نصائح أمنية

توقف	فكِر قليلا	احمِي نفسك

لن يطلب البنك الأهلي الكويتي ش.م.ك.ع(البنك) منك أبدًا الكشف عن تفاصيل معلومات الشخصية مثل رقم التعريف الشخصي للبطاقة أو رمز التحقق من البطاقة أو أي تفاصيل مصرفية سرية. يجب أن يظل رقم التعريف الشخصي لبطاقتك سريًا ومعروفًا لك انت فقط.
في حال راودتك اي شكوك بشأن أي بريد إلكتروني أو مكالمة أو رسالة نصية، فيرجى الاتصال بمركز الاتصال الذي يعمل على مدار الساعة طوال أيام الأسبوع +97146075507 (داخل/خارج الإمارات العربية المتحدة).

- الاحتيال عبر الرسائل النصية القصيرة
- التصيد الاحتيالي
- مبادلة وحدة تعريف المشترك (SIM)
- انتحال الهوية
- نصائح كلمة المرور
- نصائح كلمة المرور لمرة واحدة
- نصائح حول الأمن المصرفي عبر الهاتف المتحرك
- الاحتيال عند الإيداع النقدي
- التصيد الصوتي
- نصائح لاستخدام آمن لأجهزة الصراف الآلي
- نصائح أمان الخدمات المصرفية عبر الإنترنت
- تزوير الشيكات المصرفية
- اختراق البريد الإلكتروني للنشاط التجاري الاحتيال بالفواتير

الاحتيال عبر الرسائل النصية القصيرة

- كن متيقظاً ولا تكن ضحية للاتصالات الاحتيالية، قد تتلقى رسالة نصية قصيرة تخبرك بأن بطاقة الخصم المباشر الخاصة بك محظورة أو غير نشطة أو أن حسابك المصرفي محظور مع تعليمات للاتصال برقم معين لإعادة تنشيط بطاقة الخصم المباشر أو الحساب المصرفي الخاص بك.
- يحتمل أن يقدم المتصل نفسه/نفسها كأحد موظفي البنك ويطلب معلوماتك الشخصية والمصرفية وكلمة المرور لمرة واحدة.
- ستسمح هذه المعلومات للمحتال بالوصول وإجراء معاملات غير مصرح بها من حساباتك المصرفية لدى البنك.
- يرجى الحذر من استخدام المحتالين تقنية انتحال هوية المتصل لإخفاء رقم هاتفهم الفعلي وعرض رقم البنك.

احم نفسك من الاحتيال عبر الرسائل النصية القصيرة:

- لا تفصح عن تفاصيل حسابك المصرفي، أو أي أرقام لحسابك أو أرقام بطاقتك أو اسم المستخدم أو رقم التعريف الشخصي أو كلمة المرور لمرة واحدة لأي شخص عبر الهاتف أو الرسائل القصيرة أو البريد الإلكتروني.
- في حال تلقيت مثل هذه المكالمة أو الرسالة المشبوهة ولم تقم بالكشف عن أي من التفاصيل المذكورة أعلاه، قم بإنهاء المكالمة فوراً والاتصال بنا على رقم مركز الاتصال الخاص بنا على مدار الساعة طوال أيام الأسبوع +97146075507 (داخل/خارج الإمارات العربية المتحدة) للتحقق من صحة الطلب.
- لا تقم بالاتصال بالرقم المقدم من المحتال ابداً.

التصيد الاحتيالي

- التصيد الاحتيالي هو عملية إرسال بريد إلكتروني أو رسالة نصية أو اتصال والادعاء كذباً أنها مؤسسة شرعية وفي هذه الحالةالادعاء بأنها بنك، لخداع المستخدم لمشاركة المعلومات الخاصة به ليتم استخدامها لسرقة الهوية،و تُعرف الطلبات الواردة من القنوات غير المصرح بها للحصول على معلوماتك الشخصية بمحاولات التصيد الاحتيالي.
- في حالات هجوم التصيد عبر البريد الإلكتروني أو الرسائل النصية، ستوجه الرسالة المستخدم لزيارة موقع ويب حيث يُطلب منه تحديث المعلومات الشخصية، مثل كلمات المرور وأرقام بطاقات الائتمان والحسابات المصرفيةبحيث يكون موقع الويب مزيف وقد أُعِد فقط لسرقة معلومات المستخدم الخاصه.

احم نفسك من التصيد الاحتيالي:

- تَتَبّع علامات التحذير مثل طلبات الحصول على معلومات شخصية، ملاحظة هامة: لن يطلب البنك أبدًا أيًا من معلوماتك الشخصية عبر البريد الإلكتروني أو الرسائل النصية أو المكالمات الهاتفية العشوائية.
- احذرمن لغة ونبرة البريد الإلكتروني/الرسالة النصية، فعادة ما تحثك رسائل الاحتيال على التصرف بسرعة وتقديم اقتراح بأن حسابك مُستَهدَف أو من المحتمل إغلاقه إذا لم تقدم المعلومات الشخصية.
- في حال تلقيت أي بريد إلكتروني أو رسالة نصية أو مكالمة مشبوهة، لا تكشف عن أي من التفاصيل المذكورة أعلاه، قم بإنهاء المكالمة فوراً و الاتصال بنا على رقم مركز الاتصال الخاص بنا على مدار الساعة طوال أيام الأسبوع +97146075507 (داخل/خارج الإمارات العربية المتحدة) للتحقق من صحة الطلب.

التصيد ب انتحال رقم البنك

- يمكن للمحتال الاتصال بك عبر الإنترنت عن طريق تعديل معرف المتصل الخاص به ليتطابق مع رقم البنك الخاص بنا وتقديم نفسه/نفسها على أنه أحد موظفي البنك الأهلي الكويتي.
- تكون نية المحتال تضليلك للحصول على أرقام حسابك وأرقام البطاقة ورقم التعريف الشخصي ومعرف المستخدم عبر الإنترنت وكلمة المرور أو معلومات شخصية أخرى.
- يمكن للمحتال أيضًا عمل مكالمة هاتفية وهمية تفيد بأنك ربحت يانصيب أو جائزة نقدية على بطاقتك أو رقم هاتفك، سيطلب المحتال رقم بطاقتك ورقم تعريفك الشخصي، والذي سيستخدمه لإجراء معاملات احتيالية على حسابك/بطاقتك.
- قد يطلب منك المحتال أيضًا تحويل مبلغ معين من المال كرسوم معالجة للمطالبة بالجائزة التي فزت بها.

احم نفسك من التصيد:

- كن مدركًا لدوافع المتصل وحدد هويته قبل الكشف عن أي معلومات يطلبها المحتال منك.
- لا تفصح عن التفاصيل المصرفية الخاصة بك، مثل أرقام حسابك أو أرقام بطاقتك أو اسم المستخدم أو رقم التعريف الشخصي أو كلمة المرور لمرة واحدة.
- راقب كشف حسابك المصرفي على الدوام وتحقق من أرصدة حسابك لتحديد أي معاملات غير مصرح بها.،في حالة العثور على أي معاملات غير مصرح بها، يمكنك الاتصال بنا على مدار الساعة طوال أيام الأسبوع على رقم مركز الاتصال الخاص بنا 97146075507+ (داخل/خارج الإمارات العربية المتحدة).
- في قيامك بالفعل بالكشف عن بياناتك الشخصية والمصرفية للمحتال ثم أدركت لاحقاً أنها عملية احتيال، قم بإبلاغ البنك على الفور عن طريق الاتصال برقم مركز الاتصال الخاص بنا على مدار الساعة طوال أيام الأسبوع 97146075507+ (داخل/خارج الإمارات العربية المتحدة).

مبادلة شريحة الهاتف المحمول (SIM)

اكتسبت الخدمات المصرفية عبر الهاتف المحمول شعبية كبيرة بسبب سهولة الوصول إليها، ومع ذلك، يمكن أن يحاول المحتال إساءة استخدام هذه الخدمات:

- يمكن للمحتال أن ينتحل/تنتحل صفتك ويتواصل مع مزود خدمة الهاتف المحمول الخاص بك ويطلب تبديل شريحة الهاتف المحمول الخاصة بك (SIM).
- و بذلك يتمكنون من الاتصال بالبنك الذي تتعامل معه مستخدمين رقم الهاتف المحمول الخاص بك والوصول إلى حسابك المصرفي.
- يمكن للمحتال إضافة مستفيدين إلى حسابك وتحويل الأموال من حسابك.

منع الاحتيال بمبادلة شريحة الهاتف المحمول (SIM):

- اتصل بمزود خدمة الهاتف المحمول الخاص بك على الفور إذا:
  - اختفت الشبكة من هاتفك المحمول.
  - لم تتلق أي مكالمات أو رسائل نصية قصيرة على هاتفك المحمول.
  - إذا تلقيت إشعار « بطاقة الهاتف المحمول (SIM غير مسجلة» أو «او تم تبديل بطاقة الهاتف المحمول SIM « على هاتفك المحمول):
- قم دائمًا بمراقبة معاملاتك المصرفية، تحقق من بيانات حسابك، وإذا وجدت أي تناقض، فقم بإبلاغ البنك على الفور من خلال الاتصال برقم مركز الاتصال الخاص بنا على مدار الساعة طوال أيام الأسبوع 97146075507+ (داخل/خارج الإمارات العربية المتحدة).
- قم بالتسجيل للحصول على إشعارات الرسائل القصيرة/البريد الإلكتروني لاي حركة على حسابك المصرفي.

انتحال الهوية

يمكن للمحتال استخدام المعلومات التالية لإثبات هويتك وإجراء عملية احتيال:

- الاسم
- تاريخ الميلاد
- العنوان
- رقم الهوية الإماراتية/المدنية.
- المعلومات المصرفية
- رقم الهاتف المتحرك

احمي هويتك:

- عند ضياع أو سرقة مستنداتك المهمة مثل جواز سفرك، فإن بطاقة الخصم المباشر /الائتمان /بطاقة الهوية الامارتية قم بتبليغ البنك.
- يجب الاحتفاظ بمستنداتك المالية والشخصية في مكان آمن.
- لا تكتب رقم التعريف الشخصي على البطاقة ولا تحفظه على جهازك ولا تحمله في محفظتك، لا تكشف عن معلوماتك الشخصية عبر المكالمات الهاتفية أو رسائل البريد الإلكتروني لأي شخص.

نصائح لاستخدام آمن لأجهزة الصراف الآلي

- احفظ رقم التعريف الشخصي الخاص بك، لا تكتبه في أي مكان، ولا تكتبها أبدًا على البطاقة نفسها.
- لا تشارك رقم التعريف الشخصي أو البطاقة مع أي شخص، ولا حتى أصدقائك أو عائلتك.
- حين تكون عند جهاز الصراف الآلي، استخدم يدك لحماية لوحة المفاتيح أثناء إدخال رقم التعريف الشخصي.
- لا تطلب المساعدة من الغرباء لاستخدام بطاقة الصراف الآلي أو التعامل مع أموالك.
- في حالة ضياع أو سرقة بطاقة الصراف الآلي الخاصة بك، قم بالإبلاغ عن ذلك إلى أقرب فرع من فروع البنك الأهلي الكويتي وإبلاغ مركز الاتصال لإيقاف البطاقة على الفور.
- عند إيداع شيك أو بطاقة في جهاز الصراف الآلي الخاصة بك، تحقق من من المبلغ المودع في حسابك بعد يومين، في حالة وجود أي تعارض، قم بإبلاغ البنك على الفور عن طريق الاتصال برقم مركز الاتصال الخاص بنا على مدار الساعة طوال أيام الأسبوع 97146075507+ (داخل/خارج دولة الإمارات العربية المتحدة).
- إذا حجز بطاقتك في جهاز الصراف الآلي، أو إذا لم يتم صرف النقود بعد قيامك بإدخال معاملة، قم بإبلاغ البنك على الفور عن طريق الاتصال برقم مركز الاتصال الخاص بنا على مدار الساعة طوال أيام الأسبوع 97146075507+ (داخل/خارج الإمارات العربية المتحدة).

نصائح كلمات المرور

- لا تستخدم كلمات المرور مثل اسمك لتواريخ الميلاد واسم أطفالك أو تواريخ ميلادهم وأرقام هواتفهم وما إلى ذلك.
- لا تفصح عن كلمة المرور الخاصة بك لأي شخص.
- قم بتغيير كلمة المرور الخاصة بك بانتظام.
- في حالة استخدام كلمة المرور الخاصة بك أو الوصول إليها من قبل أي شخص، اتصل بنا على الفور على رقم مركز الاتصال الخاص بنا على مدار الساعة طوال أيام الأسبوع 97146075507+ (داخل/خارج الإمارات العربية المتحدة).

نصائح كلمة المرور لمرة واحدة

- لا تشارك كلمة المرور لمرة واحدة مع أي شخص.
- لن يطلب موظفوا البنك أبدًا كلمة المرور لمرة واحدة/رقم التعريف الشخصي /رقم التحقق من البطاقة/كلمة المرور
- أبلغنا عندما تقوم بتغيير رقم هاتفك المحمول المسجل لدى البنك
- احذر من المكالمات الهاتفية الغريبة التي تحاول الحصول على معلومات سرية أو مصرفية
- تأكد من اجراء المعاملات المصرفية من أجهزة موثوقة وآمنة

نصائح أمان الخدمات المصرفية عبر الإنترنت

- لا تقم أبدًا بملء أي معلومات مصرفية شخصية في بريد إلكتروني أو استطلاعات أو نماذج ملاحظات.
- احفظ كلمات المرور الخاصة بك بدلاً من كتابتها في مكان ما، ولا تشارك معلوماتك أو تفصح عنها أبدًا.
- في كل مرة تكمل فيها معاملة الخدمات المصرفية عبر الإنترنت، قم بتسجيل الخروج من www.eahli.com. لا تغلق متصفحك فقط.
- للوصول إلى الخدمات المصرفية عبر الإنترنت من البنك الاهلي الكويتي، اكتب دائمًا عنوان محدد موقع الموارد المُوحّد الصحيح (https://abk.eahli.com) في نافذة المتصفح. لا تنقر أبدًا فوق ارتباط يعرض عليك الانتقال إلى موقعنا على الويب.
- قم بتغيير كلمات المرور الخاصة بالخدمات المصرفية عبر الإنترنت بانتظام. مثال: مرة كل 3 أشهر.
- يجب ألا تكون كلمة مرورك سهلة التخمين، استخدم الأحرف والأرقام والأحرف الخاصة [مثل!، @، #، $،٪، ^، &، * (،)] في كلمات مرورك.
- لا تشارك أبدًا كلمات المرور الخاصة بالخدمات المصرفية عبر الإنترنت مع الآخرين، حتى أفراد العائلة.
- تحقق دائمًا من آخر تسجيل دخول إلى حساب الخدمات المصرفية عبر الإنترنت الخاص بك. سجّل الدخول إلى حساب الخدمات المصرفية عبر الإنترنت وانظر في الجزء السفلي «معلومات المستخدم» لعرض تاريخ ووقت آخر تسجيل دخول لك.
- تأكد من تثبيت برنامج مكافحة الفيروسات وتحديثه وتشغيله، استخدم دائمًا برامج الأمان مع ميزات مكافحة الفيروسات ومكافحة التجسس وجدار الحماية لحماية جهاز الكمبيوتر الخاص بك.

نصائح حول الأمن المصرفي عبر الهاتف المتحرك

- قم بإعداد رقم تعريف شخصي/كلمة مرور/بصمة للوصول إلى هاتفك المحمول.
- سجل للحصول على تنبيهات الرسائل القصيرة لتتبع معاملاتك المصرفية.
- لا تنقر على أي روابط في رسالة تطلب أي معلومات بنكية.
- إذا كان عليك مشاركة هاتفك المحمول مع أي شخص آخر أو إرساله للإصلاح/الصيانة:

– امسح سجل التصفح.

– امسح ذاكرة التخزين المؤقت والملفات المؤقتة المخزنة في الذاكرة لأنها قد تحتوي على أرقام حسابك ومعلومات حساسة أخرى.

– قم بحظر تطبيقات الخدمات المصرفية عبر الهاتف المحمول عن طريق الاتصال بالبنك الذي تتعامل معه، يمكنك إلغاء حظرهم عند استعادة الهاتف المحمول.

- لا تقم بحفظ المعلومات السرية مثل أرقام بطاقة الخصم المباشر /الائتمان الخاصة بك أو أرقام التحقق من البطاقة أو أرقام التعريف الشخصية على هاتفك المحمول.
- حافظ على تحديث نظام تشغيل هاتفك المحمول وتطبيقاته، بما في ذلك المتصفح، بأحدث تصحيحات الأمان والترقيات.
- لا تقم بتمكين الملء التلقائي أو حفظ معرفات المستخدم أو كلمات المرور للخدمات المصرفية عبر الإنترنت.
- تجنب استخدام شبكة واي فاي غير آمنة أو شبكات عامة أو مشتركة.
- قم بتنزيل التطبيقات فقط من متاجر التطبيقات الرسمية مثل آبل آي تيونز أو متجر تطبيقات جوجل.
- لا تكشف أبدًا عن المعلومات الشخصية أو بيانات الاعتماد المصرفية عبر الإنترنت عبر البريد الإلكتروني أو الرسائل النصية حيث يمكن استخدامها لسرقة الهوية.
- قم بتسجيل الخروج من الخدمات المصرفية عبر الإنترنت أو التطبيق بمجرد إتمام معاملاتك وإغلاق هذه النافذة.
- توخ مزيدًا من الحذر أثناء كتابة معلومات سرية مثل تفاصيل حسابك وكلمة المرور على هاتفك المحمول في الأماكن العامة.
- في حالة فقدان هاتفك المحمول، يرجى الاتصال بخدمة العملاء على مدار 24 ساعة لتعطيل تطبيق البنك الأهلي الكويتي.

الاحتيال على الإيداع النقدي

- تأكد من تسليم النقود إلى الصراف فقط والحصول على إيصال إيداع نقدي مختوم وموقع من قبل الصراف.
- احتفظ بنسخة من جميع المعاملات.
- قم دائمًا بمراقبة معاملاتك المصرفية، وتحقق من كشوف حسابك، إذا وجدت أي تناقض، قم بإبلاغ البنك الأهلي الكويتي على الفور عن طريق الاتصال برقم مركز الاتصال لدينا على مدار الساعة طوال أيام الأسبوع +97146075507 (داخل/خارج الإمارات العربية المتحدة).

تزوير الشيكات المصرفية

يتم الاحتيال عبر الشيكات عن طريق إيداع شيكات مزورة/تم التلاعب بها للحصول على مبالغ من حسابك و الذي يتسبب بخسارة لك، هناك أنواع مختلفة من عمليات الاحتيال طريق الشيكات، وبعضها مذكور أدناه.

- تعديل الشيكات: يتلاعب المحتالون بكل أو بعض التفاصيل المتعلقة بالمبلغ والتاريخ والمستفيد لصرف الشيك.
- استخدام قلم الحبر السحري: يحدث عند استلام شيك لمعاملة أصلية، يتم إقناع محرر الشيك بملء التفاصيل المتعلقة بالمبلغ و/أو المستفيد بواسطة قلم مقدم من الطرف الثالث، وتختفي كتابة مثل هذا الحبر السحري بعد فترة ويملأ المحتال المبلغ المطلوب واسم المستفيد ليقوم بصرف هذه الشيكات بطريقة احتيالية.
- الشيكات الوهمية: ينشئ المحتالون شيكات أصلية المظهر عن طريق نسخ التفاصيل من الشيكات الأصلية بما في ذلك التوقيعات.
- سرقة الشيكات: تُسرَق الشيكات من الضحايا أو تلك التي تكون قيد التحصيل ومن ثم إيداعها بطريقة احتيالية لدفع مبالغ.

لمنع عمليات الاحتيال في الشيكات:

- حافظ على دفاتر الشيكات الخاصة بك آمنة ومأمونة في جميع الأوقات.
- لا تترك الشيكات الموقعة دون رقابة.
- عند استلام دفتر شيكات جديد، تأكد من أن دفتر الشيكات الخاص بك سليم ولا توجد أوراق شيك مفقودة،قم بإخطار البنك على الفور في حالة فقدان أوراق الشيك.
- لا تترك مسافة قبل وبعد اسم المدفوع لأمره والمبلغ (بالأرقام والكلمات) وارسم خطوطًا في النهاية.
- قم بتسطير الشيك عن طريق رسم سطرين متوازيين أعلى الزاوية اليسرى للشيك لمنع سوء الاستخدام.
- ضع في اعتبارك وجود مجموعة مختلفة من الموقعين بناءً على حدود مبلغ الشيك.
- قم بإتلاف الشيكات التي تحتوي الأخطاء أو مكتوب فوقها أو التالفة.
- تحقق بانتظام من الرسائل القصيرة ورسائل البريد الإلكتروني للاتصال من البنك.
- قم دائمًا بمراقبة معاملاتك المصرفية، والتحقق من كشوف حسابك، والاتصال بالبنك على الفور إذا وجدت أي تناقض.
- لا تصدر شيكات لأشخاص مجهولين، ففي بعض الأحيان يقدم المحتالون صفقات «جيدة جدًا لدرجة يصعب تصديقها» للحصول على عينة فحص من الضحايا.
- إذا قدم لك أحدهم قلمًا للكتابة على مستندات معينة، فكن حذرًا وتحقق مما إذا كان هذا القلم «حبر سحري». تذكر أن استخدام مثل هذه الأقلام محظور في الإمارات العربية المتحدة وأي شخص يتبين أنه يستخدم مثل هذه الأقلام قد ينتهي به الأمر إلى إبلاغ السلطات المختصة.
- إذا تلقيت مدفوعات بشيكات من جهات خارجية، فلا تقم بتسليم البضائع / الخدمات حتى يتم إيداع الشيك في حسابك.
- لا تقم بنقل واستلام المال بين طرفين مقابل عمولة» عن طريق إيداع الشيكات نيابة عن الآخرين ودفعها جزئيًا نقدًا/تحويلات من حسابك، إذا ثبت لاحقًا أن هذا الشيك احتيالي، فقد يتعين على الشخص/الشركة الذي تم استخدام حساباته لإيداع الشيك إعادة الأموال إلى الضحية.
- تحتوي جميع الشيكات على ميزات أمنية، بعضها مطبوع على الوجه الأمامي/ الخلفي للشيك، يرجى التأكد من أن أي شيك تقدمه يحتوي على ميزات الأمان هذه.
- حاول حيثما أمكن استخدام التسهيلات المصرفية الإلكترونية التي يقدمها البنك بدلاً من إصدار شيكات للمدفوعات، في حال وقوعك ضحية للاحتيال عبر الشيكات، قم بإبلاغ البنك الأهلي الكويتي على الفور عن طريق الاتصال برقم مركز الاتصال الخاص بنا على مدار الساعة طوال أيام الأسبوع 97146075507+ (داخل/خارج الإمارات العربية المتحدة) وفكر أيضًا في تقديم شكوى للشرطة.

اختراق البريد الإلكتروني للنشاط التجاري – الاحتيال بالفواتير

لغرض تحويل الأموال غير المصرح بها ، وهو نوع من الاحتيال في الدفع يعرض للخطر البريد الإلكتروني الصحيح للأعمال التجارية بإنشاء حسابات بريد الكتروني مشابه للبريد الالكتروني الصحيح .

طلبات تحويل الأموال من الموردين أو شركاء الأعمال:

- تم اختراق معرف البريد الإلكتروني لموظف الشركة المستهدفة من قبل المحتال.
- يقوم المحتال بمراقبة رسائل البريد الإلكتروني لمستخدم الأعمال، ويبحث عن فواتير الموردين.
- يجد المحتال فاتورة شرعية ويقوم بتعديل معلومات المستفيد، مثل تغيير رقم الحساب/رقم الحساب المصرفي الدولي الذي سيتم إرسال الدفعة إليه.
- تم إخفاء معرف البريد الإلكتروني للمورد لإرسال الفاتورة المعدلة،لا يتطلب ذلك المساس بنظام البريد الإلكتروني للمورد، ولكنه بدلاً من ذلك يرسل الفاتورة من عنوان بريد إلكتروني قريب جدًا من نطاق البائع، بحيث لا يتم الانتباه الى هذا التغيير في الغالب؛ على سبيل المثال ، companyXZY.com @ بدلاً من companyXYZD.com@ .
- عندما تتلقى الشركة طلبات دفع وفواتير مزيفة عبر رسائل البريد الإلكتروني، فإنها ستتعرف على اسم المورد والخدمات المقدمة، لذلك سيقومون بمعالجة الفاتورة وتقديم طلب تحويل الأموال إليهم للدفع.

طلبات تحويل الأموال من الموردين أو شركاء الأعمال:

- يمكن للمحتال اختراق حساب البريد الإلكتروني للمسؤولين التنفيذيين في الإدارة العليا (الرئيس التنفيذي، مدير العمليات، المدير المالي، وما إلى ذلك) وإرسال طلب تحويل الأموال من معرف البريد الإلكتروني المخترق إلى موظفي الإدارة المالية.

يتعين عليك:

- تحسين البنية التحتية الأمنية لشركتك وحماية نطاق شركتك أو خوادمها.
- تساءل دائمًا عن طلبات تحويل الأموال لأي معلومات حساب مستفيد جديد.
- بالنسبة للموردين المعروفين، راقب التغيير في أنماط طلب الدفع، أي القيمة العالية، والعملة المختلفة، خارج الدورة.
- زيادة الوعي بين الموظفين.
- تحقق من صحة معرفات البريد الإلكتروني (الهجاء والمعرفات المقنعة) للمرسل الذي يطلب تحويل الأموال.
- قبل إرسال تعليمات تحويل الأموال إلى البنك الذي تتعامل معه، احصل على تأكيد هاتفي من مرسل البريد الإلكتروني الذي يمكن أن يكون الموردين أو المديرين التنفيذيين للشركة.

لمزيد من التفاصيل حول أنواع الاحتيال، يمكنك زيارة الموقع:
https://www.uaebf.ae