برنامج توعية العملاء

قسم الأمن السيبراني

(CSD-CAP)

عام

ولاء
Walaa

شركة ولاء للتأمين التعاوني
Walaa Cooperative Insurance Co.

جدول المحتويات

1.0 نظرة عامة

على الرغم من أننا نحمي عملائنا من سرقة الهوية والجرائم المالية، يجب أن يعرف العملاء كيفية حماية معلوماتهم الشخصية من خلال إتباع أفضل ممارسات الأمان عند زيارة المواقع الإلكترونية على أجهزة الكمبيوتر الشخصية أو الخاصة بالعمل. نحن نبذل قصارى جهدنا لتثقيف العملاء وتعزيز ثقة العملاء في معاملاتهم عبر الإنترنت.

فيما يلي توجد توصيات للتوعية بالمعاملات عبر الإنترنت في المجالات التالية:
التسوق عبر الإنترنت، الحماية عبر الإنترنت، حماية كلمة المرور، حماية نظام التشغيل، حماية سرقة الهوية وحماية الهوية / التأمين / بطاقة الائتمان / الدائن. الغرض من هذه التوصيات هو تعزيز ثقة العميل وتوجيهه بكيفية حماية معلوماته السرية لكي لا يقع ضحية سرقة الهوية أو الاحتيال الإلكتروني والتهديدات الأخرى.

2.0 إرشادات التسوق عبر الإنترنت

الإنترنت هو الطريقة الأسهل والأريح للشراء المنتجات . إن السهولة والاختيار اللذين يتوفران على الإنترنت للمتسوقين قامت بتغير مفهوم التسوق. فيمكنك زيارة موقع وطلب منتجات دون الحاجة لمغادرة مكانك. عند التسوق عبر الإنترنت، نوصي العملاء باتباع الإرشادات التالية:

- كن على معرفة بقدر الإمكان عن المنتج والبائع.
- إفهم سياسات الإسترداد الخاصة بالبائع.
- اختر كلمة مرور آمنة لحماية معلومات الحساب.
- استخدم طريقة دفع الآمنة.
- إذا كان العرض يبدو مشبوه أو غير واقعي، فمن المحتمل أنها عملية احتيال.

3.0 أفضل الممارسات للحماية عبر الإنترنت

اقترح العديد من الباحثين أفضل الممارسات للحماية عبر الإنترنت. فيما يلي قائمة بأفضل الممارسات:

- راجع معاملاتك البنكية يومياً وإبحث عن أي عمليات غير مؤلفة لك. قد يكون هذا مؤشرا على أن حسابك قد تم اختراقه وأن هناك خطة احتيالية قيد التنفيذ.
- لا تقم مطلقًا بإستخدام خدمات بنكية، مالية أو غيرها من الخدمات الحساسة في مقاهي الإنترنت أو المكتبات العامة. حيث قد تكون الأجهزة المتواجدة بالأماكن العامة تحمل برامج تقوم بسرقة المعلومات وأرقام الحسابات الخاصة بك، مما يتركك عرضة للاحتيال.
- قم بتنبيه البنك على الفور بعد أي عمليات مشبوهة. لديك وقت محدود لإسترداد هذه العمليات وقد يؤدي التصعيد الفوري إلى منع أو التقليل من الضرر.
- لا تشارك معرف المستخدم أو كلمة المرور الخاصة بك مع أي شخص.
- ينصح بالإبتعاد عن إستخدام الشبكات اللاسلكية. إذا كنت تستخدم شبكة لاسلكية، فمن المقترح أن تستخدم كلمة مرور آمنة.
- قم دائمًا بتسجيل الخروج من المواقع التي قد تحمل معلومات حساسة بك.
- توخي الحذر قبل مشاركة بريدك الإلكتروني مع المواقع المشكوك بها، لأن هذا يزيد من إحتمالية تلقي رسائل البريد الإلكتروني الاحتيالية.
- حذف رسائل البريد الإلكتروني المشبوهة دون فتحها، لا تقوم بفتح المرفقات في رسائل البريد الإلكتروني المشبوهة.
- عندما لا يكون جهاز الكمبيوتر الخاص بك قيد الاستخدام، قم بإغلاقه أو فصله عن الاتصال بالإنترنت.
- لا تقدم أبدًا معلومات حساسة عن الحساب ردًا على رسائل البريد الإلكتروني أو رسائل المواقع.
- قم دائمًا بمراجعة كشوف حسابك الشهرية بعناية والتحقيق في أي نشاط غير مصرح به في حسابك.
- ممارسة استخدام الإنترنت الآمن. لا تنقر أبدًا على رسائل المواقع أو روابط التطبيقات الموجودة في رسائل البريد الإلكتروني. حاول أن تقوم بالتحقق يدويًا من الروابط التي يتم إرسالها إليك. تشير دراسات إلى أنه أكثر من 80٪ من البرامج الضارة يتم الحصول عليها من خلال النقر على الإعلانات التطفلية.
- كن حذر من رسائل البريد الإلكتروني التي تتدعي أنها من مؤسسات مالية أو دوائر حكومية، والتي تطلب معلومات الحساب للتحقق، أو أوراق معتمدة للوصول إلى معلوماتك البنكية مثل اسم المستخدم وكلمة السر أو رمز الـPIN.

- توخ الحذر عند فتح المرفقات وتأكد أنها مرسلة من مصدر موثوق.
- تجنب تحميل البرامج من مصادر غير معروفة.
- لا تقم مطلقًا بإعطاء أي معلومات شخصية بما في ذلك اسم المستخدم، كلمات المرور، رقم الهوية الوطنية أو تاريخ الميلاد.
- لا تستخدم معلومات شخصية باسم المستخدم أو كلمات المرور الخاصة بك، مثل رقم الهوية الوطنية أو تاريخ الميلاد.
- حظر ملفات التعريف على متصفح الويب الخاص بك. عندما تتصفح، يتم جمع مئات من البيانات بواسطة المواقع التي قمت بزيارتها. يتم مزج هذه البيانات لتشكل "ملفك الشخصي الرقمي" ، والذي قد يتم بيعه على الشركات دون موافقتك وسوف تمنع بعض من هذه الحالات عن طريق حظر ملفات التعريف.
- لا تقدم تاريخ ميلادك الكامل على ملفك بالشبكات الاجتماعية. يستخدم لصوص الهوية تواريخ الميلاد كمعلومة أساسية في تنفيذاتهم. حاول نشر الشهر واليوم فقط، وترك السنة.
- استخدم أسماء مستخدمين وكلمات مرور متعددة. أبق أسماء المستخدمين وكلمات المرور الخاصة بالشبكات الاجتماعية والخدمات المصرفية عبر الإنترنت والبريد الإلكتروني والتسوق عبر الإنترنت منفصلة.
- يجب أن يتوخى العملاء الحذر عند فتح الصور المرفقة عبر البريد الإلكتروني، حيث قد تحتوي على ملفات مخفية ومضرة تعيد توجيههم إلى موقع المهاجم.
- يجب على العملاء عبر الإنترنت نسخ عنوان الـ URL، ولصقه في شريط العناوين للتأكد من أن هذا موقع صحيح بدلاً من النقر على عنوان الـ URL المرفق عبر البريد الإلكتروني ، ولكن بدلاً من ذلك يجب عليهم.

4.0 أفضل الممارسات لحماية كلمة المرور

فيما يلي بعض التوصيات لحماية كلمة المرور:

- تغيير كلمات المرور على الأقل كل 90 يومًا.
- قم بإنشاء كلمة مرور قوية تحتوي على 10 أحرف على الأقل تتضمن مجموعة من الأحرف والأرقام والعلامات الخاصة.
- تأكد من عدم كتابة معلومات حسابك حيث يمكن للآخرين رؤيتها أو الوصول إليها. إذا كان يجب كتابة المعلومات، فيجب تأمينها في مكان آمن ومحكم.
- لا تشارك أبدًا اسم المستخدم أو كلمة المرور الخاصة بك مع أي شخص لأي سبب.
- قم بتأمين الكمبيوتر الخاص بك باستخدام خاصية قفل الشاشة بعد 15 دقيقة حمايتها بكلمة مرور.
- تجنب استخدام ميزة تسجيل الدخول التلقائي التي تحفظ أسماء المستخدمين وكلمات المرور للعمليات عبر الإنترنت.
- قم بتثبيت تطبيقات إدارة كلمات المرور لإنشاء كلمة مرور قوية وتخزينها في قاعدة بيانات آمنة بدلاً من وضعها في أي مكان.
- تمنح بعض البنوك عملائها رمزاً مميزاً للوصول إلى حسابهم عبر الإنترنت لتحسين مستوى الأمان. يجب على المستخدم الانتظار حتى يتغير الرمز، ثم يدخل الرمز الجديد لضمان عدم سرقة الرمز.

5.0 أفضل الممارسات لحماية نظام التشغيل

فيما يلي بعض التوصيات لحماية أنظمة التشغيل:

- تأكد من استخدام برنامج حامي من الفيروسات والتجسس لحماية نفسك من البرامج الضارة التي تم إنشاؤها لغرض محدد وهو جمع المعلومات مثل اسم المستخدم وكلمات المرور والمعلومات الهامة الأخرى التي قد يتم تخزينها على جهاز الكمبيوتر الخاص بك.
- تثبيت جدار حماية يعمل طوال الوقت، خاصةً إذا كان لديك اتصال بالإنترنت، مثل DSL. يحد جدار الحماية من إمكانية الوصول غير المصرح به إلى الشبكة وأجهزة الكمبيوتر الأخرى.

6.0 أفضل الممارسات لحماية الهوية من السرقة

فيما يلي بعض النصائح لحماية سرقة الهوية:

- **الإبلاغ فورا عند فقدان أو سرقة الهوية أو بطاقات الائتمان:**

- لا تقم بإعطاء أي معلومات شخصية لأي شخص لا يمكنك التحقق من هويته. قم بتمزيق أي مستندات لا تحتاج إليها تحتوي على معلومات شخصية مثل البيانات المصرفية والشيكات غير المستخدمة وقسائم الإيداع وكشوف بطاقات الائتمان وتفاصيل الراتب والفواتير.
- عدم إعطاء أي معلومات شخصية لأي موقع إلكتروني إن لم يستخدم إحدى طرق التشفير او الأمان.

7.0 أفضل الممارسات لحماية الهوية / التأمين / بطاقات الائتمان

فيما يلي بعض التوصيات لحماية الهوية / التأمين / بطاقات الائتمان:

- عدم إعادة بطاقاتك لأي شخص.
- حمل البطاقات التي يتم استخدامها بتكرار.
- عدم ترك محفظتك أو حقيبتك في السيارة.
- استخدام جهاز صراف آخر أو عد لاحقًا إذا لاحظت أي شيء مشبوه عند استخدام جهاز الصراف الآلي، قم بالوقوف أمام الجهاز للحفاظ على معاملتك بخصوصية.
- قم بإلغاء معاملتك في حالة حدوث أي أنشطة مشبوهة تلاحظها أثناء استخدام جهاز الصراف الآلي.
- حماية الشريط المغناطيسي الحساس خلف بطاقتك. بإبقائه بعيدا عن أشعة الشمس المباشرة. تجنب ترك بطاقتك على الأجهزة الكهربائية أو بالقرب منها، مثل التلفزيون أو النظام الصوتي.
- لا تحمل بطاقتك بجوار بطاقة أخرى لأنها قد تؤدي إلى إزالة الطبقة المغناطيسية.
- الإبلاغ فورا عن جميع الأنشطة المتعلقة بجرائم الصراف الآلي إلى مالك / مشغل الجهاز ومسؤولي تنفيذ القانون المحليين.
- دائما قم بأخذ إيصالك بعد كل معاملة لضمان خصوصيتك المالية. احتفظ بإيصالاتك واستخدمها للتحقق من كشف حسابك الشهري.
- حماية بطاقات أجهزة الصراف الآلي والرقم السري الخاص بها كما تقوم بحماية الشيكات والمال. احفظ الرقم السري لبطاقاتك - لا تكتبه على بطاقتك أو في دفتر الشيكات الخاص بك.

8.0 الخلاصة

كيف تحمي نفسك:

- التأكد من أن نظام التشغيل، المتصفح او تطبيقات الهاتف محدثة.
- تثبيت وتحديث برامج الحماية بشكل دوري.
- فحص حاسوبك أو هاتفك الجوال بشكل دوري للتأكد من عدم وجود برامج تجسس.
- تجنب تحميل برامج أو تطبيقات من مصادر غير معروفة.
- تجنب مشاركة اسم المستخدم وكلمة المرور مع أي أحد.
- كلمة المرور يجب أن تحتوي على حروف، أرقام ورموز خاصة، ويجب تغيير كلمة المرور من وقت لآخر.
- تسجيل الخروج من حسابك وخاصتا المواقع المهمة مثل البنوك حيث أن اسم المستخدم وكلمة المرور مهمين.
- خذ الحيطة قبل مشاركة بريدك الإلكتروني مع المواقع الإلكترونية حيث أنها تزيد من فرصة استقبال رسائل الاحتيال.
- حذف رسائل البريد الإلكتروني المشبوهة من غير فتحها وعدم فتح المرفقات بهذه الرسائل.
- إغلاق أو إطفاء الانترنت عن جهاز الكمبيوتر الخاص بك عند الابتعاد عنه.
- عدم مشاركة أي معلومة حساسة عن طريق البريد الإلكتروني، المواقع الإلكترونية أو النوافذ المنبثقة.
- مراجعة كشف حسابك الشهري والتأكد من عدم وجود أي نشاط مشبوه.