توجهات الاحتيال

ضوابط أمن HSBC*net* عبر الإنترنت

HSBC

HSBC*net*

المحتويات

- أنواع الاحتيال
  - هجمات البرامج الضارة
  - اختراق رسائل البريد الإلكتروني التجارية
  - التصيد الصوتي ("التصيد الاحتيالي باستخدام الصوت")
  - التصيد من خلال خدمة الرسائل القصيرة (SMS) ("التصيد الاحتيالي باستخدام الرسائل القصيرة")
- كيفية تفادي التعرض لها
- أمان إضافي من HSBC*net* للخدمات المصرفية عبر الإنترنت

هجمات البرامج الضارة

- البرنامج الضار هو برنامج يُستخدم لتعطيل تشغيل الكمبيوتر أو جمع معلومات حساسة أو الحصول على إمكانية الوصول إلى أنظمة كمبيوتر خاصة

- يتم اختراق أنظمة العملاء لإجراء معاملات مزورة

- سيختبر العملاء تباطؤاً في أجهزة الكمبيوتر وظهور شاشات غير اعتيادية تطالبهم بإدخال رموز بالإضافة إلى ظهور شاشات تصرح بأنه يتوجب على المستخدم الانتظار لوقت معين قبل إعادة تسجيل الدخول

- يمكن تنزيل البرنامج الضار عن غير قصد من خلال النقر فوق الروابط داخل رسائل بريد التصيد الاحتيالي الإلكتروني وفي مواقع الويب المخترقة وعبر تنزيل برنامج تمت قرصنته

هجمات البرامج الضارة

أمثلة:

- خلال تسجيل الدخول، قد يتلقى العملاء شاشةً مكتوب "***يرجى الانتظار***" عليها
- قد يبدو الكمبيوتر بطيئاً جداً
- شاشات منبثقة ستطلب من المستخدم إدخال رمز الأمان بالإضافة إلى شاشات تطلب من العميل الضغط على الزر الأصفر
  (مطالبات بالمصادقة على الرمز أو تحدي الأمان أو إعادة المزامنة)
- شاشات تطلب أن يسجل مستخدم ثانٍ الدخول على الكمبيوتر نفسه للمصادقة

اختراق رسائل البريد الإلكتروني التجارية

- طريقة للاحتيال عبر استهداف عملاء المؤسسات المالية
- يحدث ذلك عندما ينتحل المحتالون شخصية متعاقدين أو موردين أو دائنين أو حتى الإدارة العليا للطلب من الشركة تغيير دفعتها
- تتم بعد ذلك إعادة توجيه دفعات مشروعة إلى حساب المحتال

لماذا يعد هذا النوع من الهجمات صعب الاكتشاف؟

- تحصل الهجمات في كل المؤسسات المالية ولا تنحصر بأي بلد أو منطقة
- يكون المحتالون مستعدين جيداً قبل الهجوم عبر إجراء نوع من الاستكشاف (الهندسة الاجتماعية) لضمان صحة استهداف التفاصيل والأسماء
- تكون عناوين البريد الإلكتروني المُستخدمة لطلب تغييرات في حساب المستفيد من الدفعة مماثلةً أو مشابهةً للغاية لتلك الخاصة بالموردين أو البائعين الأصليين، ما يصعّب اكتشاف الاحتيال
- لطالما اشتهر المحتالون باختراق حساب البريد الإلكتروني لدائن ما لإرسال طلب تغيير للمستفيد ليبدو بالتالي وكأنه طلب مشروع
- يتم استخدام خدمات البريد التقليدية لإرسال رسائل مزورة تبدو وكأنها آتية من الدائن
- يستغل سلوك/استجابة الإنسان التي لا يمكن أن تمنعها التكنولوجيا

اختراق رسائل البريد الإلكتروني التجارية

أمثلة:

- رسائل بريد إلكتروني من بائعين جدد أو حاليين يدّعون بأن أرقام الحساب قد تغيرت ويطلبون إرسال دفعات الآن إلى موقع وحساب جديدين
- مطالبة البائعين بتوجيه دفعات الآن إلى شركة أم أخرى في بلد مختلف
- يتلقى الموظفون بريداً إلكترونياً من مديرهم التنفيذي/مديرهم المالي يطالبهم فيه بتسديد دفعات لكن يتبين لاحقاً أنه تم اختراق رسالة البريد الإلكتروني الخاصة بالمدير التنفيذي/المدير المالي
- قد يأتي البريد الإلكتروني من مجال يبدو مماثلاً لمصدر مشروع

التصيد الصوتي ("التصيد الاحتيالي باستخدام الصوت")

- التصيد الاحتيالي باستخدام الصوت هو مصطلح يُستخدم لوصف التكتيكات التي يستخدمها المحتالون لـ "تصيد" المعلومات الشخصية (مثل بيانات اعتماد أمان المعاملات المصرفية عبر الإنترنت) عبر الهاتف.
- قد يتصل المحتالون بالعملاء ويدَّعون بأنهم من HSBC. وقد يوجهونك لتنفيذ إجراءات قد تسمح بعمليات دفع غير مصرح بها ليتم إرسالها إلى المجرم. وقد يشتمل ذلك على تقديم رموز الأمان التي يتم إنشاؤها من رمزك.

لن يطلب منك بنك HSBC أبداً معلومات عبر الهاتف قد يتم استخدامها لتسديد دفعة، كطلب توفير رموز أمان الأجهزة أو مطالبتك بالبوح بأي من تفاصيل أمانك.

التصيد من خلال خدمة الرسائل القصيرة (SMS) ("التصيد الاحتيالي باستخدام الرسائل القصيرة")

- التصيد الاحتيالي باستخدام الرسائل القصيرة هو نوع مختلف من التصيد يستخدم الرسائل القصيرة عوضاً عن رسائل البريد الإلكتروني
- قد يتصل المحتالون بالعملاء باستخدام الرسائل القصيرة ويدَّعون بأنهم من HSBC. وقد يوجهونك لتنفيذ إجراءات قد تسمح بعمليات دفع غير مصرح بها ليتم إرسالها إلى المجرم. وقد يشتمل ذلك على تقديم رموز الأمان التي يتم إنشاؤها من رمزك.

لن يطلب منك بنك HSBC أبداً معلومات قد يتم استخدامها لتسديد دفعة، كطلب توفير رموز أمان الأجهزة أو مطالبتك بالبوح بأي من تفاصيل أمانك

HSBC

كيف يمكنك تفادي التعرض لها؟

- كن متنبهاً لأي طلبات تغيير معلومات المستفيد – وشكك بكل التغييرات واعمد إلى التحقق من صلاحية أي طلب تغيير باستخدام قنوات إضافية (كإعادة الاتصال وعدم الرد مباشرةً على رسالة البريد الإلكتروني)

- ضع إجراءات ضبط داخلي لطلبات تغيير تفاصيل المستفيد

- إذا انبثقت شاشات غير اعتيادية و/أو أصبحت استجابة الكمبيوتر بطيئة بشكل غير اعتيادي، فسجل الخروج من HSBC *net* بشكل كامل وامسح الكمبيوتر بواسطة أحدث إصدار لبرنامج الحماية ضد الفيروس. إذا شككت بأمر ما، فاتصل بفريق تكنولوجيا المعلومات و/أو مدير خدمة العملاء في HSBC أو الفريق المعني.

- أشرك الموظفين في حملات توعية وتعليم عن الاحتيال

...كيف يمكنك منع التعرض لها؟

- لا تكشف أبداً عن تفاصيل أمان عبر الهاتف عندما تتلقى مكالمات غير مرغوب فيها
(مثلاً اسم المستخدم أو معلومات الرمز أو تفاصيل الدفعة)

- عندما تتلقى مكالمةً غير مرغوب فيها من HSBC، اطلب تفاصيل جهة الاتصال من المتصل واعمد إلى التحقق من صحة المعلومات مع مدير خدمة العملاء في HSBC أو مكتب المساعدة في HSBC

- لا تعدّل معلومات الدفعة إلا إذا كنت متأكداً من شرعية الأمر

- بلّغ البنك بأي محاولة احتيال وراجع إعدادات البريد الإلكتروني (مثلاً غيّر كلمة المرور)

أمان إضافي من *HSBC*net للخدمات المصرفية عبر الإنترنت

- لا تضغط أبداً على الزر الأصفر على جهاز الأمان إلا إذا كنت توقع على معاملة أنشأتها بنفسك – فبنك HSBC لا يطلب منك أبداً الاستجابة عبر الضغط على الزر الأصفر عند تسجيل الدخول
- استخدم التحكم المزدوج - للمعاملات والمستحقات (*مثلاً مطلوب فردين على الأقل لكل الأنشطة*)
- اعمد إلى تنزيل برنامج Webroot *SecureAnywhere* على www.hsbcnet.com من دون أي كلفة عليك
- اعمد إلى إعداد سقف لعدد التواقيع
- احظر كل تسجيلات الدخول غير الآتية من قائمة موافق عليها من عناوين IP
- اعمد إلى تحديث البرنامج الذي ما عاد مدعوماً من البائعين (*مثلاً Internet Explorer 7*)
- اعمد إلى الوصول إلى HSBC*net* فقط من خلال عنوان موقع الويب في شريط عنوان المستعرض
- لا تعمد أبداً إلى الوصول إليه من خلال الارتباطات التشعبية المضمنة في رسائل البريد الإلكتروني ولا تعتمد فقط على منظر موقع الويب وشكله عند استخدام HSBC*net*