Kaspersky ASAP: Automated Security Awareness Platform

مثيرة للموظفين،
فعالة للمديرين

إصدار تجريبي مجاني
k-asap.com/ar

Kaspersky
Automated Security
Awareness Platform

واجهوا المستقبل بأمان kaspersky

Kaspersky ASAP: Automated Security Awareness Platform

تنجم نسبة 82% من جميع الحوادث الإلكترونية عن خطأ بشري، وينتج عن ذلك خسائر بالملايين للشركات. ولم يتم تصميم برامج التدريب التقليدية للتعامل مع هذه المشكلة، وهناك حاجة إلى نهج جديد. رحب بحل Kaspersky ASAP.

يمثل الخطأ البشري أكبر خطر إلكتروني

%79
من الموظفين
يعترفون بالمشاركة في نشاط واحد على الأقل محفوف بالمخاطر خلال العام السابق على الرغم من إدراكهم للمخاطر*

%51
من الموظفين
يعتقدون أن أقسام تقنية المعلومات في شركاتهم يجب أن تكون مسؤولة مسؤولية كاملة عن منع وقوع أصحاب العمل ضحية للهجمات الإلكترونية*

%55
من المؤسسات
تُبلغ عن تهديدات ناجمة عن استخدام الموظفين غير المناسب لتقنية المعلومات**

%51
من الشركات الصغيرة
تعرضت لحادث أمني بسبب انتهاك الموظفين لسياسات أمن تقنية المعلومات**

%26
من الموظفين
يقولون إن بريدهم الإلكتروني الشخصي يستخدم كلمة مرور نفسها الخاصة بحساب العمل***

معوقات إطلاق برنامج توعية أمنية ناجح

تحرص الشركات على تنفيذ برامج التوعية الأمنية، لكن الكثير منها لا ترضى عن العملية ولا النتائج. وتجد الشركات الصغيرة والمتوسطة على وجه الخصوص هذه العملية صعبة، لأنها لا تمتلك الخبرة أو الموارد اللازمة.

عبء على المسؤولين	غير كافية للطلاب
كيف تنشئ برنامجًا وتحدد الأهداف؟	يُنظر إليها كعملية شاقة وصعبة ومملة وغير ذات صلة.
كيف تدير مهام التدريب؟	تتعلق بالكامل بالأمور المحظورة وليس بتعليم طريقة التصرف
كيف تتحكم في التقدم	لا يتم الاحتفاظ بالمعرفة
كيف نتأكد من مشاركة موظفينا بشكل كامل؟	القراءة والاستماع ليسا بنفس فعالية العمل

* Balancing Risk, Productivity, and Security."Delinea, 2021

** "اقتصاديات أمان تقنية المعلومات 2022"، Kaspersky

*** https://www.beyondidentity.com/blog/password-sharing-work

تدريب فعال وسهل الإدارة للمؤسسات من أي حجم

نقدم لكم "Kaspersky Automated Security Awareness Platform (ASAP)" التي تعد بمثابة قلب مجموعة التدريب على الوعي الأمني من Kaspersky. وتعد المنصة أداة عبر الإنترنت تبني المهارات القوية والعملية في مجال الحفاظ على الصحة الإلكترونية للموظفين على مدار العام.

لا يتطلب إطلاق المنصة وإدارتها موارد أو ترتيبات خاصة، وتتضمن مساعدة مضمنة في كل خطوة من خطوات رحلة التعلم نحو إنشاء بيئة إلكترونية آمنة للشركات.

محتوى هادف لا يمكنك تجاهله

تعد الكفاءة أحد أهم المعايير عند اختيار برنامج التوعية، ومع ASAP، يتم تضمين الكفاءة في محتوى التدريب وإدارته. ويعتمد المحتوى على الخبرة المتراكمة **لأكثر من 25 عامًا في مجال الأمن الإلكتروني** التي يتم التعبير عنها في نموذج الكفاءة الذي يضم أكثر من **350 مهارة عملية وأساسية في مجال الأمن الإلكتروني** يجب أن يتمتع بها جميع الموظفين.

ثقّف موظفيك عن الأمن الإلكتروني.
غيّر مواقفهم وسلوكياتهم ووفر الحماية لعملك وأنظمة تقنية المعلومات.

التدريب الفعال

متسق	- محتوى منظم ومدروس جيدًا – دروس تفاعلية وتعزيز مستمر واختبارات ومحاكاة هجمات التصيد الاحتيالي لضمان تطبيق المهارات يأخذ محتوى وهيكل المواد التدريبية في الاعتبار خصوصيات الذاكرة البشرية، وقدرتنا على استيعاب المعلومات والاحتفاظ بها.
عملي ومثير	- ذو صلة بحياة العمل اليومية للموظفين – مهارات يمكن استخدامها على الفور أمثلة من مواقف الحياة الواقعية التي يستطيع الموظفون ربطها بأنفسهم شخصيًا للمساهمة في مشاركة أفضل للمتعلمين، مما يساعد على الاحتفاظ بالمعلومات.
إيجابي	- يؤدي دورًا استباقيًا في السلوك الآمن - يشرح "السبب" و"الطريقة" بدلاً من مجرد الأمور المحظورة من الممكن أن تتسبب القواعد والقيود الكثيرة في عدم الرضا وعدم المشاركة، في حين تساهم التفسيرات والمبادئ التي تتوافق مع طريقة تفكير الأشخاص بشكل طبيعي في التبني وتغيير السلوك.

سهولة الإدارة

سهولة الإدارة	– ترتقي إدارة التعلم المؤتمتة بالكامل بكل موظف للوصول إلى مستوى المهارات المناسب لملف تعريف مخاطره دون أي تدخل من مسؤول المنصة – تتمتع بالقدرة على إدارة المنصة بطريقة مريحة وفعالة بفضل المزامنة مع AD (Active Directory) وSSO (تسجيل الدخول الفردي) وOpen API (القدرة على التفاعل مع حلول الجهات الخارجية) والإعداد عبر الإنترنت أثناء الزيارة الأولى وقسم للأسئلة الشائعة والنصائح.
سهولة التحكم	لوحة معلومات "شاملة" وتقارير قابلة للتنفيذ: - تقارير عن تقدم الدرس - تقارير عن الاختبارات وهجمات التصيد التي يتم محاكاتها
سهولة المشاركة	ترسل المنصة تلقائيا الدعوات والتذكيرات، بالإضافة إلى التقارير إلى الطلاب والمسؤولين.

إدارة ASAP: البساطة من خلال الأتمتة الكاملة

ابدأ برنامجك في 4 خطوات بسيطة

1

إضافة المستخدمين

استخدم **مزامنة AD** أو يمكنك تحميل ملف بتنسيق xlsx. أو إضافته يدويًا

2

تقسيم المستخدمين إلى مجموعات

يمكنك تقسيم المستخدمين يدويًا أو باستخدام القواعد بناءً على المستوى المستهدف المطلوب

3

بدء التدريب

يمكنك تقسيم المستخدمين يدويًا أو استخدم القواعد بناءً على المستوى المستهدف المطلوب وتحديد تاريخ البدء لكل مجموعة

4

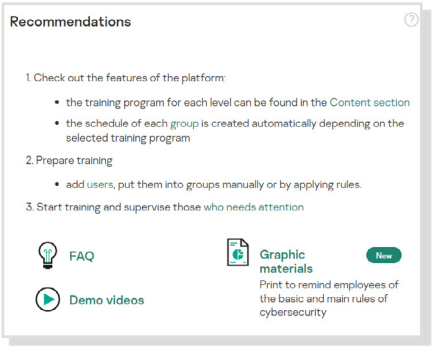
إدارة التدريب الآلي بواسطة ASAP

ينشئ ASAP جدولاً زمنيًا لكل مجموعة، للدعوات والتذكيرات والاتصالات الأخرى - يحدث كل شيء تلقائيًا

نهج تدريب جديد ومُحسن

يُغيّر Kaspersky ASAP الطريقة التي نقدم بها محتوى تعلم الأمن الإلكتروني. يمكنك الآن اختيار ما إذا كنت تريد تعيين **دورة Express (السريعة)** أساسية للموظفين ستساعدك على تلبية المتطلبات التنظيمية للتدريب على الأمن الإلكتروني بسرعة، أو تحديث معرفتهم، أو اختيار **الدورة الرئيسية** مقسمة حسب مستويات التعقيد

يوجد كل ما تحتاجه لبدء عملية التعلم على الصفحة الرئيسية للمسؤول مثل الإعداد أثناء تسجيل الدخول لأول مرة والتوصيات والأسئلة الشائعة ومقاطع الفيديو التوضيحية وشرح كيفية عمل المنصة من منظور المسؤول والمستخدم



موضوعات الدورة

موضوعات الدورة

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

تنقسم الموضوعات إلى مجموعات كبيرة، تغطي العديد من مفاهيم أمان تقنية المعلومات*.

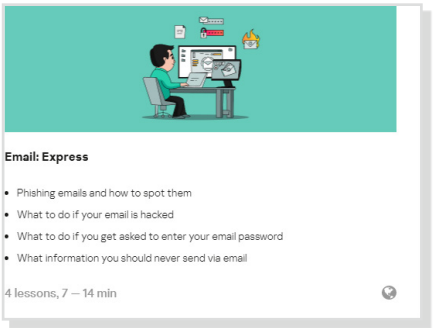
#كلمات المرور #التصيد الاحتيالي #حسابات الشركات #الرسائل الخطيرة #بطاقات البنك #برامج طلب الفدية #الهندسة_الاجتماعية #الملفات الخطيرة #العمل مع المستعرضات #أخلاقيات الشركة #برنامج مكافحة الفيروسات #البرامج الضارة #التطبيقات #المستعرض #المعلومات السرية #تخزين المعلومات #إرسال المعلومات #البيانات الشخصية #الإنترنت والقانون #التشريعات الأوروبية #الأعمال #الروابط الخطيرة #مواقع الويب المزيفة #مواقع برامج طلب الفدية #النسخ الاحتياطي #بيانات الهاتف المحمول #التشفير #الخدمات السحابية #التجسس الصناعي #معيار أمان بيانات صناعة بطاقات الدفع (PCI DSS) #المصادقة ثنائية العوامل #البصمة الرقمية #ملفات التورنت #انتحال الشخصية الإلكتروني #الهجوم المستهدف #التجزئة #الرموز المميزة #أقفال النمط #التعدين #المراقبة الأسرية

* للحصول على أحدث قائمة بالموضوعات والمفاهيم، يرجى زيارة k-asap.com

يحتوي كل موضوع على عدة مستويات، توضح بالتفصيل مهارات الأمان المحددة. يتم تحديد المستويات وفقًا لدرجة الخطر التي تساعد في القضاء عليها - على سبيل المثال، يكفي المستوى 1 عادة للحماية من أبسط الهجمات وكذلك الهجمات الجماعية. ويجب دراسة المستويات الأعلى لتعلم كيفية الحماية من الهجمات الأكثر تطورًا واستهدافًا.

مثال: المهارات التي تم التدريب عليها في موضوع "مواقع الويب والإنترنت"

مبتدئ تجنب الهجمات الجماعية (الرخيصة والسهلة)	**أساسي** تجنب الهجمات الجماعية على ملف تعريف معين	**متوسط** تجنب الهجمات المركزة المعدة جيدًا	**متقدم*** تجنب الهجمات المستهدفة
23 مهارة، تشمل ما يلي: - التعرف على النوافذ المنبثقة الزائفة - الانتباه إلى عمليات إعادة التوجيه - التمييز بين روابط التنزيل الأصلية والزائفة - التعرف على الملفات القابلة للتنفيذ الموجودة على الويب - القدرة على تحديد صحة ملحق المستعرض	**34 مهارة، تشمل ما يلي:** - إدخال البيانات فقط في المواقع التي تمتلك شهادة SSL صالحة - استخدام كلمات مرور مختلفة لعمليات التسجيل المختلفة - التعرف على المواقع الزائفة عن طريق عدد من العلامات - تجنب الروابط الرقمية - التعرف على عناوين روابط الشبكة غير الصالحة من خلال المجالات الفرعية المزيفة	**12 مهارة، تشمل ما يلي:** - التحقق من روابط المشاركة قبل الإرسال - استخدام البرامج من الشركات المصنعة الموثوقة فقط لمواقع التورنت - تنزيل المحتوى القانوني فقط من مواقع التورنت - مسح ملفات تعريف الارتباط الخاصة بالمستعرض بانتظام	**13 مهارة، تشمل ما يلي:** - التعرف على الروابط المزيفة المعقدة (بما في ذلك الروابط التي تشبه مواقع الويب الخاصة بشركتك، والروابط التي تتضمن إعادة التوجيه) - فحص المواقع باستخدام الأدوات المساعدة الخاصة - التعرف على ما إذا كان المستعرض يقوم بالتعدين - تجنب مواقع تحسين محركات البحث باستخدام أساليب القبعة السوداء
	+ تعزيز المهارات الأولية	+ تعزيز المهارات السابقة	+ تعزيز المهارات السابقة

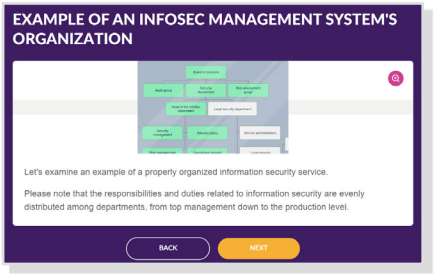


دورة ASAP Express

نسخة قصيرة من التدريب بتنسيق صوتي ومرئي. يحتوي كل موضوع من مواضيع الأمن الإلكتروني على عدة دروس قصيرة لمساعدة المستخدم على فهم مهارات الأمن الإلكتروني الأساسية.

- النظرية التفاعلية
- مقاطع فيديو
- الاختبارات

لا يتم تضمين هجمات التصيد الاحتيالي التي يتم محاكاتها في مسار التعلم، لكن يمكن تعيينها بشكل منفصل من قبل المسؤول.

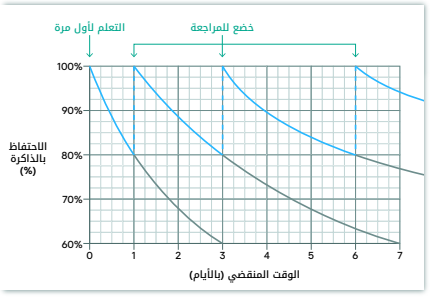


دورة ASAP الأساسية

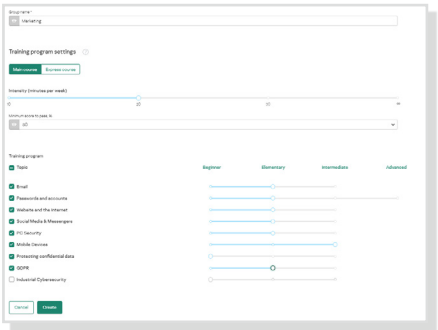
يعتمد التدريب على خصائص الذاكرة البشرية:

- محتوى متعدد الوسائط:
  - تتضمن كل وحدة: درسًا تفاعليًا والتعزيز والتقييم (اختبار ومحاكاة هجوم تصيد احتيالي، عند اللزوم)
  - تدعم جميع عناصر التدريب المهارة المعينة التي يتم تدريسها في كل وحدة، بحيث يتم استيعاب المهارات حقًا وتصبح جزءًا من السلوك الجديد المطلوب.
- التعلم باستخدام فترات زمنية:
  - تتبع عناصر التدريب بعضها البعض على فترات زمنية معينة، مما يلغي الحاجة للنقر البسيط خلال الدروس ويحسن الاحتفاظ بالذاكرة. وتعتمد الفترات الزمنية على دراسة "منحنى النسيان" لإبنغهاوس
  - يبني التكرار عادات آمنة ويمنع النسيان
- يضمن المحتوى المتوازن والمنظم ذي الصلة بالحياة الواقعية الكفاءة:
  - تتضمن أمثلة من الحياة الواقعية تسلط الضوء على الأهمية الشخصية للأمن الإلكتروني للموظفين
  - تركز المنصة على مهارات التدريس، وليس فقط على توفير المعرفة، لذا فإن التمارين العملية والمهام المتعلقة بالموظفين مدرجة في صميم كل وحدة.

"منحنى النسيان" لإبنغهاوس



مسار التعلم المرن

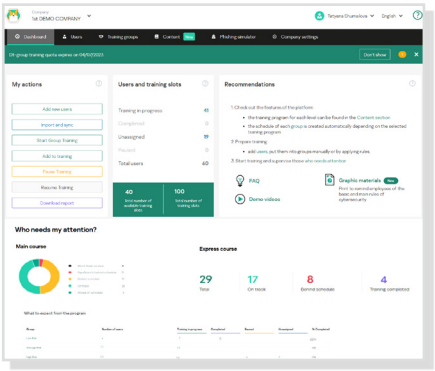


تعلم مرن

يتسم نطاق التدريب بالمرونة التامة، مع الاحتفاظ بمزايا إدارة التعلم الآلي المتسلسل. ولكل مجموعة تدريب يمكنك اختيار ما يلي:

- الدورة الرئيسية أو دورة Express، أو مزيج من الاثنتين؛
- مواضيع للتدريب في الدورة الرئيسية و/أو دورة Express التي يحتاج الطلاب في المجموعة إلى تعلمها؛
- المستوى المستهدف الذي تريد أن يحققه الطلاب لكل موضوع مختار في الدورة الرئيسية.

سيتم بناء مسار التعلم تلقائيًا بواسطة المنصة لكل مجموعة من المتعلمين بناءً على هذه الإعدادات.



تنفيذ كل شيء من لوحة المعلومات

- يمكنك تنفيذ كل ما تحتاجه للتحكم في التدريب وإدارته من لوحة المعلومات: الإحصاءات وملخصات أنشطة المستخدمين وتقدمهم وفترات التدريب والتدريب الجماعي واقتراحات عن كيفية تحسين النتائج. ويمكنك تنزيل التقارير بنقرة واحدة وتكوين تكرار التقارير هناك أيضًا.

حرية الأداء

- يستطيع الموظفون الدراسة في أي وقت مناسب لهم، ومن أي جهاز، مع تصميم ASAP المتوافق مع الهاتف المحمول الذي يجعل التعلم سهلاً ومريحًا.
- يستطيع المستخدمون الوصول إلى بوابة التدريب من الروابط المخصصة التي يتم توفيرها في دعوة التدريب أو عبر رابط واحد لجميع المستخدمين الذين يستخدمون تقنية تسجيل الدخول الأحادي (SSO) في حالة إعدادها بواسطة المسؤول.

التخصيص

يستطيع المسؤول تغيير مظهر البرنامج بسهولة:

- استبدال شعار Kaspersky بشعار شركتك في لوحة الإدارة وبوابة التدريب ورسائل البريد الإلكتروني الخاصة بالمنصة؛
- تخصيص الشهادات؛
- إضافة محتوى شخصي إلى أي درس.

التكامل

يمكنك استخدام Open API للتفاعل مع حلول الجهات الخارجية - يعمل Open API عبر بروتوكول HTTP ويقدم مجموعة من طرق الطلب / الاستجابة.

يتكامل ASAP مع منصتي Kaspersky KUMA وXDR:
- يستطيع المسؤول رؤية حدث في XDR واتخاذ الرد المناسب، بما في ذلك تعيين تدريب في ASAP
- الإثراء التلقائي لبطاقات الحوادث بمعلومات عن مستوى وعي المستخدم المهاجم

التوطين

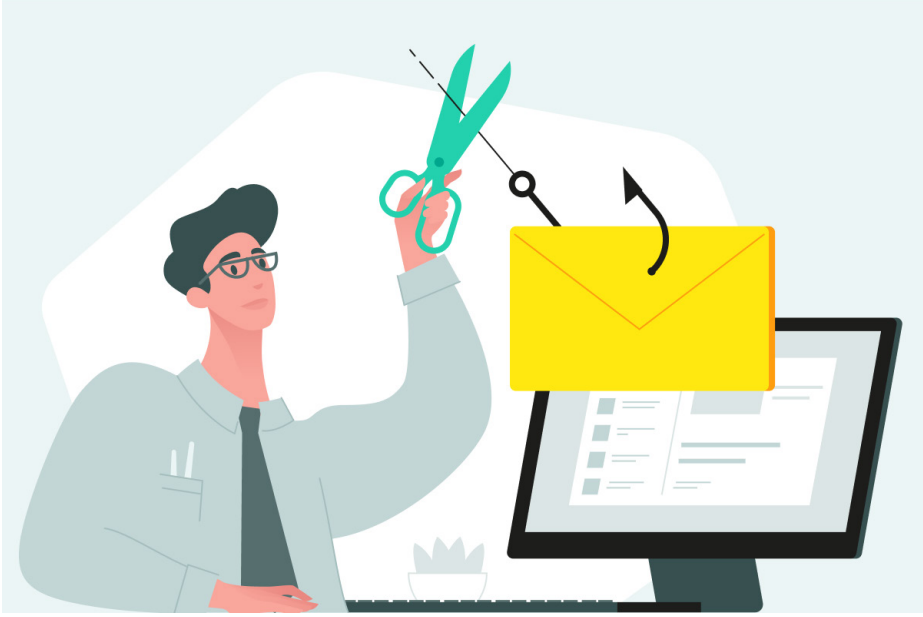
يتاح ASAP باستخدام 25 لغة*. ويتجاوز التوطين في ASAP مجرد الترجمة - لا تتم ترجمة النصوص والعناصر المرئية إلى لغات مختلفة فحسب، بل يتم تعديلها أيضًا لتعكس الثقافات المختلفة والمواقف المحلية.

* تتوافر القائمة الحالية للغات على k-asap.com

محاكاة حملات التصيد الاحتيالي

يتم تقديم حملات التصيد الاحتيالي بالإضافة إلى التدريب الرئيسي. وهي تختبر المهارات العملية للموظفين في تجنب هجمات التصيد الاحتيالي، وتساعد مديري التدريب على تحديد الثغرات في معرفة المستخدمين بسرعة وتشجع على المزيد من الدراسة للمواضيع المزعجة. وتعد حملات التصيد الاحتيالي أيضًا أداة ممتازة لتعليم الموظفين كيفية التعرف على العلامات الضارة المحتملة، ووضع معرفتهم موضع التنفيذ.

تأتي المنصة مزودة بقوالب بريد إلكتروني جاهزة تحتوي على أمثلة للتصيد الاحتيالي يمكن إرسالها إلى المستخدمين بجميع اللغات المتاحة. ويتم تحديث القوالب وإضافة قوالب جديدة بانتظام. ويمكنك أيضا إنشاء رسائل بريد إلكتروني مخصصة بناءً على قوالب محددة مسبقًا.

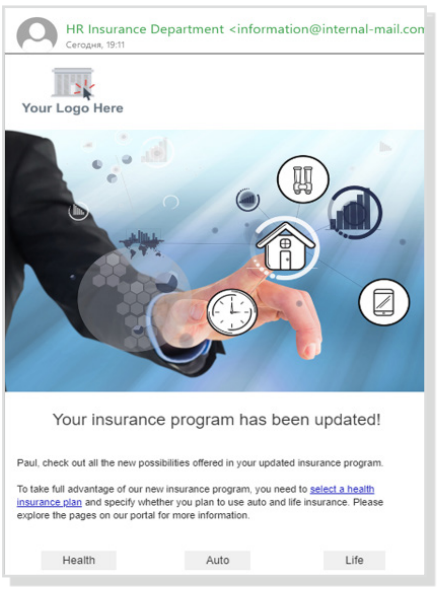


جرّب محاكاة هجوم تصيد احتيالي قبل بدء التدريب - تحقق من مرونة موظفيك! وسوف يساعد الموظفين والإدارة على رؤية فوائد التدريب.

يستطيع الموظفون أيضًا إثبات فهمهم للموضوع من خلال عدم خداعهم عن طريق هجوم التصيد الاحتيالي الذي تتم محاكاته، ومن خلال الإبلاغ عن رسائل التصيد الاحتيالي عبر أداة "الإبلاغ عن التصيد الاحتيالي".

توضح أداة "الإبلاغ عن التصيد الاحتيالي" مستوى وعي الموظفين، وتزيل البريد الإلكتروني من صندوق البريد الوارد، وترسل الرسائل ليس فقط إلى مسؤول المنصة، لكن أيضًا إلى قسم تقنية المعلومات / فرق أمان تقنية المعلومات، لمساعدة المؤسسات على تحسين مستويات اكتشاف التصيد الاحتيالي والاستجابة له.

مثال على قالب محاكاة التصيد الاحتيالي القابل للتحرير والملاحظات



Kaspersky Security Awareness – نهج جديد لإتقان مهارات أمان تقنية المعلومات

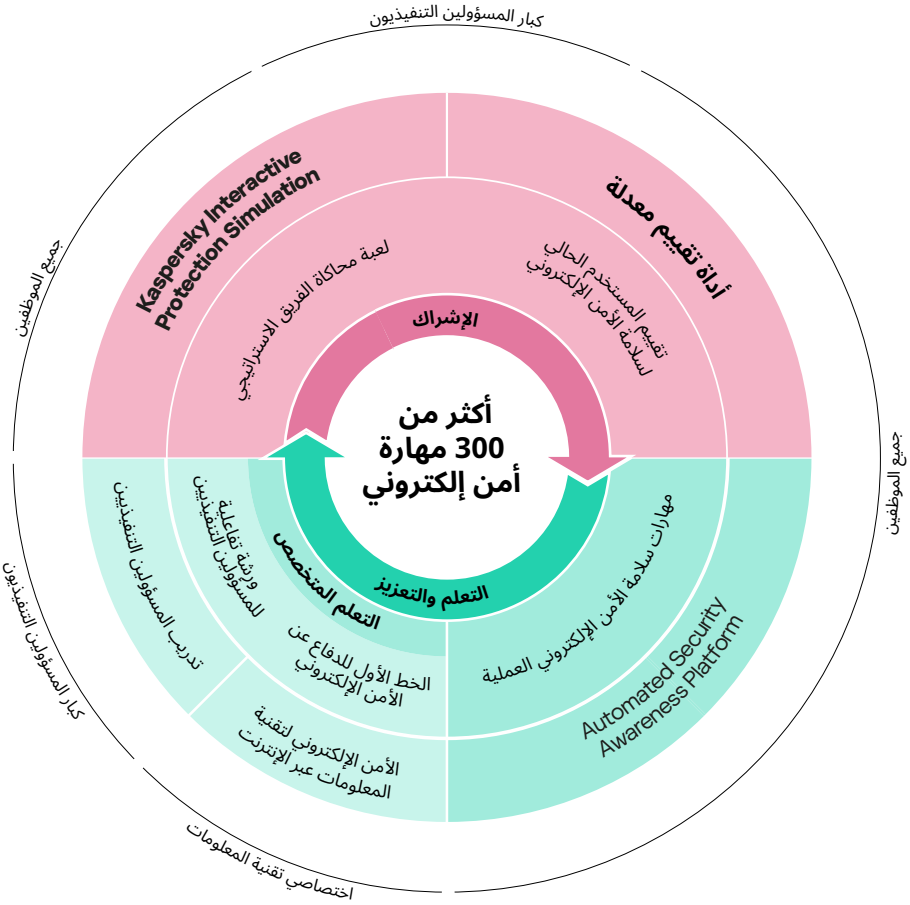
ASAP منتج أساسي في مجموعة Kaspersky للتوعية الأمنية.

حل تدريب واحد مرن للجميع

يتمتع حل Kaspersky Security Awareness بسجل حافل من النجاحات على المستوى الدولي. وتستخدمه الشركات من جميع الأحجام **لتدريب أكثر من مليون موظف في أكثر من 75 دولة**، ويجمع بين أكثر من 25 عامًا من خبرة Kaspersky في مجال الأمن الإلكتروني والخبرة الواسعة في تعليم الكبار.

تعرض المحفظة مجموعة خيارات تدريب مثيرة تزيد من وعي موظفيك بالأمن الإلكتروني على كل المستويات، وتمنحهم القدرة على أداء دورهم في الأمن الإلكتروني الشامل لمؤسستك.

نظرًا لأن التغييرات المستدامة في السلوك تستغرق وقتًا، فإن نهجنا يتضمن بناء دورة تعلم مستمر متعددة المكونات. ويُشرك التعلم القائم على الألعاب الإدارة العليا، ويحولهم إلى مؤيدين لمبادرات الأمن الإلكتروني وداعمين لبناء ثقافة سلوك الأمن الإلكتروني. ويساعد التقييم عن طريق ألعاب المحاكاة على تحديد الفجوات في معرفة الموظفين وتحفيزهم على المزيد من التعلم، بينما تزودهم المنصات والمحاكاة عبر الإنترنت بالمهارات المناسبة وتعزيزها.



ميزات البرنامج الأساسية

خبرة كبيرة في مجال الأمن الإلكتروني
تحولت أكثر من 25 عامًا من الخبرة في مجال الأمن الإلكتروني إلى مهارات أمان إلكتروني تتواجد في قلب منتجاتنا

تدريب يُغير سلوك الموظفين على كل مستوى في مؤسستك
يوفر تدريبنا عن طريق 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.

إصدار تجريبي مجاني من تدريب Kaspersky ASAP: k-asap.com/ar
الأمن الإلكتروني للمؤسسات: www.kaspersky.com/enterprise
الوعي الأمني من Kaspersky: me.kaspersky.com/awareness
أخبار أمن تقنية المعلومات: business.kaspersky.com

me.kaspersky.com

kaspersky واجهوا المستقبل بأمان

2023 AO KASPERSKY LAB. العلامات التجارية المسجلة وعلامات الخدمة مملوكة لأصحابها المعنيين.