البنك السعودي للاستثمار
The Saudi Investment Bank

كُن آمناً...كُن حذراً

برنامج التوعية بمكافحة الاحتيال

عزيزي العميل،

نظرا لأننا نعمل بجد لحماية القطاع المصرفي من الاحتيال ، فإننا نأخذ أمن معلومات عملائنا على محمل الجد. كما نعتقد أن الجهد التعاوني بيننا يمكن أن يقطع شوطاً طويلًا في مكافحة الاحتيال بشتى أنواعه.

الغرض من هذا المستند هو مشاركة بعض التحديثات المتعلقة بالاحتيال التي تُغطي أحدث الطرق والتكتيكات التي يستخدمها المحتالون ومشاركة أفضل الممارسات لحماية عملاءنا من أي عملية احتيال.

نود أيضا أن نطلب منك إبلاغنا عن أي نشاط مشتبه به أو احتيال فعلي لأن الاكتشاف المبكر هو المفتاح لمنع المزيد من الخسائر وضمان حماية معلوماتنا المتبادلة.

نعتقد أنه من خلال العمل معاً ، يمكننا تقليل التعرض للاحتيال بشكل أكبر وبالتالي حماية مصالحنا.

نشكركم على اهتمامكم بهذا الأمر ونتطلع إلى دعمكم المستمر لمبادراتنا للتوعية بالاحتيال.

تحياتي,,

البنك السعودي للاستثمار ..

فلسفتنا في مكافحة الاحتيال

نحن ملتزمون بالحفاظ على أعلى معايير الأخلاق والنزاهة في جميع جوانب أعمالنا ، بما في ذلك منع واكتشاف النشاط الاحتيالي.

نعتقد أن منع الاحتيال هو عنصر حاسم في مسؤوليتنا لحماية مصالح العملاء وجميع الأطراف التي نرتبط بها.

تتجذر فلسفة مكافحة الاحتيال في المبادئ التالية:

لا مجال للخطأ	سياسة عدم التسامح مطلقاً تجاه أي سلوك احتيالي والالتزام باتخاذ إجراءات سريعة ومناسبة ضد الجاني.
المنع الاستباقي	تعزيز نهج استباقي تجاه منع الاحتيال يتضمن تنفيذ ضوابط قوية ، وتوفير التدريب والوعي المنتظم ، وثقافة النزاهة.
الكشف المبكر	التأكيد على تنفيذ آلية للكشف المبكر عن الاحتيال مثل المراقبة والمراجعة المنتظمة، ومراجعة المعاملات والبيانات المالية في الوقت المناسب.
الاستجابة السريعة	بدء استجابة سريعة للكشف عن الاحتيال بما في ذلك التحقيق في الحوادث واسترداد الخسائر والإجراءات التأديبية المطلوبة.

حماية مصالح عملائنا هي أولويتنا القصوى, نطلب منكم الانضمام إلينا في التزامنا بمنع واكتشاف الاحتيال وضمان بيئة تشغيل آمنة للجميع ".
البنك السعودي للاستثمار

ماهي الهندسة الاجتماعية؟

الهندسة الاجتماعية هي تقنية تُستخدم بشكل أساسي للحصول على معلومات عن المستخدم المُستهدف, لذلك في الأساس، تؤدي الهندسة الاجتماعية إلى سرقة الهوية.

أنواع المخططات التي يستخدمها المحتالون لسرقة الهوية:

تصيد البريد الالكتروني Phishing	التصيد باستخدام البريد الالكتروني هو أسلوب يُستخدم للحصول على معلومات شخصية لغرض سرقة الهوية باستخدام رسائل البريد الإلكتروني الاحتيالية التي يبدو أنها واردة من مصادر مشروعة.
تصيد الرسائل القصيرة Smishing	التصيد باستخدام الرسائل القصيرة هو شكل آخر من أشكال التصيد الاحتيالي حيث يُرسل المحتال رسالة نصية قصيرة احتيالية لخداع الضحية لمشاركة التفاصيل المالية السرية أو المعلومات الشخصية.
تصيد الاحتيال الصوتي Vishing	التصيد باستخدام الاحتيال الصوتي هو شكل آخر من أشكال التصيد الذي يعتمد على استخدام المكالمات الهاتفية أو الرسائل الصوتية لخداع الأشخاص لمشاركة معلومات حساسة مثل التفاصيل المالية أو المعلومات الشخصية.
الانتحال Spoofing	الانتحال هو أسلوب يستخدم عنوان بريد إلكتروني أو اسم عرض أو رقم هاتف أو رسالة نصية أو عنوان URL لموقع الويب لإقناع الضحية بالتخلي عن التفاصيل المالية أو المعلومات الشخصية.

كيف تحمي نفسك:

- لا تفتح أي رسائل بريد إلكتروني مشبوهة من مصادر غير معروفة.
- لا تنقر على الروابط أو المرفقات المرسلة من قبل أشخاص مجهولين.
- لا ترد على رسائل البريد الإلكتروني أو المكالمات التي تبدو مشبوهة أو تطلب مشاركة معلومات شخصية مثل رقم الهوية الوطنية / الإقامة أو رقم الحساب أو رقم التعريف الشخصي أو كلمة المرور

ما هي خروقات الامن السيبراني؟

خروقات الامن السيبراني هي الحوادث التي تؤدي إلى وصول غير مصرح به إلى بيانات الكمبيوتر أو التطبيقات أو الشبكات أو الأجهزة. ينتج عنها الوصول إلى المعلومات دون إذن.

أنواع المخططات التي يستخدمها المحتالون لإحداث خروقات الأمن السيبراني:

البرامج الضارة **Malware**	عادة ما يتم تنظيم هجمات البرامج الضارة من خلال مواقع الويب الضارة ورسائل البريد الإلكتروني والبرامج وما إلى ذلك. يمكن إخفاء البرامج الضارة في ملفات أخرى مثل ملفات الصور أو المستندات أو الملفات التي تبدو غير ضارة.
برامج الخداع **Scareware**	هي برامج تستخدم تكتيك يخيف ويخدع الناس لزيارة مواقع الويب المخادعة أو تنزيل البرامج الضارة. يمكن إرسال البرامج في شكل إعلانات منبثقة أو عبر البريد الإلكتروني غير المرغوب فيه.
برامج الفدية **Ransomware**	برامج الفدية هي تقنية يتم فيها تقييد واحتجاز نظام الضحية كرهينة حتى يوافق على دفع فدية. بعد إرسال الدفعة يقدم المحتال تعليمات لاستعادة السيطرة على الكمبيوتر.
هجوم حجب الخدمة **DDOS Attack**	هي تقنية يُرسل فيها المحتال قدراً هائلًا من البيانات غير اللازمة إلى كمبيوتر الضحية ويغلقها. هذا يجعل موقع الضحية غير متاح لمستخدميه.

كيف تحمي نفسك:

- تنفيذ كلمات مرور قوية وعناصر تحكم في الوصول وتشفير البيانات لحماية حساباتك وأنظمتك من الوصول غير المصرح به.
- تنفيذ المصادقة الثنائية كطبقة أمان إضافية.
- إجراء عمليات تدقيق النظام والعمليات لتحديد المخاطر.

ماهي مسؤوليتك؟

بصفتك مقدم خدمة للبنك السعودي للاستثمار، نطلب منك الشراكة معنا في سعينا لمكافحة الاحتيال. نتوقع منك أن تظل متيقظا وأن تُبلغنا مباشرةً بأي نشاط مشتبه به أو احتيالي.

الخطوات الواجب اتباعها في حالة وجود نشاط احتيالي تم تحديده:

أوقف النشاط الاحتيالي	اتخذ خطوات فورية في إيقاف أي نشاط احتيالي يخطر ببالك لمنع أي خسارة مالية أخرى أو ضرر لسمعة البنك أو لنفسك.
تأكد من ابلاغنا	أبلغنا على الفور إذا كنت تشك في حدوث احتيال للسماح لنا باتخاذ الإجراء المناسب في الوقت المناسب للتخفيف من المخاطر. يمكنك استخدام أي من قنوات الإبلاغ المتاحة.
جمع وحفظ الأدلة	جمع وحفظ أي أدلة تتعلق بالنشاط المشتبه به أو الاحتيالي مثل رسائل البريد الإلكتروني أو الفواتير أو أي أدلة أخرى تدعم التحقيق.
التعاون في التحقيق	التعاون الكامل مع فريق التحقيق لدينا عند الحاجة بما في ذلك توفير المعلومات المتاحة عن الحادث أو أي مستندات داعمة كجزء من التحقيق.

البنك السعودي للاستثمار
The Saudi Investment Bank

شكرا