التصيد المالي ينمو ٩.٥٪ خلال موسم أعياد ٢٠١٩

البوابة العربية للأخبار التقنية[1]

دائمًا ما يمثل الربع الأخير من العام فترة مثمرة للمجرمين الإلكترونيين في التصيد المالي حيث يحرص المجرمون على استغلال سعي المستهلكين للحصول على أفضل الصفقات لموسم العطلات والأعياد لا سيما في أيام الجمعة البيضاء وإثنين الإنترنت وأيام التسوق التي تسبق عيد الميلاد، والتي تشهد نموًا كبيرًا لا يقتصر على المبيعات وحدها، وإنما يمتد ليشمل الأنشطة الرقمية التخريبية.

وقد اكتشف باحثون في (كاسبرسكي) حدوث نمو بنسبة ٩.٥٪ في عمليات التصيد المالي في الربع الأخير من عام ٢٠١٩، مع نمو في نشاط رسائل البريد الإلكتروني غير المرغوب فيه كمًّا ونوعًا.

ويتيح تحليل مشهد التهديدات خلال فترة الأعياد المنقضية فهمًا أفضل للتغيّرات الحاصلة في الأنشطة الاحتيالية، وقد استمرت حصة التصيد المالي في النمو خلال الربع الرابع ٢٠١٩، بنسبة بلغت ٥٢.٦١٪

المتغيرات التي شهدها مجال التصيد المالي في ٢٠١٩ في الجدول:

2019	الربع الثالث	الربع الرابع
إجمالي التصيد المالي	43.19%	52.61%
التسوق الإلكتروني	5.52%	8.89%
الخدمات المصرفية الإلكترونية	22.46%	29.73%
المدفوعات الإلكترونية	15.21%	14.00%

وما زال الاحتيال وسيلة فعالة لدفع المستخدمين إلى تقديم بياناتهم الشخصية وبيانات البطاقات المصرفية إلى مجرمي الإنترنت من دون علمهم، وغالبًا ما تستخدم العلامات التجارية الشعبية طُعمًا في هذه المساعي الخبيثة. واشتملت الأمثلة التي اكتشفتها (كاسبرسكي) على صفحة أمازون وهمية تستدرج المستخدمين بعروض عيد الميلاد لسرقة بيانات الاعتماد الخاصة بحساباتهم Amazon Prime.

وكثيرًا ما تؤدي محاولات التصيد هذه المطلوب منها، فقد أظهر تحليل نشاط التصيد المالي باستخدام الاسمين التجاريين eBay وAlibaba طعمين للإيقاع بالمتسوقين، نموًا ملحوظًا قبل التسوق لموسم العطلات.

[1] نقلا عن البوابة العربية للأخبار التقنية AIT، تاريخ ٩-٢-٢٠٢٠، رابط

فقبل يوم الجمعة البيضاء ببضعة أيام فقط زاد عدد المستخدمين الذين يحاولون الوصول إلى صفحات تصيد وهمية تنتحل هوية eBay، بأربعة أضعاف، ليصل إلى أكثر من ٨٠٠٠ محاولة يوميًا.

وبقيت هذه المستويات المرتفعة من الزيارات في مستواها حتى منتصف ديسمبر، قبل أن تعاود الصعود إلى ذروة أخرى قبل عيد الميلاد بأسبوع، وقد شوهد نمط مماثل مع محاولات التصيد التي جرت عبر صفحات تنتحل هوية موقع Alibaba.

من ناحية أخرى، حدث نمو طفيف خلال موسم العطلات في رسائل البريد الإلكتروني غير المرغوب فيه، ولكنها شهدت تنوعًا كبيرًا في الموضوعات، وتراوحت المخططات التخريبية بين وعود بالحصول على تبرعات عيد الميلاد، إلى محاولات احتيال تهدف إلى سرقة العملات الرقمية، ورسائل البريد الإلكتروني الضارة التي يتم إرسالها إلى الشركات باعتبارها طلبيات شراء عاجلة لعيد الميلاد.

ولا تقتصر مثل محاولات التصيد المتعلقة بالعطلات ورسائل البريد الإلكتروني غير المرغوب فيه هذه على موسم الأعياد وحده، فقد تلقى مستخدمون في جنوب شرق آسيا أيضًا عروضًا مُغرية، ولكنها ارتبطت بالسنة القمرية الجديدة.

وبهذه المناسبة، وصفت (تاتيانا سيدورينا)، المحللة الأمنية لدى (كاسبرسكي)، موسم العطلات بأنه فترة تشهد اندفاعًا محمومًا نحو التسوق واتخاذ قرارات متسرعة، مشيرة إلى أن الضغط الواقع على المتسوقين للحصول على صفقة جيدة أو شراء الهدايا في الوقت المناسب قد يعني فقدان الحذر المطلوب، مما يسهّل على مجرمي الإنترنت استغلالهم.

وقالت (تاتيانا): يصعب كثيرًا على المتسوقين في هذا الوقت من العام التخلي عن رغبتهم في الحصول على هدية رائعة بسعر ممتاز، أما المجرمون فيسعون جاهدين طوال العام إلى استغلال تلك الرغبات مع نهاية العام، الذي يُعدّ وقتًا مثمرًا لهم.

وأكّدت (سيدورينا) أن المطلوب من المستهلكين ليس التخلّي عن الرغبة في التسوق لموسم الأعياد والحصول على أفضل الصفقات، وإنما توخّي الحذر، وإيلاء عمليات الشراء وسداد المدفوعات بالبطاقات المصرفية تركيزًا إضافيًا، مضيفة كذلك إن الاشتراكات أو الدفعات المتأخرة قد تكون ناجمة عن عمليات احتيال، نظرًا لأن المجرمين قد لا يستخدمون البيانات المسروقة على الفور.

وتوصي (كاسبرسكي) المستخدمين باتباع النصائح التالية للبقاء في مأمن من محاولات التصيّد عبر البريد غير المرغوب فيه :

- عند تلقي رابط لعرض رائع عبر البريد الإلكتروني، فينبغي التحقق من الرابط المضمَّن فيه، إذ قد يختلف في بعض الأحيان عن الرابط المكتوب الظاهر في الرسالة الإلكترونية، فإذا كان الأمر كذلك، يمكن الوصول إلى الصفحة التي تشتمل على العرض مباشرةً من خلال موقع الويب الرسمي الذي تتبعه .
- تجنب عمليات الشراء إلا من خلال الأسواق الرسمية والانتباه إلى عناوين الويب إذا جرى توجيه المستخدم إليها من صفحات أخرى، فإذا كانت الصفحة تختلف عن موقع المتجر الرسمي، ينبغي التحقّق من العرض الذي جرى التوجيه إليه من خلال البحث عنه في صفحة الويب الرسمية للمتجر .
- استخدم حلاً أمنيًا مزودًا بتقنيات مكافحة التصيد القائم على السلوك، مثل Kaspersky Security Cloud أو Kaspersky Total Security، والذي سيُعلِمُك إذا كنت تحاول زيارة صفحة ويب للتصيّد الاحتيالي .
- تجنب استخدام كلمة المرور نفسها في مواقع ويب وخدمات مختلفة، لأن سرقتها يعني إمكانية اختراق جميع الحسابات الأخرى، ويمكن إنشاء كلمات مرور قوية ومقاومة للاختراق دون مواجهة صعوبة تذكرها، باستخدام تطبيقات إدارة كلمات المرور، مثل تطبيق Kaspersky Password Manager .