اقتصاد, تقنية وسيارات

8 أغسطس 2024 16:59 مساء

معلومات مهمة لحماية البريد الإلكتروني 6

دبي: «الخليج»

مع توقّع نمو عدد مستخدمي البريد الإلكتروني حول العالم إلى 4.73 مليار بحلول العام 2026، أصبح البريد الإلكتروني أحد أهم منصات الاتصال في العصر الرقمي. فبالنسبة لكثير من الناس، يعد عنوان البريد الإلكتروني هويتهم الرقمية الرئيسية. لذا، تبحث كاسبرسكي ما يمكن للمحتالين فعله باستخدام عنوان البريد الإلكتروني لأحدهم، وكيفية الحفاظ عليه آمناً.

قال براندون مولر، الخبير الفني لمنطقة الشرق الأوسط وإفريقيا لدى كاسبرسكي: «تماماً كما اسمك، هناك كمية هائلة من المعلومات المرتبطة بعنوان البريد الإلكتروني. إذ تُعتبر كل من عناوين بريدنا الإلكتروني المهنية والشخصية من بين الأصول الرئيسية التي تستقطب اهتمام مجتمع متنامٍ من مجرمي الإنترنت المتطورين في جميع أنحاء العالم».

• نماذج تسجيل الدخول

تتطلب معظم نماذج تسجيل الدخول عبر الإنترنت، والبوابات الرقمية، وتجار التجزئة الإلكترونية، وتطبيقات الهاتف المحمول عنوان بريد إلكتروني. لذا، حتى مع حاجة المخترقين إلى كلمات المرور الخاصة بالبريد الإلكتروني

والحسابات الرقمية للشخص لإمكانية الوصول، فإن عنوان البريد الإلكتروني نقطة بداية مهمة بالنسبة لهم لتنفيذ سيناريوهات احتيالية مختلفة.
يمكن لمجرمي الإنترنت استهداف الفرد برسائل التصيد الاحتيالي التي تحتوي على مرفقات برمجيات خبيثة، أو روابط خبيثة لمواقع إلكترونية احتيالية. كما بمقدورهم أيضاً توظيف أساليب الهندسة الاجتماعية المتطورة للحصول على تفاصيل شخصية، مثل رقم الحساب المصرفي للشخص، أو رقم هويته، أو عنوانه الفعلي، أو رقم هاتفه، أو كلمات مروره من بين أشياء أخرى.

• انتحال عنوان

كما يعد انتحال عنوان بريد إلكتروني أحد الأخطار الأخرى. ويتضمن ذلك إنشاء عنوان بريد إلكتروني زائف، ليبدو كعنوان شخص ما، ولكنه يحتوي على تغييرات بسيطة يصعب اكتشافها (مثل تبديل رقم بحرف أو إضافة فاصلة). ويمكن للمتسللين بعد ذلك انتزاع المعلومات من أصدقاء وعائلة ذلك الشخص في الوقت الذي ينتحلون فيه شخصيته. وغالباً ما يجري إغفال هذا النهج من قبل مرشحات البريد العشوائي المستخدمة على منصات البريد الإلكتروني.
بالإضافة لذلك، يمكن لمجرمي الإنترنت اكتشاف هوية صاحب عنوان بريد إلكتروني معين باستخدام أداة البحث العكسي عن البريد الإلكتروني. ويمكن أن يوفر لهم هذا نقطة انطلاق مهمة للحصول على أكبر قدر ممكن من البيانات الشخصية المتاحة مجاناً حول أحدهم. وبما أن رسائل البريد الإلكتروني للعديد من الأشخاص غالباً ما تحتوي على أسمائهم، وأرقام يمكن تذكرها، عادةً ما تكون تاريخ الميلاد، فإن هذين العاملين التعريفيين كافيان للعديد من مجرمي الإنترنت للبدء في جمع مزيد من البيانات الشخصية المربحة عبر الإنترنت، والتي يمكن استخدامها لسرقة هوية ما أو القيام باحتيال مالي.

• حماية العنوان

مع المخاطر التي يمكن أن يشكلها الكشف عن عنوان (أو عناوين) البريد الإلكتروني على الخصوصية والسلامة الشخصية والمهنية، فمن المهم معرفة كيفية حماية عنوان البريد الإلكتروني من الوصول غير المصرح به.

• كلمات المرور القوية

يقول براندون مولر: «إحدى أفضل الطرق كي يحافظ المرء على أمان عنوان بريده الإلكتروني هي استخدام كلمات مرور قوية. فمن الصعب سرقة المعلومات الشخصية عبر عنوان بريد إلكتروني فقط بدون كلمة مرور. ويجعل ذلك كلمات المرور القوية (التي تكون بطول 10 إلى 12 رمزاً، وتشتمل على مزيج من رموز خاصة، وأرقام، وأحرف كبيرة وصغيرة)، أحد من أفضل الطرق للحفاظ على عنوان البريد الإلكتروني آمناً».
قد يكون استذكار كلمات المرور أمراً صعباً، خاصة للحسابات نادرة الاستخدام، وهنا يمكن أن يغدو مدير كلمات المرور بمثابة أداة لا غنى عنها، فيعمل كخزنة خاصة مشفرة، لا تحتاج سوى كلمة مرورك الرئيسية لفتحها. وتجري مزامنة هذا النوع من الحلول عبر الأجهزة، ويساعد في الملء التلقائي لبيانات تسجيل الدخول، وتفاصيل الدفع بالبطاقة، والبيانات الشخصية للاستمارات على أي تطبيق أو موقع إلكتروني.

• الحظر وفلاتر البريد العشوائي

من المهم التأكد من التفعيل الدائم لفلتر البريد العشوائي لمزود البريد الإلكتروني. إذ يقلل ذلك من احتمالية النقر على رابط أو رسالة بريد إلكتروني خبيثة. لكن وحتى مع وجود الفلاتر، فمن الجيد دائماً أن تظل يقظاً في حالة تجاوز مثل

هذه الرسائل الإلكترونية لفلتر البريد العشوائي (وهو ما قد يكون الحال مع التزييف على سبيل المثال) وحظر أي رسائل إلكترونية مشبوهة والإبلاغ عنها إلى مزود الخدمة، أو فريق تكنولوجيا المعلومات عندما يتعلق الأمر برسائل البريد .الإلكتروني الخاصة بالعمل

• المصادقة الثنائية

لقد أصبحت المصادقة الثنائية ضرورة للشركات والمستهلكين على حد سواء. حيث يقدم معظم عملاء البريد الإلكتروني الموثوقين هذه الخدمة كميزة قياسية. ويتطلب هذا الإجراء الأمني من الشخص إدخال معلومات تعريفية .إضافية، مثل إجابة سرية عن سؤال ما، أو كود مصادقة يتم إرساله إلى الهاتف المحمول لذلك المستخدم

• حساب البريد الإلكتروني المؤقت

من الأفكار الجيدة أيضاً أن يستخدم الشخص حساب بريد إلكتروني مؤقت عند التسجيل في موقع إلكتروني أو تطبيق يبدو مشبوهاً. وتعد هذه الحسابات مجرد حسابات بريد إلكتروني ذات معلومات تعريفية زائفة أو محدودة للغاية، وفي .حال تعرضه للاحتيال أو الاختراق، فلا خوف من العواقب السلبية

• الحفاظ على الحذر

لا يعد تثقيف ذاتك حول أفضل ممارسات الأمن السيبراني شيئاً يمكن القيام به لمرة واحدة. إذ يحتاج الناس إلى مواكبة أحدث برامج التدريب المتاحة من الشركة. ويجب على المستخدمين المنزليين أيضاً تحديث برامجهم، وعدم النقر على أي شيء مشبوه أبداً.
يختتم براندون مولر قائلاً: «لن تعرف قيمة ما لديك حتى تفقده. تنطبق هذه العبارة في معظم الأحوال على رسائل البريد الإلكتروني أيضاً. فسواء للاستخدام التجاري أو الشخصي، أصبح البريد الإلكتروني هو الأساس لأنماط حياتنا الرقمية. ويجب على الناس أن يضعوا في أذهانهم مدى أهمية الحفاظ على أمان حسابات البريد الإلكتروني خاصتهم، مع البقاء .«حذرين من بيئة الجرائم الإلكترونية دائمة التحول