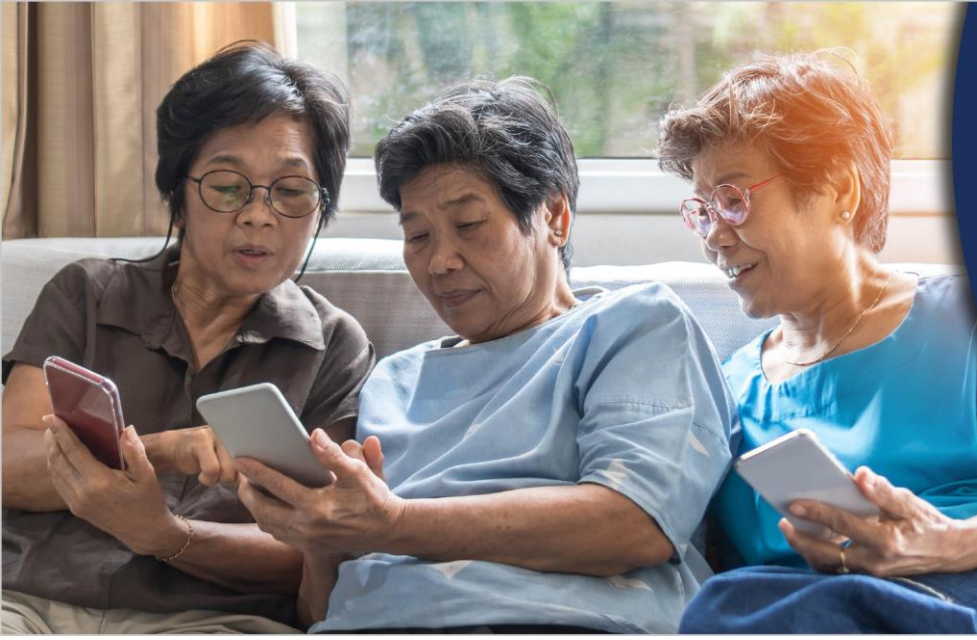

كن ذكياً كن ذكياً في مجال الأمن الإلكتروني المعلوماتي

#CyberMonth

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

خلق كلمة المرور

يعد إنشاء كلمة مرور قوية خطوة مهمة لحماية نفسك عبر الإنترنت. أن استخدام كلمة مرور طويلة ومعقدة، يعد من أسهل الطرق للدفاع عن نفسك من الجرائم الإلكترونية. لا أحد محصن ضد المخاطر الإلكترونية، ولكن من خلال حملة #BeCyberSmart، يمكنك تقليل هذه المخاطر.

نصائح بسيطة

- **استخدم كلمة مرور طويلة.** وفقاً لإرشادات المعهد الوطني للمعايير والتكنولوجيا (NIST) ، يجب أن تفكر في استخدام أطول كلمة أو عبارة مرور مسموح بها. على سبيل المثال ، يمكنك استخدام عبارة مرور مثل عناوين الأخبار أو حتى عنوان آخر كتاب قرأته. ثم أضف بعض علامات الترقيم والأحرف الكبيرة.
- **لاتجعل كلمات المرور سهلة التخمين.** لا تقم بتضمين معلومات شخصية في كلمة المرور مثل أسمك أو أسماء الحيوانات الأليفة. غالباً ما يكون من السهل العثور على هذه المعلومات على وسائل التواصل الاجتماعي، مما يسهل على مجرمي الإنترنت اختراق حساباتك.
- **تجنب استخدام الكلمات الشائعة.** استبدل الأحرف بأرقام وعلامات ترقيم أو رموز. على سبيل المثال ، يمكن أن تحل علامة @ محل الحرف "A" ويمكن أن تحل علامة التعجب (!) محل الأحرف "I" أو "L."
- **كن مبدع باختيارك لكلمة المرور.** استخدم البدائل الصوتية ، مثل "PH" بدلاً من "F". أو ارتكب أخطاء إملائية متعمدة ولكن واضحة ، مثل "enjin" بدلاً من "engine".
- **احتفظ بكلمات المرور الخاصة بك لنفسك.** لاتخبر أي شخص بكلمات المرور وراقب المتسللسن الذين يحاولون خداعك للكشف عن كلمات المرورالخاصة بك من خلال البريد الإلكتروني أو المكالمات. عندما تشارك كلمة المرور الخاصة بك مع شخص آخر أو تعيد استخدامها، فهذا من شأنه أن يقلل من حمايتك بالكامل من خلال فتح المجال لمختلف الطرق التي يمكن من خلالها إساءة استخدامها أو سرقتها.
- **أستخدم كلمة مرور واحدة مختلفة، لكل حساب.** يساعد عمل كلمات مرور مختلفة لحسابات مختلفة على منع مجرمي الإنترنت من الوصول إلى هذه الحسابات وحمايتك في حالة حدوث خرق. من المهم الخلط بين الأشياء - اعثر على طرق سهلة التذكر لتخصيص كلمة مرورك القياسية لمواقع مختلفة.
- **ضاعف من عملية حمايتك.** استخدم خاصية التحقق بخطوتين (MFA) للتأكد من أن الشخص الوحيد الذي لديه حق الوصول إلى حسابك هو أنت. استخدم الخاصية للبريد الإلكتروني، الخدمات المصرفية، وسائل التواصل الاجتماعي، وأي خدمة أخرى تتطلب تسجيل الدخول. قم بتمكين MFA ، 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، لمزيد من المعلومات.
- **استخدم برنامج إدارة كلمات المرور.** الطريقة الأكثر أمانًا لتخزين جميع كلمات المرور الفريدة الخاصة بك هي استخدام برنامج إدارة كلمات المرور. باستخدام كلمة مرور واحدة فقط ، يمكن للكمبيوتر إنشاء كلمات مرور وحفظها لكل حساب لديك - لحماية معلوماتك عبر الإنترنت ، بما في ذلك أرقام بطاقات الائتمان ورموزها المكونة من ثلاثة أرقام، وإجابات أسئلة الأمان ، والمزيد.

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/.