التسوق الآمن عبر الإنترنت

نظرة عامة

باقتراب مواسم العطلات بالنسبة للكثيرين منا، سرعان ما يبحث ملايين الأشخاص عن شراء الهدايا المثالية. والكثير منا سيتسوق عبر الإنترنت بحثًا عن صفقات رائعة وتجنب الحشود المزعجة في الأسواق. لسوء الحظ، مجرمو الإنترنت سيكونون نشيطين أيضًا في هذه المواسم، حيث ينشئون مواقع تسوق مزيفة ويستخدمون أساليب متنوعة لخداع الأشخاص. في هذه النشرة، سنوضح كيف يمكنك التسوق عبر الإنترنت بأمان وتجنب الوقوع ضحية لهم.

متاجر وهمية على الانترنت

يقوم مجرمو الإنترنت عادة بإنشاء متاجر وهمية على الإنترنت تحاكي مظهر المواقع الحقيقية أو حتى تستخدم أسماء المتاجر أو العلامات التجارية المعروفة. عندما تبحث عن أفضل الصفقات عبر الإنترنت، قد تجد نفسك في أحد هذه المواقع المزيفة. ومن خلال الشراء من هذه المواقع، قد ينتهي بك الأمر ببضائع مزيفة أو مسروقة، وفي بعض الحالات، قد لا تستلم مشترياتك أبدًا. احم نفسك من المتاجر المزيفة عبر الإنترنت:

عندما يكون ذلك ممكنًا، قم بالشراء عبر الإنترنت من المتاجر التي تعرفها بالفعل، والتي تثق بها أو قمت بالتعامل معها من قبل. وقم بتسجيل عنوان الصفحة في محفوظات المتصفح لديك.

ابحث عن أسعار أفضل بكثير من تلك التي تراها في المتاجر الموجودة على الإنترنت. لكن إذا كانت الصفقة جيدة جدًا للدرجة التي تكاد تكون غير واقعية، انتبه فقد تكون خدعة.

كن متشككا في حال كان موقع الويب يشبه الموقع الذي استخدمته في الماضي، ولكن اسم نطاق موقع الويب أو اسم المتجر مختلف قليلاً. على سبيل المثال، قد تكون معتادًا على التسوق في Amazon، وعنوان موقع الويب الخاص به هو www.amazon.com، ولكن ينتهي بك الأمر إلى التسوق في موقع مزيف له عنوان موقع ويب مماثل ولكن تم استبدال الحرف «o» بالرقم «0».

اكتب اسم المتجر على الإنترنت أو عنوان الويب الخاص به في محرك بحث لمعرفة ما قاله الآخرون حوله. ابحث عن مصطلحات مثل «النصب» أو «الاحتيال» أو «لن أفعلها مرة أخرى» أو «المزيفة».

استخدم كلمة مرور فريدة لكل حساب من حساباتك على الإنترنت. لا تستطيع تذكر كل كلمات مرورك.؟ فكر في تخزينها جميعًا في مدير كلمات المرور.

المخادعون على مواقع التسوق الشرعية (الأصلية)

حافظ على حذرك حتى عند التسوق في مواقع موثوق بها. غالبًا ما تقدم المتاجر الكبيرة على الإنترنت منتجات تباع بواسطة أفراد أو شركات مختلفة قد يكون لديها نوايا احتيالية. مثل هذه الوجهات على الإنترنت تشبه أسواق العالم الحقيقي، حيث يكون بعض البائعين أكثر جدارة بالثقة من الآخرين. تحقق من سمعة كل بائع قبل الطلب. وكن حذرًا من البائعين الجدد على المتجر أو الذين يبيعون سلعًا بأسعار منخفضة بشكل غير منطقي أو غير معتاد. راجع سياسة المتجر عبر الإنترنت بشأن المشتريات من هذه الجهات الخارجية. عندما تكون في شك، يمكنك شراء سلع يتم بيعها مباشرة من المتجر عبر الإنترنت، وليس عن طريق البائعين الخارجيين الذين يشاركون في السوق عبر الإنترنت.

الدفع الإلكتروني عبر الإنترنت للمشتريات

راجع بانتظام بيانات بطاقة الائتمان الخاصة بك لتحديد الدفعات المالية المشبوهة. قم بتمكين خيار التنبيه -إذا كان ذلك ممكنًا -عن طريق البريد الإلكتروني أو الرسائل النصية أو تطبيقات الهاتف المحمول في كل مرة يتم فيها اقتطاع مبالغ مالية من بطاقة ائتمانك. إذا وجدت أي نشاط مشبوه، فاتصل بشركة بطاقة الائتمان الخاصة بك على الفور وأبلغ عنها. أيضاً تجنب استخدام بطاقات الصراف الآلي كلما أمكن ذلك. وذلك لأنها تخصم الأموال من حسابك المصرفي مباشرةً، فإذا تم حصول عملية احتيال، فسيكون لديك وقت ضيق وصعب للغاية لاستعادة أموالك. هناك خيار آخر وهو استخدام خدمات الدفع المعروفة، مثل PayPal، لعمليات الشراء عبر الإنترنت، والتي لا تتطلب منك الكشف عن رقم بطاقة الائتمان الخاصة بك للبائع. أيضا، فكر في استخدام بطاقة تسوق خاصة مشحونة بمبلغ محدد «gift cards»في عمليات الشراء عبر الإنترنت.

أخيراً، لمجرد أن متجراً على الإنترنت لديه تصميمات احترافية مصممة تصميما جيدا فلا يعني أنه شرعي. إذا كان موقع الويب يشعرك بعدم الارتياح، فلا تستخدمه. بدلاً من ذلك، توجه إلى موقع معروف يمكنك الوثوق به أو استخدمته بأمان في الماضي. قد لا تجد تلك الصفقة مذهلة احيانا، لكن من الأرجح أن ينتهي بك الأمر بمنتج شرعي متفادياً التعرض للخداع.

الضيف المحرر

ليني زيلتسر هو كبير مدراء أمن المعلومات في أكسونوس وكبير مدربين وكاتب بمعهد *SANS*. يمكنك متابعته على تويتر @ *lennyzeltser* وقراءة مدونته على *zeltser.com*.

مصادر إضافية

Social Engineering: http://www.sans.org/u/X7k

Scamming You Through Social Media: http://www.sans.org/u/X7p

Making Passwords Simple: http://www.sans.org/u/Xu9