SECURITY GUIDELINES

INVESTBANK
البنك الإستثماري

SECURITY GUIDELINES

INVESTBANK
البنك الإستثماري

في البنك الإستثماري، نحن نأخذ أمن و سرية المعلومات الخاصة بك على محمل الجد. نحن ملتزمون بحماية معلوماتك من خلال سعينا المستمر لتحسين و تطوير التدابير الأمنية المتعلقة بأمن المعلومات حتى تتمكن من الاستمتاع بأحدث الخدمات المصرفية الإلكترونية بشكل آمن.

تالياً بعض الخطوات المهمة التي ينبغي اتخاذها للحفاظ على معلوماتك الشخصية و حساباتك و تعاملاتك الإلكترونية بمأمن:

كلمة السر

تعتبر كلمة السر بمثابة مفتاح الدخول الى الخدمات المصرفية الألكترونية عبر الأنترنت (ككخدمة iBank)، حيث أن كشف كلمة السر الخاصة بك من قبل أشخاص آخرين يمكنهم من الدخول الى حساباتك البنكية الألكترونية و الإطلاع عليها و القيام بعمليات احتيال. لذا، فإنه من الضروري جداً حماية كلمة السر و الحفاظ عليها.

النصائح التالية ستساعدك في حماية كلمة السر الخاصة بك:

- لا تفصح لاحد عن كلمة السر الخاصة بك.
- اختر كلمة سر مناسبة يصعب على الآخرين تخمينها.
- لا تستخدم كلمة السر ذاتها لحساباتك المختلفة. على سبيل المثال، يجب أن تكون كلمة السر الخاصة بحسابك على iBank مختلفة تماما عن كلمة السر الخاصة ببريدك الإلكتروني.
- اختر كلمة سر يمكنك تذكرها دون الحاجة الى كتابتها.
- قم بتغيير كلمة السر بشكل دوري.
- تأكد من عدم مراقبة أي أشخاص آخرين لك عند استخدام كلمة السر أو الرقم السري (PIN).

كيفية إنشاء كلمة سر مناسبة:

- يجب أن تكون كلمة السر قوية بحيث تحتوي على حروف (A a) و أرقام و رموز خاصة (& @ ! #).
- كلما كانت كلمة السر أطول، كلما كان اختراقها أصعب.
- تجنب استخدام معلومات شخصية يسهل على الأخرين معرفتها كتاريخ ميلادك أو اسم مدرستك أو جامعتك.

لتسهيل حفظ كلمة السر، يمكنك استخدام عبارة أو جملة ذات معنى لتكون كلمة سر قوية. على سبيل المثال، العبارة التالية:
"Be the change you wish to see in the world"
يمكن أن تستخدم لتشكل كلمة السر "B+cUw2c"
وذلك بأخذ الحرف الأول من كل كلمة و استخدام أرقام و رموز خاصة.

تذكر: لا تقم بكشف كلمة السر أو الرقم السري لأحد، البنك الاستثماري لن يطلب منك ذلك أبداً. اذا قام أحد ما بطلب كلمة السر أو الرقم السري الخاص بك سواءً من خلال الهاتف أو البريد الإلكتروني أو أي وسيلة أخرى فإن ذلك على الأرجح سيكون بغرض الإحتيال.

الهندسة الإجتماعية:

أسلوب يستخدمه المحتالون لخداع الأشخاص و الحصول على معلومات حساسة يمكن استخدامها فيما بعد لأغراض الاحتيال. يعتمد هذا الأسلوب على استغلال الصفات الاجتماعية للأشخاص و خداعهم لكسب ثقتهم وبالتالي الحصول على معلومات لا يكشفها الفرد عادةً للغرباء، كأن يتصل بك شخص ما و يدعي بأنه يعمل لدى البنك الذي تتعامل معه و يطلب منك معلومات شخصية.

يمكن أن تتخذ الهندسة الإجتماعية أشكال عدة، كالخداع الإلكتروني (Spoofing) و التصّيد (Phishing)، كما يمكن أن تتم بوسائل عدة كالهاتف و البريد الإلكتروني و الرسائل النصية.

الخداع الإلكتروني (Spoofing)

هو أسلوب يستخدمه المحتالون للتخفي على اعتبار أنهم مصدر موثوق، حيث يقوم المحتالون بإرسال رسائل بريد إلكتروني مزيفة بعد إجراء تعديلات عليها لكي تظهر للمستقبل على أنها قادمة من مصدر موثوق (كالبنك الذي تتعامل معه)، و هذا ما يسمى بـ 'الخداع من خلال البريد الإلكتروني' (Email Spoofing). من الطرق الأخرى الشائعة أيضاً انشاء موقع الكتروني مزيف يشبه الى حد كبير جداً الموقع الأصلي الخاص بالبنك الذي تتعامل معه و ذلك بهدف الإحتيال، و هذا ما يسمى بـ 'الخداع من خلال المواقع الإلكترونية' (Website Spoofing).

التصيّد (Phishing)

هو أسلوب آخر يتم ارسال الاف رسائل البريد الإلكتروني المزيفة و التي تظهر بأنها صادرة من مصدر موثوق بهدف تضليل الناس للحصول منهم على معلومات سرية (مثل معلومات البطاقة الائتمانية، كلمة السر الخاصة بالحسابات البنكية الإلكترونية، أو حتى معلومات شخصية). يستخدم المحتالون أساليب الخداع الإلكتروني المذكورة سابقا في عملية التصيّد.

مثال:
قد يقوم المحتالون بإرسال الاف رسائل البريد الإلكتروني المزيفة على أنها صادرة من البنك الذي تتعامل معه، و يطلبون من العميل التوجه الى الموقع الالكتروني الخاص بالخدمة المصرفية عبر الأنترنت و ذلك بالنقر على رابط الكتروني داخل الرسالة نفسها، و قد يبررون ذلك لغايات تحديث البيانات الشخصية الخاصة بالعميل أو لأسباب أخرى. في حال قيام العميل بالنقر على الرابط، يقوم الرابط بتوجيه العميل الى موقع الكتروني مزيف يشبه الى حد كبير جدا الموقع الفعلي للخدمة الإلكترونية الخاصة بالبنك بحيث يصعب على العميل اكتشاف ذلك، و عند قيام العميل بإدخال المعلومات على الموقع المزيف يحصل عليها المحتالون و يستخدمونها للدخول الى الحسابات و القيام بعمليات احتيال.

كيف تحمي نفسك؟

- لا تقم بالرد على أية رسائل بريد الكتروني أو رسائل نصية قصيرة (SMS) مشبوهة، ولا تقم بالنقر على أية روابط داخل الرسالة. يمكنك الاتصال بمركز الخدمة الهاتفية للاستفسار عن أية رسائل قد تبدو أنها صادرة من البنك الاستثماري.
- تحقق من هوية الذين يتصلون بك لطلب معلومات شخصية دون سابق معرفة، كأن تسأل عن اسم المتصل، و مكان عمله، و الغاية من طلب المعلومات، وتحقق أيضاً من رقم هاتف المتصل.
- انتبه دائماً لعنوان المواقع الإلكترونية عند تصفح الانترنت. عند قيامك بزيارة المواقع الإلكترونية، فإنه يفضل أن تقوم بإدخال عنوان الموقع الإلكتروني (على سبيل المثال، موقع iBank) بنفسك بدلاً من النقر على روابط قد تجدها في رسائل البريد الإلكتروني أو حتى من خلال مواقع الكترونية أخرى.
- تجنب الدخول الى المواقع الإلكترونية التي تدعي أنها تقدم خدمات مصرفية عبر الأنترنت في حال عرض متصفح الأنترنت أي اشارات تحذير. تذكر دائماً أن العنوان الإلكتروني (URL) لموقع الخدمة المصرفية عبر الأنترنت iBank يبدأ بـ https (بدلاً من http)، و ذلك لتقديم خدمات مصرفية آمنة لكم.
- ينصح بمراجعة الحركات المتعلقة بحساباتكم بانتظام و ذلك لكشف أية محاولات احتيال.
- قم بإبلاغ البنك على الفور في حال التعرض لأية محاولات احتيال أو استقبال أية رسائل أو مكالمات مشبوهة، وذلك من خلال مركز الخدمة الهاتفية على الرقم +٩٦٢(٦)١٥١٥٠٠

نصائح عامة:

- دائما استعن بحدسك و لا تعطي معلومات تعتبرها حساسة يمكن أن يستفيد منها آخرون للقيام بعمليات احتيال.
- ينصح بتوفير الحماية الضرورية لجهاز الحاسوب الذي تستخدمه للدخول الى خدماتنا الإلكترونية من خلال:
- استخدام برامج الحماية من الفيروسات، و تحديثها باستمرار.
- تحديث نظام التشغيل (على سبيل المثال نظام التشغيل ويندوز) و برنامج تصفح الأنترنت باستمرار.
- تجنب الدخول الى الخدمة المصرفية الإلكترونية iBank من الاماكن العامة أو مقاهي الانترنت.
- عند الانتهاء من استخدام الخدمة المصرفية الإلكترونية، قم بالضغط على 'log out' و إغلاق متصفح الإنترنت.

فيما يتعلق بالبطاقات الإئتمانية، فإنه ينصح بما يلي:

- لا تشارك أي شخص بطاقتك الإئتمانية أو الرقم السري.
- استخدم بطاقة الإئتمان أو معلوماتك الشخصية فقط على المواقع التي تثق بها.
- عند استخدام بطاقتك عند نقاط البيع، تأكد من أن البائع يستخدم البطاقة أمام نظرك بغض النظر عن أية أعذار يقدمها وذلك حتى لا يتمكن أحد من تصوير البطاقة أو تدوين تفاصيلها.

للاتصال بمركز الخدمة الهاتفية: هاتف رقم +٩٦٢(٦)١٥١٥٠٠