كن ذكياً في مجال الأمن الإلكتروني

#CyberMonth

شهر التوعية بالأمن الإلكتروني المعلوماتي 2021

مالمقصود بشهر التوعية في الأمن الإلكتروني المعلوماتي؟

يزيد شهر التوعية بالأمن الإلكتروني المعلوماتي من مستوى نشر الوعي بأهمية هذا الموضوع في أمتنا.

الأمن الإلكتروني المعلوماتي «وماذا في ذلك؟»

هل تعلم؟

أن برامج مكافحة الفيروسات للأجهزة المحمولة متوفرة، والتي تكون هدف سهل وشائع للقراصنة وغيرهم من الجهات الفاعلة السيئة.

الإدراك البديهي للصواب فيما يخص الأمن الإلكتروني المعلوماتي

- لايختلف الشعور بالأمان عبر الإنترنت كثيراً عن الأمان في العالم المادي!
- حافظ على هدوئك وثق بشعورك!

المصطلحات الشائعة الأستخدام

- التمثيل والخداع
- مخترق
- مهاجمات الإنترنت

هناك حالياً ما يقدر
5.2 مليار مستخدم للإنترنت أو
63٪ من سكان العالم.

قم بدورك .
#BeCyberSmart

يبدأ الأمن الإلكتروني المعلوماتي معك وهو مسؤولية **الجميع**.

جرائم الإنترنت

ماهي؟

جرائم الإنترنت هي أي جريمة تُرتكب إلكترونياً.

يمكن أن يشمل ذلك ...

- السرقة
- التزوير
- وفي بعض الأحيان حتى القتل

لماذا يجب عليك الاهتمام؟

- الجريمة تشكل خطراً أثناء وعدم الاتصال!
- يمكن لأساسيات الدفاع عن النفس عبر الإنترنت أن تقطع شوطًا طويلاً لإبعادك أنت وبياناتك عن أيدي الجهات السيئة.

أمثلة

- الأستحواذ وأنتحال الهوية
- الاعتداء الجنسي على الأطفال
- السرقة المالية
- انتهاكات الملكية الفكرية
- البرمجيات الخبيثة الفايروسية
- الهندسة الاجتماعية الخبيثة

البرامج الخبيثة الفايروسية

ماهي؟

أي برنامج يهدف إلى ...

- تلف
- تعطيل
- أو تمكين شخصاً ما الوصول الغير مصرح به إلى جهاز الكمبيوتر الخاص بك أو أي جهاز آخر متصل بالإنترنت

لماذا يجب عليك الاهتمام؟

- تبدأ معظم الجرائم الإلكترونية بنوع من البرامج الضارة. أنت وعائلتك ومعلوماتك الشخصية معرضون للخطر بشكل شبه مؤكد إذا وجدت البرامج الضارة طريقها إلى جهاز الكمبيوتر أو الأجهزة.

أمثلة

- برامج الفدية أو الرانسموير
- البرامج التطفلية
- بوت نت أو شبكة الروبوت
- البرامج الخبيثة الخفية (Rootkits)
- برامج التجسس
- الفايروسات
- فايروس متنقل (Worms)

برامج الفدية أو الرانسموير

ماهي؟

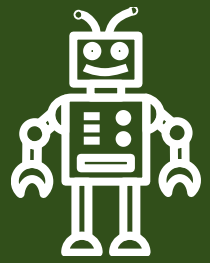
هي برامج ضارة مصممة لجعل البيانات أو الأجهزة غير قابلة للوصول إلى المستخدم بدون دفع فدية.

لماذا عليك الاهتمام؟

- غالباً ما يتم تنزيله كروابط بريد إلكتروني ضارة
- الإضرار بالاستقرار المالي والسمعة
- لا يوجد ضمان لاستعادة بياناتك، حتى لو دفعت
- غالباً ما تستخدم هذه البرامج كخدعة أو شرك لأنشطة ضارة أخرى

أمثلة

- تشفير
- وينلوك
- كريبتوول
- ريفنتون
- Bad rabbit
- كرايسز
- وانكراي



برامج الروبوت

ماهي؟

هي نوع من البرامج المستخدمة لأتمتة المهام على الإنترنت.

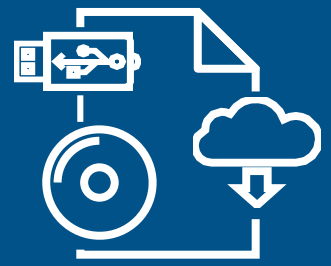
هل تعلم؟

ليست كل الروبوتات سيئة. عند استخدام محرك بحث، تصبح هذه النتائج ممكنة بمساعدة الروبوتات التي تنتشر على الإنترنت وتقوم بعملية فهرسة المحتوى. روبوتات الدردشة مثل Siri و Alexa هي نوع آخر شائع من الروبوتات "الجيدة".

لماذا عليك الاهتمام؟

يمكن للروبوتات الخبيثة:

- جمع كلمات المرور
- تسجيل ضغطات المفاتيح
- الحصول على المعلومات المالية
- الاستحواذ على حسابات وسائل التواصل الاجتماعي
- استخدام بريدك الإلكتروني لإرسال بريد مزعج أو خداعي
- فتح الأبواب الخلفية للجهاز المصاب



الهجمات الإلكترونية المادية

ماهي؟

الهجمات الإلكترونية المادية تستخدم الأجهزة أو أجهزة التخزين الخارجية أو أي كيان مادي أخر لإصابة الأنظمة الرقمية أو إتلافها أو إختراقها بأي شكل آخر. يمكن أن يشمل ذلك ...

- أجهزة التخزين الخارجية USB
- CD/DVD
- الأجهزة المادية المرتبطة بشبكة الإنترنت (IoT)

لماذا عليك الاهتمام؟

- من السهل عدم الأنتباه لها وأغفالها
- من الصعب تحديدها والكشف عنها
- من الصعب للغاية إزالتها
- بأمكان هذه البرامج فعل أي شيء من تثبيت برامج الفدية إلى إرسال نسخ من أنظمة المعلومات أو تعديلها إلى تفكيك الشبكات

هل تعلم؟

من المحتمل أن يكون أي شيء متصل بالإنترنت معرضاً للخطر، من دراجات السكوتر الإلكترونية إلى أجهزة الكمبيوتر المحمولة إلى سفن شحن البضائع.

الهندسة الاجتماعية

ماهي؟

- يمكن لمجرمي الإنترنت أستغلالك من خلال أستخدام المعلومات المتاحة بشكل شائع من خلال ...
- منصات التواصل الاجتماعي
- مشاركة موقعك
- المحادثات الشخصية

لماذا يجب عليك الاهتمام؟

- خصوصيتك لها أهمية - إنها تحتاج إلى توفير إجراء أمني
- حتى مع القليل من المعرفة بالبرمجة، يمكن أن تكون الهجمات ناجحة
- يمكن للتدابير الأمنية التكنولوجية أن تحميك إلى حد ما – لكن تبقى أنت أفضل من يحمي هذه الخصوصية

أمثلة

- الخداع
- بريتكستنك
- الُطعم (Baiting)
- المقايضة
- التتبع (Tailgating)
- الاقتحام الداخلي (Inside job)
- المكالمات الهاتفية الخادعة

الخداع

ماهو؟

رسائل مزيفة من مصدر موثوق أو حسن السمعة مصممة بشكل يبدو مقنع لك...

- بكشف المعلومات
- منح حق الوصول غير المصرح به إلى النظام
- الضغط فوق رابط
- الموافقة على صفقة مالية

لماذا عليك الاهتمام؟

- لأنها شائعة بشكل كبير
- يمكن أن يكون لها عواقب وخيمة
- تدخلها في تفاصيل مهمة

أمثلة

- البريد الإلكتروني
- الرسائل النصية
- المكالمات الهاتفية
- الرسائل والمشاركات في مواقع التواصل الاجتماعي
- الارتباطات التشعبية المشبوهة

هل سيخدعك هذا الإيميل؟

رسالة جديدة

من Legitimate-Looking-Source@notquiteyourworkemail.com

الموضوع تحديث عاجل : برمجيات معرضة للإصابة بفيروس

تحديث برمجيات

مساء الخير توم،

تم التعرف على ثغرة أمنية في «اسم لبرنامج معروف» بحيث تسمح للمهاجمين بتسجيل المكالمات ومقاطع الفيديو من جهاز الكمبيوتر الخاص بك دون علمك. الرجاء تثبيت التحديث لتجنب الإصابة، بنهاية اليوم، وإلا سيتم إغلاق محطة العمل الخاصة بك.

لقد أنشأنا أيضا تطبيقا لجميع الموظفين لتحديد ما إذا كانوا قد تأثروا بهذه الثغرة الأمنية. انقر هنا لتشغيل التطبيق.

www.fakewebsite.com/gotcha.exe
أضغط على الرابط.

مع خالص التقدير،
بوسمان
قسم تكنولوجيا المعلومات الخاص بشركتك

رد

مكالمات هاتفية خادعة SWATTING

ماهي؟

هجوم يتمحور حول موقع ما، حيث يتصل الأشخاص المخادعون بالشرطة مدعين أن الضحية قد ارتكبت جريمة مثل...

- تهديد بالقنابل
- شخص دخيل مسلح
- حادث عنيف

لماذا عليك الاهتمام؟

- تتسبب في عواقب جسدية فورية
- في بعض الأحيان يكون المقصود منها مجرد مزحة
- ممكن أن تتسبب في الاعتقال وإصابات خطيرة
- قلل المخاطر من خلال مشاركة موقعك مع أفراد موثوق بهم فقط ، ولا تشارك صورك عندما تكون في إجازة إلا بعد عودتك إلى المنزل بأمان

أمثلة

يتم خزن موقعك كبيانات وصفية في كل صورة تلتقطها بهاتفك. قم بإيقاف تشغيل خدمات الموقع عند عدم استخدامها لجعل الأمر أكثر صعوبة على الجهات المخادعة لعرض هذه المعلومات.

الطرق الأخرى للهجوم

ماهي؟

- أي جهاز متصل بالأنترنت
- أي جهاز متصل بشبكتك
- جمع المعلومات
- الوصول عن بعد
- بلوتوث
- المنافذ المفتوحة

لماذا عليك الاهتمام؟

- يمكن استخدام شبكتك لمهاجمة شخص آخر
- يمكن أن يمثل أي جهاز يخزن المعلومات أو متصلاً بالإنترنت ثغرة أمنية
- دائماً أفترض أنك معرض للاختراق، وأتخذ تدابير لفهم المخاطر وتخفيفها
- لا تكن فريسة سهلة للمتصيدين

أمثلة

- الأجهزة الذكية
- هاتف محمول
- منظم الحرارة
- المركبات
- لوحات المفاتيح الخاصة بألعاب الكومبيوتر
- طابعات
- معدات طبية
- الأنظمة الصناعية

كيف يمكنك حماية نفسك بشكل أفضل عند أستخدامك الإنترنت؟

تأمين الحماية لشبكاتك بشكل تام.

تعد أجهزة الموجهات اللاسلكية وسيلة يستخدمها مجرمو الإنترنت للوصول إلى الأجهزة عبر الإنترنت.

إذا قمت بتوصيله، تأكد من الحماية.

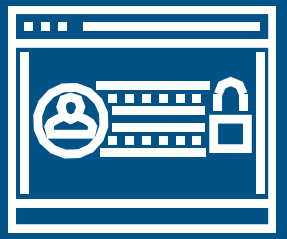
أحد وسائل الدفاع المؤكدة ضد التطفل هو التحديث المستمر لأحدث برامج الحماية من الفيروسات.

ابق على اطلاع بآخر التحديثات.

حافظ على تحديث البرامج إلى أحدث الإصدارات وقم بتعيين برامج الأمان لإجراء عمليات الفحص المنتظمة.

ضاعف حماية تسجيل الدخول الخاص بك.

قم بتمكين خاصية التحقق متعددة العوامل(MFA) للتأكد من أن الشخص الوحيد الذي لديه حق الوصول إلى حسابك هو أنت.



نصائح عند أختيار كلمة المرور

هل تعلم؟

أن وسيلة جمع وتتبع كلمة المرور أو بيانات الاعتماد مستخدمة في الهجوم الإلكتروني، حيث تتم محاولة تتبع اسم المستخدم وكلمات المرور المكونة بالفعل من موقع إلى موقع آخر على أمل أن يستخدم المستخدم نفس معلومات تسجيل الدخول عبر الأنظمة الأساسية.

أستخدم كلمات مرور مختلفة على أنظمة وحسابات مختلفة	******
استخدم أطول كلمة مرور مسموح بها	******
استخدم مزيجاً من الأحرف الكبيرة والصغيرة والأرقام والرموز	******
أعد تعيين كلمة المرور الخاصة بك كل بضعة أشهر	******
استخدم برنامج إدارة كلمات المرور	******

سمة وطابع شهر التوعية للأمن الإلكتروني المعلوماتي

الطابع:

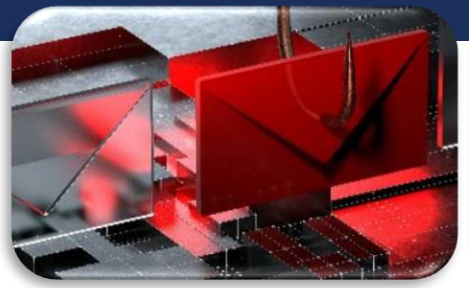
- قم بدورك.

#BeCyberSmart.

جدول شهر التوعية بالأمن الإلكتروني المعلوماتي

أكتوبر1:
الأفتتاح الرسمي

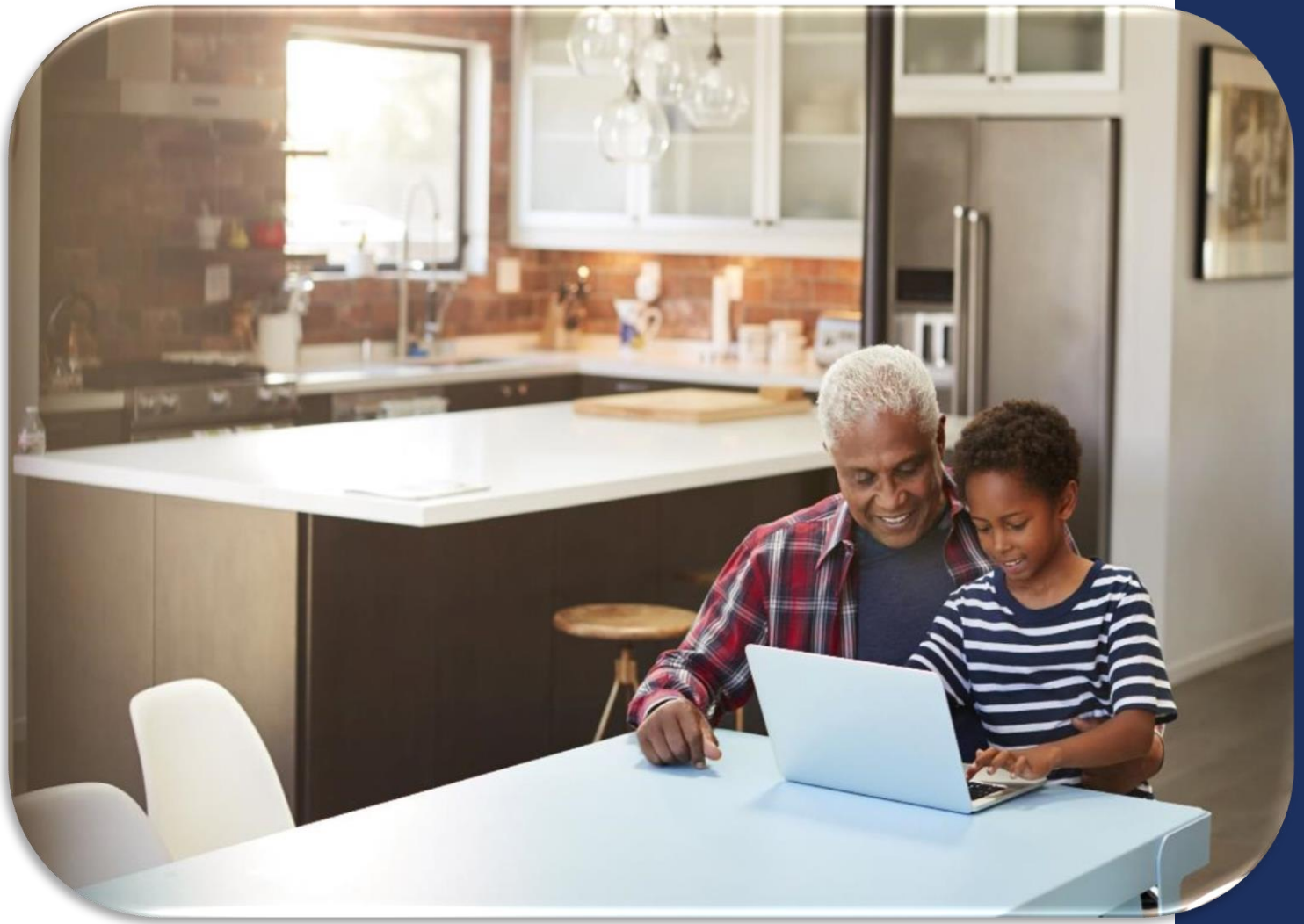
الأسبوع 1:
أسبوع 4 أكتوبر
كن ذكياً في مجال الأمن الإلكتروني المعلوماتي.



الأسبوع 2:
أسبوع 11 أكتوبر
حارب الخداع!

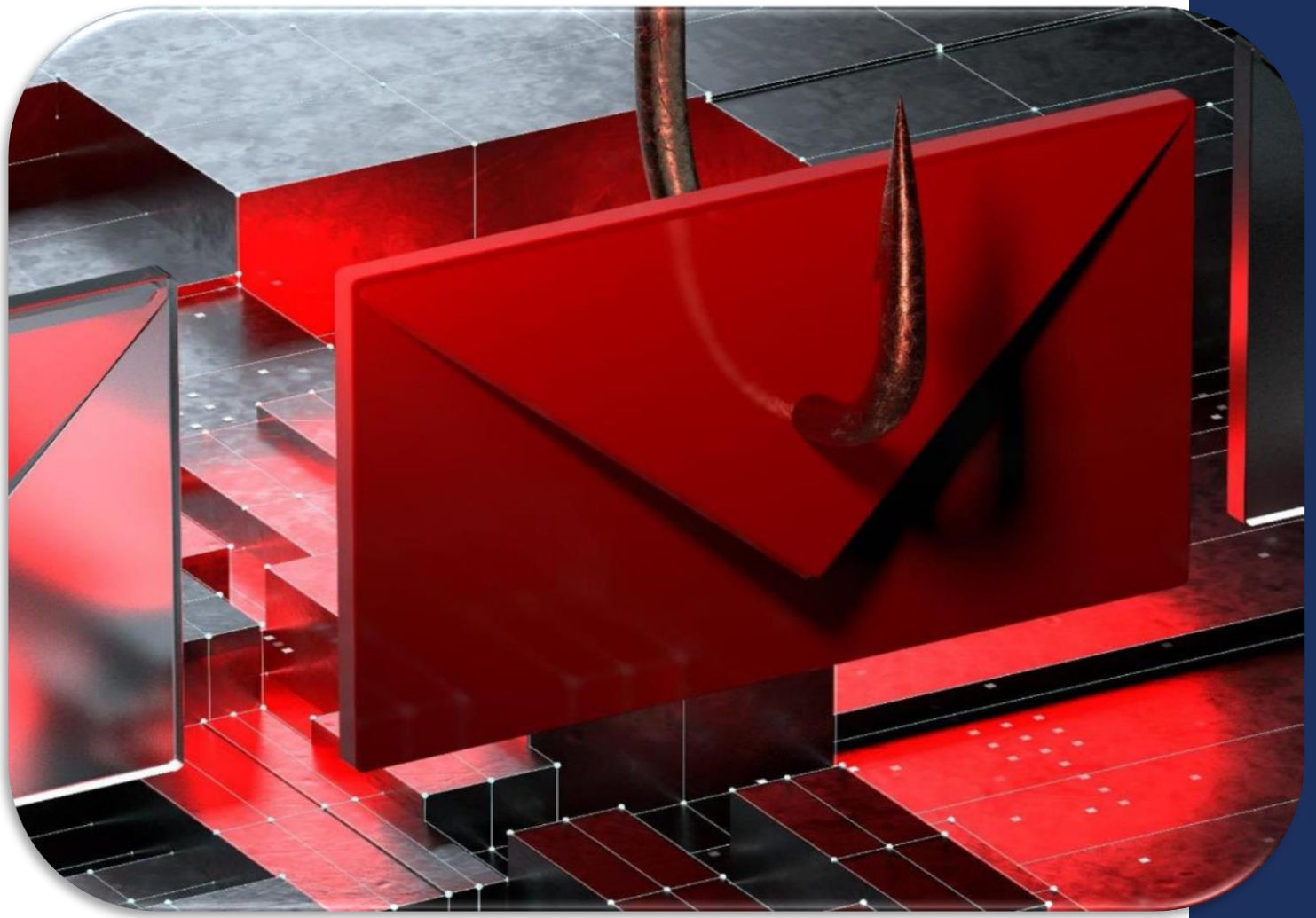
الأسبوع 3:
أسبوع 18 أكتوبر
أستكشاف. خبرة. مشاركة. (أسبوع التوعية المهنية في مجال الأمن المعلوماتي)

الأسبوع 4:
أسبوع 25 أكتوبر
الأمن الإلكتروني المعلوماتي أولاً

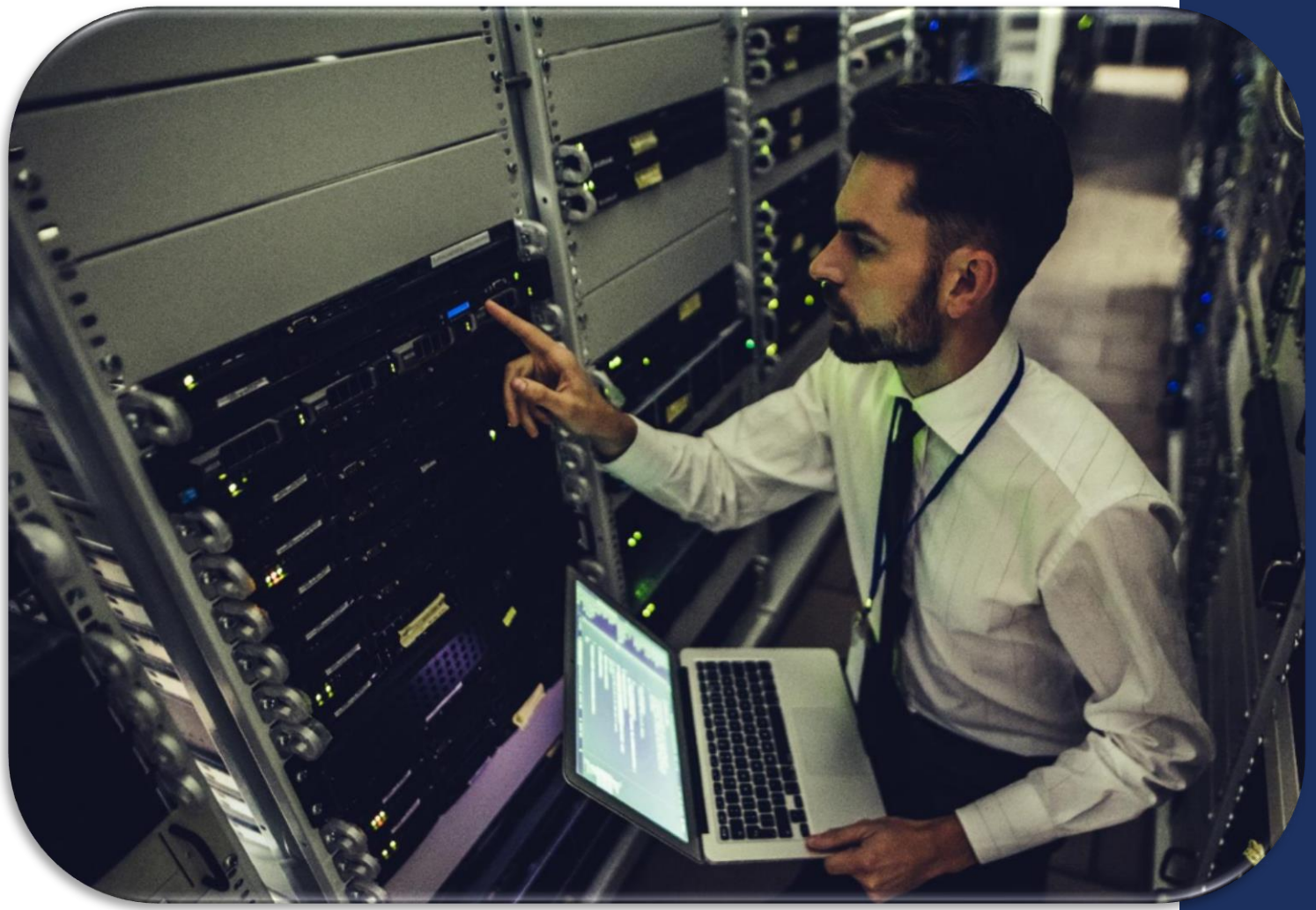


الأسبوع 1:

كن ذكياً في مجال الأمن الإلكتروني المعلوماتي.



الأسبوع 2:
حارب الخداع!



الأسبوع 3:

أستكشاف. خبرة. مشاركة. أسبوع التوعية المهنية في مجال الأمن المعلوماتي

الأسبوع 4:
الأمن الإلكتروني المعلوماتي أولاً.

نشر التوعية والمشاركة

- كن أحد مناصري شهر الأمن الإلكتروني المعلوماتي
- اعمل على الترويج لشهر التوعية بالأمن الإلكتروني المعلوماتي من خلال وسائل التواصل الاجتماعي ؛ استخدم #BeCyberSmart
- تطوع للتحدث في مشاركات شهر التوعية بالأمن الإلكتروني المعلوماتي
- شارك في تداول نصائح الأمن الإلكتروني المعلوماتي مع أصدقائك وعائلتك وزملائك في العمل

لمزيد من المعلومات يرجى مراسلة
CyberAwareness@cisa.dhs.gov

لمزيد من المعلومات قم بزيارة الموقع cisa.gov/cybersecurity-awareness-month أو staysafeonline.org/cybersecurity-awareness-month/