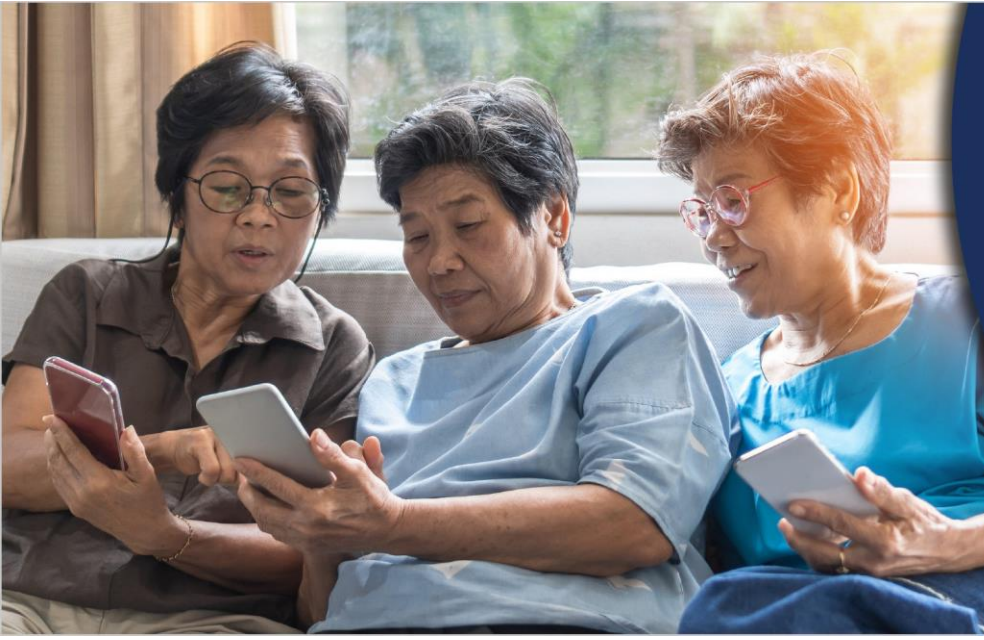

كن ذكياً كن ذكياً في مجال الأمن الإلكتروني المعلوماتي
#CyberMonth

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

الأمن الإلكتروني المعلوماتي أثناء السفر

في عالمنا اليوم الذي نكون فيه متصلين باستمرار بالإنترنت، لا يمكن أن يقتصر الأمن الإلكتروني المعلوماتي أو مايعرف بالأمن السيبراني، على المنزل أو المكتب. عندما تسافر - سواء كان سفرك محلياً أو دولياً - من المهم دائماً ممارسة السلوك الآمن عبر الإنترنت واتخاذ خطوات استباقية لتأمين حماية الأجهزة التي تدعم الإنترنت. كلما سافرنا أكثر، زاد تعرضنا لخطر الهجمات الإلكترونية.استخدم النصائح ضمن #BeCyberSmart للتواصل بثقة أثناء التنقل.

نصائح بسيطة:

قبل سفرك

- **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. أقرأ صفحة نصائح ضد الخداع ، لمزيد من المعلومات.
- **عمل نسخ احتياطية لمعلوماتك.** قم بعمل نسخة احتياطية من جهات الاتصال والبيانات المالية والصور ومقاطع الفيديو وبيانات الجهاز المحمول الأخرى إلى جهاز آخر أو خدمة (cloud) سحابية لاستخدامها في حال تعرض جهازك للخطر، وعليك إعادة تعيينه إلى إعدادات المصنع.
- **تواصل فقط مع الأشخاص الذين تثق بهم.** في حين أن بعض الشبكات الاجتماعية قد تبدو أكثر أمانًا للاتصال بسبب المعلومات الشخصية المحدودة التي يتم مشاركتها من خلالها، حافظ على اتصالاتك مع الأشخاص الذين تعرفهم وتثق بهم.
- **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.
- **ضاعف من عملية حمايتك.** استخدم خاصية التحقق بخطوتين (MFA) من خلال تفعيلها 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. أقرأ دليل خاصية التحقق بخطوتين MFA، لمزيد من العلومات.

أثناء رحلتك

- **اعمل على إيقاف الاتصال التلقائي.** تقوم بعض الأجهزة تلقائياً بالبحث عن الشبكات اللاسلكية المتاحة أو أجهزة Bluetooth والاتصال بها. يفتح هذا الاتصال الفوري الباب أمام مجرمي الإنترنت للوصول عن بُعد إلى أجهزتك. قم بتعطيل هذه الميزات لكي تتمكن من اختيار وقت الاتصال بشبكة آمنة.

- **حافظ على الحماية أثناء الاتصال**. قبل الاتصال بأي نقطة اتصال لاسلكية عامة - مثل المطار أو الفندق أو المقهى - تأكد من تأكيد اسم الشبكة وإجراءات تسجيل الدخول الدقيقة مع الموظفين المناسبين لضمان شرعية الشبكة. إذا كنت تستخدم نقطة وصول عامة غير آمنة ، فاحرص على ممارسة سليمة 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 أمانًا لشبكة Wi-Fi المجانية. استخدم فقط المواقع التي تبدأ بـ "https://"، عند التسوق عبر الإنترنت أو الخدمات المصرفية.
- **تصرف بحزم مع المتطفلين**. يستخدم مجرمو الإنترنت تكتيكات التصيد والتسلل، على أمل خداع ضحاياهم. إذا لم تكن متأكداً من هوية مرسل البريد الإلكتروني - حتى إذا كانت التفاصيل تبدو دقيقة - أو إذا كان البريد الإلكتروني يبدو "احتيالياً" ، فلا ترد ولا تنقر على أي روابط أو مرفقات موجودة في هذا البريد الإلكتروني. استخدم خيار "البريد غير الهام" أو "الحظر" متى ماكان متاحا، لعدم تلقي رسائل من نفس المرسل بعد الآن. أقرأ صفحة نصائح ضد الخداع ، لمزيد من المعلومات.
- **لا تقم 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. أقرأ صفحة نصائح الأمن السيبراني لوسائل التواصل الاجتماعي، لمزيد من المعلومات.
- **حماية الأجهزة المحمولة الخاصة بك**. لمنع السرقة والوصول غير المصرح به أو فقدان المعلومات الحساسة ، لا تترك أبداً أجهزتك - بما في ذلك أي USB أو أجهزة تخزين خارجية - دون رقابة في مكان عام. حافظ على أجهزتك مؤمنة في سيارات الأجرة والمطارات والطائرات وفي غرفتك بالفندق.

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/