نصائح وارشادات لحماية بياناتك ومعلوماتك المالية

تعد المحافظة على معلومات العملاء وسريتها من أولويات شركة الأهلي لتمويل الأصغر، من هذا المنطلق تقوم شركة الأهلي لتمويل الأصغر بمواكبة آخر المستجدات في مجال أمن وحماية المعلومات لتوفير أفضل طرق حماية بيانات العملاء وحساباتهم.

وبالإضافة إلى التقنيات الحديثة وحلول الحماية الأمنية التي تطبقها شركة الأهلي لتمويل الأصغر لجعل تجربتك المصرفية عبر الانترنت أكثر أماناً وسهولة، نقدم لك تالياً اهم النصائح الخاصة بأمن المعلومات التي عليك اتباعها عند إتمام تعاملاتك المالية:

1.حماية كلمات السر:

- استخدم كلمة سر تتكون من 8 خانات على الأقل.

- استخدم كلمة سر تحتوي على حروف وأرقام ورموز خاصة مثل (#,!,@,$,*,&,?,%) .وتجنب استخدام تسلسل الأرقام (123456) أو الحروف (a b c d) في تكوين كلمة السر.
- لا تكتب كلمتك السرية ابدأ، أو تتركها في مكان مكشوف.
- لا تفصح لاحد عن كلمتك السرية سواء عبر الهاتف أو بالبريد الإلكتروني.
- احرص على تغيير كلمتك السرية بشكل منتظم أو كلما دعت الحاجة.
- يتوجب تغيير كلمتك السرية فوراً اذا راودك الشك بأنه تم كشفها.
- لا تنشئ كلمتك السرية مستخدماً كلمات وأشياء معروفة يسهل تخمينها (اسم والدك، العائلة، رقم الهاتف، تاريخ الميلاد)
- عند تغيير كلمة السر استخدم كلمة سر تختلف عن السابقة.

2.التصيد أو الاحتيال الالكتروني عبر الإنترنت (Phishing)

التصيد أو الاحتيال الالكتروني هو نوع من الخداع على شبكة الإنترنت للحصول على بيانات العميل الشخصية والحساسة مثل (رقم بطاقة الائتمان ، كلمة السر، رمز المستخدم) لاستخدامها في أغراض احتيالية، حيث يقوم المحتالون بالاتصال الإلكتروني بالضحية وذلك بإرسال رسائل البريد الالكتروني مجهولة/مغشوشة المصدر وإيهامهم بأنها من مصدر موثوق وأن المرسل جدير بالثقة ، كالتظاهر بأنه شركة الأهلي لتمويل الأصغر الذي تتعامل معه، وتطلب تقديم معلوماتك الشخصية أو تطلب النقر على رابط يوجهك إلى مواقع مضللة تم إنشائها لأغراض الاحتيال.

عند الدخول إلى المواقع الإلكترونية المضللة يتم طلب البيانات الحساسة مثل أرقام الحسابات وكلمة السر، كما يمكن أن تحتوي هذه المواقع على برمجيات خبيثة/فيروسات يتم تحميلها على جهاز المستخدم.

تذكر شركة الأهلي لتمويل الأصغر لن يطلب منك أبداً:

- **رقمك السري الخاص بالبطاقة .**
- **كلمتك السرية .**

سواء من خلال البريد الإلكتروني أو عن طريق الرسائل النصية القصيرة (SMS).

3.نصائح لتجنب الاحتيال الالكتروني عبر الانترنت

- كن حذراً في كافة اتصالاتك الإلكترونية، فكّر قبل أن تضغط على أي رابط إلكتروني.
- تجنب استخدام الخدمة المصرفية عبر الانترنت من خلال مقاهي الإنترنت و/ أو الأماكن العامة.
- عند استقبالك لأي بريد إلكتروني كن حذراً عند فتح أية ملفات مرفقة.
- لا تكشف بياناتك الشخصية مثل رقم الهوية ، أرقام الحسابات أو كلمات السر عبر الهاتف ، البريد الالكتروني او غيرها من وسائل الاتصال الالكترونية.
- اقرأ بعناية كافة تعليمات الخصوصية والأمن في المواقع التي تتعامل معها.
- كن حذرا عند استلامك رسائل إلكترونية تمنحك الحصول على مبالغ مالية أو استخدام حسابك لتحويل الأموال إليه، حيث أن هذه الرسائل لا تعود للبنك وإنما لشخص يحاول سرقة معلومات، فلا تقم بالاستجابة لهذه الرسائل.

4.ارشادات الاستخدام الآمن للمحافظ الالكترونية

نظراً لتزايد هجمات التصيد والقرصنة الإلكترونية، وبروز العديد من التهديدات السيبرانية وعمليات الاحتيال والانتحال التي تستهدف سرقة حسابات مستخدمي المحافظ الإلكترونية، نرجو اتباع الارشادات الأمنية التالية لضمان الاستخدام الآمن لهذه المحافظ في حال كنت من مستخدميها وحماية نفسك واموالك:

- لا تعطي رمز تفعيل محفظتك أو رقمها السري لأي أحد ابداً وخاصة عبر مواقع التواصل الاجتماعي.
- لا تقم بكتابة او بتخزين معلوماتك المتعلقة بمحفظتك الإلكترونية (اسم المستخدم وكلمة المرور) سواء ورقياً او الكترونياً على اجهزتك الإلكترونية الشخصية (الهاتف المحمول، جهاز الكمبيوتر، الخ ..)
- تجنب الاتصال بالشبكات اللاسلكية المفتوحة وغير الآمنة في الأماكن العامة فقد تكون نقطة لكشف بياناتك ومعلومات حسابك.
- ضرورة تحديد كلمة مرور لجهازك وعدم تركه بدون كلمة مرور.
- احذر عمليات الاحتيال للوصول إلى معلوماتك وانتحال شخصية الجهة المزودة للخدمة من خلال الاتصال الصوتي معك او عن طريق رسائل التصيد الإلكتروني.

- يمثل رقم هاتفك المحمول اسم المستخدم لحامل المحفظة الإلكترونية وهويتك للدخول إلى محفظتك، فحافظ عليه، وفي حالة فقدان هاتفك او خطك يتوجب تبليغ الجهات المسؤولة.
- تجنب تحميل البرامج والتطبيقات المجانية من الانترنت، حيث تعتبر أكثر الوسائل لنشر البرامج الخبيثة التي تستخدم للوصول إلى اجهزتك وسرقة بياناتك.
- تأكد من استخدام وتفعيل برامج الحماية من الفيروسات على هاتفك المحمول.

يمكننا الاجابة على جميع استفساراتكم من خلال مكالمة واحدة

+962 79 7 530530