إجراءات الحد من مخاطر الاحتيال الإلكتروني (كيف تحمي بياناتك؟).

(HDB Official Website)

ما هو الاحتيال

هو نوع من أنواع الاستغلال للطبيعة البشرية لكسب الثقة بهدف الكشف عن معلومات خاصة تسمح للمحتال بسرقة المعلومات أو الأموال. يقوم المحتالون بانتحال موظفي البنوك وتجار التجزئة والمؤسسات الرسمية باستخدام رسائل البريد الإلكتروني والمكالمات الهاتفية والرسائل النصية التي تبدو حقيقية.

بعض الأساليب الشائعة للتصيد الاحتيالي لعملاء البنك:

من خلال البريد الإلكتروني

يتضمن التصيد المحتالين الذين يرسلون رسالة بريد إلكتروني غير مرغوب بها قد تبدو الرسالة البريدية حقيقية وتحتوي على شعار البنك أو شركة موثوق بها وبصيغة كتابة مماثلة لتلك المستخدمة بالرسائل المشروعة.

وقد تطلب منك تحديث معلوماتك الشخصية والمالية، مثل تاريخ الميلاد أو الإسم بالكامل أو رقم البطاقة الشخصية أو رقم بطاقة الدفع/الائتمان أو الرقم السري أو رمز الأمان الموجود خلف البطاقة أو الرقم السري المتغير (OTP) أو بيانات تسجيل الدخول إلى خدمة الانترنت/الموبايل البنكي وتفاصيل الحساب وغير ذلك من معلومات.

وقد تحتوي رسالة البريد الإلكتروني أيضاً على رابط أو مرفق يحولك إلى موقع على الإنترنت يشبه أو يتشابه إلى حد كبير مع موقع البنك الحقيقي. وذلك ليتمكن المحتالين من إلتقاط البيانات الشخصية مثل كلمات السر أثناء كتابتها أو تنصيب (إعداد) برامج ضارة على الجهاز الخاص بك.

من خلال الرسائل النصية القصيرة

هي رسائل نصية يرسلها المحتالون وتبدو أنها من البنك بهدف الإيقاع بالعميل لتقديم معلومات شخصية ومالية من خلال الإتصال برقم أو النقر على رابط. ويقوم المحتالون أيضاً باستخدام رسائل نصية مزيفة لتعمد تزوير رقم الهاتف لتبدو وكأنها صادرة من الرقم الخاص ببنك التعمير والإسكان

من خلال المكالمات الهاتفية

وتتمثل في إجراء مكالمات هاتفية أو ترك رسائل صوتية يُزعم أنها من البنك من أجل حث الأفراد على الكشف عن المعلومات الشخصية، مثل التفاصيل المصرفية وأرقام بطاقات الائتمان.

لتجنب الوقوع ضحية لهذه الأنواع المختلفة من الاحتيال:

1. أعلم أن البنك لن يقوم أبداً بإرسال رسالة إلكترونية يطلب منك بها تغيير أو تحديث بياناتك أو يطلب منك الدخول على رابط موقع.

2. لا تكشف مطلقًا عن الرقم السري الخاص المتغير الخاص بك او كلمة سر في الرسالة نصية قصيرة التي يتم إرسالها إلى تليفونك المحمول او رقم بطاقة الدفع/الائتمان أو رمز الأمان الموجود خلف البطاقة او كلمة سر أو رموز خدمة الإنترنت البنكية او تفاصيل شخصية عنك ما لم تكن متأكدًا من هوية الشخص الذي تتحدث إليه.
3. لا تتعامل مع رسائل البريد الإلكترونية أو الرسائل النصية غير المرغوب فيها التي تطلب منك تحديث أو التحقق من بياناتك الشخصية أو بيانات تسجيل الدخول إلى خدمة الانترنت البنكي.
4. لا تفتح أي رابط في أي رسالة إلكترونية إذا كنت لا تعرف أو تشك في شخص الراسل.
5. لا تفتح المرفقات في أي رسالة إلكترونية، إفتح فقط التي تتوقع وصولها من أشخاص موثوق بها.
6. لا تكشف أي معلومات هامة، مثل كلمات السر، لأي شخص يتصل بك.
7. لا ترسل أي تفاصيل عن بطاقة الائتمان أو أرقام الحسابات المصرفية من خلال البريد الإلكتروني.
8. إحذر من التعليمات التي تطلب منك الرد أو ملء نموذج أو مستند مرفق برسالة البريد الإلكترونية أو الضغط عبر موقع إلكتروني للتحقق من حسابك.
9. لا ترسل معلومات شخصية أو مالية لأي أحد عن طريق البريد الإلكتروني.
10. عليك الإبلاغ عن أي واقعة إلى مركز إتصال البنك على الخط المعتمد 19995
11. توخَ الحذر من المكالمات الهاتفية التي يدعي أو يزعم فيها المحتالون عرض إعادة أموال أو تعويض أو إرجاع أموال لحسابك.
12. لا تسمح لأي شخص لا تعرفه أو تثق به بالوصول إلى الكمبيوتر الخاص بك.
13. لا تسجل الدخول مطلقًا إلى خدمات البنك عبر الإنترنت أثناء وصول شخص أخر إلى الجهاز الخاص بك.
14. لا تسجل الدخول مطلقًا إلى خدمات البنك عبر الإنترنت أو تضع رقم بطاقة الدفع/الائتمان من أجهزة غير موثوق بها.
15. قم بتثبيت برنامج مضاد للفيروسات وحافظ على تحديثه لحمايتك من الفيروسات مثل البرامج الضارة وأحصنة طروادة وبرامج التجسس والبرامج الإعلانية
16. حافظ على تحديث برنامج المتصفح لديك حيث يوفر برنامج المتصفح الحديث حماية إضافية ضد المواقع الالكترونية المزيفة
17. حافظ على تحديث برامجك لأنه من الصعب على الفيروسات إحداث الضرر للبرامج المحدثة

إذا كانت لديك شكوك حول صحة رسالة البريد الإلكتروني/الرسالة القصيرة أو تشككت بمكالمة هاتفية، أو كنت تعتقد أنك وقعت ضحية لتصيد احتيالي على البريد الإلكتروني أو رسالة نصية قصيرة، أو عبر مكالمة هاتفية فيرجى التواصل مع مركز إتصال البنك على الخط المعتمد 19995 فوراً.