الدورة التدريبية: حماية الأصول الرقمية للمبتدئين والموظفين غير التقنيين



19 - 23 اكتوبر 2026
باكو
5100 € (للشخص الواحد)
Ref: #CYB7548_328486

مقدمة الدورة التدريبية / لمحة عامة:

تُعد هذه الدورة التدريبية الشاملة نقطة انطلاق أساسية لكل من يرغب في فهم أساسيات الأمن السيبراني وحماية البيانات في عالم رقمي متزايد التعقيد. فمع تزايد الاعتماد على التكنولوجيا في حياتنا اليومية والمهنية، أصبح التهديد السيبراني يمثل تحديًا كبيرًا للأفراد والمؤسسات على حد سواء. هذه الدورة مصممة خصيصًا لتمكين المبتدئين والموظفين غير التقنيين من اكتساب المعرفة والمهارات اللازمة للتعامل مع هذه التحديات بفعالية. نحن نؤمن بأن الأمن السيبراني ليس مسؤولية الخبراء التقنيين فقط، بل هو مسؤولية جماعية تتطلب وعيًا وفهمًا من الجميع. سيتمكن المشاركون من التعرف على مفاهيم رئيسية مثل التهديدات السيبرانية الشائعة، أمن المعلومات الأساسي، حماية الخصوصية الرقمية، وأفضل ممارسات الأمن السيبراني. يستند المحتوى إلى أحدث الأبحاث والممارسات الموصي بها في هذا المجال، بما في ذلك الأفكار المستنيرة من أعمال خبراء مثل البروفيسور روس أندرسون (Ross Anderson)، الذي يُعد مرجعًا عالميًا في مجال أمن الكمبيوتر والأنظمة الموثوقة. يقدم BIG BEN Training Center هذه الدورة بهدف بناء ثقافة أمنية قوية، تمكّن الأفراد من التعرف على المخاطر واتخاذ خطوات استباقية لحماية أنفسهم وبياناتهم الحساسة. ستوفر هذه الدورة فهمًا عميقًا لكيفية تجنب الاحتيال الإلكتروني، تأمين الشبكات اللاسلكية المنزلية، وإدارة كلمات المرور القوية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- الموظفون الإداريون في مختلف الأقسام.
- الموظفون الجدد في أي بيئة عمل تتطلب التعامل مع البيانات الرقمية.
- الأفراد المهتمون بتعزيز أمنهم الرقمي الشخصي.
- أصحاب الأعمال الصغيرة الذين لا يملكون فرق أمن سيبراني متخصصة.
- طلاب الجامعات من التخصصات غير التقنية الذين يرغبون في فهم أساسيات الأمن السيبراني.
- أي شخص يسعى لزيادة وعيه بمخاطر الإنترنت وكيفية حماية الأجهزة.

القطاعات والصناعات المستهدفة:

- قطاع الخدمات المالية والبنوك نظرًا لحساسية البيانات.
- القطاع الصحي والمستشفيات لحماية بيانات المرضى السرية.
- القطاع التعليمي والجامعات لتعزيز الأمن السيبراني للمؤسسات التعليمية.
- القطاع الحكومي والهيئات العامة وما في حكمها نظرًا لأهمية أمن المعلومات الحكومية.
- قطاع التجزئة والتجارة الإلكترونية لحماية بيانات العملاء المالية.
- قطاع الصناعات التحويلية والطاقة لتعزيز أمن البنية التحتية الحيوية.

الأقسام المؤسسية المستهدفة:

- إدارة الموارد البشرية لضمان وعي الموظفين بالأمن السيبراني.
- إدارة التسويق والمبيعات لحماية بيانات العملاء التسويقية.
- إدارة العمليات والإدارة العامة لتعزيز الأمن التشغيلي.
- إدارة الشؤون القانونية والامتثال لضمان الامتثال لقوانين حماية البيانات.
- إدارة العلاقات العامة والإعلام لتعزيز الوعي الأمني للمؤسسة.

أهداف الدورة التدريبية:

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

- فهم المفاهيم الأساسية للأمن السيبراني ومكوناته الرئيسية.
- التعرف على أنواع التهديدات السيبرانية الشائعة وكيفية اكتشاف هجمات التصيد الاحتيالي.
- تطبيق أفضل الممارسات لحماية البيانات الشخصية والمعلومات الحساسة.
- القدرة على إنشاء كلمات مرور قوية وإدارة الحسابات عبر الإنترنت.
- فهم أهمية النسخ الاحتياطي للبيانات وتأمين الأجهزة المحمولة.
- الوعي بأمن الشبكات المنزلية وحماية الواي فاي.
- التعرف على مخاطر الهندسة الاجتماعية وكيفية تجنبها.

منهجية الدورة التدريبية:

تتبع هذه الدورة التدريبية منهجية تفاعلية وشاملة مصممة لضمان أقصى استفادة للمشاركين، بغض النظر عن خلفيتهم التقنية. نركز على تقديم المفاهيم النظرية بأسلوب مبسط ومفهوم، يليه تطبيق عملي مكثف من خلال دراسات حالة واقعية وتمارين عملية. سيتم تشجيع المشاركين على العمل في مجموعات صغيرة لمناقشة التحديات الأمنية المشتركة وتطوير حلول مبتكرة. تتضمن الجلسات التفاعلية ورش عمل تطبيقية تتيح للمتدربين ممارسة المهارات المكتسبة مباشرة، مثل التعرف على رسائل البريد الإلكتروني الاحتيالية أو إعداد إعدادات الخصوصية في التطبيقات. بالإضافة إلى ذلك، سيتم توفير تغذية راجعة مستمرة لضمان فهم عميق للمفاهيم وتطبيق الممارسات الأمنية الفعالة. سيتمكن المشاركون من طرح الأسئلة ومناقشة التحديات التي يواجهونها في بيئاتهم الخاصة، مما يعزز من تجربة التعلم الشاملة. يلتزم BIG BEN Training Center بتقديم بيئة تعليمية داعمة ومشجعة تساهم في بناء قدرات المشاركين في مجال الأمن السيبراني الشخصي والمؤسسي.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني والمفاهيم الأولية

- مقدمة إلى عالم الأمن السيبراني.
- تعريفات رئيسية: التهديد، الثغرة الأمنية، المخاطر.
- أهمية حماية البيانات في العصر الرقمي.
- أنواع المعلومات الحساسة.
- مقدمة إلى الأمن السيبراني للمستخدم العادي.
- المصطلحات الشائعة في أمن المعلومات.
- الأمن السيبراني في حياتنا اليومية.

الوحدة الثانية: التهديدات السيبرانية الشائعة وكيفية التعرف عليها

- البرامج الضارة: الفيروسات، أحصنة طروادة، برامج الفدية.
- التصيد الاحتيالي (Phishing): أنواعه وكيفية اكتشاف رسائل البريد الإلكتروني الاحتيالية.
- الهندسة الاجتماعية: التكتيكات المستخدمة وكيفية الحماية منها.
- هجمات حجب الخدمة الموزعة (DDoS): فهم بسيط.
- الوصول غير المصرح به وسرقة الهوية.
- تهديدات الويب الشائعة.
- أمن البيانات ضد الهجمات.

الوحدة الثالثة: حماية البيانات الشخصية والخصوصية الرقمية

- إدارة كلمات المرور القوية وأهمية المصادقة متعددة العوامل.
- أمن الأجهزة المحمولة: الهواتف الذكية والأجهزة اللوحية.
- النسخ الاحتياطي للبيانات وأهميته.
- إعدادات الخصوصية على وسائل التواصل الاجتماعي.
- حماية الخصوصية عبر الإنترنت.
- تشفير البيانات الأساسي.
- حماية المعلومات الشخصية.

الوحدة الرابعة: أمن الشبكات والاتصالات

- تأمين الشبكات اللاسلكية المنزلية (Wi-Fi).
- استخدام الشبكات الافتراضية الخاصة (VPN).
- أمن البريد الإلكتروني.
- تصفح الإنترنت الآمن.
- الجدران النارية (Firewalls): مفهومها الأساسي.
- الوعي بالتهديدات السيبرانية للشبكات.
- أمن نقاط النهاية.

الوحدة الخامسة: الاستجابة للحوادث الأمنية وأفضل الممارسات

- ماذا تفعل في حالة التعرض لهجوم سيبراني أو انتهاك للبيانات.
- الإبلاغ عن التهديدات الأمنية.
- أهمية تحديث البرامج والأنظمة.
- الوعي الأمني المستمر.
- خطة الاستجابة للحوادث الأساسية.
- ثقافة الأمن السيبراني.
- الامتثال الأمني للموظفين.

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:

في عالم تتطور فيه التهديدات السيبرانية باستمرار وتصبح أكثر تعقيدًا، كيف يمكن للأفراد والمؤسسات غير التقنية أن يظلوا في طليعة الدفاع السيبراني، وأن يحولوا الوعي الأمني إلى ممارسة يومية فعالة؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العملي والموجه خصيصًا لتمكين المبتدئين والموظفين غير التقنيين من فهم أساسيات الأمن السيبراني وتطبيقها في حياتهم اليومية والمهنية. بدلاً من الغوص في التفاصيل التقنية المعقدة، نركز على تقديم رؤى عملية وأمثلة واقعية تتيح للمشاركين استيعاب المفاهيم بسرعة وفعالية. نبتعد عن الأدوات والبرمجيات المحددة، ونركز على تنمية الوعي الأمني والمهارات الوقائية التي تبقى ذات قيمة بغض النظر عن التغيرات التكنولوجية. تشمل الدورة دراسات حالة تفاعلية تُظهر سيناريوهات التهديدات السيبرانية الشائعة وكيفية الاستجابة لها بفعالية. يعتمد المحتوى على أحدث الأبحاث الأكاديمية والممارسات الصناعية الموصي بها في مجال أمن المعلومات وحماية البيانات. هذه الدورة ليست مجرد معلومات نظرية، بل هي دعوة لتبني عقلية أمنية استباقية، تمكن المشاركين من أن يصبحوا خط الدفاع الأول ضد المخاطر السيبرانية.