الدورة التدريبية: الوعي السيبراني للموظفين - تعزيز ثقافة الأمن



18 - 22 اكتوبر 2026
عمان
3800 € (للشخص الواحد)
Ref: #CYB4777_397490

مقدمة الدورة التدريبية / لمحة عامة:

يُعد العنصر البشري خط الدفاع الأول والأكثر أهمية في أي استراتيجية للأمن السيبراني. مع تزايد التهديدات السيبرانية مثل هجمات التصيد الاحتيالي (Phishing) والبرامج الضارة (Malware)، أصبح من الضروري أن يكون جميع الموظفين على دراية بمخاطر الأمن السيبراني وكيفية التصرف بشكل آمن. تقدم هذه الدورة التدريبية التفاعلية والشاملة لجميع موظفي المؤسسات، بغض النظر عن مناصبهم، المعرفة والمهارات الأساسية لحماية أنفسهم ومؤسساتهم من التهديدات الرقمية. سنتناول في هذه الدورة أساسيات الأمن السيبراني، التعرف على الهجمات الشائعة، أفضل الممارسات لأمن كلمات المرور، والتعامل الآمن مع المعلومات الحساسة. سيكتسب المشاركون القدرة على اتخاذ قرارات آمنة في حياتهم المهنية والشخصية، مما يقلل بشكل كبير من احتمالية وقوع حوادث أمنية. تهدف الدورة إلى بناء ثقافة أمنية قوية في المؤسسة، حيث يصبح الأمن مسؤولية جماعية. يستند المحتوى إلى أحدث الممارسات والمعايير الأمنية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل الدكتور جوزيف كانون (Joseph Cannon)، المعروف بأعماله في التوعية الأمنية وسلوك المستخدم. يقدم BIG BEN Training Center هذه الدورة لتمكين الموظفين من أن يصبحوا درعًا منيعًا ضد الهجمات السيبرانية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- جميع موظفي المؤسسة من مختلف الأقسام والمستويات.
- المديرون وقادة الفرق.
- موظفو الإدارة والموارد البشرية.
- الموظفون الجدد.
- فرق المبيعات وخدمة العملاء.
- الفرق التقنية وغير التقنية.

القطاعات والصناعات المستهدفة:

- جميع القطاعات والصناعات.
- القطاع المالي والمصرفي.
- الرعاية الصحية.
- القطاع الحكومي وما في حكمها.
- شركات التجزئة.
- الشركات الصغيرة والمتوسطة.

الأقسام المؤسسية المستهدفة:

- جميع الأقسام المؤسسية.
- إدارة الموارد البشرية.
- إدارة المبيعات والتسويق.
- الإدارة التنفيذية.
- إدارة تقنية المعلومات.
- إدارة العمليات.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم مفاهيم الأمن السيبراني الأساسية وأهميتها.
- التعرف على التهديدات السيبرانية الشائعة (التصيد، البرامج الضارة).
- القدرة على تحديد رسائل البريد الإلكتروني المشبوهة والروابط الضارة.
- تطبيق أفضل الممارسات لإنشاء كلمات مرور قوية وآمنة.
- حماية البيانات الحساسة والمعلومات السرية للمؤسسة.
- التعامل الآمن مع الأجهزة الشخصية وشبكات Wi-Fi.
- الإبلاغ الفعال عن الحوادث الأمنية المحتملة.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية تفاعلية وجذابة، مصممة لجعل مفاهيم الأمن السيبراني سهلة الفهم والتطبيق لجميع الموظفين. سيتمكن المتدربون من خلال ورش العمل العملية التي تتضمن محاكاة هجمات التصيد الاحتيالي، ودراسات الحالة الواقعية لحوادث أمنية، من فهم تأثير سلوكهم على أمن المؤسسة. تتضمن المنهجية مقاطع فيديو توضيحية وأنشطة جماعية لتعزيز الوعي وبناء ثقافة أمنية قوية. سيتم التركيز على الجانب السلوكي للأمن، وتشجيع الموظفين على أن يكونوا يقظين ومسؤولين. يقدم BIG BEN Training Center هذه الدورة لضمان أن الأمن السيبراني ليس مجرد مسؤولية فريق تكنولوجيا المعلومات، بل هو مسؤولية مشتركة بين جميع أفراد المؤسسة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الوعي السيبراني للموظفين

- مقدمة إلى الأمن السيبراني وأهميته في مكان العمل.
- التهديدات السيبرانية الشائعة وكيفية عملها.
- الموظف كخط دفاع أول.
- التعامل مع المعلومات السرية والبيانات الحساسة.
- أمن الأجهزة الشخصية في بيئة العمل.
- التعرف على هجمات الهندسة الاجتماعية.
- المسؤولية الفردية في الأمن السيبراني.

الوحدة الثانية: التصيد الاحتيالي (Phishing) والهندسة الاجتماعية

- أنواع هجمات التصيد الاحتيالي (Spear Phishing, Smishing).
- كيفية التعرف على رسائل البريد الإلكتروني المشبوهة.
- التعامل مع الروابط والمرفقات الضارة.
- حماية المعلومات الشخصية من الهندسة الاجتماعية.
- محاكاة هجمات تصيد عملية.
- الإبلاغ عن رسائل التصيد الاحتيالي.
- أهمية اليقظة الدائمة.

الوحدة الثالثة: تأمين كلمات المرور والوصول

- أفضل الممارسات لإنشاء كلمات مرور قوية.
- استخدام المصادقة متعددة العوامل (MFA).
- مخاطر استخدام نفس كلمة المرور في أكثر من مكان.
- إدارة كلمات المرور بشكل آمن.
- أمن الوصول إلى أنظمة الشركة.
- حماية حسابات الموظفين من الاختراق.
- التعامل مع كلمات المرور على الأجهزة المحمولة.

الوحدة الرابعة: حماية البيانات والأجهزة في مكان العمل

- أمن البيانات والخصوصية في مكان العمل.
- التعامل مع البيانات السرية وفقًا لسياسات المؤسسة.
- أمن الأجهزة المحمولة (الهواتف، الأجهزة اللوحية).
- أمن الشبكات اللاسلكية (Wi-Fi).
- التعامل الآمن مع الأجهزة الخارجية (USB).
- مخاطر استخدام شبكات Wi-Fi العامة.
- إجراءات الأمن عند العمل عن بعد.

الوحدة الخامسة: الاستجابة للحوادث وبناء ثقافة أمنية

- ماذا تفعل عند وقوع حادث أمني؟
- الإبلاغ الفوري عن الحوادث الأمنية.
- دور الموظف في الاستجابة للحوادث.
- بناء ثقافة أمنية إيجابية في المؤسسة.
- أهمية التدريب المستمر.
- التحديات في التوعية الأمنية.
- مكافآت السلوك الأمني الإيجابي.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

بما أن العنصر البشري هو أضعف حلقة في سلسلة الأمن السيبراني، كيف يمكن للمؤسسات أن تبتكر استراتيجيات توعية أمنية مستدامة لا تقتصر على مجرد التدريب، بل تحول الوعي الأمني إلى سلوك طبيعي، وتُنشئ ثقافة أمنية قوية تُمكن كل موظف من أن يكون درعًا استباقيًا ضد التهديدات الرقمية المتزايدة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل والعملي على الوعي السيبراني للموظفين، مما يوفر محتوى مصممًا خصيصًا ليناسب جميع مستويات الخبرة في المؤسسة. بدلاً من مجرد سرد المعلومات، نغوص في التطبيق العملي لمفاهيم الأمن من خلال محاكاة هجمات واقعية ودراسات حالة تفاعلية. نقدم أمثلة عملية ونصائح قابلة للتطبيق الفوري، مما يضمن أن المشاركين سيخرجون بمهارات عملية لحماية أنفسهم ومؤسساتهم. نركز على بناء ثقافة أمنية إيجابية، حيث يُشجع الموظفون على تحمل المسؤولية والمشاركة في حماية الأصول الرقمية. إنها ليست مجرد دورة نظرية، بل هي تجربة تعليمية مصممة لتغيير السلوك وبناء مجتمع مؤسسي واعٍ أمنيًا.