كن ذكياً كن ذكياً في مجال الأمن الإلكتروني المعلوماتي

#CyberMonth

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

سرقة الهوية الشخصية والخداع عبر الإنترنت

تتيح لنا تكنولوجيا اليوم الاتصال حول العالم، وإجراء المعاملات المصرفية والتسوق عبر الإنترنت، والتحكم في أجهزة التلفزيون والمنازل والسيارات من هواتفنا الذكية. مع توفر هذه الراحة الإضافية، تزداد مخاطر سرقة الهوية وعمليات الاحتيال عبر الإنترنت. كن ذكياً عند استخدامك الإنترنت #BeCyberSmart - في المنزل والمدرسة وأثناء العمل وعلى الأجهزة المحمولة وأثناء التنقل.

هل تعلم؟

- بلغ متوسط الخسائر المترتبة من اختراق البيانات ، لشركة أمريكية في عام 2020 ما قيمته 8.84 مليون دولار أمريكي[1]. هذه زيادة عن الرقم المعلن لسنة 2019 ، والبالغ 8.64 مليون دولار.
- حوالي 7-10٪ من سكان الولايات المتحدة هم ضحايا الاحتيال المتعلق في الهوية الشخصية، لكل عام ، وحوالي 21٪ منهم يتعرضون لحوادث متعددة من الاحتيال في الهوية [2].
- في عام 2020 ، تعرض 47٪ من الأشخاص الذين يعيشون في الولايات المتحدة لسرقة الهوية [3].

عمليات احتيال الإنترنت الشائعة

مع استمرار تطور التكنولوجيا ، يستخدم مجرمو الإنترنت تقنيات أكثر تعقيداً لاستغلال الأنظمة والحسابات والأجهزة لسرقة هويتك ومعلوماتك الشخصية وأموالك. لحماية نفسك من التهديدات عبر الإنترنت ، يجب أن تعرف الشكل الذي تأتي به هذه التهديدات. تتضمن بعض عمليات الاحتيال عبر الإنترنت الأكثر شيوعاً ما يلي:

- **عمليات الاحتيال المتعلقة بوباء COVID-19** تكون على شكل رسائل بريد إلكتروني تحتوي على مرفقات ضارة أو روابط إلى مواقع ويب احتيالية لخداع الضحايا للكشف عن معلومات حساسة أو التبرع للجمعيات الخيرية أو لأسباب احتيالية. توخ الحذر عند التعامل مع أي بريد إلكتروني يحتوي على سطر موضوع أو مرفق أو ارتباط تشعبي متعلق بكوفيد-19، وكن حذراً من نداءات أو نصوص أو مكالمات وسائل التواصل الاجتماعي المتعلقة بوباء بكوفيد-19.
- **عمليات احتيال مخادعة متنوعة** تحدث عندما تتلقى بريداً إلكترونياً أو مكالمة من شخص يدعي أنه مسؤول حكومي أو أحد أفراد العائلة أو صديق يطلب معلومات شخصية أو مالية. على سبيل المثال ، قد يتصل بك محتال من إدارة الضمان الاجتماعي لإعلامك بتعليق رقم الضمان الاجتماعي (SSN) الخاص بك ، على أمل أن تكشف عن رقم الضمان الاجتماعي الخاص بك أو تدفع لإعادة تنشيطه.
- **عمليات الاحتيال على مدفوعات المساعدة الاقتصادية لوباء كوفيد-19** والتي تستهدف صكوك المساعدة المالية للشعب الأمريكي. تحث وكالة CISA، جميع الأمريكيين على التنبه للاحتيال الإجرامي المتعلق بمدفوعات المساعدة الاقتصادية نتيجة لوباء كوفيد-19، لا سيما الاحتيال باستخدام اغراض تحججية بفيروس كورونا لسرقة المعلومات الشخصية والمالية ، بالإضافة إلى المدفوعات المالية نفسها - و تعطيل جهود الدفع.

نصائح بسيطة

- **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.

- **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. اقرأ النصائح حول كيفية خلق كلمة المرور، لمزيد من المعلومات.
- **أبق على اطلاع لآخر التحديثات.** حافظ على تحديث برنامجك إلى أحدث إصدار متاح. حافظ على إعدادات الأمان الخاصة بك للحفاظ على أمان معلوماتك عن طريق تشغيل التحديثات التلقائية حتى لا تضطر إلى التفكير في الأمر أو نسيانه وتعيين برنامج الأمان الخاص بك لإجراء عمليات فحص منتظمة.

احمي نفسك من مخاطر الاحتيال والخداع عبر الإنترنت

حافظ على الحماية أثناء الاتصال: خلاصة القول هي أنه عندما تكون متصلاً بالإنترنت، ستكون عرضة للخطر. إذا تم اختراق الأجهزة الموجودة على شبكتك لأي سبب من الأسباب أو إذا اخترق المتسللون جدار حماية مشفر، فقد يتنصت شخص ما عليك - حتى في منزلك باستخدام شبكة Wi-Fi مشفرة.

- تدرب على تصفح آمن للويب أينما كنت عن طريق التحقق من "القفل الأخضر" أو رمز القفل في شريط متصفح الإنترنت - وهذا يدل على اتصال آمن.
- عندما تجد نفسك في محيط خارجي عام ومزود "بشبكة Wi-Fi "، تجنب الوصول المجاني إلى الإنترنت بدون تشفير.
- في حال كنت تستخدم نقطة وصول عامة غير آمنة، فاحرص على سلامة ممارستك للإنترنت عن طريق تجنب الأنشطة الحساسة (مثل الخدمات المصرفية) التي تتطلب كلمات مرور أو بطاقات ائتمان. غالباً ما تكون نقطة الاتصال الشخصية الخاصة بك (hotspot) بديلاً أكثر أماناً لشبكة Wi-Fi المجانية.
- لا تكشف عن معلومات التعريف الشخصية مثل رقم حسابك المصرفي أو رقم التأمين الاجتماعي أو تاريخ الميلاد لمصادر غير معروفة.
- اكتب عناوين URL الخاصة بالموقع مباشرة في شريط العناوين بدلاً من النقر على الروابط أو استنساخها من البريد الإلكتروني.

الموارد المتاحة لك

إذا اكتشفت أنك أصبحت ضحية لجرائم الإنترنت، فأبلغ السلطات على الفور لتقديم شكوى. قم بحفظ وتسجيل جميع أدلة الحادث ومصدره المشتبه به. تحدد القائمة أدناه المنظمات الحكومية التي يمكنك تقديم شكوى إليها إذا كنت ضحية لجرائم الإنترنت.

- **FTC.gov:** يساعدك مورد FTC المجاني الشامل www.identitytheft.gov/ على الإبلاغ عن سرقة الهوية والتعافي منها. قم بالتبليغ عن عمليات الاحتيال إلى FTC على ftc.gov/OnGuardOnline أو www.ftccomplaintassistant.gov .
- **US-CERT.gov:** بلغ عن نقاط ضعف الكمبيوتر أو الشبكة إلى US-CERT عبر الخط الهاتفي للمساعدة: 1-888-282-0870 أو us-cert.cisa.gov. قم بإعادة توجيه رسائل البريد الإلكتروني أو مواقع الويب الخاصة بالتصيد الاحتيالي إلى US-CERT على phishing-report@us-cert.gov .
- **IC3.gov:** إذا كنت ضحية لجريمة عبر الإنترنت، فقم بتقديم شكوى إلى مركز شكاوى جرائم الإنترنت (IC3) باستخدام الموقع www.IC3.gov .
- **SSA.gov:** إذا كنت تعتقد أن شخصاً ما يستخدم رقم الضمان الاجتماعي الخاص بك ، فاتصل بالخط الهاتفي للمساعدة والخاص بعمليات الاحتيال في إدارة الضمان الاجتماعي على الرقم 1-800-269-0271.

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. لمزيد من المعلومات 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/ .

الموارد

1. Brook, Chris (18 أغسطس، 2020). *كم كانت كلف خرق البيانات في عام 2020؟* الحارس الرقمي . https://digitalguardian.com/blog/what-does-data-breach-cost-2020
2. Ricks, A, Irvin-Erickson, Y ، دكتوراه (2021). موجز بحثي: سرقة الهوية والاحتيال. مركز بحوث ضحايا الاحتيال. https://ncvc.dspacedirect.org/bitstream/item/1228/CVR Research Syntheses_Identity Theft and Fraud_Brief.pdf
3. GIACT. (2021). سرقة الهوية الأمريكية: الواقع الصارخ. أنظمةGIACT، شركة ذات مسؤولية محدودة. https://www.giact.com/aite-report-us-identity-theft-the-stark-reality/