كن ذكياً كن ذكياً في مجال الأمن الإلكتروني المعلوماتي

#CyberMonth

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

الأمن السيبراني خلال العمل

تواجه الشركات خسارة مالية كبيرة عند حدوث هجوم إلكتروني، عبر الإنترنت. في عام 2020، تم الإبلاغ عن زيادة حادة في الهجمات الإلكترونية التي تستهدف الشركات باستخدام معلومات تسجيل الدخول وكلمات المرور المسروقة.[1] غالباً ما يعتمد مجرمو الإنترنت على خطأ بشري – مثل عدم تثبيت تصحيحات البرامج أو النقر على الروابط الضارة، من قبل الموظفين - للوصول إلى الأنظمة. من القيادة العليا إلى أصغر منصب وظيفي، يتطلب الأمن السيبراني يقظة الجميع للحفاظ على البيانات والعملاء والأموال آمنة. كن ذكياً في مجال استخدام الإنترنت #BeCyberSmart للتواصل بثقة ودعم ثقافة الأمن السيبراني في مؤسستك.

نصائح بسيطة

- **التعامل مع المعلومات الخاصة بعملك كانها معلومات شخصية.** تتضمن معلومات العمل عادةً مزيجاً من البيانات الشخصية والخاصة بالعمل. إضافة إلى الأسرار التجارية وحسابات ائتمان الشركة، فإنها تتضمن أيضاً معلومات تعريف شخصية للموظفين (PII) من خلال نماذج الضرائب وحسابات الرواتب. لا تشارك معلومات تحديد الهوية الشخصية مع جهات غير معروفة أو عبر شبكات غير آمنة.
- **لاتجعل كلمات المرور سهلة التخمين.** مع تطور التكنولوجيا "الذكية" أو التي تعتمد على البيانات، من المهم أن تتذكر أن الإجراءات الأمنية لا تعمل إلا إذا تم استخدامها بشكل صحيح من قبل الموظفين. تعمل التكنولوجيا الذكية على البيانات، مما يعني أن الأجهزة مثل الهواتف الذكية وأجهزة الكمبيوتر المحمولة والطابعات اللاسلكية والأجهزة الأخرى تتبادل البيانات باستمرار لإكمال المهام. اتخذ احتياطات الأمان المناسبة وتأكد من التكوين والإعداد الصحيح للأجهزة اللاسلكية من أجل منع اختراق البيانات. لمزيد من المعلومات حول التكنولوجيا الذكية ، راجع بطاقة إرشادات الأجهزة المرتبطة مع بعض من خلال الإنترنت.
- **ابق على اطلاع بآخر التحديثات.** حافظ على تحديث برنامجك إلى أحدث إصدار متاح. حافظ على إعدادات الأمان الخاصة بك للحفاظ على أمن معلوماتك عن طريق تشغيل التحديثات التلقائية حتى لا تضطر إلى التفكير في الأمرأو نسيناه وتعيين برنامج الأمان الخاص بك لإجراء عمليات فحص منتظمة.
- **وسائل التواصل الاجتماعي هي جزء من مجموعة أدوات الاحتيال.** من خلال البحث في Google، وتصفح مواقع الشبكات الاجتماعية لمؤسستك، يمكن لمجرمي الإنترنت جمع معلومات عن شركائك وموردیك ، بالإضافة إلى الموارد البشرية والإدارات المالية. يجب على الموظفين تجنب المشاركة على وسائل التواصل الاجتماعي بشكل مفرط به، وعدم إجراء أعمال رسمية أو تبادل المدفوعات أو مشاركة معلومات تحديد الهوية الشخصية على منصات وسائل التواصل الاجتماعي. اقرأ نصائح الأمن السيبراني لوسائل التواصل الاجتماعي، لمزيد من المعلومات.
- **غالباً مايحتاج الهجوم لوجود ثغرة لمرة واحدة فقط.** لا تحدث خروقات البيانات عادةً عندما يخترق مجرم إلكتروني البنية التحتية للمؤسسة. يمكن تتبع العديد من خروقات البيانات إلى ثغرة أمنية واحدة، أو محاولة تصيد، أو حالة تعرض غير مقصود. كن حذراً من المصادر غير المعتادة، ولا تنقر على روابط غير معروفة، واحذف الرسائل المشبوهة بعد الإبلاغ عن جميع محاولات التصيد الاحتيالي أو إعادة توجيهها إلى المشرف، بحيث يمكن وضع أي تحديثات أو تنبيهات أو تغييرات تنظيمية ضرورية. لمزيد من المعلومات حول رسائل البريد الإلكتروني وعمليات الخداع ، راجع الصفحة الخاصة بنصائح ضد الخداع.

إذا كنت تعمل من المنزل

- **استخدم فقط الأدوات المعتمدة.** استخدم فقط البرامج والأدوات المعتمدة من المؤسسة أو عملك، بما في ذلك أدوات مؤتمرات الفيديو والأدوات الساندة التي توفرها الشركة أو المؤسسة والتي تمت الموافقة عليها لبدء الاجتماعات وجدولتها
- **.حافظ على أمن جلسات اجتماعك.** خصص احتياطات الأمان لتكون مناسبة للمشاركين بالاجتماع. خطط لما يجب فعله إذا تعطل الاجتماع العام. اتخذ الاحتياطات اللازمة للتأكد من أن اجتماعك سيحضره الأفراد المقصودون فقط.
- **تأمين حفظ المعلومات الخاصة بك.** خصص احتياطاتك الأمنية بشكل مناسب لحساسية بياناتك. قم بمشاركة البيانات الضرورية فقط، لغرض تحقيق أهداف اجتماعك.
- **تأمين وحماية نفسك.** اتخذ الاحتياطات اللازمة لتجنب الكشف عن المعلومات دون قصد. تأكد من أمن الشبكات المنزلية. لمزيد من المعلومات ، قم بزيارة المواد المرجعية اللازمة للعمل من المنزل .

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/ .

الموارد

1. مركزموارد سرقة الهوية .(2021) . *2020* تقرير حول البيانات المخترقة https://www.idtheftcenter.org/annual-reports/