Kaspersky Security Awareness

البرامج التدريبية
باستخدام الكمبيوتر
لكل المستويات
التنظيمية

kaspersky واجهوا المستقبل بأمان

تفضل بمعرفة المزيد على kaspersky.com/awareness

Kaspersky Security Awareness

الطريقة الفعالة لبناء الأمان عبر الإنترنت في جميع أنحاء مؤسستك

يتسبب الخطأ البشري في أكثر من 80% من كل الحوادث الإلكترونية. وتعد ثقافة سلوك الأمان عبر الإنترنت جنبًا إلى جنب مع المهارات الأساسية للأمن الإلكتروني والوعي المنتشر في جميع أنحاء مؤسستك عناصر أساسية للحد من سطح الهجوم وعدد الحوادث التي يتعين عليك التعامل معها. وتعاني المؤسسات في كثير من الأحيان للعثور على الأدوات والطرق المناسبة للتدريب الفعال للموظفين الذي يُغير السلوك إلى الأفضل. ويعد المفتاح لتحقيق ذلك نشر التدريب الذي يستخدم أحدث الأساليب والتقنيات في تعليم الكبار ويقدم المحتوى الأكثر صلة وحداثة.

العامل البشري - العنصر الأكثر ضعفًا في الأمن الإلكتروني

تشهد حلول الأمن الإلكتروني تطورًا سريعًا وتتكيف مع التهديدات المعقدة، مما يجعل الحياة أكثر صعوبة على مجرمي الإنترنت الذين يتجهون إلى العنصر البشري الأكثر ضعفًا في الأمن الإلكتروني.

52% من المديرين التنفيذيين يقولون إن الموظفين هم أكبر تهديد للأمن التشغيلي*

43% من الشركات الصغيرة تعرضت لحادث أمني بسبب انتهاك الموظفين لسياسات أمن تقنية المعلومات**

60% من الموظفين لديهم بيانات سرية على أجهزتهم التابعة للشركة (بيانات مالية، قاعدة بيانات البريد الإلكتروني، وما إلى ذلك)***

30% من الموظفين يعترفون بأنهم يشاركون تفاصيل تسجيل الدخول وكلمة المرور الخاصة بجهاز الكمبيوتر التابع للعمل مع الزملاء***

23% من المؤسسات لا تمتلك أي قواعد أو سياسات للأمن الإلكتروني مطبقة على تخزين بيانات الشركة***

Kaspersky Security Awareness – نهج جديد لإتقان مهارات أمن تقنية المعلومات

يوفر Kaspersky Security Awareness مجموعة من حلول التدريب التي تتسم بالتفاعل العالي والفعالة التي تعزز وعي الموظفين بالأمن الإلكتروني ليؤدوا جميعًا دورهم في الأمان عبر الإنترنت الشامل لمؤسستك. ونظرًا لأن التغييرات المستدامة في السلوك تستغرق وقتًا، فإن نهجنا يتضمن بناء دورة تعلم مستمر متعددة المكونات.

دورة التعلم المستمر

المشاركة / التحفيز	نقطة البداية	التعلم	التعزيز
– لماذا أحتاج هذا؟ – الإدراك	– هل أنا على علم بالموقف؟ – ماذا أعرف وأين الفجوات؟	– التعلم المصغر – التعلم المستمر – القدرة على التكيف	– هل فهمت بشكل صحيح؟ – هل أتذكر هذا؟ – هل أتصرف وفقًا لذلك؟

ميزات البرنامج الأساسية

خبرة كبيرة في مجال الأمن الإلكتروني

تحولت أكثر من 20 عامًا من الخبرة في مجال الأمن الإلكتروني إلى مهارات أمان عبر الإنترنت تحتل قلب منتجاتنا

تدريب يُغير سلوك الموظفين على كل مستوى في مؤسستك

يوفر تدريبنا باستخدام الألعاب المشاركة والتحفيز من خلال التعليم الترفيهي، بينما تساعد منصات التعلم على استيعاب مجموعة مهارات الأمن الإلكتروني لضمان عدم ضياع المهارات المكتسبة على طول الطريق.

* تقرير "تجاوز العاصفة المثالية: تأمين الأنظمة المادية الإلكترونية للبنية التحتية الحرجة". 2020

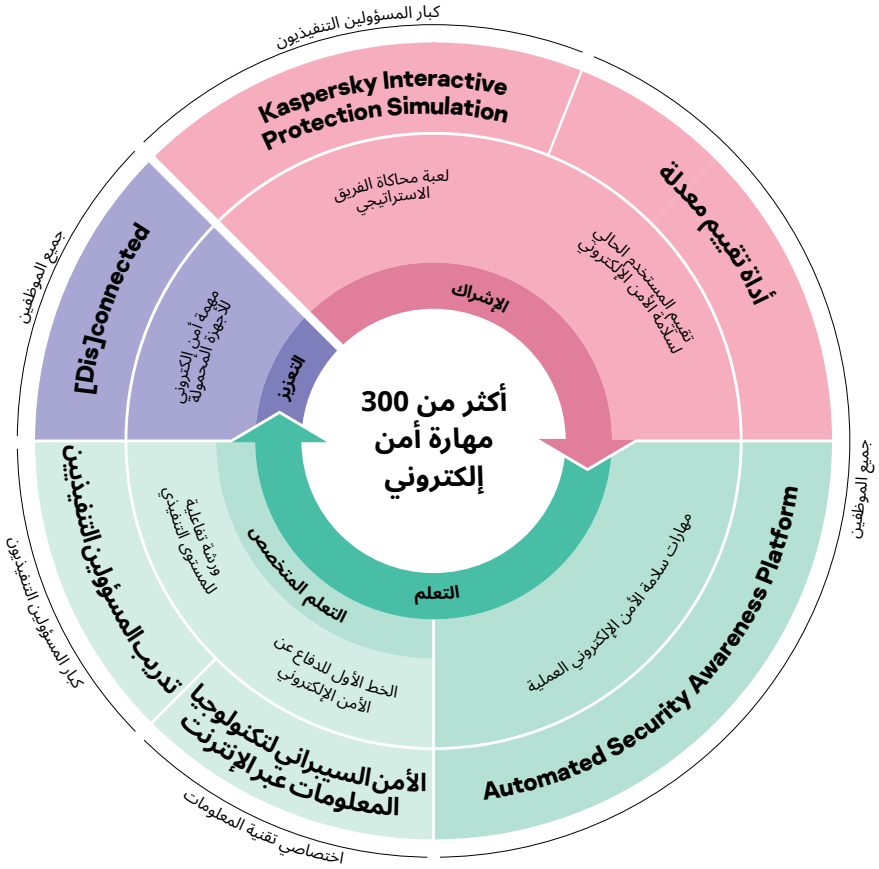
** تقرير "اقتصاديات أمن تقنية المعلومات لعام 2021"، شركة Kaspersky.

*** التخلص من الفوضى الرقمية". Kaspersky Lab، 2019.

خلق الحافز للتمتع بالوعي الأمني الفعال

يمثل تغيير سلوك الموظفين التحدي الأكبر الذي يواجهك في مجال الأمن الإلكتروني. ولا يتلقى الناس عمومًا التحفيز لاكتساب المهارات وتغيير عاداتهم، ولهذا السبب تتحول العديد من الجهود التعليمية إلى أكثر من مجرد إجراء شكلي فارغ. ويتكون التدريب الفعال من مكونات مختلفة، ويضع في الاعتبار خصوصيات الطبيعة البشرية والقدرة على استيعاب المهارات المكتسبة. وبصفتنا خبراء في الأمن الإلكتروني، فإن Kaspersky تعرف كيف يبدو سلوك المستخدم الآمن عبر الإنترنت. وبالاستفادة من رؤيتنا وخبراتنا، أضفنا أساليب وطرقًا تعليمية لتحصين موظفينا ضد الهجمات مع منحهم حرية الأداء دون قيود.

تنسيقات تدريب مختلفة للمستويات التنظيمية المختلفة



الموظفون يرتكبون الأخطاء. والمؤسسات تخسر الأموال...

1,315,000 دولار أمريكي
لكل مؤسسة
متوسط التأثير المالي لخرق بيانات ناجم عن الاستخدام غير المناسب لموارد تقنية المعلومات من قبل الموظفين*

%50
من الشركات
أبلغت عن مواجهتها لتهديدات ناجمة مباشرة عن سلوك غير لائق للموظفين، مما يجعل هذا التهديد الأكثر شيوعًا لأمن تقنية المعلومات*

%86
من الشركات
قالت إن شخصًا واحدًا على الأقل نقر على رابط للتصيد الاحتيالي**

5,01 مليون دولار أمريكي
متوسط التكلفة لكل خرق
من هجمات BEC (BEC - اختراق البريد الإلكتروني التابع للشركة) - وهي نوع من التصيد الاحتيالي يستولي المهاجمون من خلاله على حسابات بريد إلكتروني الشرعية التابعة للشركة أو ينتحلون هذه الحسابات)

* "اقتصاديات أمن تقنية المعلومات لعام 2021"، شركة Kaspersky
** اتجاهات تهديدات الأمن الإلكتروني 2021، CISCO
*** تكلفة خرق البيانات، 2021، IBM

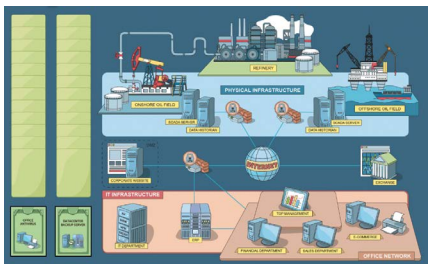
الحافز

لا يحرص الموظفون دائمًا على الالتحاق بالتدريب الإلزامي، وعندما يتعلق الأمر بالأمن الإلكتروني، فإن الكثيرون يعتبرونه معقدًا جدًا أو مملاً، أو يعتقدون أنه لا علاقة له بهم. ومع الافتقار إلى حافز للتعلم، من غير المرجح أن تكون نتيجة التعلم إيجابية للغاية. كما يوجد تحد آخر يواجهه المكلفون بالتعليم هو إشراك مديري الأعمال في التدريب، رغم أن أخطاءهم قد تكلف الشركة التكلفة نفسها التي قد يتسبب فيها خطأ أي شخص آخر. وهنا يأتي دور التحفيز - لأنه جذاب للغاية، فهو الطريقة الأكثر فاعلية لتشجيع الموظفين على التغلب على مقاومتهم الأولية للتدريب.

%70
مما يتم تعلمه
يتم نسيانه في غضون يوم واحد في أشكال التدريب التقليدية

%42 من المشاركين الذين يعملون في شركات يزيد عدد موظفيها عن 1000 موظف
قالوا إن غالبية البرامج التدريبية التي حضروها كانت عديمة الفائدة ومملة**

يستهدف تدريب KIPS كبار المديرين وخبراء أنظمة الأعمال ومتخصصي تقنية المعلومات، لزيادة وعيهم بالمخاطر والتحديات المرتبطة باستخدام جميع أنواع أنظمة وعمليات تقنية المعلومات.



Kaspersky Interactive Protection Simulation (KIPS): الأمن الإلكتروني من منظور الأعمال

يمثل حل KIPS لعبة جماعية تفاعلية مدتها ساعتان تؤسس تفاهمًا بين صانعي القرار (كبار مسؤولي الأعمال وتقنية المعلومات والأمن الإلكتروني) وتُغير تصوراتهم عن الأمن الإلكتروني. ويقدم محاكاة برمجية للتأثير الحقيقي الذي تتسبب فيه البرامج الضارة والهجمات الأخرى على أداء الأعمال والإيرادات. ويجبر اللاعبين على التفكير بشكل استراتيجي، وتوقع عواقب أي هجوم، والاستجابة وفقًا لذلك ضمن قيود الوقت والمال. ويؤثر كل قرار على جميع العمليات التجارية، حيث يتمثل الهدف الرئيسي في الحفاظ على سير الأمور بسلاسة. ويفوز في اللعبة الفريق الذي ينهي اللعبة بأكبر قدر من الإيرادات، بعد أن يعثر على جميع المخاطر في نظام الأمن الإلكتروني ويحللها ويستجيب بشكل مناسب.

13 سيناريو متعلقة بالصناعة
(نضيف المزيد طوال الوقت)

يوضح كل سيناريو دور الأمن الإلكتروني من حيث استمرارية الأعمال والربحية، ويسلط الضوء على التحديات والتهديدات الناشئة والأخطاء النموذجية التي ترتكبها المؤسسات عند بناء نظام الأمن الإلكتروني الخاص بها. ويعزز كذلك التعاون بين الفرق التجارية والأمنية، مما يساعد في الحفاظ على استقرار العمليات والاستدامة ضد التهديدات الإلكترونية.

تخصيص السيناريوهات

اعتبارًا من الربع الثالث من عام 2022، فيما يخص سيناريوهات صناعية محددة، ستكون الشركات قادرة على إنشاء سيناريوهات اللعبة الخاصة بها بهجمات مختلفة. وباستخدام مجموعات هجوم مختلفة، تستطيع الشركات التي تمتلك ترخيص مؤسسة من KIPS أن تكرر لعب السيناريو الصناعي نفسه عدة مرات.

الواقع الافتراضي في KIPS

KIPS Power Station VR عبارة عن تجربة غامرة جديدة في بيئة واقعية أقرب ما تكون إلى العمليات الحقيقية لمحطة توليد كهرباء. وتتيح التقنية للمديرين "العمل" كمتخصصين في أمن المعلومات، مما يدل على دور الأمن الإلكتروني وتأثيره على الأعمال بشكل مرئي، ليتمكنوا من رؤية عواقب قراراتهم الخاصة بتقنية المعلومات في رسومات ثلاثية الأبعاد واقعية للغاية بدلاً من الحصول على فكرة مجردة عنها فحسب.

Gamified Assessment Tool: طريقة سريعة ومثيرة لتقييم مهارات الموظفين في مجال الأمن الإلكتروني

تتيح لك Kaspersky Gamified Assessment Tool (GAT) تقييم مستويات معرفة موظفيك بالأمن الإلكتروني بسرعة. ويقضي الأسلوب التفاعلي الجذاب على الملل المصاحب غالبًا لأدوات التقييم الكلاسيكية. ويستغرق الموظفون 15 دقيقة فقط لاستعراض 12 موقفًا يوميًا تتعلق بالأمن الإلكتروني، وتقييم ما إذا كانت تصرفات الشخصية محفوفة بالمخاطر أم لا والتعبير عن مستوى الثقة في استجابتهم.

بعد إكمال التدريب، يتلقى المستخدمون شهادة تتضمن درجة تعكس مستوى وعيهم بالأمن الإلكتروني. ويتلقون أيضًا تعليقات حول كل منطقة، مع توضيحات ونصائح مفيدة.

يحفز نهج GAT المعتمد على الألعاب الموظفين بينما يوضح في الوقت نفسه أثناء حل بعض مواقف الأمن الإلكتروني احتمال وجود فجوات في معرفتهم. وهذا مفيد أيضًا لأقسام تقنية المعلومات / الموارد البشرية لاكتساب فهم أفضل لمستويات الوعي بالأمن الإلكتروني في مؤسساتهم، وقد يكون بمثابة خطوة تمهيدية لحملة تعليم على نطاق أوسع.

نقطة البداية

لا يدرك الناس عادة مستوى عدم كفاءتهم، مما يجعلهم معرضين للخطر بشكل خاص. ويحتاجون للخضوع إلى الاختبار، كما يحتاجون إلى تلقي ملاحظات مفصلة وواضحة حول مستوى كفاءتهم في مجال الأمن الإلكتروني لكي يكون التدريب الإضافي فعالاً. ويضمن هذا أيضًا عدم إضاعة الوقت على مواد مألوفة بالفعل.

منصة Kaspersky Automated Security Awareness Platform: كفاءة وسهولة إدارة التدريب للمؤسسات من أي حجم

تعد Kaspersky ASAP أداة فعالة وسهلة الاستخدام عبر الإنترنت تتولى تشكيل مهارات الأمن عبر الإنترنت للموظفين وتحفيزهم على التصرف بالطريقة الصحيحة.

رغم أن التدريب يلبي احتياجات الوعي الأمني لجميع الشركات، إلا أن الإدارة الآلية ستروق بشكل خاص للأشخاص الذين لا يمتلكون موارد مخصصة لإدارة التدريب.

الفوائد الرئيسية:

- **البساطة من خلال الأتمتة الكاملة:** من السهل جدًا تشغيل البرنامج وتكوينه ومراقبته، كما أن الإدارة المستمرة مؤتمتة بالكامل - دون الحاجة إلى مشاركة إدارية. وتبني المنصة جدول تعليم لكل مجموعة من الموظفين، مما يوفر التعلم المتقطع الذي يتم تقديمه تلقائيًا من خلال مزيج من تنسيقات التدريب، بما في ذلك وحدات التعلم وتعزيز البريد الإلكتروني والاختبارات ومحاكاة هجمات التصيد الاحتيالي.
- **الكفاءة:** تم تنظيم محتوى البرنامج لدعم التعلم التراكمي مع التعزيز المستمر. وتعتمد المنهجية على خصائص الذاكرة البشرية لضمان الاحتفاظ بالمعرفة وتطبيق المهارات اللاحق.
- **التعلم المرن:** حدد خيار تدريب الموظفين المناسب لك: سواء أكنت ستعين للموظفين دورة Express أساسية تساعدك على تلبية المتطلبات التنظيمية للتدريب على الأمن الإلكتروني بسرعة أو تسعى إلى تحديث معارفهم، أو ستختار دورة Main مقسمة إلى مستويات تعقيد لتطوير مهارات الأمن الإلكتروني بصورة أكثر تفصيلاً وعمقًا.
- **الترخيص المرن** (لمقدمي الخدمات المُدارة): من الممكن أن يبدأ نموذج الترخيص لكل مستخدم من 5 تراخيص فقط.

التعلم

تمثل منصتنا للتعلم عبر الإنترنت أساس برنامج التوعية. وتحتوي على **أكثر من 300 مهارة للأمن الإلكتروني** تغطي جميع الموضوعات الرئيسية في مجال أمن تقنية المعلومات.
ويتضمن كل درس حالات وأمثلة من الحياة الواقعية ليتمكن الموظفون من الشعور بالارتباط بما يتعين عليهم التعامل معه في عملهم اليومي. ويمكنهم استخدام هذه المهارات مباشرة بعد الدرس الأول.

Kaspersky ASAP: أداة على الإنترنت سهلة الإدارة تبني مهارات الموظفين في مجال الأمن الإلكتروني حسب المستوى

الموضوعات التي تتناولها ASAP:

- كلمات المرور والحسابات
- البريد الإلكتروني
- مواقع الويب والإنترنت
- مواقع التواصل الاجتماعية وتطبيقات المراسلة
- أمن الكمبيوتر الشخصي
- الأجهزة المحمولة
- حماية البيانات السرية
- التوجيه العام لحماية البيانات
- الأمن الإلكتروني في القطاع الصناعي

دورة ASAP Express

نسخة قصيرة من التدريب بتنسيق سمعي وبصري.

- النظرية التفاعلية
- مقاطع فيديو
- الاختبارات

Kaspersky ASAP حل متعدد اللغات.

ASAP حل مثالي لمقدمي الخدمات المدارة ومقدمي الخدمات الموسعة - يمكن إدارة خدمات التدريب للعديد من الشركات من خلال حساب واحد، وتتوفر كذلك اشتراكات ترخيص شهرية.

جرب إصدارًا كامل الوظائف من Kaspersky ASAP على asap.kaspersky.com - شاهد بنفسك مدى سهولة إعداد وإدارة برنامجك التدريبي للتوعية بأمن الشركة.

الدورة الرئيسية

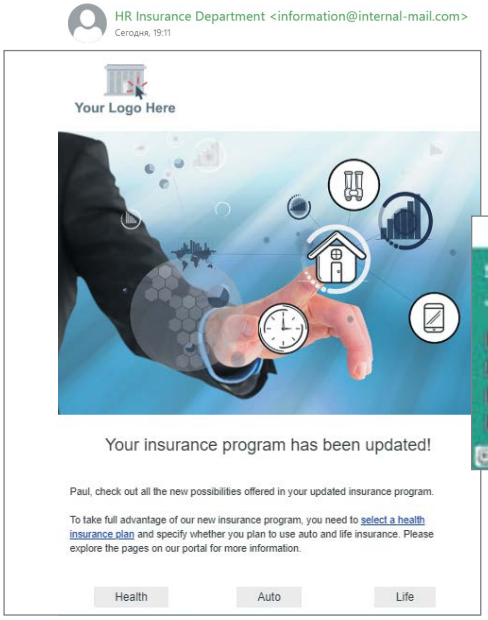
Express ةرود

محاكاة حملات التصيد الاحتيالي

يمكن استخدام محاكاة هجمات التصيد الاحتيالي قبل التدريب وأثنائه وبعده لاختبار قدرة الموظفين على مقاومة الهجمات الإلكترونية ومساعدتهم ومساعدة إدارة الشركة على معرفة فوائد التدريب.

الدروس التفاعلية

محاكاة هجمات التصيد الاحتيالي



تتبع النتائج

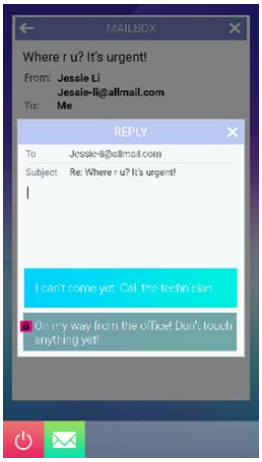
يمكنك متابعة تقدم الموظفين من لوحة المعلومات وتقييم تقدم الشركة بأكملها وجميع المجموعات بنظرة واحدة. ويمكنك أيضا البحث عن المزيد من التفاصيل على المستوى الفردي.

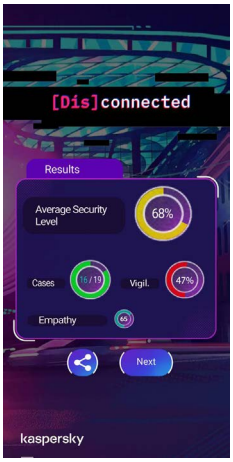
[Dis]connected: مهمة أمن إلكتروني للأجهزة المحمولة

[Dis]connected عبارة عن لعبة أمن إلكتروني للأجهزة المحمولة غامرة للغاية غنية بالقصص المرئية تتحدى المستخدمين في سعيهم للحفاظ على توازن صحي بين العمل والحياة والنجاح على الصعيدين الشخصي والمهني.

تم دمج عناصر الأمن الإلكتروني في مخطط اللعبة، وتكشف اللعبة كيف يمكن أن تساعد قراراتنا بشأن الأمن الإلكتروني في تحقيق هذه الأهداف، أو إفسادها. وتوجد 24 حالة يجب حلها، بما في ذلك موضوعات حول كلمات المرور والحسابات والبريد الإلكتروني وتصفح الويب ومواقع التواصل الاجتماعي وتطبيقات المراسلة وأمان الكمبيوتر والأجهزة المحمولة.
وتضمن التطبيقات المدمجة التي تم محاكاتها، مثل تطبيقات المراسلة وتطبيقات الخدمات المصرفية وما إلى ذلك، التمتع بتجربة غامرة تمامًا.

في نهاية اللعبة، يتلقى اللاعبون ملخصًا عن مدى نجاحهم في التعامل مع المشروع ومعرفة ما إذا كانت مهاراتهم الأمنية كافية لليوم، وغدًا.





تعمل اللعبة على الهواتف المحمولة. ويتوافر **عرض مجاني** في Google Play وAppStore:
https://kas.pr/mobilestores

التعزيز

يمثل التعزيز جزءًا أساسيًا من برنامج التعلم، وهو ضروري لترسيخ المعرفة والمهارات المكتسبة أثناء التعلم.

أفضل طريقة لتحويل المهارات المكتسبة إلى عادات هي وضعها موضع التنفيذ. وفي الوقت نفسه، يخطئ الناس أحيانًا ويتعلمون من التجربة الشخصية. لكن عندما يتعلق الأمر بالأمن الإلكتروني، فإن التعلم من أخطائك قد يكون مُكلفًا للغاية.

يمكنك باستخدام التدريب عن طريق الألعاب "عيش" الموقف وتجربة عواقبه دون التسبب في أي ضرر لنفسك أو لشركتك.

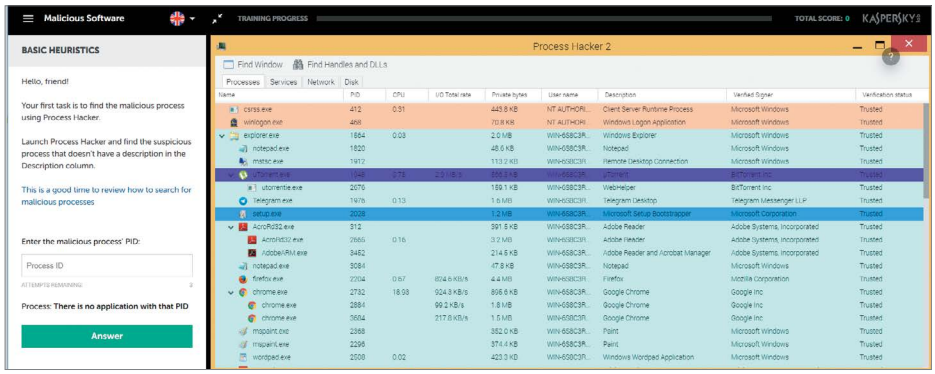
الأمن الإلكتروني لتقنية المعلومات عبر الإنترنت:
خط الدفاع الأول ضد الحوادث

الأمن الإلكتروني لتقنية المعلومات عبر الإنترنت عبارة عن تدريب تفاعلي لأي شخص يعمل في مجال تقنية المعلومات. ويبني مهارات قوية في مجال الأمن الإلكتروني والاستجابة للحوادث من المستوى الأول.

يزود البرنامج متخصصي تقنية المعلومات بالمهارات العملية للتعرف على سيناريو هجوم محتمل في حادث كمبيوتر غير ضار ظاهريًا. ويثير كذلك الرغبة في اكتشاف الأعراض الضارة، مما يعزز دور جميع أعضاء فريق تقنية المعلومات كخط أول للدفاع الأمني.

يُعلم CITO أيضًا أساسيات التحقيق وكيفية استخدام أدوات وبرامج أمن تقنية المعلومات، لتزويد متخصصي تقنية المعلومات بالمهارات النظرية والعملية والمعتمدة على التمرين، مما يتيح لهم القدرة على جميع بيانات الحوادث لتسليمها إلى أمن تقنية المعلومات.

يُوصى بتقديم هذا التدريب لجميع متخصصي تقنية المعلومات داخل مؤسستك، لكن يُوصى به في المقام الأول لمكاتب الخدمة ومسؤولي النظام. وسيستفيد معظم أعضاء فريق أمن تقنية المعلومات غير الخبراء من هذه الدورة أيضًا.



التعلم المتقدم

متخصصو تقنية المعلومات العاديون: يحدث في الغالب استبعاد لموظفي مكاتب الدعم والموظفين المتمرسين تقنيًا من التدريب لأن برامج التوعية القياسية ليست كافية بالنسبة لهم، لكن الشركات أيضًا لا تحتاج إلى تحويلهم إلى خبراء في الأمن الإلكتروني: تكلفة هذا التدريب مرتفعة للغاية ويستغرق وقتًا طويلاً وغير ضروري.

يسعدنا أن نعلن عن تدريب يملأ هذه الفجوة - ليس بتعمق مثل تدريب الخبراء، لكنه أكثر تقدمًا من التدريب المخصص للموظفين العاديين.

وحدات التدريب على الأمن الإلكتروني لتقنية المعلومات عبر الإنترنت:

- البرامج الضارة
- البرامج والملفات التي يحتمل أن تكون غير مرغوب فيها
- أساسيات التحقيق
- الاستجابة لحوادث التصيد الاحتيالي
- أمان الخادم
- أمان Active Directory

طريقة تقديم الأمن الإلكتروني لتقنية المعلومات عبر الإنترنت:
عبر الخدمات السحابية أو بتنسيق SCORM

جرب واحدة من وحدات CITO مجانًا:
cito-training.com

تدريب المسؤولين التنفيذيين: زيادة مرونة الأعمال لتحقيق التحول الرقمي

يتعلم قادة الأعمال وكبار المديرين أساسيات الأمن الإلكتروني من خلال دورة يقودها مدرب وتمنحهم فهمًا أفضل للتهديدات الإلكترونية وكيفية الحماية منها.

تشير الأبحاث إلى وجود صلة مباشرة بين سرعة وكفاءة الاستجابة للحوادث ودرجة الضرر التي يمكن أن يسببها الحادث. وتولي الدورة اهتمامًا خاصًا بالجوانب المالية للأمن الإلكتروني وجدوى الاستثمار فيه، مما يمنح المديرين التنفيذيين فهمًا أفضل للعلاقة بين الأمن الإلكتروني وكفاءة الأعمال.

يمكن استخدام Kaspersky Interactive Protection simulation (KIPS) بالإضافة إلى هذا التدريب لزيادة دمج المواد من خلال التمرين العملي.

أهدف الدورة التدريبية

- مشاركة أحدث المعلومات حول التهديدات الإلكترونية الحديثة ومخاطرها على الأعمال
- إطلاع المتعلمين على آخر التطورات في مجال التهديدات الإلكترونية الحديثة
- توفير فرصة لممارسة القواعد الأساسية لثقافة الأمن الإلكتروني للشركات والأفراد
- التأكد من فهم تأثير القضايا التنظيمية الرئيسية في مجال أمن المعلومات على الأعمال
- توضيح المفاهيم الأساسية للأمن الإلكتروني، وطرق الحماية من الهجمات المستهدفة
- تقديم توصيات عملية لسياسة الشركة
- تقديم المشورة بشأن الاتصالات للاستجابة للحوادث والتحقيق فيها

يُعد كبار المديرين من بين أكثر الأهداف المرغوبة لمجرمي الإنترنت، ومع ذلك فهم يمثلون غالبًا تحديًا حقيقيًا للمعلمين. ومع ذلك، بدون مشاركتهم ودعمهم لمختلف مبادرات الأمن الإلكتروني وتأييدها، فمن المستحيل إنشاء ثقافة الأمان عبر الإنترنت في المؤسسة.

يعد الأمن الإلكتروني جانبًا مهمًا من جوانب تحقيق الإيرادات جنبًا إلى جنب مع إدارة المشروعات والأدوات المالية والكفاءة التشغيلية للأعمال. وهذا هو محور دورتنا التدريبية للمسؤولين التنفيذيين.

Kaspersky Security Awareness: طرق مرنة للتدريب

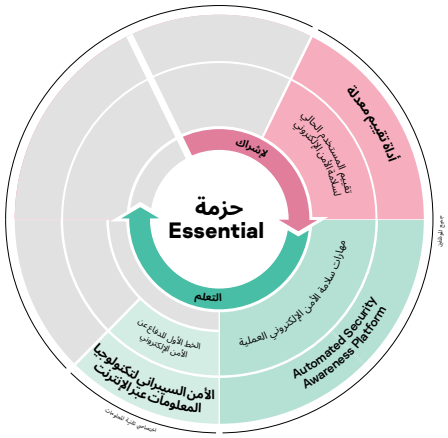
تغطي حلول التدريب من Kaspersky كل مستوى من مستويات شركتك ويمكن استخدامها بمفردها أو بشكل جماعي. ونيسر أيضًا بدء استخدام حزم مصممة خصيصًا لاحتياجاتك.

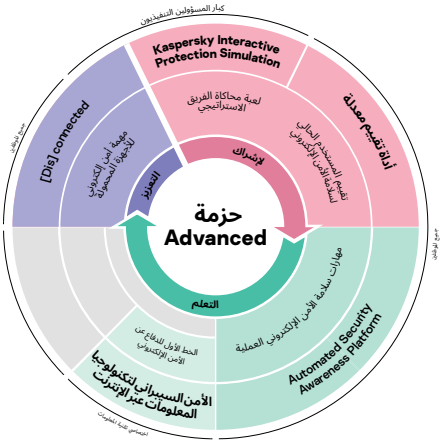
الخيار الخالي من المتاعب لتعزيز التوعية حول الأمن الإلكتروني لدى الموظفين - إعداد بسيط ويسهل إدارته.

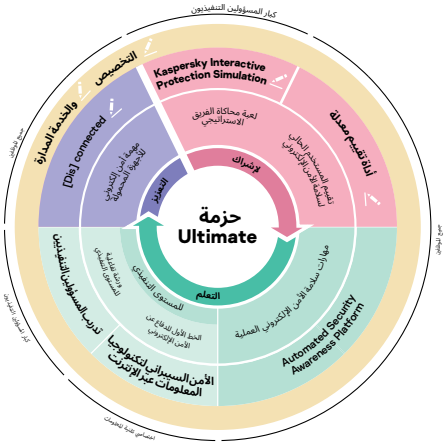
يوفر مستوى أساسيًا من التدريب الأمني لمساعدتك على العمل بنجاح وتلبية المتطلبات التنظيمية أو متطلبات الأطراف الأخرى للتدريب العام على الأمن الإلكتروني

يساعد المؤسسات الكبيرة في الحفاظ على استمرارية الأعمال باستخدام حل تدريب بسيط "جاهز للاستخدام". يدعم كل مستوى تنظيمي ويُغير السلوك من خلال تغطية كل مرحلة من مراحل دورة التعلم.

يضمن أقصى قدر من الوعي بالأمن الإلكتروني، ويتضمن ميزات التخصيص والخدمات المدارة، بحيث يتمتع المديرون التنفيذيون بدراية جيدة بسيناريوهات التهديدات، ويتمتع الموظفون بمهارات تلقائية للأمان عبر الإنترنت، ويدعمك موظفو تقنية المعلومات المتخصصون بصفتك خط الدفاع الأول.







يستخدم تدريب Kaspersky Security Awareness أحدث أساليب التدريب والتقنيات المتقدمة لضمان النجاح. ويمكن تصميم حلول مرنة جديدة ومجهزة معًا وفقًا لاحتياجاتك، لذلك يوجد حل يناسب الجميع. تفضل بمعرفة المزيد على kaspersky.com/awareness

Kaspersky Security Awareness: kaspersky.com/awareness
أخبار أمن تقنية المعلومات: me.kaspersky.com/blog/category/business/

kaspersky.com

© 2022 AO Kaspersky Lab.
جميع الحقوق محفوظة. العلامات التجارية المسجلة وعلامات الخدمة مملوكة لأصحابها المعنيين.

kaspersky واجهوا المستقبل بأمان