

مجموعة الأدوات الخاصة بشهر التوعية بالأمن الإلكتروني المعلوماتي 2021

الرسالة الرئيسية، المقالات، وسائل التواصل الاجتماعي والمزيد للترويج لشهر
التوعية بالأمن الإلكتروني المعلوماتي 2021



جدول المحتويات

3	مرحباً في شهر التوعية بالأمن الإلكتروني المعلوماتي 2021
3	طابع الحملة والرسالة الرئيسية لشهر أكتوبر 2021
3	الطابع لحملة 2021
3	الرسالة الرئيسية 2021
4	كيف تتمكن من المشاركة
4	أفكار للمشاركة
4	أهم النصائح للتشارك بها ونشرها في شهر التوعية بالأمن الإلكتروني المعلوماتي
5	مصادر الأمن الإلكتروني المعلوماتي
6	قنوات الاتصال
6	نموذج لتقويم الاتصالات
7	التواصل عبر وسائل التواصل الاجتماعي
11	نموذج لمدونة (BLOG)
12	نموذج لبريد إلكتروني للعملاء والموظفين
12	نموذج بريد إلكتروني للعملاء:
13	نموذج أيميل إلى الموظفين:

كن ذكياً كن ذكياً في مجال الأمن الإلكتروني المعلوماتي #CybersecurityAwarenessMonth



مرحباً في شهر التوعية بالأمن الإلكتروني المعلوماتي 2021

يتم عقد شهر التوعية بالأمن الإلكتروني المعلوماتي أو ما يسمى بالأمن السيبراني أحياناً، في شهر أكتوبر من كل عام، وهو جهد تعاوني بين الحكومة والصناعة لضمان حصول كل أمريكي على الموارد التي يحتاجها للبقاء آمناً أثناء استخدامه للإنترنت مع زيادة التهديدات في مجال الأمن الإلكتروني المعلوماتي.

تشارك وكالة الأمن الإلكتروني المعلوماتي وأمن البنية التحتية (CISA)، مع التحالف الوطني للأمن الإلكتروني المعلوماتي (NCSA)، في ترأس قيادة شهر التوعية بالأمن الإلكتروني المعلوماتي .

شكراً لك على المشاركة في شهر التوعية هذا. للمساعدة في جهودك ومشاركتك، يتضمن هذا المستند مجموعة هائلة من الموارد لك ولؤمؤستك، بغض النظر عن الحجم أو الصناعة، للمشاركة والترويج لطابع الحملة الأساسي ورسائل التوعية الهامة خلال شهر أكتوبر وكذلك الأيام الذي سبقته.

طابع الحملة والرسالة الرئيسية لشهر أكتوبر 2021

شهر التوعية بالأمن المعلوماتي له موضوع شامل نطلب منك استخدامه في مبادرات أكتوبر الخاصة بك. هذا العام، تحت عنوان "قم بدورك" #BeCyberSmart، ستركز الحملة على الدور الذي يلعبه كل فرد في الأمان عبر الإنترنت والتأكيد على أهمية اتخاذ خطوات استباقية لتعزيز الأمان السيبراني في المنزل وفي مكان العمل.

الطابع لحملة 2021

قم بدورك. #BeCyberSmart

الرسالة الرئيسية 2021

للمساعدة في تأطير المحادثات وتصميم الموارد وترويج إقامة الفعاليات مع أصحاب المصلحة الداخليين والخارجيين، نقوم بتقسيم الطابع الشامل إلى أربع رسائل أسبوعية. سيتم عرض الرسائل الرئيسية أدناه على مدار الشهر للمساعدة في ترويج وإقامة الفعاليات والموارد والأنشطة التي تنفذها وكالة الأمن الإلكتروني المعلوماتي وأمن البنية التحتية (CISA) والتحالف الوطني للأمن الإلكتروني المعلوماتي (NCSA)، وقد قمنا بتضمين موضوعات محتملة للمساعدة في بدء جهود شهر التوعية بالأمن الإلكتروني المعلوماتي.

- **الأسبوع 1: كن ذكياً في مجال أمن المعلومات الإلكتروني**
اتخذ إجراءات بسيطة للحفاظ على حياتنا الرقمية آمنة.
- **الأسبوع 2: حارب الخداع!**
تعرف على كيفية اكتشاف محاولات التصيد الاحتيالي والإبلاغ عنها لمنع هجمات برامج الفدية (الرانسموير) والبرامج الضارة الأخرى.
- **الأسبوع 3: استكشف. خبرة. مشاركة.**
احتفل بذكرى المبادرة الوطنية للتنظيف في مجال الأمن الإلكتروني (NICE) فيما يخص أسبوع التوعية المهنية في مجال الأمن الإلكتروني.
- **الأسبوع 4: الأمن الإلكتروني المعلوماتي أولاً**
اكتشف مدى أهمية الأمن السيبراني والبقاء آمناً عبر الإنترنت بشكل متزايد ونحن نواصل العمل تقريباً من خلال الإنترنت في كل من حياتنا العملية والشخصية.

كيف تتمكن من المشاركة

يقدم هذا القسم نصائح لنشر رسائل التوعية بالأمن الإلكتروني المعلوماتي، لضمان وصول حملة شهر التوعية بالأمن الإلكتروني المعلوماتي إلى العامة. الهدف من حملة 2021 هو تعزيز المساءلة الشخصية وتغيير السلوك الإيجابي عندما يتعلق الأمر بالأمن الإلكتروني المعلوماتي. لضمان النجاح في أكتوبر، ضع هذا الهدف في الاعتبار عند وضع خطط الفعاليات.

أفكار للمشاركة

- ساهم بصوتك ومواردك في محادثات وسائل التواصل الاجتماعي باستخدام #BeCyberSmart و #CybersecurityAwarenessMonth
- تضمين رسالة حول مدى أهمية الأمن الإلكتروني المعلوماتي في الرسائل الإخبارية والمراسلات ومواقع الإنترنت خلال شهر أكتوبر
- استضيف حدثاً أو اجتماعاً لمناقشة قضايا الأمن الإلكتروني المعلوماتي المحلية ذات الصلة
- تنظيم التدريب على ممارسة الأمن الإلكتروني المعلوماتي أو توفيره أو الترويج له لأصحاب المصلحة الداخليين والخارجيين
- المشاركة في تدريب أو تمرين محلي أو من خلال الإنترنت لتحسين الأمن الإلكتروني المعلوماتي والمرونة في مؤسستك
- استخدم النصائح المتوفرة على الرابط cisa.gov/cybersecurity-awareness-month لقراءة مواضيع مختلفة في هذا المجال
- سواء في مكان العمل أو في المنزل، هذه النصائح هي معلومات مفيدة للجميع
- انضم كصديق لحملة توقف. فكر. اتصل. حملة (STOP. THINK. CONNECT. ™) عن طريق زيارة الرابط cisa.gov/stophinkconnect
- يمكن لمتخصصي الأمن الإلكتروني المعلوماتي التعهد بمساعدة المجتمعات الضعيفة المعرضة للهجمات #SecureTogether ومساعدتهم على تحسين وضع الأمن الإلكتروني المعلوماتي لديهم من خلال الإجراءات الرئيسية على الرابط www.cybercrimesupport.org

أهم النصائح للتشارك بها ونشرها في شهر التوعية بالأمن الإلكتروني المعلوماتي

- **مضاعفة حماية تسجيل الدخول الخاص بك.** قم بتمكين خاصية التحقق متعددة العوامل (MFA) لجميع حساباتك والأجهزة للتأكد من أن الشخص الوحيد الذي لديه حق الوصول إلى حسابك هو أنت. استخدمه للبريد الإلكتروني، الخدمات المصرفية، ووسائل التواصل الاجتماعي، وأي خدمة أخرى تتطلب تسجيل الدخول. إذا كان MFA خياراً متوفراً ، فقم بتمكينه باستخدام جهاز محمول موثوق به ، مثل هاتفك الذكي ، أو البرنامج الذي يتحقق من مدى صحة الدخول، أو من خلال جهاز الحماية (token) - وهو جهاز صغير مادي يمكن ربطه بحلقة المفاتيح اقرأ دليل خاصية التحقق متعددة العوامل (MFA) للحصول على مزيد من المعلومات.
- **اعمل تغيير جذري على عملية اختيار كلمة المرور الخاصة بك.** وفقاً لإرشادات المعهد الوطني للمعايير والتكنولوجيا (NIST)، يجب أن تفكر في استخدام أطول كلمة مرور أو عبارة مرور مسموح بها. كن مبدعاً وخصص كلمة مرورك القياسية لمواقع مختلفة ، والتي يمكن أن تمنع مجرمي الإنترنت من الوصول إلى هذه الحسابات وحمايتك في حالة حدوث خرق. استخدم نظام إدارة كلمات المرور لإنشاء كلمات مرور مختلفة معقدة ويمكنك تذكرها لكل حساب من حساباتك. اقرأ النصائح حول إنشاء كلمة مرور لمزيد من المعلومات.

- **إذا قمت بالاتصال ، يجب عليك توفير الحماية لنفسك.** 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 ضد الفيروسات ومتصفح الويب وأنظمة التشغيل. قم بالتسجيل للحصول على التحديثات التلقائية، إذا استطعت، وقم بحماية أجهزتك باستخدام برامج مكافحة الفيروسات. اقرأ [الصفحة الخاصة بالنصائح ضد الخداع](#) لمزيد من المعلومات.
- **تصرف بحزم مع الغرباء.** يستخدم مجرم الإنترنت تكتيكات التصيد، على أمل خداع ضحاياهم. إذا كنت غير متأكد من هوية مرسل البريد الإلكتروني - حتى إذا كانت التفاصيل تبدو دقيقة - أو إذا كانت الرسالة الإلكترونية تبدو "احتمالية" ، فلا ترد ولا تضغط على أي روابط أو مرفقات موجودة في هذا البريد الإلكتروني. عندما يكون متاحاً ، استخدم خيار "الإبلاغ عن التصيد الاحتمالي" أو "الإبلاغ" لمساعدة مؤسستك أو مزود البريد الإلكتروني على حظر رسائل البريد الإلكتروني المشبوهة الأخرى قبل وصولها إلى صندوق الوارد الخاص بك.
- **لا تَقم بالضغط على أي رابط، وأعطاء معلوماتك الخاصة.** حدد المعلومات التي تنتشرها 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 يحتاج جميع المجرمين إلى معرفتها لاستهدافك واستهداف أحيائك 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 الإجازات والرحلات. قم بتعطيل خدمات الموقع التي تسمح لأي شخص برؤية مكانك - ومكان تواجدك - في أي وقت. اقرأ [الصفحة الخاصة بنصائح الأمن الإلكتروني لوسائل التواصل الاجتماعي](#) لمزيد من المعلومات.
- **حافظ على سلامة تطبيقاتك.** يتم دعم معظم الأجهزة والألعاب والأجهزة المتصلة بواسطة تطبيق الهاتف المحمول. يمكن أن يمتلئ جهازك المحمول بتطبيقات مشبوهة تعمل في الخلفية أو تستخدم أذونات افتراضية لم تدرک أبداً أنك موافق عليها - جمع معلوماتك الشخصية دون علمك مع تعريض هويتك وخصوصيتك للخطر. تحقق من أذونات التطبيق واستخدم "قاعدة الامتياز الأقل" لحذف ما لا تحتاجه أو لم تعد تستخدمه. تعلم أن تقول "لا" لطلبات الامتياز التي لا معنى لها. قم بتنزيل التطبيقات فقط من البائعين والمصادر الموثوق بهم.
- **حافظ على امن وسلامة الاستخدام أثناء الاتصال.** قبل الاتصال بأي نقطة اتصال لاسلكية عامة - مثل المطار أو الفندق أو المقهى - تأكد من اسم الشبكة وإجراءات تسجيل الدخول الدقيقة مع الموظفين المناسبين لضمان شرعية الشبكة. إذا كنت تستخدم نقطة وصول عامة غير آمنة ، فاحرص على ممارسة السلامة الشخصية للإنترنت عن طريق تجنب الأنشطة الحساسة (مثل الخدمات المصرفية) التي تتطلب كلمات مرور أو بطاقات ائتمان. غالباً ما تكون نقطة الاتصال الشخصية الخاصة بك بديلاً أكثر أماناً لشبكة Wi-Fi المجانية. استخدم فقط المواقع التي تبدأ ب "https:///" عند التسوق عبر الإنترنت أو الخدمات المصرفية.

مصادر الأمن الإلكتروني المعلوماتي

- فيما يلي عدد من المصادر المفيدة لتعزيز ونشر الوعي بالأمن الإلكتروني المعلوماتي خلال شهر أكتوبر وطوال العام. استكشف هذه المواقع ومحتوياتها لاستخدامها في مدوناتك، المقالات والرسائل داخل مؤسستك وخارجها.
- يقوم التحالف الوطني للأمن الإلكتروني المعلوماتي (NCSA) ببناء شراكات قوية بين القطاعين العام والخاص لإنشاء وتنفيذ جهود تعليمية وتوعوية واسعة النطاق لتمكين المستخدمين في المنزل، مكان العمل والمدرسة من المعلومات التي يحتاجون إليها للحفاظ على أنفسهم، مؤسساتهم، أنظمتهم ومعلوماتهم الحساسة لتكون آمنة ومأمونة عبر الإنترنت وتشجع ثقافة الأمن الإلكتروني المعلوماتي . لمعرفة فعاليات NCSA، أضغط على الرابط <https://staysafeonline.org>
- تم تصميم **حملة كن ذكياً في مجال أمن المعلومات الإلكتروني، "Be Cyber Smart"** وهي جهد وطني من قبل وزارة الأمن الداخلي الأمريكية ، لإلهام الجيل الأصغر من الأمريكيين لتحمل مسؤولية سلامتهم أثناء استخدام الإنترنت. تعرف على أساسيات الأمن المعلوماتي عبر الإنترنت وعمليات الاحتيال الشائعة وكيفية الإبلاغ عن حوادث الأمن الإلكتروني المعلوماتي من خلال زيارة الحملة عبر الإنترنت.
- هل تبحث عن معلومات حول منصب أو دورة تدريبية معينة في مجال الأمن الإلكتروني المعلوماتي؟ **تعد المبادرة الوطنية لشغل وظائف ودراسات الأمن السيبراني (NICCS)** مورداً وطنياً لتعليم الأمن الإلكتروني المعلوماتي والتدريب وتطوير القوى العاملة. يتميز NICCS بأدوات ومعلومات لمتخصصي الأمن الإلكتروني المعلوماتي الحاليين والمستقبليين ، بدءاً من الطلاب والمدرسين من مرحلة رياض الأطفال حتى نهاية التعليم الثانوي إلى الموظفين الفيدراليين إلى قدامى المحاربين ووصولاً إلى المهنيين. تتوفر هذه الأدوات والموارد لأي شخص يسعى للحصول على مزيد من المعلومات حول مجال الأمن السيبراني ، وكيفية النهوض به ، والمزيد.

قنوات الاتصال

روابط الهاشتاك الرسمية لشهر التوعية بالأمن الإلكتروني المعلوماتي 2021 هي #BeCyberSmart و #CybersecurityAwarenessMonth. لتسليط الضوء عليك ولمشاركة مؤسستك من خلال الاستفادة من علامات التصنيف هذه قبل وأثناء شهر أكتوبر للترويج والمشاركة في أنشطة الحملة.

نموذج لتقويم الاتصالات

استخدم تقويم الاتصالات التالي للمساعدة في تخطيط جهود التوعية والتنفيذ الرائدة خلال شهر التوعية. تم إعداد هذا كدليل فقط وليس المقصود منه تقييد أنشطتك أو الحد منها.

أغسطس

- ابدأ شهر التوعية بالأمن السيبراني بالتخطيط بين التسويق والقيادة في أنشطة أكتوبر والمشاركة، بما في ذلك اتصالات الشركة المحتملة والأخبار والأبحاث التي يمكن إصدارها خلال الشهر
- 19 أغسطس: **طلب مواد توعية بالأمن الإلكتروني المعلوماتي** من لجنة التجارة الفيدرالية (FTC) لتيتم توزيعها خلال شهر أكتوبر
- 27 أغسطس: هذا التاريخ هو آخر يوم لدعوة ممثل CISA أو الوكالات الفيدرالية المحلية للتحديث لموظفيك حول الأمان عبر الإنترنت. اطلب متحدثي CISA من خلال زيارة الرابط <http://www.cisa.gov/contact-us> ، قسم "طلب متحدث CISA"

سبتمبر

- 1 سبتمبر: إنشاء جدول زمني للاتصالات الرقمية للمنشورات الاجتماعية للشركات والتنفيذيين والمدونات ورسائل البريد الإلكتروني والعروض الترويجية الأخرى لشهر التوعية بالأمن السيبراني على مدار الشهر
- 20 سبتمبر: بدء العد التنازلي لمدة أسبوعين لشهر التوعية بالأمن السيبراني على قنوات التواصل الاجتماعي
- 21 سبتمبر: أرسل بريد إلكتروني إلى الموظفين للإعلان عن مشاركتك في الحملة وتحديد كيفية مشاركة شركتك خلال شهر التوعية بالأمن السيبراني
- 30 سبتمبر: عرض رسومات وإعلانات شهر التوعية بالأمن السيبراني في عملك في المناطق التي تستقبل عدد كبير من الزيارات أو على مواقع الويب الخاصة بمؤسستك
- 30 سبتمبر: عقد مأدبة غداء للموظفين لمناقشة الأمن السيبراني لشركتك وسياسات الاستخدام المقبول ومشاركة العرض التقديمي لشهر التوعية بالأمن السيبراني مع الموظفين

أكتوبر

- 1 أكتوبر: اعمل مع رؤسائك لإصدار إعلان رسمي للشركة لدعم #CyberMonth والتزامهم بحملة قم بدورك. #BeCyberSmart
- 1 أكتوبر: أرسل خطاباً للعميل يسلط الضوء على مشاركة نشاطك التجاري في شهر التوعية بالأمن السيبراني وقدم نصائح مفيدة حول الأمن الإلكتروني المعلوماتي لهم إلى #BeCyberSmart
- 1 أكتوبر: أرسل / جدولة السلسلة الأولى من النصائح اليومية أو الأسبوعية إلى وسائل التواصل الاجتماعي / الموظفين حول كيفية البقاء آمناً على الإنترنت
- 4 أكتوبر: إصدار بيان إخباري للشركة متعلق بالشهر (تحديثات المنتج أو العرض ، فوز العميل ، إلخ.)
- 11 أكتوبر: أرسل / جدولة السلسلة الثانية من النصائح اليومية أو الأسبوعية إلى وسائل التواصل الاجتماعي / الموظفين حول كيفية البقاء آمناً على الإنترنت
- 18 أكتوبر: إرسال / جدولة السلسلة الثالثة من النصائح اليومية أو الأسبوعية إلى وسائل التواصل الاجتماعي / الموظفين حول كيفية البقاء آمناً على الإنترنت وكيفية الانضمام إلى القوى العاملة على الإنترنت
- 19 أكتوبر: إجراء محاكاة وهمية للتصيد الاحتيالي مع الموظفين باستخدام خدمات السلامة في الفضاء الإلكتروني [Cyber Hygiene](#) [Services التابعة لوكالة CISA](#)

- **25 أكتوبر:** أرسل / جدولة السلسلة الرابعة من النصائح اليومية أو الأسبوعية إلى وسائل التواصل الاجتماعي / الموظفين حول كيفية البقاء آمناً على الإنترنت
- **26 أكتوبر:** استضيف حدث بصفقتك شريك لشهر التوعية بالأمن السيبراني للموظفين و / أو مجتمعك المحلي
- **28 أكتوبر:** أرسل توزيعاً نهائياً لمواد الأمان عبر الإنترنت لإبراز مدى أهمية التعامل بذكاء على الإنترنت طوال العام
- **29 أكتوبر:** أرسل إلى الموظفين رسالة إلكترونية تلخص المعلومات التي تعلموها على مدار الشهر - ضع في اعتبارك تقديم جوائز صغيرة لأولئك الذين قدموا أداءً جيداً أثناء الأنشطة أو شاركوا فعلياً.

التواصل عبر وسائل التواصل الاجتماعي

فيما يلي نماذج من مشاركات وسائل التواصل الاجتماعي للترويج لشهر التوعية بالأمن السيبراني في مؤسستك. تشجعك CISA و NCSA بشدة على النشر على قنوات الاتصال الخاصة بك عبر الإنترنت حتى شهر أكتوبر وطوال هذه الفترة.

:TWITTER

أسبوع الأفتتاح

#CyberMonth يعود الشهر في أكتوبر للعام الثامن عشر لتتقيف الأمة حول الأمن الإلكتروني المعلوماتي وكيف يمكن لجميع الأمريكيين أن يكونوا أكثر أماناً عبر الإنترنت. تعرف على كيفية القيام بدورك #BeCyberSmart من خلال زيارة cisa.gov/cybersecurity-awareness-month

الأسبوع 1 - كن ذكياً في مجال الأمن الإلكتروني المعلوماتي:

قم بدورك #BeCyberSmart! في الأسبوع الأول من شهر التوعية بالأمن السيبراني ، سنستكشف أساسيات الأمن السيبراني ، ونعلمك كيف تتمكن من تأمين حياتك الرقمية بشكل أفضل وتحسين أمان أجهزتك. #CyberMonth #cybersecurity #InformationSecurity

الأسبوع 2 - حارب الخداع !:

حارب الخداع! سيركز شهر التوعية بالأمن السيبراني في هذا الأسبوع، على كيفية اكتشاف الأفراد لنقاط الضعف التي تمكنهم من محاولات التصيد. غالباً ماينجح التصيد الاحتيالي بسبب وجود ثغرات والتي يمكن أن تؤدي إلى برامج الفدية أو أنواع أخرى من البرامج الضارة. #FightThePhish #Phishing #Ransomware #BeCyberSmart #CyberMonth

الأسبوع 3 - استكشف. خبرة. مشاركة:

انضم إلى CISA والمبادرة الوطنية لتعليم الأمن السيبراني (NICE) هذا الأسبوع للاحتفال بأسبوع التوعية المهنية في الأمن السيبراني. سنعرض هذا الأسبوع مساهماتهم وابتكاراتهم. بناء قوة عاملة للأمن السيبراني لتعزيز الأمن. #CyberMonth #CyberCareer

الأسبوع 4 - الأمن الإلكتروني المعلوماتي أولاً:

إنه الأسبوع الأخير من شهر التوعية بالأمن السيبراني ، يجب أن تستمر في أداء دورك و تذكر بأن إجراءات #BeCyberSmart! اليوم، سيكون لها تأثير على مستقبلنا. يُعد الأمن السيبراني جهداً على مدار العام وقد أصبح أكثر اعتباراً لكيفية عملنا وتعلمنا وحياتنا. #CyberMonth #cybersecurity

:FACEBOOK

أسبوع الأفتتاح:

يعود شهر التوعية في أكتوبر للعام الثامن عشر 2021، لتتقيف الأمة حول الأمن الإلكتروني المعلوماتي. الموقع الخاص الموقع الخاص بشهر التوعية في الأمن الإلكتروني المعلوماتي (cisa.gov/cybersecurity-awareness-month) يسلط الضوء على الحاجة لتتقيف الأفراد والمؤسسات حول أهمية سلامة استخدام الإنترنت والتأكيد على أن كافة الأمريكيين لديهم الموارد اللازمة ليكونوا أكثر أماناً عند استخدام الإنترنت.

- الأسبوع 1: كن ذكياً في مجال أمن المعلومات الإلكتروني
- الأسبوع 2: حارب الخداع!
- الأسبوع 3: استكشف. خبرة. المشاركة. أسبوع التوعية المهنية في الأمن الإلكتروني المعلوماتي
- الأسبوع 4: الأمن الإلكتروني المعلوماتي أولاً

#BeCyberSmart #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

الأسبوع 1- كن ذكياً في مجال أمن المعلومات الإلكتروني:

قم بدورك! #BeCyberSmart في الأسبوع الأول من شهر التوعية بالأمن السيبراني ، سنستكشف أساسيات الأمن السيبراني ، ونعلمك كيف يمكنك تأمين حياتك الرقمية بشكل أفضل وتحسين أمان أجهزتك. يمكن أن تساعد الإجراءات البسيطة في تأمين حياتك الرقمية وتحسين أمان الأجهزة المتصلة بالإنترنت
#CyberMonth #Cybersecurity #InformationSecurity

تتضمن فعاليات هذا الأسبوع _____، _____ . لمزيد من المعلومات قم بزيارة رابط الموقع الخاص بشهر التوعية في الأمن الإلكتروني المعلوماتي،
cisa.gov/cybersecurity-awareness-month

#CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity
#InfoSecurity #NetworkSecurity #NetSec

الأسبوع 2 - حارب الخداع! :

حارب الخداع! سيركز شهر التوعية بالأمن السيبراني هذا الأسبوع على كيفية اكتشاف الأفراد لنقاط الضعف التي تمكنهم من محاولات التصيد. غالبًا ماينجح التصيد الاحتيالي بسبب وجود ثغرات والتي يمكن أن تؤدي إلى برامج الفدية أو أنواع أخرى من البرامج الضارة. قلل من فرص الوقوع ضحية لهجمات التصيد الاحتيالي أثناء استخدام الإنترنت.

تتضمن فعاليات هذا الأسبوع _____، _____ . لمزيد من المعلومات قم بزيارة رابط الموقع الخاص بشهر التوعية في الأمن الإلكتروني المعلوماتي،
cisa.gov/cybersecurity-awareness-month

#Phishing #Ransomware #Malware #respond #recover

الأسبوع 3 - استكشف. خبرة. المشاركة:

انضم إلى CISA والمبادرة الوطنية لتعليم الأمن السيبراني (NICE) هذا الأسبوع للاحتفال بأسبوع التوعية المهنية في الأمن السيبراني. سنعرض هذا الأسبوع مساهماتهم وابتكاراتهم. يلعب محترفو الأمن السيبراني دورًا حيويًا في المجتمع والأمن على الصعيد العالمي. سنعرض هذا الأسبوع مساهماتهم وابتكاراتهم. يعزز بناء قوة عاملة عالمية في مجال الأمن السيبراني أمن كل دولة ، ويمكننا شرح كيفية ذلك.

#ExploreExperienceShare #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

الأسبوع 4 - الأمن الإلكتروني المعلوماتي أولاً:

إنه الأسبوع الأخير من شهر التوعية بالأمن السيبراني ، يجب أن تستمر في أداء دورك و تذكر بأن إجراءات #BeCyberSmart اليوم، سيكون لها تأثير على مستقبلنا. يُعد الأمن السيبراني جهدًا على مدار العام وقد أصبح أكثر اعتبارًا لكيفية عملنا وتعلمنا وحياتنا. يُعد الأمن السيبراني جهدًا على مدار العام ويجب أن يكون أحد اعتباراتنا الأولى عند إنشاء أو شراء أجهزة جديدة وخدمات متصلة.

انضم إلى المحادثة حول شهر التوعية بالأمن السيبراني باستخدام #BeCyberSmart.

#BeCyberSmart #CybersecurityFirst #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity
#StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

:INSTAGRAM

أسبوع الافتتاح:

يعود شهر التوعية بالأمن السيبراني في أكتوبر لعامه الثامن عشر للمساعدة في تثقيف الأمة حول الأمن السيبراني وكيف يمكن لجميع الأمريكيين أن يكونوا أكثر أمانًا عند استخدامهم الإنترنت. تعرف على كيفية القيام بدورك #BeCyberSmart من خلال زيارتك للرابط cisa.gov/cybersecurity-awareness-month

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

الأسبوع 1 - كن ذكياً في مجال أمن المعلومات الإلكتروني:

قم بدورك! #BeCyberSmart في الأسبوع الأول من شهر التوعية بالأمن السيبراني ، سنستكشف أساسيات الأمن السيبراني ، ونعلمك كيف يمكنك تأمين حياتك الرقمية بشكل أفضل وتحسين أمان أجهزتك. #CyberMonth #cybersecurity #InformationSecurity

انضم إلى المناقشة حول شهر التوعية بالأمن السيبراني. يمكنك المساهمة باستخدام هاشتاك #BeCyberSmart

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

الأسبوع 2 - حارب الخداع !:

حارب الخداع! سيركز شهر التوعية بالأمن السيبراني هذا الأسبوع على كيفية اكتشاف الأفراد لنقاط الضعف التي تمكنهم من محاولات التصيد. غالباً ماينجح التصيد الاحتيالي بسبب وجود ثغرات والتي يمكن أن تؤدي إلى برامج الفدية أو أنواع أخرى من البرامج الضارة. قلل من فرص الوقوع ضحية لهجمات التصيد الاحتيالي أثناء استخدام الإنترنت.

انضم إلى المناقشة حول شهر التوعية بالأمن السيبراني. يمكنك المساهمة باستخدام هاشتاك #BeCyberSmart

#FightThePhish #Phishing #Ransomware #CyberMonth #Cybersecurity #BeCyberSmart #InfoSec
#InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

الأسبوع 3 - أستكشف. خبرة. المشاركة:

انضم إلى CISA والمبادرة الوطنية لتعليم الأمن السيبراني (NICE) هذا الأسبوع للاحتفال بأسبوع التوعية المهنية في الأمن السيبراني. سنعرض هذا الأسبوع مساهماتهم وابتكاراتهم. بناء قوة عاملة للأمن السيبراني سيعزز الأمن.

#CyberCareers #CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity
#StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

الأسبوع 4 - الأمن الإلكتروني المعلوماتي أولاً:

إنه الأسبوع الأخير من شهر التوعية بالأمن السيبراني ، يجب أن تستمر في أداء دورك و تذكر بأن إجراءات #BeCyberSmart اليوم، سيكون لها تأثير على مستقبلنا. يُعد الأمن السيبراني جهدًا على مدار العام وقد أصبح أكثر اعتبارًا لكيفية عملنا وتعلمنا وحياتنا. يُعد الأمن السيبراني جهدًا على مدار العام ويجب أن يكون أحد اعتباراتنا الأولى عند إنشاء أو شراء أجهزة جديدة وخدمات متصلة.

-
-
-

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

LINKEDIN

أسبوع الافتتاح:

الآن، في شهر أكتوبر، هذا هو العام الثامن عشر لشهر التوعية بالأمن السيبراني. كل عام تعمل الحملة للمساعدة في تثقيف الأمة حول الأمن السيبراني وكيف يمكن لجميع الأميركيين أن يكونوا أكثر أماناً عند استخدامهم الإنترنت.

يمكن للأفراد والشركات المشاركة في شهر التوعية بالأمن السيبراني باستخدام موارد CISA لإنشاء حملات التوعية الخاصة بك! يمكن للشركاء إنشاء حملات التوعية الخاصة بهم باستخدام الموضوعات الأسبوعية لهذا العام:

- الأسبوع 1: كن ذكياً في مجال أمن المعلومات الإلكتروني
- الأسبوع 2: حارب الخداع!
- الأسبوع 3: الاستكشاف. خبرة. المشاركة. أسبوع التوعية المهنية في الأمن الإلكتروني المعلوماتي
- الأسبوع 4: الأمن الإلكتروني المعلوماتي أولاً

لمزيد من المعلومات عن حملة التوعية، قم بزيارة الرابط cisa.gov/cybersecurity-awareness-month!

الأسبوع 1 - كن ذكياً في مجال أمن المعلومات الإلكتروني

قم بدورك! #BeCyberSmart في الأسبوع الأول من شهر التوعية بالأمن السيبراني ، سنستكشف أساسيات الأمن السيبراني ، وتثقيف المؤسسات في كيفية القيام بدورهم وكيفية التعامل مع الإنترنت بشكل ذكي وسليم #BeCyberSmart ونعلمك كيف يمكنك تأمين حياتك الرقمية بشكل أفضل وتحسين أمان أجهزتك بإتخاذ خطوات بسيطة .

تتضمن فعاليات هذا الأسبوع _____، _____ . لمزيد من المعلومات قم بزيارة رابط الموقع الخاص بشهر التوعية في الأمن الإلكتروني المعلوماتي، cisa.gov/cybersecurity-awareness-month

#CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

الأسبوع 2 - حارب الخداع !:

حارب الخداع! سيركز شهر التوعية بالأمن السيبراني هذا الأسبوع على كيفية اكتشاف الأفراد لنقاط الضعف التي تمكنهم من محاولات التصيد. غالبًا ماينجح التصيد الاحتيالي بسبب وجود ثغرات والتي يمكن أن تؤدي إلى برامج الفدية أو أنواع أخرى من البرامج الضارة. قلل من فرص الوقوع ضحية لهجمات التصيد الاحتيالي أثناء استخدام الإنترنت.

تتضمن فعاليات هذا الأسبوع _____، _____ . لمزيد من المعلومات قم بزيارة رابط الموقع الخاص بشهر التوعية في الأمن الإلكتروني المعلوماتي، cisa.gov/cybersecurity-awareness-month

الأسبوع 3 - استكشاف. خبرة. المشاركة:

انضم إلى CISA والمبادرة الوطنية لتعليم الأمن السيبراني (NICE) هذا الأسبوع للاحتفال بأسبوع التوعية المهنية في الأمن السيبراني. يلعب محترفو الأمن

السيبراني دورًا حيويًا في المجتمع والأمن على الصعيد العالمي. سنعرض هذا الأسبوع مساهماتهم وابتكاراتهم. بناء قوة عاملة عالمية للأمن السيبراني يعزز أمن كل دولة ، انضم إلينا لمعرفة السبب.

الأسبوع 4 - لأمن الإلكتروني المعلوماتي أولاً:

إنه الأسبوع الأخير من شهر التوعية بالأمن السيبراني ، يجب أن تستمر في أداء دورك و تذكر بأن إجراءات #BeCyberSmart! اليوم، سيكون لها تأثير على مستقبلنا. يُعد الأمن السيبراني جهدًا على مدار العام وقد أصبح أكثر اعتبارًا لكيفية عملنا وتعلمنا وحياتنا. يُعد الأمن السيبراني جهدًا على مدار العام ويجب أن يكون أحد اعتباراتنا الأولى عند إنشاء أو شراء أجهزة جديدة وخدمات متصلة.

تتضمن فعاليات هذا الأسبوع _____ ، _____ . لمزيد من المعلومات قم بزيارة رابط الموقع الخاص بشهر التوعية في الأمن الإلكتروني المعلوماتي، cisa.gov/cybersecurity-awareness-month

نموذج لمدونة (BLOG)



حملة شهر التوعية بالأمن الإلكتروني المعلوماتي 2021

يستمر شهر التوعية بالأمن الإلكتروني المعلوماتي، والذي هو حالياً في عامه الثامن عشر، في رفع مستوى الوعي حول أهمية الأمن الإلكتروني المعلوماتي في جميع أنحاء أمتنا. يُعد شهر التوعية بالأمن الإلكتروني المعلوماتي، والذي يُعقد في شهر أكتوبر من كل عام، جهداً تعاونياً بين الحكومة والصناعة لضمان حصول جميع الأمريكيين على الموارد التي يحتاجون إليها ليكونوا أكثر أماناً عند استخدامهم شبكة الإنترنت.

#BECYBERSMART. قم بدورك.

خلال كل عام، بقيادة وكالة الأمن الإلكتروني المعلوماتي وأمن البنية التحتية (CISA) والتحالف الوطني للأمن الإلكتروني المعلوماتي (NCSA)، يقدم شهر التوعية بالأمن الإلكتروني المعلوماتي، رسالة واضحة للشراكة بين الحكومة والصناعة، من البيت الأبيض إلى الفرد.

من خلال سمة الحملة الدائم التجديد - قم بدورك. #BeCyberSmart - الحث على تشجيع الأفراد والمنظمات على امتلاك دورهم في حماية الجزء الخاص بهم من الفضاء الإلكتروني ، والتأكيد على المساءلة الشخصية وأهمية اتخاذ خطوات استباقية لتعزيز الأمن السيبراني.

الرسائل الأسبوعية

لمساعدتك أنت ومؤسساتك في إنشاء حملة توعية فعالة بالأمن السيبراني ، ابتكر CISA و NCSA أربعة موضوعات أسبوعية للتركيز عليها خلال شهر التوعية بالأمن السيبراني:

- **الأسبوع 1: كن ذكياً في مجال أمن المعلومات الإلكتروني**
يستكشف الأسبوع الأول أساسيات الأمن السيبراني: كيف يمكن للإجراءات البسيطة أن تساعد في تأمين حياتك الرقمية ، وتحسين أمان الأجهزة الذكية والمتصلة بالإنترنت ، وكيف يمكن أن تساعد الأساسيات الأخرى في تقليل المخاطر السيبرانية.
- **الأسبوع 2: حارب الخداع!**
سيركز الأسبوع الثاني على كيفية اكتشاف الأفراد لمحاولات التصيد الاحتمالي المحتملة - والتي تؤدي غالباً إلى نقاط ضعف يمكن أن تؤدي إلى برامج الفدية أو أنواع أخرى من البرامج الضارة. سيقدم نصائح حول كيفية تقليل الأفراد من فرص الوقوع ضحية لهجمات التصيد - إما عن طريق الإبلاغ عن الأنشطة المشبوهة أو حذفها - بالإضافة إلى كيفية الرد عليها والتعافي منها.
- **الأسبوع 3: استكشف. خبرة. المشاركة.**
بالشراكة مع المبادرة الوطنية للتنظيف في مجال الأمن الإلكتروني المعلوماتي (NICE) ، يحتفل الأسبوع الثالث بأسبوع التوعية المهنية في الأمن السيبراني. سيوضح هذا الأسبوع كيف يلعب محترفو الأمن السيبراني دوراً حيوياً في المجتمع والأمن على الصعيد العالمي ويلفت الانتباه إلى مساهماتهم وابتكاراتهم. يعرض هذا الأسبوع أيضاً كيف أن بناء قوة عاملة عالمية للأمن السيبراني يعزز أمن كل دولة ويعزز الازدهار الاقتصادي.
- **الأسبوع 4: الامن الإلكتروني المعلوماتي أولاً.**
سيؤكد الأسبوع الأخير على أن الأمن السيبراني يجب أن يكون أولوية وليس فكرة عابرة ، وسوف يتم التركيز على كيف من الممكن أن يؤثر ما نقوم به اليوم على مستقبل الأمن السيبراني الشخصي والمستهلك والأعمال. سوف يسلط هذا الأسبوع أيضاً الضوء على كيف أن الأمن السيبراني يمثل جهداً على مدار السنة ، وينبغي أن يكون الاعتبار الأول للفرد أو المؤسسة عند إنشاء أو شراء أجهزة جديدة وخدمات متصلة.
في هذا الشهر على وجه الخصوص ، نطلب منك عدم التعامل مع الأمن السيبراني باعتباره موضوعاً محظوراً: تحدث مع الآخرين حول كيفية "أن تكون ذكياً عبر الإنترنت" وتأكد من مشاركة موارد شهر التوعية بالأمن السيبراني مع مجتمعك - مع أصدقائك وعائلتك وزملائك في العمل . من خلال القيام بذلك ، يمكننا جميعاً أن نخطو خطوات كبيرة في حماية أجهزتنا.
استخدم هاشتاك لشهر التوعية بالأمن السيبراني **#BeCyberSmart** للمساعدة في تعزيز الوعي بالأمن السيبراني. تأكد أيضاً من الاستمرار في التحقق من موقع الويب لمعرفة المزيد حول جهود شهر التوعية بالأمن السيبراني القادمة في أكتوبر.

نموذج لبريد إلكتروني للعملاء والموظفين

يوجد أدناه نموذج بريد إلكتروني قد تستخدمه أنت ومنظمتك للإعلان عن شهر التوعية بالأمن السيبراني والترويج له لكل من قاعدة عملائك وداخل مؤسستك. يشجعك CISA و NCSA بشدة على التواصل مع أصحاب المصلحة الخاصين بك ومؤسستك حتى شهر أكتوبر وطوال هذا الشهر.

نموذج بريد إلكتروني للعملاء:

السادة <اسم العملاء أو أصحاب المصلحة>

[ادخل اسم المؤسسة] تتضم مع حملة شهر التوعية للأمن الإلكتروني المعلوماتي.

في شهر أكتوبر من كل عام ، يستمر **شهر التوعية بالأمن السيبراني** في رفع مستوى الوعي حول أهمية الأمن السيبراني عبر أمتنا. بقيادة **وكالة الأمن السيبراني وأمن البنية التحتية (CISA)** و**التحالف الوطني للأمن السيبراني (NCSA)** ، يشارك شهر التوعية بالأمن السيبراني الرسائل والموضوعات الأسبوعية حول أهمية البقاء آمناً على الإنترنت. موضوع دائم التجدد - **قم بدورك #BeCyberSmart** - يشجع الأفراد والمنظمات على امتلاك دورهم في حماية الجزء الخاص بهم من الفضاء الإلكتروني ، والتأكيد على المساءلة الشخصية وأهمية اتخاذ خطوات استباقية لتعزيز الأمن السيبراني.

على مدار العام ونصف العام الماضي ، اعتمد عالمنا الافتراضي بالفعل بشكل أكبر على الإنترنت. منظمات مثل **[ادخل اسم المؤسسة]** وأفراد مثلك نقلوا أعمالهم إلى الإنترنت أكثر من أي وقت مضى - للتواصل الاجتماعي ، لممارسة الأعمال التجارية والاستمتاع باستخدام الإنترنت.

في حين أن التواجد المتزايد عبر الإنترنت يمكن أن يكون إيجابياً ، فإن شهر التوعية بالأمن السيبراني يشجع الجميع وبشكل متزايد على الممارسات الأمنية المهمة التي تصاحب استخدام الإنترنت. تعتمد السلامة الافتراضية لمجتمعنا ، وفي النهاية ، أمتنا ، على ممارسات الأمان الشخصية على الإنترنت.

الأمن السيبراني مهم لـ [ادخل أسم المؤسسة] ونحن ملتزمون بمساعدة عملائنا ليصبحوا أكثر مرونة. خلال شهر أكتوبر سنتعلم كيفية:

• كن ذكياً في مجال الأمن الإلكتروني

أخذ خطوات بسيطة للمحافظة على حياتنا الرقمية.

• حارب الخداع!

سلط الضوء على مخاطر محاولات التصيد الاحتيالي - التي يمكن أن تؤدي إلى هجمات برامج الفدية أو البرامج الضارة الأخرى - وكيفية الإبلاغ عن رسائل البريد الإلكتروني المشبوهة.

• استكشاف. خبرة. مشاركة.

احتفل بأسبوع التوعية المهنية للأمن السيبراني للمبادرة الوطنية لتعليم الأمن السيبراني والقوى العاملة العالمية في مجال الأمن السيبراني وسلط الضوء على كيف يمكن للأفراد أن يصبحوا متخصصين في الأمن السيبراني.

• الأمن الإلكتروني المعلوماتي أولاً

اكتشف كيف يتزايد أهمية الأمن السيبراني والبقاء آمناً عبر الإنترنت مع استمرار عالمنا للعمل بشكل افتراضي من أجل الكثير من العمل ومجرد التصفح واللهو.

يجب علينا جميعاً التعامل مع الأمن السيبراني بعناية في امتلاك وتأمين وحماية جميع حساباتنا عبر الإنترنت والمعلومات. تقدم [ادخل أسم المؤسسة] هذه الموارد التي يمكنك استخدامها للمحافظة على سلامة استخدامك للإنترنت:

• موقع شهر التوعية بالأمن السيبراني الخاص بوكالة CISA: cisa.gov/cybersecurity-awareness-month

• أساسيات CISA's - أفضل الممارسات الإلكترونية الأساسية لقادة الأعمال: cisa.gov/cyber-essentials

• تعرف على وظائف في مجال الأمن السيبراني من خلال المبادرة الوطنية لشغل وظائف ودراسات الأمن السيبراني: niccs.cisa.gov

إذا كان لديك المزيد من الأسئلة حول كيفية مشاركة [ادخل أسم المؤسسة] في حملة شهر التوعية بالأمن السيبراني لهذا العام، يرجى إرسال بريد إلكتروني إلى [ادخل عنوان البريد الإلكتروني لحملة المؤسسة لشهر التوعية في مجال الأمن الإلكتروني المعلوماتي]

<التوقيع>

نموذج إيميل إلى الموظفين:

السادة <اسم المؤسسة>،

يصادف **شهر التوعية بالأمن السيبراني** في أكتوبر 2021! انضمت [ادخل أسم المؤسسة] إلى الحملة السنوية التي تقودها وكالة الأمن السيبراني وأمن البنية التحتية (CISA) والتحالف الوطني للأمن السيبراني (NCSA). تتفهم الحملة كيفية عمل القطاعين العام والخاص معاً والقيام بهما كدور فردي في بناء عالم آمن عبر الإنترنت. نواصل هذا العام استخدام الطابع الشامل "قم بدورك، #BeCyberSmart."

يدرك العديد من المتخصصين في الإنترنت المخاطر والقضايا في عالمنا الافتراضي المتزايد. في [ادخل أسم المؤسسة] ، نحن نريد مساعدتك لتحسين الموقف الإلكتروني واستخدام المعرفة التي تحصل عليها في العمل لمساعدة الآخرين على اتباع نهج آمن وواعي للأمن السيبراني.

خلال شهر أكتوبر سنتعرف على أربع رسائل أسبوعية:

• الأسبوع 1: كن ذكياً في مجال الأمن الإلكتروني

كيف يمكنك اتخاذ إجراءات بسيطة للحفاظ على حياتنا الرقمية آمنة.

• الأسبوع 2: حارب الغش والاحتيال!

سنسلط الضوء على مخاطر محاولات التصيد الاحتيالي - التي يمكن أن تؤدي إلى هجمات برامج الفدية أو البرامج الضارة الأخرى - وكيفية الإبلاغ عن رسائل البريد الإلكتروني المشبوهة.

• **الأسبوع 3: أستكشاف. خبرة. مشاركة.**

سنحتفل معاً بأسبوع التوعية المهنية للأمن السيبراني التابع للمبادرة الوطنية لتعليم الأمن السيبراني (NICE) والقوى العاملة العالمية في مجال الأمن السيبراني ، ونستضيف معرض التوظيف الخاص بالأمن السيبراني الخاص بنا، ونسلط الضوء على الأدوات التعليمية المتنوعة التي تمتلكها CISA.

• **الأسبوع 4: الأمن الإلكتروني المعلوماتي أولاً**

أكتشف كيف يتزايد أهمية الأمن السيبراني والبقاء آمناً أثناء استخدام الإنترنت مع استمرار عالمنا بالعمل بالشكل الافتراضي من أجل الكثير من العمل ومجرد التصفح والهوا.

يمكن لكل واحد منا المشاركة في شهر أكتوبر من هذا العام لمساعدتنا جميعاً على أن نكون أكثر أماناً عبر الإنترنت. قم بدورك. #BeCyberSmart من خلال استخدام الموارد التالية:

• موقع شهر التوعية بالأمن السيبراني CISA: cisa.gov/cybersecurity-awareness-month

• أساسيات CISA's - أفضل الممارسات الإلكترونية الأساسية لقادة الأعمال: cisa.gov/cyber-essentials

• تعرف على الوظائف في الإنترنت من خلال المبادرة الوطنية لشغل وظائف ودراسات الأمن السيبراني: niccs.cisa.gov

إذا كان لديك المزيد من الأسئلة حول كيفية مشاركة [ادخل أسم المؤسسة] في حملة شهر التوعية بالأمن السيبراني لهذا العام أبعث بريد إلكتروني إلى [ادخل عنوان البريد الإلكتروني لحملة المؤسسة لشهر التوعية في مجال الأمن الإلكتروني المعلوماتي] أو إذا كنت ترغب في الإبلاغ عن الأنشطة المشبوهة إلى البريد الإلكتروني لقسم تكنولوجيا المعلومات والإسناد الفني [ادخل عنوان البريد الإلكتروني الخاص بقسم تكنولوجيا المعلومات].

<التوقيع>