حماية أمن وسرية معلوماتكم أولويتنا

نلتزم في الدولية السريعة للشحن IEL بحماية المعلومات الحساسة لعملائنا ونأخذ هذا الأمر على محمل الجد ونواظب على مراقبة المعلومات والبيانات المتاحة لدينا من أجل تفادي ومنع أي سلوك احتيالي أو مشبوه.

وفي حين أننا نبذل أقصى ما بوسعنا لحماية عملائنا وشركائنا، فإننا نحثكم أيضاً على دعم جهودنا هذه عبر القيام بواجبكم في رصد أي سلوك احتيالي محتمل من قبل أطراف خبيثة تستغل اسم IEL لتضليلكم.

فيما يلي بعض النصائح حول كيفية التعرف على أساليب الاحتيال الإلكتروني لضمان الحفاظ على سلامة وأمن معلوماتكم الحساسة.

رصد أساليب الاحتيال الإلكتروني

لا شك أن التحلي بالوعي والفطنة للتعرف على رسائل البريد الإلكتروني الاحتيالية والضارة وغيرها من أشكال التواصل الاحتيالية يمثل ركناً أساسياً للحماية من الاحتيال والسرقة، وتتضمن علامات التحذير الشائعة من الأساليب الاحتيالية عبر الإنترنت ما يلي:

- **طلبات دفع الأموال:** طلبات غير متوقعة لسداد مبالغة مالية تحمل طابعاً مستعجلاً، في كثير من الأحيان، نظير توصيل شحنات وطرود، وتستخدم هذه الطريقة من أجل إرسال الأموال وتقديم معلومات شخصية مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان.
- **طلبات الحصول على معلومات شخصية:** طلبات للحصول على معلومات شخصية و/أو مالية لغرض الاحتيال، وسرقة الهوية وغيرهما من الجرائم.
- **أسماء نطاقات مُضلِّلة:** روابط تتضمن أخطاء إملائية أو تحمل عناوين مشابهة إلى حد ما للمواقع الحقيقة. فإذا كنتم في شك من صحة أي موقع يستخدم اسم IEL، يرجى دائماً زيارة موقعنا الإلكتروني (www.iel.sa) أو الاتصال بمركز خدمة عملاء iel عبر الرقم الموحد (920003298).

أنواع الاحتيال الإلكتروني

رسائل البريد الإلكتروني الاحتيالية والضارة: هي أكثر طرق الاحتيال شيوعاً عبر الإنترنت، وتهدف إلى خداعكم من خلال التظاهر بأن مصدرها معروف كشركة IEL (على سبيل المثال: استلام رسالة إلكترونية تبدو في ظاهرها أنها مرسلة من شركة IEL) من أجل حثكم على مشاركة معلومات شخصية ذات طبيعة حساسة، أو بيانات الحساب أو إرسال أموال، وقد تتضمن أيضا طلباً بالتسجيل في مسابقة من أجل الفوز بجوائز.

في هذا الشأن، نحث عملاءنا على التحقق من صحة أي طلب لا يأتي مباشرة من موظف IEL أو اسم النطاق الصحيح للشركة.

سرقة الهوية: تحدث عندما يخدعكم شخص ما لكي تقوموا بالكشف عن/ تقديم معلومات شخصية أو مالية أو بيانات حساباتكم. وعادة ما يدعي سارقو المعلومات بأنهم من شركات معروفة ويرسلون إليكم رسائل إلكترونية أو يتصلون بكم هاتفياً ويطلبون منكم الرد على أسئلتهم أو يقومون بتوجيهكم إلى صفحة ويب احتيالية تطلب منكم تقديم معلومات شخصية مثل رقم بطاقة الائتمان أو كلمة مرور الحساب أو حتى بيانات اعتماد IEL.

الاحتيال باستخدام بطاقات الائتمان: يحدث ذلك، في بعض الحالات، عند فقدان بطاقة الائتمان أو سرقتها من قبل شخص يقوم باستخدامها، وتتم عمليات الاحتيال باستخدام بطاقات الائتمان في المقام الأول من خلال اختراق بيانات حساب البطاقة في سياق الاستخدام المعتاد. وغالباً ما تُستخدم بيانات البطاقات المسروقة لمحاولة إتمام عمليات شراء احتيالية عبر الإنترنت.

البريد المزعج والفيروسات: بالنسبة لمجال عملنا، يستلم العملاء في الغالب رسالة بريد إلكتروني مفاداها أن IEL تحاول توصيل طردٍ أو شحنة ما إليكم وتطلب منكم فتح ملف مرفق بالبريد الإلكتروني لإتمام عملية التوصيل، ومن المرجح أن يكون هذا المرفق فيروساً. لذا، فإننا نرجو منكم عدم فتح ذلك الملف المرفق وتبليغ مركز خدمة العملاء عبر البريد الإلكتروني التالي: (info@iel.sa) إلا إذا كنتم تنتظرون فعلاً استلام رسالة بريد إلكتروني مماثلة.

رسائل البريد الإلكتروني الخاصة بتتبع الشحنات: يستلم العملاء، في بعض الحالات، رسالة بريد إلكتروني تحتوي على رقم تتبع مسار شحناتهم، ويمكن التحقق من هذا الرقم عن طريق إدخاله في خانة تتبع "مسار الشحنة" على موقعنا الإلكتروني: www.iel.sa. فإذا لم تحصلوا على أي نتائج للبحث، يرجى العلم بأن رقم التتبع المذكور ليس صحيحاً، وأن IEL ليست من أرسلت رسالة البريد الإلكتروني، ونرجو منكم في هذه الحالة تبليغ مركز خدمة العملاء عن هذه الرسالة عبر البريد الإلكتروني التالي: (info@iel.sa).

رمز التفعيل: يتم إرسال رسائل نصية تحتوي على رمز التفعيل فقط لإتمام عملية التسجيل بعد تحميل تطبيق IEL للهاتف النقال. يرجى تجاهل أي رسالة تصلكم غير ذلك. لن تقوم IEL بطلب رمز التفعيل الخاص بكم عن طريق الهاتف أو الإيميل؛ لحماية خصوصية حسابكم يرجى عدم مشاركة رمز التفعيل مع أي شخص كان.

واجباتنا

نلتزم في IEL باعتماد أرقى المعايير المتبعة في القطاع ونطبق أفضل الإجراءات الأمنية والإدارية والفنية والمادية لحماية المعلومات الشخصية التي تقدمونها من التلف أو الفقدان أو التغيير أو الوصول أو الإفصاح أو الاستخدام غير المشروع أو غير المصرح به أو العرضي وغير ذلك من أشكال المعالجة غير القانونية. كما نستثمر باستمرار في أحدث التقنيات العالمية لتقليل جميع المخاطر المحتملة بما يصب في مصلحة عملائنا، ونظل ملتزمين بضمان تلبية متطلبات الأمن الأكثر صرامة وتعزيز ثقافة الحماية الأمنية داخل مؤسستنا، مع العلم بأن التزامنا بأمن المعلومات يخضع للمراجعة والتدقيق .

ويستخدم موقعنا الإلكتروني وتطبيقنا الخاص بالهواتف الذكية العديد من التقنيات الأمنية بما في ذلك الخوادم الآمنة، إذ يتم تشفير جميع معلوماتكم الشخصية، بما في ذلك تفاصيل بطاقاتكم الائتمانية، حتى قبل إغلاق المتصفح أو الجهاز. كما تم اعتماد منصتنا للدفع الإلكتروني بحصولنا على شهادة معايير أمن وحماية بيانات البطاقات الائتمانية (PCI-DSS).

واجباتكم

بينما تقوم IEL بمراجعة هذه التدابير الأمنية وتعزيزها من وقت لآخر حسب الضرورة، إلا أن جزءاً من المسؤولية يقع على عاتقكم في حماية معلوماتكم مثل بيانات تسجيل الدخول وكلمات المرور من أي استخدام غير مصرح به، مع العلم بأنه لا توجد طريقة آمنة 100٪ لنقل الملفات عبر الإنترنت أو التخزين الإلكتروني. لذلك، لا تستطيع IEL ضمان الأمن المطلق لمعلوماتكم الشخصية.

الاتصال بنا

إذا كان لديكم أي ملاحظات أو أسئلة حول إجراءات حماية العملاء ومنع الاحتيال المتبعة في IEL، يرجى الاتصال بمركز خدمة العملاء عبر البريد الإلكتروني التالي: (info@iel.sa).

إخلاء المسؤولية:

لا ولن تطلب IEL منك تقديم أي معلومات شخصية أو بيانات الدفع من خلال البريد التقليدي أو الإلكتروني. ولا شك بأن توخي الحيطة والحذر وحماية معلوماتك الحساسة أفضل سبيل لمنع الاحتيال. فإذا استلمت طلباً لتقديم معلومات شخصية أو بيانات الدفع عبر أي من أشكال التواصل المذكورة آنفاً، يرجى عدم الرد أو التعاون مع المرسل والإبلاغ عنها فوراً إلى مركز خدمة العملاء

لا تتحمل IEL أي مسؤولية عن أي تكاليف أو رسوم أو مدفوعات تكون نتيجة أي نشاط احتيالي. يجب توخي الحيطة والحذر من وسائل الاحتيال المذكورة أعلاه ووضعها في الاعتبار لحماية معلوماتك وبياناتك من السرقة تفادياً للوقوع ضحية أي عملية احتيال في المستقبل.