكنك أن تحافظ على أمانك؟

- إحرص دائماً على تحديث برامج الحماية من الفيروسات. من شأن ذلك أن يساعد في حمايتك من البرامج التي تحاول تثبيت نفسها على حاسوبك للاستيلاء على معلومات شخصية. يوصى أيضاً باستخدام برامج الحماية من التجسس بهدف التصديّ للبرامج الضارّة المعروفة باسم "البرمجيات الخبيثة".
- إحرص دائماً على تحديث نظام تشغيل حاسوبك. تحقّق بانتظام من توفّر الرّقع الأمنيّة.
- تحقّق دائماً من اسم الموقع الإلكتروني للبنك في متصفّحك. يجب أن يظهر: "https://corporate.byblosonline.com". أمّا إذا ظهر عنوان آخر فلا تكون حينها في موقع بنك بيبلوس ويجب إغلاق النافذة مباشرةً.
- لا ترسل أبداً بريداً إلكترونياً يتضمّن معلوماتك الشخصية، بما في ذلك العنوان أو أرقام الحساب أو أرقام بطاقات الائتمان أو بيانات اعتماد تسجيل الدخول. إذا كان التوقيع الذي يذيلّ بريدك الإلكتروني يتضمّن معلومات مماثلة، يجب أن تغيّر توقيعك. إذ إنّ البريد الإلكتروني غير مشفّر ويمكن اعتراضه. لإرسال معلومات سرّية إلينا، سجّل الدخول إلى حساب الخدمات المصرفية للشركات عبر الإنترنت الخاصّ بك واستخدم خدمة الرسائل الآمنة التي نوفّرها.
- لا تردّ أبداً على أيّ بريد إلكتروني يطلب منك النقر على رابط للاتصال بالبنك. تُعدّ هذه الرسائل الإلكترونيّة جزءاً مما يسمّى "التصيد الاحتيالي" أو الخداع الإلكتروني. لن يرسل إليك بنك بيبلوس بريداً إلكترونياً يطلب منك تقديم مثل هذه المعلومات الشخصية، ولن نتصل بك أبداً لهذا الغرض. يُرجى الاتصال بممثل البنك الذي تتعامل معه في حال تلقيت رسالةً إلكترونيّةً أو مكالمة هاتفيّة من هذا القبيل.
- لا تستخدم أبداً ميزات البرامج التي تعرض عليك تذكر كلمة مرورك. قد توفّر هذه الميزات القليل من الراحة، لكنّها في المقابل تتيح الكشف عن كلمة المرور الخاصّة بك لشخص آخر يستخدم جهازك.
- تجنّب تنفيذ أعمالك المصرفية من حاسوب عام (على سبيل المثال، مكتبة أو مقهى أو صالة مطار).