كن ذكياً كن ذكياً في مجال الأمن الإلكتروني المعلوماتي

#CyberMonth

شهر التوعية بالأمن الإلكتروني المعلوماتي أو السيبراني 2021:
قم بدورك. #BECYBERSMART

التصيد والخداع

تستخدم هجمات التصيد الاحتيالي البريد الإلكتروني أو مواقع الويب الضارة لإصابة جهازك بالبرامج المهاجمة والفيروسات لجمع المعلومات الشخصية والمالية. يحاول مجرمو الإنترنت إغراء المستخدمين للنقر على رابط أو فتح مرفق يصيب أجهزة الكمبيوتر الخاصة بهم، مما يخلق ثغرات أمنية يستخدمها المجرمون للهجوم. قد تبدو رسائل البريد الإلكتروني المخادعة وكأنها واردة من مؤسسة مالية حقيقية، موقع تجارة إلكترونية، وكالة حكومية أو أي خدمة أو شركة أو فرد آخر. قد يطلب البريد الإلكتروني أيضاً معلومات شخصية مثل أرقام الحسابات أو كلمات المرور أو أرقام الضمان الاجتماعي. عندما يستجيب المستخدمون بالمعلومات أو ينقرون على رابط ، سوف يستخدمها المهاجمون للوصول إلى حسابات المستخدمين.

تستخدم هجمات الانتحال عناوين البريد الإلكتروني أو أسماء المرسلين أو أرقام الهواتف أو عناوين URL لمواقع الويب التي تتمثل على انها مصدر موثوق. يحاول مجرمو الإنترنت خداع المستخدمين عن طريق تغيير حرف أو رمز أو رقم واحد ضمن الاسم. يستخدم هذا التكتيك لإقناع المستخدمين بأنهم يتفاعلون مع مصدر مألوف. يهدف مجرمو الإنترنت أن تصدق أن هذه الاتصالات المخادعة حقيقية تقودك إلى تحميل برامج ضارة على جهازك أو إرسال أموال أو الكشف عن معلومات شخصية أو مالية أو غيرها من المعلومات الحساسة.

كيف يغرك المجرمون

الرسائل التالية من OnGuardOnline التابع للجنة التجارة الفيدرالية، هي أمثلة لما قد يرسله المهاجمون عبر البريد الإلكتروني أو يرسلون رسائل نصية عند التصيد الاحتيالي للحصول على معلومات حساسة:

- "نحن نشك في وجود معاملة غير مصرح بها في حسابك. لضمان عدم اختراق حسابك، يرجى النقر على الرابط أدناه وتأكيد هويتك."
- "أثناء التحقق المنتظم للحسابات، لم نتمكن من التحقق من معلوماتك. الرجاء النقر هنا لتحديث معلوماتك والتحقق منها."
- "تشير سجلاتنا إلى أن حسابك قد تم تحميله بشكل زائد. يجب عليك الاتصال بنا في غضون 7 أيام لاسترداد أموالك."

للاطلاع على أمثلة على رسائل البريد الإلكتروني المخادعة الفعلية ، والخطوات التي يجب اتخاذها إذا كنت تعتقد أنك تلقيت رسالة بريد إلكتروني للتصيد الاحتيالي ، يرجى زيارة StopRansomware.gov.

نصائح بسيطة

- **تعامل بحزم وذكاء ضد المتطفلين عبر الإنترنت.** غالباً ما تكون الروابط في البريد الإلكتروني والمنشورات عبر الإنترنت هي الطريقة التي يتخرق بها مجرمو الإنترنت جهاز الكمبيوتر الخاص بك. إذا كنت غير متأكد من هوية مرسل البريد الإلكتروني - حتى إذا كانت التفاصيل تبدو دقيقة - فلا ترد ولا تنقر على أي روابط أو مرفقات موجودة في هذا البريد الإلكتروني. كن حذراً من التحيات العامة مثل "Hello Bank Customer"، لأنها غالباً ما تكون علامات تدل على محاولات التصيد الاحتيالي. إذا كنت قلقاً بشأن شرعية البريد الإلكتروني ، فاتصل بالشركة مباشرةً.
- **فكر قبل أن تتصرف.** كن حذراً من الاتصالات التي تطلب منك التصرف على الفور. تحاول العديد من رسائل البريد الإلكتروني المخادعة خلق شعور بالإلحاح ، مما يجعل المستلم يخشى أن تكون حساباته أو معلوماته في خطر. إذا تلقيت بريداً إلكترونياً مشبوهاً يبدو أنه من

شخص تعرفه ، فاتصل بهذا الشخص مباشرةً على نظام أساسي آمن منفصل. إذا كان البريد الإلكتروني يأتي من مؤسسة ولكن لا يزال يبدو "احتيالياً" ، فتواصل معها عبر خدمة العملاء للتحقق من الاتصال.

- **حماية معلوماتك الشخصية.** إذا كان لدى الأشخاص الذين يتصلون بك تفاصيل أساسية من حياتك - المسمى الوظيفي الخاص بك ، وعناوين البريد الإلكتروني المتعددة ، والاسم الكامل، والمزيد مما قد تكون نشرته عبر الإنترنت في مكان ما - فيمكنهم محاولة عمل هجوم تصيد احتيالي مباشر عليك. يمكن لمجرمي الإنترنت أيضاً استخدام الهجوم من خلال معلوماتك على وسائل التواصل الاجتماعية وبتفاصيل دقيقة لمحاولة التلاعب بك لتخطي بروتوكولات الأمان العادية.
- **كن حذرا من الارتباطات التشعبية.** تجنب النقر فوق الارتباطات التشعبية في رسائل البريد الإلكتروني وقم بالمرور فوق الروابط للتحقق من صحتها. تأكد أيضاً من أن عناوين URL تبدأ بـ "https" ، حيث يشير الحرف "s" إلى تمكين التشفير لخاصية حماية معلومات المستخدمين.
- **ضاعف من عملية حمايتك.** استخدم خاصية التحقق بخطوتين (MFA) للتأكد من أن الشخص الوحيد الذي لديه حق الوصول إلى حسابك هو أنت. استخدم هذه الخاصية للبريد الإلكتروني، الخدمات المصرفية، وسائل التواصل الاجتماعي، وأي خدمة أخرى تتطلب تسجيل الدخول. إذا كان خيار MFA، متوفر قم بتفعيله ، باستخدام جهاز محمول موثوق به، مثل هاتفك الذكي، أوالتطبيق الخاص بالتحقق، أو من خلال رمز آمن - جهاز مادي صغير يمكن ربطه بحلقة المفاتيح الخاصة بك. اقرأ دليل خاصية التحقق بخطوتين MFA، لمزيد من المعلومات.
- **اعمل تغيير جذري في عملية اختيار كلمة المرور الخاصة بك.** وفقاً للمعهد الوطني للمعايير (NIST) ، كن مبدعاً وخصص أطول كلمة مرورمسموح بها ومن شأنها أن تمنع مجرمي الإنترنت من الوصول إلى هذه الحسابات وحمايتك في حالة حدوث اختراق. استخدم نظام إدارة كلمات المرور لتوليد كلمات مرور وممكن تذكرها وتكون مختلفة ومعقدة لكل حساب من حساباتك. أقرأ النصائح حول كيفية خلق كلمة مرور ، لمزيد من المعلومات.
- **تثبيت وتحديث برامج مكافحة الفيروسات.** تأكد من أن جميع أجهزة الكمبيوتر والأجهزة المرتبطة بالإنترنت من هواتف والأجهزة اللوحية مجهزة ببرامج مكافحة فيروسات وجدران الحماية وعوامل تصفية البريد الإلكتروني وبرامج مكافحة التجسس التي يتم تحديثها بانتظام.

كيفية الإبلاغ

للإبلاغ عن محاولات التصيد الاحتيالي أو الانتحال أو للإبلاغ على أنك ضحية ، قم بزيارة www.IC3.gov لتقديم شكوى.
لمزيد من المعلومات حول طرق الحماية، يرجى زيارة الموقع StopRansomware.gov .

اتصل بفريق شهر التوعية بالأمن الإلكتروني المعلوماتي أوالسيبراني CISA

شكراً لك على دعمك المستمر والتزامك بشهر التوعية بالأمن السيبراني ومساعدة جميع الأمريكيين في البقاء آمنين عبر الإنترنت. لمعرفة المزيد يرجى إرسال بريد إلكتروني إلى فريقنا على CyberAwareness@cisa.dhs.gov أو زيارة الموقع www.cisa.gov/cybersecurity-awareness-month أو staysafeonline.org/cybersecurity-awareness-month/ .