النموذجية
الإسلامية للتمويل الأصغر

أمن المعلومات و نصائح ارشادية لعملاء الشركة النموذجية الاسلامية للتمويل الأصغر

مقدمة:

ان المحافظة على معلومات العملاء وسريتها تعد من الاولويات لدى الشركة النموذجية الاسلامية للتمويل الأصغر، لذلك فاننا نقوم بالاطلاع المستمر على اخر المستجدات في مجال امن وحماية المعلومات من اجل توفير أقصى وأفضل السبل لحماية المعلومات والبيانات التي تخص العملاء وتمويلاتهم لدى الشركة. ومن منطلق سياسة امن المعلومات في توفير الحماية لمعلومات وبيانات العملاء، فانه يتم اتخاذ الإجراءات الضرورية المناسبة وتطويرها في هذا المجال ومنها: تطبيق أنظمة متخصصة في مجال الحماية من الفيروسات ،النسخ الاحتياطي ،وتشفير البيانات المتناقلة لحمايتها من خطر السرقة، إضافة إلى تطبيق الجدران النارية وأجهزة الحماية الخاصة. وفيما يلي بعض النصائح الخاصة بامن المعلومات والتي يجب الانتباه اليها ومراعاتها:

أولاً : حماية كلمة السر (الرقم السري):

الرقم السري : هو مفتاح الوصول إلى البيانات ،المعلومات والحسابات التي تخصك.

افضل الممارسات لحماية كلمة السر:

1. استخدم كلمة سر مكونة من 8 خانات على الاقل .
2. استخدم كلمة سر قوية تحتوي على حروف وارقام ورموز خاصة مثل (#@$*&) حتى لا يمكن للمخترق الحصول عليها بسهولة .
3. لا تفصح لاحد عن كلمة السر الخاصة بك.
4. كلمة السر تحفظ في الذاكرة لا تكتبها ابدا ، او تتركها في مكان مكشوف.
5. قم بتغيير كلمة السر الخاصة بك بشكل دوري او كلما اقتضت .
6. قم بالتغطية اثناء ادخالك لكلمة السر.
7. لا تستخدم كلمة سر من السهل تخمينها مثل (اسم والدك، اسمك، رقم الهاتف، تاريخ الميلاد).
8. لا تستخدم حروف وارقام متكررة مثل (aaa،1234).
9. معظم المواقع تقدم خدمة تذكير في حال نسيان كلمة المرور ، فكن حذرا من اختيارك للاسئلة التذكيرية لكلمة السر بحيث لا تكون قابلة للتخمين مثل (اذا اخترت اسم والدك كجواب لسؤال التذكير ، كن حذرا ممن يعرفون هذه المعلومة).
10. عند تغيير كلمة السر استخدم كلمة سر تختلف عن السابقة.
11. لا تقم بإدخال كلمات المرور عندما يتمكن الآخرون من ملاحظة ما تكتبه.

ثانيا : سرقة الهوية / انتحال الشخصية Identity Theft

هي نوع من الجرائم تهدف الى الحصول على البيانات والمعلومات الشخصية الخاصة بك ، وبالتالي يتمكن المجرم من انتحال شخصيتك واستغلال تلك البيانات والمعلومات في الخداع بهدف تحقيق مكاسب مالية غير مشروعة ، من الامثلة على البيانات الشخصية المعرضة للسرقة:

1. رقم الحساب.
2. اسم المستخدم، كلمة السر.
3. تاريخ الميلاد، رقم الهاتف او عنوانك.
4. رقم بطاقة الائتمان .
5. كلمة السر الخاصة ببطاقة الصراف الآلي.

افضل الممارسات لتجنب الوقوع في عمليات الاحتيال:

1. لا تثق باي رسالة او اي شخص يطلب منك معلومات شخصية عبر الهاتف ، حتى لو وصلتك رسالة الكترونية من بريد الكتروني يطلب منك معلومات شخصية حتى وان كانت من شخص تعرفه.
2. قم باتلاف كشف حسابك او البيانات الشخصية غير الضرورية بشكل امن.
3. راقب حساباتك واطلب كشف بالحركات المالية بشكل دوري.
4. تفقد فواتير مشترياتك للتأكد من عدم وجود مشتريات لم تقم بشرائها.
5. لا تحمل بيانات حساسة او كلمة السر في محفظتك او حقيبة اليد.
6. اشترك في خدمات الرسائل القصيرة SMS لمراقبة الحركات التي تتم على حسابك البنكي.
7. تجنب الدخول الى الخدمات المصرفية الخاصة بك من الاماكن العامة مثل مقاهي الانترنت او الانترنت المجاني.
8. عند عملية الشراء عبر الانترنت حاول ان تستخدم بطاقة شراء خاصة تصدرها البنوك لهذه الغاية ، وعدم استخدام بطاقة الائتمان البنكية.
9. لا تحتفظ برقمك السري على جهاز الهاتف المحمول او جهاز الكمبيوتر المحمول بشكل واضح ومفهوم الدلالة.
10. لا تدخل معلومات شخصية او الرقم السري من خلال القنوات الالكترونية والانترنت الا اذا بدأ الموقع بـHTTPS:\\
11. قم بالضغط على مفتاح (sign out)عند الانتهاء من استخدام الخدمة وتأكد من انك قمت بالخروج من الخدمة عند عدم ملازمتك جهاز الحاسب.

ثالثا : الهندسة الاجتماعية او الاحتيال الالكتروني عبر الانترنت (Social Engineering):

التصيد او الاحتيال الالكتروني هو نوع من الخداع على شبكة الانترنت للحصول على بيانات العميل الشخصية مثل رقم بطاقة الائتمان ، كلمة السر ، من اجل استخدامها في أغراض احتيالية، حيث يقوم المحتالون بإرسال الآلاف من رسائل البريد الالكتروني مغشوشة المصدر (او الرسائل القصيرة) التي تظهر بأنها مصدر موثوق، مثل البنك الذي تتعامل معه وتطلب تقديم معلومات شخصية او تطلب إتباع رابط يوجهك الى مواقع مزيفه انشأت لأغراض الاحتيال، بهدف استخدام المعلومات لاستخدام الحساب المصرفي للعميل لأغراض المحتالين غير المشروعة.

ملاحظة: لن تقوم الشركة النموذجية الاسلامية للتمويل الأصغر بطلب أي معلومات خاصة بحساب العميل / التمويل من خلال البريد الالكتروني ،أو وسائل الاتصال المختلفة.

نصائح لحمايتك من الاحتيال الالكتروني عبر الانترنت:

1. لا تكشف بياناتك الشخصية مثل رقم الهوية ، ارقام الحسابات او كلمات المرور عبر الهاتف ، البريد الالكتروني او غيرها من وسائل الاتصال الالكترونية.
2. كن حذرا عند استلامك رسائل الكترونية تمنحك الحصول على مبالغ مالية او استخدام حسابك لتحويل الأموال إليه، حيث أن هذه الرسائل لا تعود للبنك وإنما لشخص يحاول سرقة معلومات، فلا تقم بالاستجابة لهذه الرسائل.

نصائح لحمايتك من القرصنة باستخدام اجهزة الصراف الآلي او البطاقات الالكترونية:

1. احرص على متابعة اي اشخاص من حولك او اي حركات مشبوهة ، انتبه الى سيارات تصطف قريبة من جهاز الصراف الالي.
2. انتبه جيدا الى جهاز الصراف الالي الذي تنوي استخدامه اذا لاحظت وجود اشياء غريبة مثل : اجهزة ، اسلاك ، مواد لاصقة، اشرطة مغناطيسية، لا تستخدم ذلك الجهاز . انظر الى قارئ البطاقات ، اذا شاهدت شريطا بلاستيكيا او ما شابه ذلك لا تضع بطاقتك في الجهاز وابلغ البنك عنه فورا.
3. اذا حاولت ادخال بطاقة الصراف الالي ولم تدخل بسلاسة لا تحاول ادخالها بالقوة.
4. احرص على تذكر الرقم السري لبطاقتك ، لا تفصح لاي شخص عنه ، ولا تحتفظ به مكتوبا في محفظتك او حقيبتك او محفوظا مع البطاقة .
5. قم بالتغطية اثناء ادخالك لكلمة السر الخاصة باجهزة الصراف الآلي.