كن ذكياً كن ذكياً في مجال الأمن الإلكتروني المعلوماتي

#CyberMonth

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

حماية منزلك الرقمي

المزيد من أجهزتنا المنزلية - بما في ذلك منظمات الحرارة وأقفال الأبواب وآلات القهوة وأجهزة إنذار وجود الأدخنة - متصلة الآن بالإنترنت. يتيح لنا ذلك التحكم في الأجهزة الموجودة من خلال هواتفنا الذكية مما يوفر لنا الوقت والمال مع توفير الراحة وحتى الأمان. تعتبر هذه التطورات في التكنولوجيا مبتكرة ومثيرة للاهتمام، ولكنها تشكل أيضاً مجموعة جديدة من المخاطر الأمنية. اتبع #BeCyberSmart للتواصل بثقة وحماية منز لك الرقمي.

نصائح بسيطة

- **حماية شبكة WI-FI الخاصة بك.** جهاز التوجيه اللاسلكي في منزلك هو المدخل الأساسي لمجرمي الإنترنت بغاية الوصول إلى جميع أجهزتك المتصلة. حماية شبكة Wi-Fi والأجهزة الرقمية يتم عن طريق تغيير كلمة المرور الافتراضية واسم المستخدم. لمزيد من المعلومات حول حماية شبكتك المنزلية ، تحقق من صفحة حماية الشبكات اللاسلكية، الخاصة بـ CISA.
- **ضاعف من مستوى حماية تسجيل الدخول.** قم بتمكين ميزة التحقق بخطوتين (MFA)، للتأكد من أن الشخص الوحيد الذي لديه حق الوصول إلى حسابك هو أنت. استخدم هذه الخاصية للبريد الإلكتروني، الخدمات المصرفية، ووسائل التواصل الاجتماعي وأي خدمة أخرى تتطلب تسجيل الدخول. إذا كان خيار ميزة MFA، متوفراً فقم بتفعيله باستخدام جهاز محمول موثوق به مثل هاتفك الذكي أو تطبيق المصادقة أو رمز آمن - وهو جهاز صغير يمكن ربطه بحلقة المفاتيح الخاصة بك. اقرأ دليل خاصية التحقق بخطوتين، للحصول على مزيد من المعلومات.
- **إذا قمت بتوصيل جهازك مع الإنترنت، قم بحماية هذا الاتصال.** سواء كان جهاز الكمبيوتر أو الهاتف الذكي أو جهاز الألعاب أو أجهزة الشبكة الأخرى ، فإن أفضل دفاع ضد الفيروسات والبرامج الضارة هو التحديث إلى أحدث برامج الأمان ومتصفح الويب وأنظمة التشغيل. قم بالتسجيل للحصول على التحديثات التلقائية، كلما كان ذلك ممكناً، وقم بحماية أجهزتك ببرنامج مكافحة الفيروسات. إذا كان متوفر لديك خيار تمكين التحديثات التلقائية للحماية من أحدث المخاطر، فقم بتشغيلها. وإذا كنت تضع شيئاً ما في جهازك، مثل USB لمحرك أقراص ثابت خارجي، فتأكد من فحص برنامج حماية جهازك للبحث عن الفيروسات والبرامج الضارة. أخيراً، قم بحماية أجهزتك ببرنامج مكافحة الفيروسات وتأكد من إجراء نسخ احتياطية دورية لأية بيانات لا يمكن إعادة إنشائها مثل الصور أو المستندات الشخصية.
- **حافظ على سلامة استخدامك للبرامج والتطبيقات.** يتم دعم معظم الأجهزة والألعاب والأجهزة المتصلة بواسطة تطبيق الهاتف المحمول. يمكن أن يمتلئ جهازك المحمول بتطبيقات مشبوهة تعمل في الخلفية أو تستخدم تصريحات افتراضية لم تدرك أبداً أنك فعلاً موافق عليها - جمع معلوماتك الشخصية دون علمك مع تعريض هويتك وخصوصيتك للخطر. تحقق من تصريحات التطبيق واستخدم "قاعدة الامتياز الأقل" لحذف ما لا تحتاجه أو لم تعد تستخدمه. تعلم أن تقول "لا" لطلبات الامتياز التي لا تعني شيئاً. قم باعمال تحميل التطبيقات على جهازك فقط من البائعين والمصادر الموثوق بهم.
- **لاتقم بالضغط على أي رابط وأعطاء معلوماتك الخاصة.** حدد المعلومات التي تنشرها على وسائل التواصل الاجتماعي - من العناوين الشخصية إلى المكان الذي تريد تناول القهوة فيه. ما لا يدركه الكثير من الناس هو أن هذه التفاصيل التي تبدو عشوائية هي كل ما يحتاج المجرمون إلى معرفته لاستهدافك واستهداف أحبائك وممتلكاتك المادية - عبر الإنترنت وفي العالم الحقيقي. حافظ على خصوصية أرقام الضمان الاجتماعي وأرقام الحسابات وكلمات المرور، بالإضافة إلى معلومات محددة عنك، مثل الاسم الكامل والعنوان وتاريخ الميلاد

وحتى خطط العطلات والمناسبات. قم بتعطيل خدمات الموقع التي تسمح لأي شخص برؤية مكانك - أو عدم تواجدك - في أي وقت. اقرأ ورقة نصائح الأمن السيبراني لوسائل التواصل الاجتماعي ، لمزيد من المعلومات.

- **استخدم خاصية مشاركة الملفات مع الآخرين بحذر**. يجب تعطيل مشاركة الملفات بين الأجهزة عند عدم الحاجة إليها. يجب عليك دائماً اختيار السماح بمشاركة الملفات فقط عبر شبكات المنزل أو العمل، وليس على الشبكات العامة مطلقاً. قد ترغب في التفكير في إنشاء دليل مخصص لمشاركة الملفات وتقييد امكانية الوصول إلى جميع الأدلة الأخرى. بالإضافة إلى ذلك ، يجب أن توفر كلمة مرور لأي عملية مشاركه، لزيادة الحماية.
- **تحقق من خيارات الحماية اللاسلكية لمزود الإنترنت أو الشركة المصنعة لجهاز التوجيه**. قد يوفر مزود خدمة الإنترنت والشركة المصنعة لجهاز التوجيه معلومات أو موارد للمساعدة في تأمين شبكتك اللاسلكية. تحقق من منطقة دعم العملاء في مواقع الويب الخاصة بهم للحصول على اقتراحات أو إرشادات محددة.
- **الاتصال باستخدام شبكة افتراضية خاصة (VPN)**. تمتلك العديد من الشركات والمؤسسات شبكة افتراضية لموظفيها. تسمح هذه الشبكات للموظفين بالاتصال بشكل آمن بشبكتهم عندما يكونون بعيداً عن مكتب عملهم. تقوم شبكات VPN ، بتشفير الاتصالات عند طرفي الإرسال والاستلام وتمنع حركة المرور غير المشفرة بشكل صحيح. إذا كانت شبكة VPN متاحة لك ، فتأكد من تسجيل الدخول إليها في أي وقت تحتاج فيه إلى استخدام نقطة وصول لاسلكية عامة.
- **الحد من الوصول**. اسمح فقط للمستخدمين المصرح لهم بالوصول إلى شبكتك. كل قطعة من الأجهزة المتصلة بشبكة لها عنوان تحكم في الوصول إلى الوسائط (MAC). يمكنك تقييد الوصول إلى شبكتك عن طريق تصفية عناوين MAC هذه. راجع وثائق المستخدم الخاصة بك للحصول على معلومات محددة حول تمكين هذه الميزات. يمكنك أيضاً استخدام حساب "الضيف" ، وهو ميزة مستخدمة على نطاق واسع في العديد من أجهزة التوجيه اللاسلكية. تتيح لك هذه الميزة منح الوصول اللاسلكي للضيوف على قناة لاسلكية منفصلة بكلمة مرور منفصلة، مع الحفاظ على خصوصية بيانات الاعتماد وتسجيل الدخول الأساسية الخاصة بك.

اتصل بفريق شهر التوعية بالأمن الإلكتروني المعلوماتي أوالسيبرانيCISA

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/ .