kaspersky واجهوا المستقبل بأمان

Kaspersky Security Awareness

التدريب على الأمن الإلكتروني للمديرين التنفيذيين

تؤثر التقنيات الرقمية تأثيرًا عميقًا على كل جزء من جوانب الحياة، حيث توفر فرصًا أكبر، وفعالية من حيث التكلفة، والقدرة على التوسع عالميًا، والعديد من الفوائد المثرية الأخرى. لكن لتحقيق الاستفادة الكاملة منها، أصبح الوعي الأمني والاستخدام السليم لمهارات الأمن الإلكتروني أكثر أهمية من أي وقت مضى.

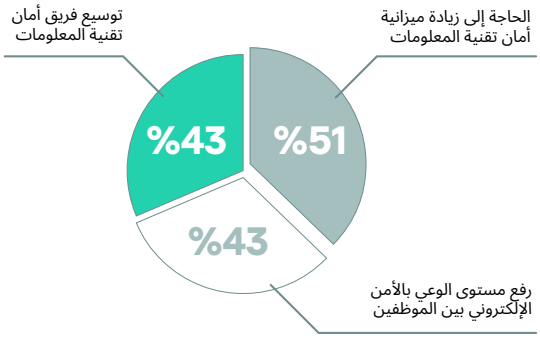
تؤدي الهجمات والانتهاكات الإلكترونية الناجحة، في أفضل الأحوال، إلى حدوث مشكلات في تقنية المعلومات الخاصة بالشركة، مع حدوث اضطرابات طفيفة في الأنظمة الداخلية. وفي أسوأ الأحوال، يمكنها التسبب في تدمير مؤسستك. ويتطلب استباق تهديدات الأمان المشاركة النشطة ليس فقط من جانب مديري أمن المعلومات وتقنية المعلومات، لكن من جانب القيادة غير الفنية أيضًا، مع التزام مشترك ببناء ثقافة للسلامة الإلكترونية في كل أرجاء مؤسستك.

عن طريق الوصول إلى أعلى مستوى من الأمان والمعلومات السرية، أصبح كبار المديرين أهدافًا مطلوبة لمجرمي الإنترنت. وقد تتحمل شركتك تكاليف باهظة بسبب الافتقار إلى المعرفة بالأمن الإلكتروني، والفجوات في مهارات السلامة الإلكترونية الأساسية، وحتى الأخطاء غير المقصودة التي يرتكبها هؤلاء المسؤولون التنفيذيون.

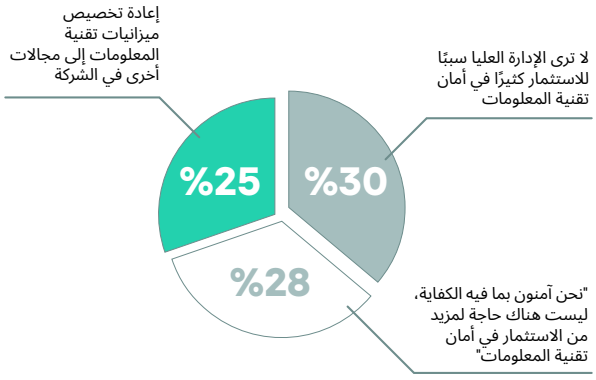
هل يوجد توافق بين المديرين التنفيذيين على مستوى الإدارة العليا ومديري أمان تقنية المعلومات في هذا الشأن؟

على الرغم من أن التعاون بين فرق أمان تقنية المعلومات ومجلس الإدارة مفيد لجميع الشركات، إلا أن 50% فقط من مسؤولي تقنية المعلومات يعتقدون أن الإدارة العليا تدرك تمامًا المخاطر الإلكترونية. وفي الواقع، يزعم 90% من صناع القرار في مجال تقنية المعلومات أن قادة أعمالهم سيكون لديهم استعداد للتنازل بشأن الأمن الإلكتروني لصالح التحول الرقمي أو الإنتاجية أو أهداف أخرى*. وتجعل هذه الطريقة في التفكير مناقشة أهمية ميزانيات أمان تقنية المعلومات واحدة من أصعب ثلاث محادثات بالنسبة لموظفي تقنية المعلومات مع المسؤولين التنفيذيين على مستوى الإدارة العليا.

تشمل المناقشات الثلاث الأكثر صعوبة **:



أهم ثلاثة أسباب تؤدي إلى انخفاض ميزانيات أمان تقنية المعلومات للمؤسسات*:**



يعترف 62% من المديرين بأن هذا الانفصال بين أمان تقنية المعلومات والمديرين التنفيذيين على مستوى الإدارة العليا قد أدى إلى حادث واحد على الأقل يتعلق بالأمن الإلكتروني**

مشاركة المديرين التنفيذيين في الأمن الإلكتروني - تحدٍ للمدربين

تتمتع المؤسسات التي يساهم فيها مديروها بشكل فعال في المناقشات والقرارات المتعلقة بحماية أعمالهم من التهديدات الإلكترونية باستعداد أكبر لمواجهة الهجمات الإلكترونية، ولديها مقدرة أفضل على التعافي من هذه الهجمات بسرعة. وتعد مشاركة الرئيس التنفيذي باعتباره عنصرًا مؤثرًا رئيسيًا أمرًا حيويًا لضمان الوعي الأمني المتسق والفعال في جميع أنحاء المؤسسة. لكنهم أشخاص مشغولون، ولديهم أولويات أخرى وجداول مواعيد مزدحمة. كيف يمكن تشجيعهم على تخصيص وقت للتدريب؟

تكمن الإجابة في التدريب المصمم خصيصًا لتلبية احتياجات المديرين التنفيذيين على مستوى الإدارة العليا. ويأخذ هذا التدريب شكل برنامج مصمم خصيصًا يساعدهم على فهم مشهد الأمن الإلكتروني، والعلاقة الرئيسية بين هذا المشهد وكفاءة الأعمال، مع توفير رؤى حول الحقائق التشغيلية لبناء وتطبيق إستراتيجيات الأمن الإلكتروني التي تفيد المؤسسة بأكملها.

---

* دراسة عالمية "Business friction is exposing organizations to cyber threats"، بواسطة Trend micro

** "Fluent in Infosec"، بواسطة Kaspersky 2023

*** "Managing the trend of growing IT complexity"، بواسطة Kaspersky

تدريب المسؤلين التنفيذيين من Kaspersky والتدريب على الأمن الإلكتروني للمديرين التنفيذيين عبر الإنترنت: بناء الوعي بالأمن الإلكتروني بين كبار المديرين وصناع القرار

يعد الأمن الإلكتروني جانبًا مهمًا من جوانب تحقيق الإيرادات جنبًا إلى جنب مع إدارة المشروعات والأدوات المالية وكفاءة الأعمال. وهذا هو محور الدورة التدريبية من Kaspersky للمسؤولين التنفيذيين. ويتعلم قادة الأعمال وكبار المديرين أساسيات الأمن الإلكتروني من خلال دورة يقودها مدرب وتمنحهم فهمًا أفضل للتهديدات الإلكترونية وكيفية الحماية منها.

ما الذي يقدمه التدريب

تغطي الدورة الجوانب الهامة والمتعلقة بالأعمال التجارية للأمن الإلكتروني، بلغة غير تقنية يسهل فهمها. وتركز الدورة على عائد الاستثمار في الأمن الإلكتروني، وتعزز التفاهم والتعاون المتبادل بين الإدارات عندما يتعلق الأمر بالأمن الإلكتروني.

يتوفر تدريب المديرين التنفيذيين في شكلين: ورشة تفاعلية وجهًا لوجه، وهي عبارة عن **تدريب للمديرين التنفيذيين** يقوده أحد خبراء Kaspersky، ودورة عبر الإنترنت – **التدريب على الأمن الإلكتروني للمديرين التنفيذيين عبر الإنترنت.**

يتكون التدريب على الأمن الإلكتروني للمديرين التنفيذيين عبر الإنترنت من 6 موضوعات:

1. مقدمة عن الأمن الإلكتروني
   - أ. ما هو الأمن الإلكتروني
   - ب. لماذا يجب أن يشارك المديرون في الأمن الإلكتروني
   - ج. خطاب يوجين كاسبيرسكي: من الدفاع الإلكتروني إلى المناعة الإلكترونية
2. المخاطر الإلكترونية للشركات
   - أ. خسائر الأعمال نتيجة لهجوم إلكتروني
   - ب. التدابير والأساليب لإدارة المخاطر الإلكترونية
   - ج. دراسات حالة لإدارة المخاطر الإلكترونية الناجحة وغير الناجحة
3. الهجمات الإلكترونية وأدوات المهاجمين
   - أ. أدوات المهاجمين: الهندسة الاجتماعية والبرمجيات الضارة وثغرات الاستغلال والسوق المظلمة
   - ب. الهجمات الإلكترونية: أنواعها، وعوامل نجاحها، والهجمات الموجهة، والهجمات الجماعية، وتسرب البيانات، وكيف تحمي نفسك
4. حماية نفسك وشركتك من الهجمات الإلكترونية
   - أ. الصحة الإلكترونية للمديرين
   - ب. التدريب والتوعية للموظفين في مجال الأمن الإلكتروني
   - ج. الأمن الإلكتروني على مستويات مختلفة من نضج الشركة
   - د. تدقيق الأمن الإلكتروني وخدمات الأمن الإلكتروني
5. إدارة عواقب الهجمات الإلكتروني
   - أ. كيفية التفاعل والرد على هجوم إلكتروني
   - ب. خطة إدارة الأزمات الإلكترونية
   - ج. الاتصالات الخاصة بالحوادث
6. مستقبل الأمن الإلكتروني
   - أ. التهديدات الإلكترونية: الإحصائيات ونواقل الهجوم
   - ب. الصناعة 4.0. وإنترنت الأشياء
   - ج. الحصانة الإلكترونية

توجد مهمة عملية ومن 5 إلى 10 أسئلة للتقييم الذاتي وتعزيز معرفتك الجديدة في نهاية كل موضوع. وعند الانتهاء من جميع المهام والدروس، يتعين عليك اجتياز الاختبار النهائي.

بمجرد الانتهاء من ذلك، ستتلقى شهادة إكمال الدورة.

الفوائد الرئيسية:

- **سهلة الإتقان:** التعلم المصغر + المهام العملية + الاختبارات = توحيد المعرفة والحفاظ عليها
- **تنسيق ملائم:** تم تكييف الدورة التدريبية عبر الإنترنت للأجهزة المحمولة وأجهزة سطح المكتب
- **استنادًا إلى المعرفة العميقة باحتياجات الإدارة العليا:** وضع كبار المديرين في Kaspersky هذه الدورة التدريبية
- **المبادئ التوجيهية العملية وقوائم المراجعة:** تحتوي على مواد جاهزة للاستخدام

نتائج التدريب

بعد الانتهاء من الدورة، سيكون المديرون قادرين على ما يلي:

- التحدث باللغة نفسها التي يتحدث بها متخصصو تقنية المعلومات وأمان المعلومات
- وضع خطة لإدارة الأزمات الإلكترونية جنبًا إلى جنب مع فرق تقنية المعلومات وأمان تقنية المعلومات
- التخطيط لاتصالات فعالة خاصة بالحوادث
- اتخاذ قرارات إستراتيجية بناءً على تقييمات المخاطر الإلكترونية
- تطبيق قواعد الصحة الإلكترونية
- حماية أنفسهم من التهديدات الإلكترونية

وضع هذه الدورة كبار المديرين في Kaspersky وخبراء بارزين في مجال الأمن الإلكتروني. وفي المجمل، تحتوي على 50 درسًا مدة كل درس منها 3 إلى 6 دقائق. ويمكن تقديمها عبر الوصول إلى منصة سحابية أو بتنسيق النموذج المرجعي لعنصر المحتوى القابل للمشاركة (SCORM) لدمجها في نظام إدارة التعلم (LMS) الخاص بك.

هذه البرامج جزء من مجموعة التوعية الأمنية من Kaspersky، التي تقدم مجموعة من خيارات التدريب الجذابة لتعزيز الوعي بالأمن الإلكتروني لدى موظفيك وتمكينهم من القيام بدورهم في السلامة الإلكترونية الشاملة لمؤسستك.

لمعرفة المزيد، يرجى زيارة
kaspersky.com/awareness

www.kaspersky.com