منع الإحتيال

التزامنا بالحماية

في إسناد ، نأخذ حماية المعلومات الحساسة لعملائنا على محمل الجد ونراقب باستمرار معلوماتنا وبياناتنا لمنع السلوك الاحتيالي أو المشبوه.

نحن نسعى جاهدين لحمايتك ونشجعك على أن تكون على دراية بأي سلوك احتيالي محتمل من جانب الأطراف المؤذية التي تستخدم علامة إسناد التجارية. فيما يلي بعض النصائح حول كيفية التعرف على الاحتيال لضمان الحفاظ على أمان المعلومات الحساسة.

التعرف على الاحتيال

يعد التعرف على رسائل البريد الإلكتروني الاحتيالية والخداع وأنواع الاتصالات الأخرى أمرًا أساسيًا لحماية نفسك من الاحتيال والسرقة. تشمل علامات التحذير الشائعة حول عمليات الاحتيال عبر الإنترنت:

أ. طلبات الحصول على المال: طلبات غير متوقعة للحصول على أموال مقابل تسليم بضاعة ، وغالبًا ما يكون ذلك مع شعور بالإلحاح ، وتستخدم لخداع الأشخاص لإرسال الأموال وتوفير المعلومات الشخصية مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان.

ب. طلبات المعلومات الشخصية: طلبات المعلومات الشخصية و / أو المالية لغرض ارتكاب السرقة وانتحال الشخصية والجرائم الأخرى.

ج. أسماء النطاقات الخادعة: روابط لعناوين مواقع الويب التي بها أخطاء إملائية أو غيرت بشكل طفيف (على سبيل المثال ، esnadcourier / esndxpress.org / esnd.com). إذا كنت تشك في سلامة أي موقع ويب باستخدام علامة تجارية إسناد ، فيرجى زيارة موقعنا العالمي: www.esnadexpress.com أو الاتصال بمركز خدمات العملاء العالمي في إسناد على العنوان

support@esnadexpress.com

.

أنواع الاحتيال

رسائل البريد الإلكتروني الاحتيالية وعمليات الاحتيال عبر البريد الإلكتروني: هذه هي عمليات الاحتيال الأكثر شيوعًا عبر الإنترنت. تحاول رسائل البريد الإلكتروني هذه خداعك من خلال التظاهر أنك تأتي من مصدر حسن السمعة ، مثل من إسناد (على سبيل المثال من ما يبدو أنه بريد إلكتروني إسناد). سيحاولون منك مشاركة معلوماتك الشخصية الحساسة أو معلومات الحساب أو إرسال دفعة. قد يطلبون منك أيضًا التسجيل في الفوز بجائزة أو الدخول في مسابقة.

نحث العملاء على أن يكونوا متشككين في أي طلب لا يأتي مباشرةً من أحد موظفي إسناد أو اسم المجال.

سرقة الهوية: يحدث هذا عندما يخدعك شخص ما للكشف عن / توفير معلومات شخصية أو مالية أو معلومات حساب. وباعتبارها شركات معروفة ، فإن لصوص المعلومات عادة ما يرسلون رسائل بريد إلكتروني أو يتصلون بك عبر الهاتف

يطلبون منك الرد أو توجيهك إلى صفحة ويب احتيالية تطلب منك تقديم معلومات شخصية ، مثل رقم بطاقة الائتمان أو كلمة مرور الحساب ، أو حتى أوراق اعتماد إسناد الخاصة بك.
الاحتيال في بطاقة الائتمان: في بعض الحالات ، يحدث الاحتيال في بطاقة الائتمان عند فقد أو سرقة بطاقة ائتمان مادية لشخص ما من قِبل طرف آخر يستخدمها. يتم الاحتيال في بطاقة الائتمان في المقام الأول عن طريق تسوية بيانات حساب بطاقة الائتمان أثناء استخدامهم العادي. غالبًا ما تُستخدم بيانات بطاقة الائتمان المسروقة لمحاولة الشراء عبر الإنترنت بطريقة احتيالية.

الرسائل غير المرغوب فيها والفيروسات: في صناعتنا ، يتلقى العملاء عادةً بريدًا إلكترونيًا يشير إلى أن إسناد يحاول توصيل حزمة ويطلب منك فتح مرفق البريد الإلكتروني للمطالبة بالتسليم. قد يكون هذا المرفق فيروس كمبيوتر. ما لم تكن تتوقع تلقي بريد إلكتروني مثل هذا ، فالرجاء عدم فتح المرفق والإبلاغ عنه إلى مركز إسناد العالمي لخدمة العملاء على

support@esnadexpress.com

رسائل تتبع الحزمة: في بعض الحالات ، يتلقى العملاء رسالة بريد إلكتروني تحتوي على رقم التتبع. يمكن التحقق من هذا الرقم عن طريق إدخاله في مربع "تعقب الشحنة" علىwww.esnadexpress.com إذا لم يتم إرجاع نتائج التتبع ، فهذا ليس رقم تتبع صالحًا ، ولم يرسل إسناد رسالة البريد الإلكتروني. يرجى الإبلاغ عن هذه الرسالة الإلكترونية إلى مركز إسناد العالمي لخدمة العملاء على العنوان

support@esnadexpress.com

مفتاح التنشيط: يتم إرسال الرسائل التي تحتوي على مفاتيح التنشيط فقط لإكمال التسجيل بعد تنزيل تطبيق إسناد للجوال. إذا تلقيت رسائل دون محاولة التسجيل على تطبيقنا للجوال ، فنحن نحثك على تجاهلها. إسناد لن يطلب منك مفتاح التنشيط عبر الهاتف أو البريد الإلكتروني ؛ من أجل أمان حسابك ، يرجى عدم مشاركة مفتاحك مع أي شخص.

القيام بدورنا

أمان معلوماتك الشخصية مهم بالنسبة لنا. في إسناد ، نحن نعترف بمعايير الصناعة ونستخدم ضمانات أمنية إدارية وفنية ومادية مناسبة لحماية المعلومات الشخصية التي تقدمها ضد التلف العرضي أو غير القانوني أو غير المصرح به أو الخسارة أو التغيير أو الوصول أو الإفصاح أو الاستخدام وغيرها من أشكال المعالجة غير القانونية. نستثمر باستمرار في أحدث التقنيات ذات المستوى العالمي لتقليل جميع المخاطر المحتملة لصالح عملائنا ، ونظل ملتزمين بضمان تلبية متطلبات الأمان الأكثر صرامة وتعزيز ثقافة الأمان داخل مؤسستنا. يتم دائمًا تدقيق التزامنا بأمن المعلومات وتم الاعتراف به من قبل هيئات الاعتماد الدولية مثل المعهد البريطاني للمعايير (BSI) ، حيث أن قياسات الأمان الخاصة بنا حاصلة على شهادة ISO 27001: 2013.

يستخدم موقع الويب الخاص بالشركة وتطبيقات الأجهزة المحمولة العديد من تقنيات الأمان بما في ذلك الخوادم الآمنة. يتم تشفير جميع معلوماتك الشخصية ، بما في ذلك تفاصيل بطاقة الائتمان الخاصة بك قبل مغادرة المتصفح أو الجهاز. تم اعتماد نظام الدفع الخاص بنا أيضًا للامتثال لمعايير صناعة بطاقات الأمان وأمن البيانات مثل(PCI-DSS).

أداء الجزء الخاص بك

ستبقي إسناد هذه التدابير قيد المراجعة ويعززها من وقت لآخر حسب الضرورة. من المهم بالنسبة لك الحماية من الوصول غير المصرح به إلى معلومات تسجيل الدخول الخاصة بك ، بما في ذلك كلمة المرور الخاصة بك. يرجى

ملاحظة أن أي وسيلة نقل عبر الإنترنت ، أو طريقة التخزين الإلكتروني ، هي آمنة 100 ٪. لذلك ، لا يمكن لـ إسناد ضمان الأمان المطلق لمعلوماتك الشخصية.

اتصل بنا

للحصول على أي تعليقات أو أسئلة حول إجراءات حماية العملاء ومنع الاحتيال في إسناد ، يرجى الاتصال بمركز إسناد Global لخدمة العملاء على

support@esnadexpress.com

اخلاء المسؤولية:

إسناد لا ولن تطلب منك تقديم أي معلومات شخصية أو معلومات الدفع عبر البريد التقليدي أو عبر البريد الإلكتروني. إن إدراك وحماية معلوماتك الحساسة هو أفضل طريقة لمنع الاحتيال. إذا تلقيت طلبًا للحصول على معلومات شخصية أو عن طريق الدفع من خلال هذه الأنواع من الاتصالات ، فالرجاء عدم الرد أو التعاون مع المرسل وإبلاغ الحالة على الفور إلى مركز رعاية العملاء التابع لـ إسناد على

support@esnadexpress.com

لا تتحمل إسناد أي مسؤولية عن أي تكاليف أو تكاليف أو مدفوعات يتم دفعها نتيجة لنشاط احتيالي. من المهم أن تضع في اعتبارك الطرق المذكورة أعلاه التي يمكن من خلالها سرقة معلوماتك وبياناتك لمنع أي احتيال في المستقبل.