Habib Bank AG Zurich

Habib Bank AG Zurich (HBZ) is committed to protecting your account information and transaction details. We have implemented a number of controls and security measures designed to monitor and secure your data.

Please note that HBZ will never request you to share confidential information such as your personal data, account number, Internet banking username and/or password, credit card details, etc. via email, text messages or automated phone calls.

Unfortunately online fraud is growing and criminal elements continue targeting consumers. One of the most common attacks is known as "phishing" where a fraudulent email appears to be sent from HBZ. This scam email includes a link to a web page that looks like the Bank's site and requests personal information. This is not a legitimate HBZ email and the link does not go to a genuine HBZ web page. Under no circumstances should you provide your personal information by replying to the fraudulent email, click on any links and login.

HBZ never requests this information from its customers in this manner.

HBZ Security Tips

Please do not be alarmed but remain vigilant. Below are some simple tips to remember, which will help keep you protected:

- Never respond to email requests that ask for any bank details. Please do not reply or click on any link that requires you to login to a bank account. Simply delete the e-mail.
- Never send your account information via an email system other than the email system within your secure online banking web site.
- If you have previously replied to a suspicious email and provided personal or sensitive information about your account, please contact your branch immediately at +971 4 260 7999.

Also refer to the Security Advisory notice on the login page.

To login to your account, always type: https://online.habibbank.com

يلتزم حبيب بنك إيه جي زيورخ (HBZ) بحماية معلومات حسابك وتفاصيل المعاملات. لقد قمنا بتنفيذ عدد من الضوابط والتدابير الأمنية المصممة لمراقبة وتأمين بياناتك.

يرجى ملاحظة أن حبيب بنك اي جي زيوريخ (HBZ) لن يطلب منك أبدًا مشاركة المعلومات السرية مثل بياناتك الشخصية ورقم حسابك واسم المستخدم و / أو كلمة المرور الخاصة بالخدمات المصرفية عبر الإنترنت وتفاصيل بطاقة الائتمان وما إلى ذلك عبر البريد الإلكتروني أو الرسائل النصية أو المكالمات الهاتفية الآلية.

لسوء الحظ، يتزايد الاحتيال عبر الإنترنت وتستمر العناصر الإجرامية في استهداف المستهلكين. يُعرف أحد أكثر الهجمات شيوعًا باسم «التصيد الاحتيالي» حيث يبدو أن البريد الإلكتروني الاحتيالي قد تم إرساله من قبل حبيب بنك اي جي زيوريخ (HBZ). يتضمن هذا البريد الإلكتروني الاحتيالي رابطًا إلى صفحة إلكترونية تشبه موقع البنك وتطلب معلومات شخصية. يرجى العلم بأن هذا ليس بريدًا إلكترونيًا شرعيًا لحبيب بنك إيه جي زيوريخ (HBZ) ولا ينتقل الرابط إلى صفحة إلكترونية حقيقية / رسمية لحبيب إيه جي زيوريخ (HBZ). لا يجوز لك تحت أي ظرف من الظروف تقديم معلوماتك الشخصية عن طريق الرد على البريد الإلكتروني الاحتيالي والنقر فوق أي روابط وتسجيل الدخول.

حبيب بنك إيه جي زيوريخ لا يطلب هذه المعلومات من عملائه بهذه الطريقة.

إرشادات ونصائح أمنية من حبيب بنك اي جي زيوريخ (HBZ):

من فضلك لا تنزعج ولكن كن يقظا وحذراً. فيما يلي بعض النصائح البسيطة التي يجب تذكرها، والتي ستساعدك في الحفاظ على حمايتك:

- لا ترد مطلقا على طلبات البريد الإلكتروني التي تطلب أي تفاصيل بنكية. يرجى عدم الرد أو النقر فوق أي رابط يتطلب منك تسجيل الدخول إلى حساب مصرفي. ما عليك سوى حذف البريد الإلكتروني.
- لا ترسل معلومات حسابك عبر نظام البريد الإلكتروني بخلاف نظام البريد الإلكتروني داخل موقع الإلكتروني الآمن للخدمات المصرفية عبر الإنترنت.
- إذا قمت مسبقًا بالرد على رسالة بريد إلكتروني مشبوهة وقدمت معلومات شخصية أو سرية حول حسابك، فيرجى الاتصال بفرعك على الفور على الرقم 7999 260 4 971+.

قم بمراجعة إشعار النصائح والارشادات الأمنية على صفحة تسجيل الدخول.

لتسجيل الدخول إلى حسابك، اكتب: https://online.habibbank.com

NOTE:

HBZ expressly dissociates itself from any transaction based on such scam correspondence or any other representation made via any fictitious websites/e-mail addresses. The Bank will not be liable for any loss incurred by any person based on actions taken through these websites/e-mail addresses.

ملاحظة:

ينأى حبيب بنك إيه جي زيوريخ بنفسه عن أي معاملة بناءً على المراسلات الاحتيالية أو أي تمثيل آخر يتم عبر أي مواقع إلكترونية / عناوين بريد إلكتروني وهمية. لن يكون البنك مسؤولاً عن أي خسارة يتكبدها أي شخص بناءً على الإجراءات المتخذة من خلال هذه المواقع / عناوين البريد الإلكتروني.