Kaspersky Security Awareness

مهارات الأمن الإلكتروني للموظفين على كل المستويات

تفضل بمعرفة المزيد على
me.kaspersky.com/enterprise-security/security-awareness

واجهوا المستقبل بأمان kaspersky

Kaspersky Security Awareness
بناء ثقافة الأمان عبر الإنترنت في جميع أنحاء مؤسستك

يتسبب الخطأ البشري في أكثر من 80% من كل الحوادث الإلكترونية. وعن طريق بناء ثقافة سلوك الأمان عبر الإنترنت، إلى جانب مهارات الأمن الإلكتروني الأساسية والوعي، في جميع أنحاء مؤسستك، يمكنك تقليل سطح الهجوم بالإضافة إلى عدد الحوادث التي يتعين عليك التعامل معها. وتعد أفضل طريقة لتحقيق التغييرات في السلوك التي تحل مشكلة "العامل البشري" في الأمن الإلكتروني من خلال 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.

55% من الشركات تُبلغ عن انتهاكات لسياسة أمان تقنية المعلومات من قبل موظفيها*

43% من الشركات الصغيرة تُبلغ عن أن انتهاكات سياسة أمان تقنية المعلومات من قِبل الموظفين تسبب حوادث أمنية **

تسرب البيانات مشكلة الأمان الأكثر شيوعًا التي **يتسبب فيها غالبًا الموظفون** (22%) والمهاجمون (23%).*

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 أمان تقنية المعلومات

يعد Kaspersky Security Awareness حلاً مُثبتًا وفعالاً ويتمتع بسجل حافل من النجاح لفترات طويلة على المستوى الدولي. واستخدمت الشركات من جميع الأحجام هذا الحل لتدريب أكثر من مليون موظف في أكثر من 75 دولة، ويجمع بين أكثر من 25 عامًا من خبرة Kaspersky في مجال الأمن الإلكتروني مع الخبرة الواسعة في تعليم الكبار.

تعزز حلول التدريب التي تتسم بالإثارة والفعالية العالية وعي الموظفين بالأمن الإلكتروني ليؤدوا جميعًا دورهم في الأمان عبر الإنترنت الشامل لمؤسستك. نظرًا لأن التغييرات المستدامة في السلوك تستغرق وقتًا، فإن نهجنا يتضمن بناء دورة تعلم مستمر متعددة المكونات.

دورة التعلم المستمر

1 المشاركة / التحفيز
- لماذا أحتاج هذا؟
- الإدراك

2 نقطة البداية
- هل أنا على علم بالموقف؟
- ماذا أعرف وأين الفجوات؟

3 التعلم
- التعلم المصغر
- التعلم المستمر
- القدرة على التكيف

4 الدمج
- هل فهمت بشكل صحيح؟
- هل أتذكر هذا؟
- هل أتصرف كما ينبغي؟

ميزات البرنامج الأساسية

خبرة كبيرة في مجال الأمن الإلكتروني

تحولت أكثر من 25 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.

* "اقتصاديات أمان تقنية المعلومات لعام 2022"، شركة Kaspersky

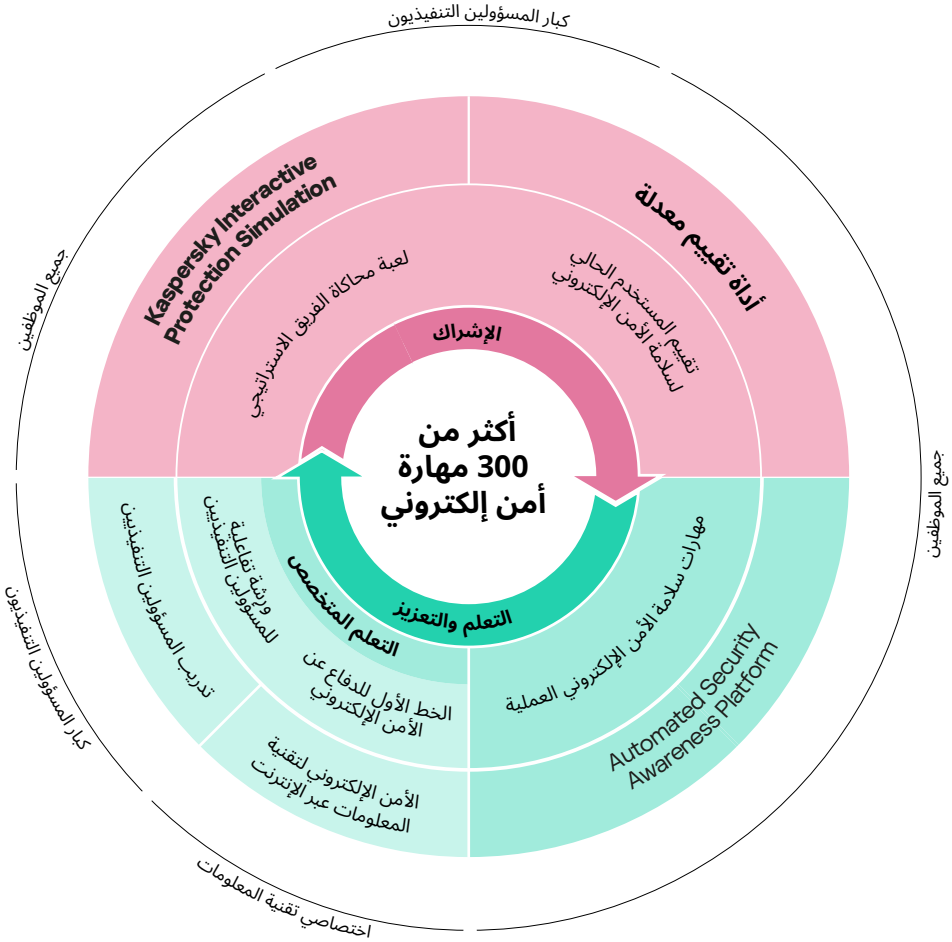
** تقرير "اقتصاديات أمان تقنية المعلومات لعام 2021"، شركة Kaspersky.

*** "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



يرتكب الموظفون الأخطاء، وتخسر المؤسسات الأموال...

52.887 دولارًا أمريكيًا
لكل مؤسسة
متوسط تكلفة الهجوم الإلكتروني الناجم عن الاستخدام غير المناسب لموارد تقنية المعلومات من قِبل الموظفين*

%30
من اختراقات البرامج الضارة
تحدث عبر رسائل البريد الإلكتروني التي تحتوي على روابط ومرفقات مزيفة**

%79
من الموظفين
اعترفوا بالمشاركة في نشاط واحد على الأقل محفوف بالمخاطر خلال عام على الرغم من إدراكهم للمخاطر***

164 دولارًا أمريكيًا
لكل سجل
متوسط التكلفة العالمية للانتهاكات التي تنطوي على ما بين 2200 و102000 سجل****

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

* "اقتصاديات أمان تقنية المعلومات لعام 2022"، شركة Kaspersky
** تقرير تحقيقات اختراق البيانات، 2022
*** "Balancing Risk, Productivity, and Security"، Delinea 2021
**** تكلفة اختراق البيانات، 2022. IBM
***** Capgemini "فجوة المواهب الرقمية"

حلول Kaspersky Security Awareness

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

يمثل حل KIPS لعبة جماعية تفاعلية مدتها ساعتين 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.

يتوفر حل KIPS في شكلين

ينشئ خيار KIPS Live الشهير جدًا جوًا لا يوصف من الإثارة والحماس بفضل القدرة التنافسية المباشرة في الموقع. وهو أداة رائعة للمشاركة وبناء ثقافة الأمن الإلكتروني داخل المؤسسة.

في إصدار KIPS Online، يستطيع المستخدمون التفاعل مع عدد كبير من المشاركين من أي مكان. وهذا الإصدار مثالي للمؤسسات العالمية أو الأنشطة العامة، ويمكن دمج KIPS Online مع KIPS Live لإضافة فرق بعيدة إلى الحدث الذي يجري تنفيذه في الموقع.

- حتى 300 فريق (= 1000 متدرب) في وقت واحد من أي مكان.
- تستطيع الفرق المختلفة اختيار واجهة اللعبة بلغات مختلفة.
- يستطيع العملاء تخصيص السيناريوهات المُثبتة مسبقًا من خلال تحديد عدد وأنواع الهجمات في اللعبة من المكتبة.
- توجد فائدة أخرى للنسخة المتاحة عبر الإنترنت هي الحصول على إحصائيات عن اختيارات اللاعبين، والحصول على بيانات عن تصرفات الفرق في مواقف معينة، والحصول على معيار قياسي لتصرفات اللاعب فيما يتعلق باللعبة السابقة.

KIPS للمؤسسات

يستطيع العملاء الذين يمتلكون ترخيصًا يسمح لهم بالتدريب على KIPS بقدر ما يحلو لهم خلال فترة الترخيص تغيير الإعدادات المحددة مسبقًا، أو تخصيص سيناريو اللعبة في كل مرة يلعبون فيها، واختيار ودمج هجمات مختلفة من المكتبة. وتُغيّر هذه الوظيفة اللعبة في كل مرة، مما يجعلها أكثر إثارة.

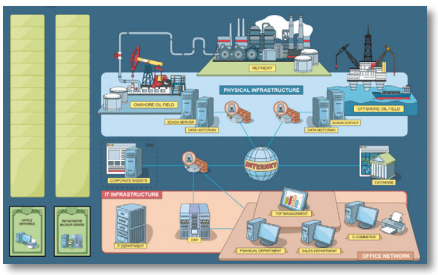
المشاركة والتحفيز

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.

%76 من الرؤساء التنفيذيين يعترفون بتجاوز بروتوكولات الأمان لإنجاز شيء ما بصورة أسرع والتضحية بالأمان من أجل السرعة*.

%62 من المديرين يعترفون بأن سوء التواصل فيما يتعلق بأمان تكنولوجيا المعلومات داخل مؤسساتهم أدى إلى حادثة أمن إلكتروني واحدة على الأقل**

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



* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritysgreatest-insider-threat-is-in-thec-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speakfluent-infosec-2023/

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.

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.

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.

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. تبني المنصة نفسها جدولاً تعليميًا لكل مجموعة من الموظفين، وذلك لتوفير التعلم على فترات زمنية الذي يتم تقديمه تلقائيًا من خلال مزيج من تنسيقات التدريب.
- **سهولة الاستخدام للمسؤولين**.....: تتوافر إدارة المنصة بطريقة مريحة وفعالة بفضل المزامنة مع AD (Active Directory) SSOg (تسجيل الدخول الفردي) Open APIg (القدرة على التفاعل مع حلول الجهات الخارجية) ولوحة معلومات سهلة الاستخدام والإعداد عبر الإنترنت أثناء الزيارة الأولى وقسم للأسئلة الشائعة والنصائح.
- **والمتدربين**.....: يتم توفير عملية تعلم ممتعة ومثيرة وفعالة عن طريق هيكل الدروس الواضح والدروس الصغيرة والأمثلة من الحياة الواقعية والواجهة سهلة الاستخدام وتذكيرات البريد الإلكتروني والقدرة على العودة وتكرار الدروس إذا لزم الأمر والواجهة المتوافقة مع الكمبيوتر الشخصي والهاتف المحمول.

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

الموضوعات التي تغطيها ASAP:

- كلمات المرور والحسابات
- البريد الإلكتروني
- مواقع الويب والإنترنت
- وسائل التواصل الاجتماعي وتطبيقات المراسلة
- أمان الكمبيوتر الشخصي
- الأجهزة المحمولة
- حماية البيانات السرية
- التوجيه العام لحماية البيانات
- الأمن الإلكتروني في القطاع الصناعي
- البيانات الشخصية
- أمان البطاقات البنكية ومعيار أمان بيانات صناعة بطاقات الدفع (PCI DSS)
- نشر المعلومات الشخصية للغير بغرض خبيث على الإنترنت
- أمان العملات المشفرة
- أمان المعلومات عند العمل عن بُعد
- القانون الاتحادي الروسي 152-FZ

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/ar - شاهد بنفسك مدى سهولة إعداد وإدارة برنامجك التدريبي للتوعية بأمن الشركة.

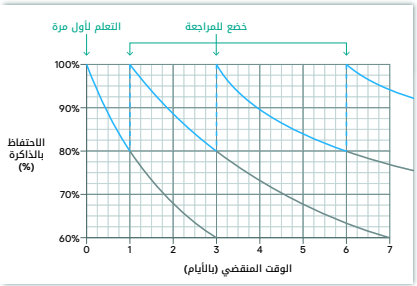
الدمج

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.

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



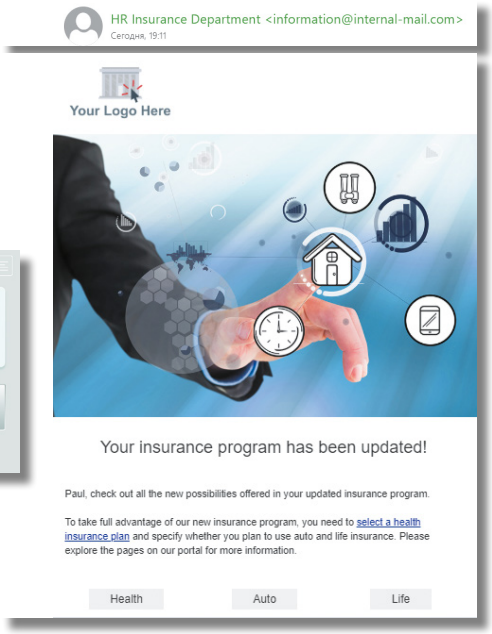
- **كفاءة التعلم المحددة مسبقًا:** تم تنظيم محتوى البرنامج لدعم التعلم التراكمي مع التعزيز المستمر. وتعتمد المنهجية على خصائص الذاكرة البشرية لضمان الاحتفاظ بالمعرفة وتطبيق المهارات اللاحق.
- **التخصيص:** من السهل تغيير مظهر برنامج التدريب - يمكنك استبدال شعار Kaspersky ووضع شركتك بدلاً منه في بوابة المسؤولين والمتدربين ورسائل البريد الإلكتروني الخاصة بالمنصة، وتخصيص الشهادات وإضافة محتوى شخصي إلى أي درس.
- **التعلم المرن:** حدد خيار تدريب الموظفين المناسب لك: تعيين دورة Express أساسية للموظفين تساعدك على تلبية المتطلبات التنظيمية للتدريب على الأمن الإلكتروني بسرعة أو تحديث معرفتهم، أو اختيار دورة أساسية 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، ويمكن إدارة العديد من الشركات من حساب واحد.

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.

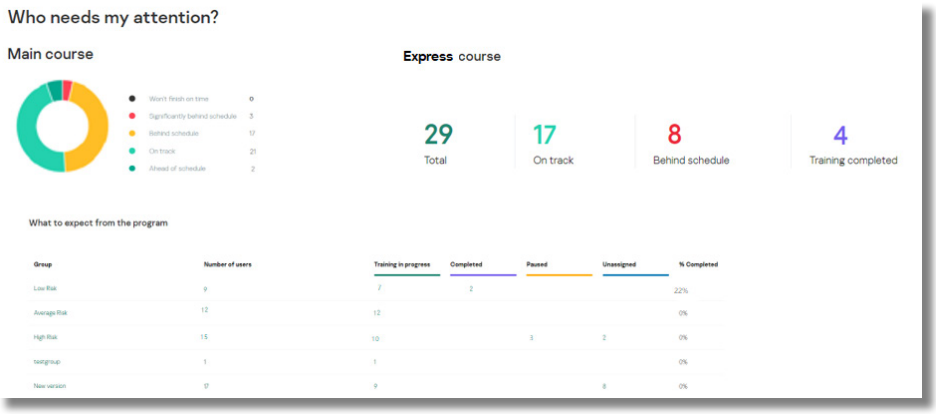
الدروس التفاعلية

محاكاة هجمات التصيد الاحتيالي



تتبع النتائج

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



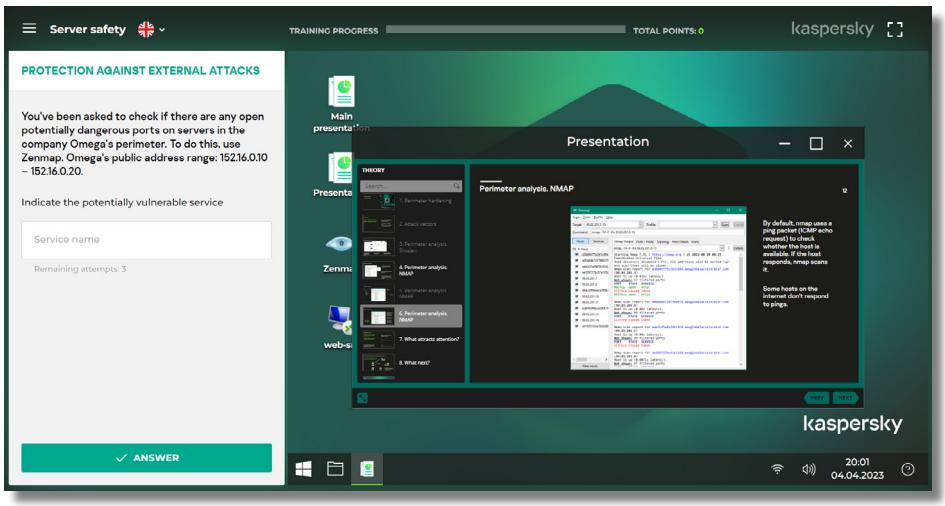
الأمن الإلكتروني لتقنية المعلومات عبر الإنترنت: خط الدفاع الأول ضد الحوادث

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 الأمن الإلكتروني لتقنية المعلومات عبر الإنترنت (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 المتخصص

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

تدريب المسؤولين التنفيذيين:

في برنامجنا التدريبي للمسؤولين التنفيذيين، يتعلم قادة الأعمال وكبار المديرين أساسيات الأمن الإلكتروني من خلال ورشة تفاعلية يقودها المدرب أو دورة عبر الإنترنت تمنحهم فهمًا أفضل للتهديدات الإلكترونية وكيفية الحماية منها.

يتم إيلاء اهتمام خاص بالجوانب المالية للأمن الإلكتروني وجدوى الاستثمار فيه، مما يمنح المديرين التنفيذيين فهمًا أفضل للعلاقة بين الأمن الإلكتروني وكفاءة الأعمال. وسيكتشفون ما يعنيه مشهد التهديدات الحالي لعملك، والإجراءات التي يجب اتخاذها في حالة وقوع هجوم إلكتروني، بالإضافة إلى مجموعة من المعلومات الأخرى المثيرة وذات الصلة والمفيدة.

لتحقيق أقصى استفادة من هذه الدورة، من المثالي دمجها مع تدريب KIPS. ويمكن الحصول على تدريب المسؤولين التنفيذيين قبل تدريب KIPS أو بعده، اعتمادًا على نهج الوعي الأمني.

إشراك المديرين التنفيذيين

يُعد كبار المديرين من بين أكثر الأهداف المرغوبة لمجرمي الإنترنت، ومع ذلك فهم يمثلون غالبًا تحديًا حقيقيًا للمدربين. 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.

* تتاح القائمة الحالية للوحدات على cito-training.com

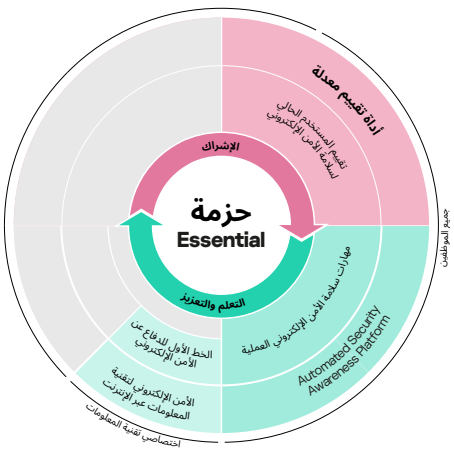
Kaspersky Security Awareness: طرق مرنة للتدريب

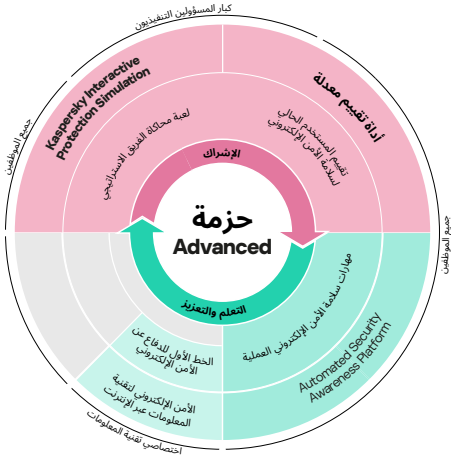
تغطي حلول التدريب من Kaspersky كل مستوى من مستويات شركتك ويمكن استخدامها بمفردها أو بشكل جماعي. ونيسر أيضًا بدء استخدام حزم مصممة خصيصًا لاحتياجاتك.

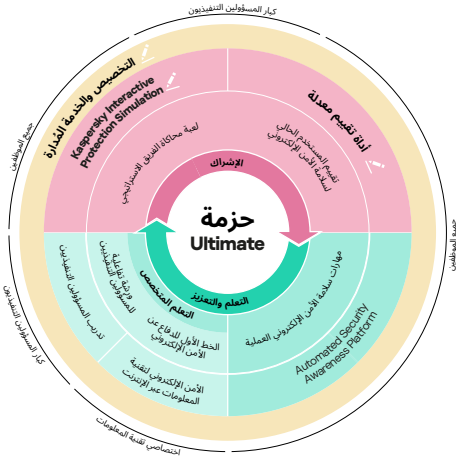
يضمن أقصى قدر من الوعي بالأمن الإلكتروني، ويتضمن ميزات التخصيص والخدمات المدارة، بحيث يتمتع المديرون التنفيذيون بدراية جيدة بسيناريوهات التهديدات، ويتمتع الموظفون بمهارات تلقائية للأمان عبر الإنترنت، ويدعمك موظفو تقنية المعلومات المتخصصون بصفتك خط الدفاع الأول.

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

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.







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

me.kaspersky.com

© 2023 AO Kaspersky Lab.
العلامات التجارية المسجلة وعلامات الخدمة
مملوكة لأصحابها المعنيين.

kaspersky