توعية الأمن السيبراني لتعزيز مهارات الحفاظ على السلامة والأمان الرقمي

AGILE LEADERS
Training Center

توعية الأمن السيبراني لتعزيز مهارات الحفاظ على السلامة والأمان الرقمي

نظرة عامة على الدورة:

تدريب توعية الأمن السيبراني: المهارات الرقمية والسلامة الإلكترونية يزود الموظفين بالقدرات الرقمية والسلوكيات الآمنة اللازمة للعمل بثقة في المؤسسات الحديثة. استناداً إلى إطار عمل DigComp 2.2، والإطار العالمي لمحو الأمية الرقمية لليونسكو، ومعايير المهارات الرقمية الأساسية 2026، وإرشادات الوكالة الأوروبية للأمن السيبراني ENISA لتعزيز الوعي السيبراني، يجمع المساق بين تدريب عملي على المهارات الرقمية وتوعية بمخاطر الأمن السيبراني تركز على بيئة العمل.

يتعلم المشاركون كيفية التعرف على التصيد الاحتيالي، والهندسة الاجتماعية، وعمليات الاحتيال عبر الإنترنت، واختراق البريد الإلكتروني التجاري، والخداع المدعوم بالذكاء الاصطناعي. كما يطور مساق توعية الأمن السيبراني ممارسات آمنة لكلمات المرور، والمصادقة متعددة العوامل، والهوية الرقمية، والأجهزة المحمولة، والمنصات السحابية، والعمل عن بُعد. من خلال سيناريوهات تدريب توعية الأمن السيبراني للموظفين، يدرس المشاركون كيف يمكن للإجراءات اليومية مثل فتح المرفقات، ومشاركة الملفات، والانضمام إلى الاجتماعات عبر الإنترنت، أو إدخال المعلومات في أدوات الذكاء الاصطناعي أن تعرض بيانات المؤسسة للخطر.

على عكس مساق توعية الأمن السيبراني التقني البحت، يربط هذا البرنامج تدريب توعية أمن المعلومات بالاتصالات الرقمية، وتقييم المعلومات، والخصوصية، والتعاون الآمن، والاستخدام المسؤول للتكنولوجيا. يتدرب المشاركون على التحقق من الرسائل المشبوهة، وحماية الحسابات، وإدارة الأذونات، والإبلاغ عن الحوادث دون تأخير. وبالتالي، يدعم المساق كلاً من مرونة الأمن السيبراني وإنتاجية مكان العمل. من خلال الجمع بين تدريب توعية الأمن السيبراني في مكان العمل، وتدريب النظافة السيبرانية، وتدريب السلامة عبر الإنترنت، فإنه يمكّن الموظفين من أن يصبحوا مستخدمين أكثر أماناً ونقداً ومسؤولية للتكنولوجيا الرقمية مع المساهمة في ثقافة أمن مؤسسية إيجابية.

الجمهور المستهدف:

- الموظفون الذين يستخدمون أجهزة الكمبيوتر، والأجهزة المحمولة، والبريد الإلكتروني، أو المنصات السحابية
- موظفو الدعم الإداري والمكتبي
- ممثلو خدمة العملاء ومراكز الاتصال
- متخصصو الموارد البشرية والتوظيف
- موظفو المالية والمحاسبة وكشوف المرتبات
- فرق المبيعات والتسويق وتطوير الأعمال
- موظفو المشتريات وسلسلة التوريد
- منسقو المشاريع وقادة الفرق
- الموظفون العاملون عن بُعد والهجينون

AGILE LEADERS
Training Center

الأقسام المستهدفة:

- تكنولوجيا المعلومات وأمن المعلومات
- الموارد البشرية والتعلم والتطوير
- المالية والمحاسبة وكشوف المرتبات
- الإدارة والخدمات المؤسسية
- المبيعات والتسويق والاتصالات
- المشتريات وسلسلة التوريد
- خدمة العملاء ومراكز الاتصال
- الشؤون القانونية والمخاطر والامتثال
- مكاتب إدارة المشاريع
- العمليات ودعم الأعمال

القطاعات المستهدفة:

- الخدمات المصرفية والتأمين والمالية
- المؤسسات الحكومية والقطاع العام
- خدمات الرعاية الصحية والصيدلانية
- مؤسسات التعليم والتدريب
- النفط والغاز والطاقة والمرافق
- الاتصالات والتكنولوجيا
- التجزئة والضيافة والتجارة الإلكترونية
- النقل والطيران والخدمات اللوجستية
- الإنشاءات والهندسة والعقارات
- الخدمات المهنية والاستشارية
- المؤسسات الصناعية والتصنيعية
- المنظمات غير الحكومية والدولية

أهداف الدورة:

بنهاية هذا المساق، سيتمكن المشاركون من:

- شرح التهديدات السيبرانية الشائعة وعواقبها على المؤسسة.
- تطبيق المهارات الرقمية الأساسية بأمان في الأنشطة اليومية لمكان العمل.
- التعرف على رسائل البريد الإلكتروني التصيدية، والمرفقات الضارة، والروابط الخادعة.
- اكتشاف محاولات الهندسة الاجتماعية، وانتحال الشخصية، واختراق البريد الإلكتروني التجاري.
- تحديد علامات التحذير من التصيد الاحتيالي الذي يتم إنشاؤه بواسطة الذكاء الاصطناعي وعمليات الاحتيال المدعومة بالخدع العميقة deepfake.
- إنشاء كلمات مرور أقوى واستخدام مديري كلمات المرور بشكل مناسب.
- شرح كيفية حماية المصادقة متعددة العوامل لحسابات مكان العمل.
- حماية المعلومات الشخصية، ومعلومات العملاء، والمعلومات المؤسسية.
- إدارة الخصوصية، وأذونات التطبيقات، والهويات الرقمية.
- استخدام البريد الإلكتروني، والتخزين السحابي، ومنصات التعاون بشكل أكثر أمانًا.
- تطبيق ممارسات آمنة عند العمل عن بُعد أو استخدام الأجهزة المحمولة.
- تقييم موثوقية المعلومات عبر الإنترنت وتلك التي تم إنشاؤها بواسطة الذكاء الاصطناعي.

منهجية التدريب:

يستخدم المساق منهجية تفاعلية تركز على السلوك، مصممة للموظفين ذوي مستويات مختلفة من المعرفة التقنية. تقدم جلسات قصيرة يقودها الميسرون المبادئ الأساسية للمهارات الرقمية وتدريب توعية الأمن السيبراني، تليها أمثلة واقعية من مكان العمل توضح كيف تبدأ الحوادث السيبرانية وكيف يمكن للموظفين إيقافها.

يدرس المشاركون رسائل بريد إلكتروني ورسائل نصية ورموز QR وصفحات تسجيل دخول ودعوات مشاركة سحابية واتصالات تم إنشاؤها بواسطة الذكاء الاصطناعي، وذلك خلال أنشطة تدريب توعية التصيد الاحتيالي وتدريب توعية الهندسة الاجتماعية. تحدد المجموعات الصغيرة علامات التحذير، وتناقش الاستجابات المناسبة، وتقارن قراراتها بممارسات النظافة السيبرانية الموصى بها. توضح حالات اختراق البريد الإلكتروني التجاري كيف يتم استخدام الاستعجال والسلطة والسرية والضغط المالي للتلاعب بالموظفين.

توضح العروض التوضيحية الموجهة حماية كلمات المرور، والمصادقة متعددة العوامل MFA، وأذونات الحساب، والمشاركة الآمنة للملفات، وأمن الأجهزة المحمولة، والأمن السيبراني للعمل عن بُعد. تتناول مناقشات السيناريوهات الأجهزة المفقودة، والكشف العرضي للبيانات، وتحذيرات برامج الفدية، ونشاط الحساب المشبوه. يقوم المشاركون أيضًا بتقييم المصادر عبر الإنترنت والمحتوى الذي يتم إنشاؤه بواسطة الذكاء الاصطناعي لتعزيز الحكم الرقمي وتوعية الاحتيال عبر الإنترنت.

تعزز فحوصات المعرفة اليومية، والملاحظات الميسرة، وجلسات التفكير السلوكيات الصحيحة. تستند المنهجية إلى مبادئ التوعية الخاصة بالوكالة الأوروبية للأمن السيبراني ENISA من خلال التركيز على مدى ملاءمة الجمهور، والاتصال العملي، والتغيير السلوكي. تطور الأنشطة إجراءات قابلة للملاحظة في مكان العمل بدلاً من مهارات الإدارة التقنية، مما يجعل البرنامج مناسبًا لتدريب توعية الأمن السيبراني على مستوى المؤسسة.

أدوات الدورة:

- دليل المشارك لتوعية الأمن السيبراني
- قائمة التحقق للتقييم الذاتي للمهارات الرقمية
- قائمة التحقق من علامات التحذير من التصيد الاحتيالي
- دليل تقييم البريد الإلكتروني المشبوه
- بطاقات سيناريوهات الهندسة الاجتماعية
- دراسات حالة لاختراق البريد الإلكتروني التجاري
- دليل تحديد التصيد الاحتيالي المدعوم بالذكاء الاصطناعي
- قائمة التحقق من كلمات المرور وعبارات المرور
- دليل مرجعي للمصادقة متعددة العوامل
- قائمة التحقق لمراجعة أمان الحساب
- قائمة التحقق لأمن الأجهزة المحمولة
- أمثلة لتصنيف البيانات الشخصية

ملاحظة: لا يتم توفير البرامج أو منصات الأمن السيبراني أو الأدوات التجارية. يقدم المساق الأدوات ذات الصلة من خلال الشروحات والأمثلة والعروض التوضيحية الموجهة عند الاقتضاء.

محتوى الدورة :

AGILE LEADERS
Training Center

اليوم الأول: المهارات الرقمية الأساسية وأسس الأمن السيبراني

- الموضوع 1: فهم تدريب توعية الأمن السيبراني ودور الموظف في حماية معلومات المؤسسة
- الموضوع 2: تدريب المهارات الرقمية للاستخدام الآمن والواثق والمنتج للتكنولوجيا في مكان العمل
- الموضوع 3: فهم التهديدات السيبرانية، ونقاط الضعف، والمخاطر، والهجمات، وعواقبها التجارية
- الموضوع 4: إدارة ملفات مكان العمل، والمجلدات، والمعلومات السحابية، والسجلات الرقمية الآمنة
- الموضوع 5: تقييم المعلومات عبر الإنترنت، والمواقع الإلكترونية، ونتائج البحث، والمحتوى الذي يتم إنشاؤه بواسطة الذكاء الاصطناعي
- الموضوع 6: بناء عادات النظافة السيبرانية للاستخدام الآمن للإنترنت في العمل
- تأمل ومراجعة: مراجعة العادات الرقمية الشخصية وتحديد فرص تحسين الأمن السيبراني في مكان العمل

اليوم الثاني: التصيد الاحتيالي، الهندسة الاجتماعية، وعمليات الاحتيال عبر الإنترنت

- الموضوع 1: تدريب توعية التصيد الاحتيالي: التعرف على رسائل البريد الإلكتروني، والرسائل، والروابط، والمرفقات الخادعة
- الموضوع 2: تدريب توعية الهندسة الاجتماعية: التلاعب من خلال الاستعجال، والسلطة، والخوف، والثقة
- الموضوع 3: توعية أمن البريد الإلكتروني: التحقق من المرسلين، والنطاقات، والطلبات، والمرفقات، والروابط المضمنة
- الموضوع 4: تدريب اختراق البريد الإلكتروني التجاري: اكتشاف انتحال شخصية المديرين التنفيذيين، والموردين، والدفع
- الموضوع 5: توعية الاحتيال عبر الإنترنت: تحديد المواقع الإلكترونية الاحتيالية، ورموز QR، والمكالمات، ورسائل وسائل التواصل الاجتماعي
- الموضوع 6: توعية التصيد الاحتيالي المدعوم بالذكاء الاصطناعي: الخداع العميقة deepfakes، واستنساخ الصوت، والخداع شديد التخصيص
- تأمل ومراجعة: تحليل الاتصالات المشبوهة وشرح الاستجابة الأكثر أمانًا لكل سيناريو

اليوم الثالث: كلمات المرور، الحسابات، والهوية الرقمية

- الموضوع 1: تدريب أمان كلمات المرور: إنشاء بيانات اعتماد قوية، وفريدة، وقابلة للإدارة
- الموضوع 2: مديري كلمات المرور، وعبارات المرور، ومخاطر إعادة استخدام كلمات المرور
- الموضوع 3: تدريب المصادقة متعددة العوامل: فهم أساليب المصادقة وتحديات تسجيل الدخول
- الموضوع 4: تدريب توعية المصادقة متعددة العوامل MFA: التعرف على إرهاق المصادقة متعددة العوامل، وسرقة رموز التحقق، وعمليات الاحتيال للموافقة
- الموضوع 5: تدريب أمان الحساب: الاستجابة لعمليات تسجيل الدخول غير المألوفة واختراق الحساب
- الموضوع 6: توعية سرقة الهوية وتوعية التحكم في الوصول في بيئات مكان العمل
- تأمل ومراجعة: تطوير خطة شخصية لحماية الحساب بناءً على مبادئ الوصول الآمن

اليوم الرابع: البيانات، الأجهزة، والعمل الرقمي الآمن

- الموضوع 1: تدريب توعية حماية البيانات: تحديد المعلومات الشخصية والسرية والحساسة
- الموضوع 2: تدريب أمان الأجهزة المحمولة: تأمين الهواتف الذكية، والأجهزة اللوحية، والتطبيقات، والاتصالات
- الموضوع 3: الأمن السيبراني للعمل عن بُعد: حماية المعلومات خارج مكان العمل العادي
- الموضوع 4: توعية أمان السحابة: التخزين الآمن، والأذونات، والروابط، ومشاركة الملفات الخارجية
- الموضوع 5: التعاون الرقمي الآمن من خلال البريد الإلكتروني، والرسائل، واجتماعات الفيديو، ومساحات العمل المشتركة
- الموضوع 6: تدريب الأمن الرقمي لتحديثات البرامج، والنسخ الاحتياطية، والتطبيقات المعتمدة، والوسائط القابلة للإزالة
- تأمل ومراجعة: تقييم سيناريو العمل عن بُعد واختيار ضوابط الأمان المناسبة

اليوم الخامس: البرامج الضارة، الإبلاغ عن الحوادث، وثقافة الأمن السيبراني

- الموضوع 1: التعرف على البرامج الضارة، وبرامج الفدية، والتنزيلات الخبيثة، والسلوك غير المعتاد للجهاز
- الموضوع 2: الإجراءات الفورية للموظف بعد نقرة مشبوهة، أو مرفق، أو الكشف عن معلومات
- الموضوع 3: الإبلاغ عن الحوادث السيبرانية: ماذا تبلغ، ومتى تبلغ، وما هي المعلومات التي تقدمها
- الموضوع 4: حماية الخصوصية الرقمية، وإدارة الأذونات، والحفاظ على هوية رقمية احترافية
- الموضوع 5: مسؤوليات الموظف، وسياسات المؤسسة، والاستخدام المقبول للتكنولوجيا
- الموضوع 6: بناء ثقافة أمن سيبراني مستدامة في مكان العمل من خلال التوعية المستمرة
- تأمل ومراجعة: توحيد الدروس الرئيسية وإعداد خطة عمل شخصية لتدريب النظافة السيبرانية

الأسئلة الشائعة:

ما هي المؤهلات أو المتطلبات المسبقة المحددة المطلوبة للمشاركين قبل التسجيل في المساق؟

لا توجد مؤهلات رسمية أو خبرة تقنية في الأمن السيبراني مطلوبة. يجب أن يكون لدى المشاركين معرفة أساسية بأجهزة مكان العمل، والبريد الإلكتروني، واستخدام الإنترنت. تم تصميم المساق للموظفين التقنيين وغير التقنيين ويشرح مفاهيم الأمن السيبراني بلغة واضحة وعملية.

كم مدة كل جلسة يومية، وهل هناك عدد إجمالي من الساعات المطلوبة للمساق بأكمله؟

عادةً ما يتم تنظيم جلسة كل يوم لتستمر حوالي 5-4 ساعات، مع فترات راحة وأنشطة تفاعلية متضمنة. يمتد إجمالي مدة المساق على مدار خمسة أيام، أي ما يقرب من 25-20 ساعة من التدريب.

هل هذا المساق تقني، وهل سيتعلم المشاركون تهيئة أنظمة الأمن السيبراني؟

المساق هو برنامج تدريب توعية أمن المعلومات يركز على الموظفين بدلاً من كونه مساقًا تقنيًا لإدارة الأمن السيبراني. يتعلم المشاركون التعرف على التهديدات، وحماية المعلومات، وتأمين الحسابات، والاستجابة بشكل مناسب للنشاط المشبوه. قد يتم شرح الأدوات التقنية أو عرضها كأمثلة، ولكن تهيئة الأنظمة وهندسة الأمن المتقدمة تقع خارج نطاق المساق.

كيف يختلف هذا المساق عن مساقات تدريب توعية الأمن السيبراني الأخرى:

تدريب توعية الأمن السيبراني: المهارات الرقمية والسلامة الإلكترونية يتجاوز مجرد عرض قوائم بالتهديدات السيبرانية. يربط توعية الأمن بالمهارات الرقمية التي يستخدمها الموظفون يوميًا، بما في ذلك البحث عن المعلومات، وإنشاء المحتوى، والتواصل عبر الإنترنت، ومشاركة الملفات السحابية، واستخدام الأدوات المدعومة بالذكاء الاصطناعي. يعكس هذا النهج المتكامل إطار عمل DigComp 2.2، والإطار العالمي لمحو الأمية الرقمية لليونسكو، ومعايير المهارات الرقمية الأساسية 2026.

يركز المساق بشكل خاص على السلوك البشري. لا يتعلم المشاركون مجرد تعريفات التصيد الاحتيالي، أو برامج الفدية، أو سرقة الهوية؛ بل يحللون رسائل واقعية، ويتخذون قرارات، ويمارسون إجراءات الإبلاغ المناسبة. يتم تقديم تدريب الوقاية من التصيد الاحتيالي، وتدريب اختراق البريد الإلكتروني التجاري، وتوعية التصيد الاحتيالي المدعوم بالذكاء الاصطناعي من خلال مواقف تشمل المديرين التنفيذيين، والموردين، والزملاء، والعملاء.

يتناول البرنامج أيضًا مجالات قد تعالجها مساقات توعية الأمن السيبراني التقليدية بشكل منفصل، بما في ذلك الهوية الرقمية، وموثوقية المعلومات، وإعدادات الخصوصية، والتعاون الرقمي الآمن، والأجهزة المحمولة، والعمل عن بُعد. تنعكس مبادئ توعية الوكالة الأوروبية للأمن السيبراني ENISA من خلال التواصل الملائم للجمهور، والتعزيز المتكرر، والنتائج السلوكية العملية.

يظل المساق متاحًا للمشاركين غير التقنيين مع توفير عمق كافٍ في مكان العمل للمديرين والإدارات الحساسة للمخاطر. لا يعد المساق بتوفير أدوات أمن تجارية أو يقدمها. بدلاً من ذلك، يتلقى المشاركون رؤى موضوعية، وأمثلةً واقعية، ومواد مرجعية، وقوائم تحقق عملية تساعدهم على استخدام تكنولوجيا المؤسسة بشكل أكثر أمانًا ومسؤولية.

AGILE LEADERS
Training Center

فئات الدورات التدريبية

- الدورات التدريبية في مجال البيئة والاستدامة
- دورات إدارة و تحليل البيانات ودورات علم البيانات
- دورات الأمن السيبراني ودورات تقنية المعلومات
- دورات التدريب القانوني والمشتريات والتعاقدات
- دورات الحوكمة وإدارة المخاطر والامتثال
- دورات الصحة والسلامة والأمن المهني
- دورات المحاسبة و التمويل و دورات الإدارة المالية
- دورات في مجالات القيادة والإدارة
- دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيقة
- دورات إدارة الجودة وتطوير العمليات
- دورات إدارة و تطوير الموارد البشرية
- دورات الاتصال الجماهيري و السياسات والعلاقات العامة
- دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات
- دورات السكرتارية و إدارة المكاتب
- دورات الصيانة ودورات المجالات الهندسية المتنوعة
- دورات المهارات الشخصية وتطوير الذات
- دورات معتمدة من قبل هيئات دولية

AGILE LEADERS
Training Center

مدن التدريب

أثينا اليونان	أكرا غانا	أمستردام هولندا
اسطنبول تركيا	الجبيل المملكة العربية السعودية	الدار البيضاء المغرب
الدوحة قطر	الرياض المملكة العربية السعودية	القاهرة مصر
الكويت الكويت	المنامة مملكة البحرين	باريس فرنسا
باكو أذربيجان	بانكوك تايلند	براغ جمهورية التشيك
برشلونة إسبانيا	برلين ألمانيا	بورتو البرتغال
بوكيت تايلاند	تبليسي جورجيا	تورنتو كندا
جاكرتا جمهورية إندونيسيا	جنيف سويسرا	جوهانسبرغ جنوب إفريقيا
دبي الإمارات العربية المتحدة	روما إيطاليا	زنجبار تنزانيا
سان دييغو الولايات المتحدة الأمريكية	سنغافورة سنغافورة	سيول كوريا الجنوبية
شرم الشيخ مصر	شيكاغو الولايات المتحدة الأمريكية	طرابزون تركيا
طشقند أوزبكستان	طوكيو اليابان	عمان المملكة الأردنية الهاشمية
عن بعد منصة زووم	فرانكفورت ألمانيا	فيينا النمسا

AGILE LEADERS
Training Center

مدن التدريب

كوالالمبور ماليزيا	كيب تاون جنوب إفريقيا	لانكاوي ماليزيا
لشبونة البرتغال	لندن المملكة المتحدة	ماربيا اسبانيا
مدريد إسبانيا	مسقط سلطنة عمان	مونترو سويسرا
ميلان ايطاليا	ميونخ ألمانيا	نيروبي كينيا
نيويورك الولايات المتحدة الأمريكية		