الدورة التدريبية: حماية الهوية الرقمية والخصوصية على الإنترنت للأفراد والمؤسسات

15 - 19 نوفمبر 2026
عمان
3800 € (للشخص الواحد)
Ref: #CYB4913_397521

مقدمة الدورة التدريبية / لمحة عامة:

في عصر الرقمنة المتسارع، أصبحت الهوية الرقمية والخصوصية على الإنترنت من أهم القضايا التي تواجه الأفراد والمؤسسات. مع تزايد التهديدات السيبرانية، مثل سرقة الهوية وانتهاك البيانات، أصبح من الضروري فهم كيفية حماية المعلومات الشخصية والبيانات الحساسة. تقدم هذه الدورة التدريبية الشاملة لجميع الأفراد وموظفي المؤسسات، المعرفة والمهارات اللازمة لتأمين هويتهم الرقمية وحماية خصوصيتهم على الإنترنت. سنتناول في هذه الدورة مفاهيم الهوية الرقمية، التهديدات الشائعة، أفضل الممارسات لأمن الحسابات، واستخدام أدوات الخصوصية. سيكتسب المشاركون القدرة على تحديد المخاطر الأمنية، اتخاذ قرارات آمنة، وتطبيق ضوابط حماية فعالة في حياتهم الرقمية. تهدف الدورة إلى بناء وعي أمني قوي يمكن أن يقي من الكثير من المخاطر. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات الدولية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور ديفيد تشا (David Chaum)، المعروف بأعماله الرائدة في الخصوصية الرقمية والعملات المشفرة. يقدم BIG BEN Training Center هذه الدورة لتمكين الأفراد والمؤسسات من التحكم في بصمتهم الرقمية وحماية أصولهم الشخصية والمعلوماتية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- جميع مستخدمي الإنترنت من الأفراد.
- موظفو المؤسسات من جميع المستويات.
- مديرو الأمن السيبراني والمخاطر.
- المسؤولون عن حماية البيانات والخصوصية.
- المحترفون في مجالات الموارد البشرية والشؤون القانونية.
- الآباء والأمهات الراغبين في حماية أسرهم.

القطاعات والصناعات المستهدفة:

- جميع القطاعات والصناعات.
- القطاع المالي والمصرفي.
- شركات التكنولوجيا.
- الرعاية الصحية.
- القطاع الحكومي وما في حكمها.
- قطاع التعليم.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة الموارد البشرية.
- إدارة الشؤون القانونية والامتثال.
- إدارة الاتصالات.
- إدارة تكنولوجيا المعلومات.

أهداف الدورة التدريبية:

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

- فهم مفاهيم الهوية الرقمية وأهمية الخصوصية على الإنترنت.
- القدرة على تحديد التهديدات الشائعة مثل سرقة الهوية والاحتيال.
- تطبيق أفضل الممارسات لتأمين الحسابات وكلمات المرور.
- التعامل الآمن مع البيانات الشخصية على منصات التواصل الاجتماعي.
- استخدام أدوات وتقنيات الخصوصية مثل VPNs.
- حماية الأجهزة الشخصية من البرامج الضارة.
- التعرف على حقوق الخصوصية والالتزامات القانونية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية وتشاركية، مصممة لجعل مفاهيم حماية الهوية الرقمية سهلة الفهم والتطبيق. سيتمكن المتدربون من خلال دراسات الحالة الواقعية لحوادث سرقة الهوية وانتهاك البيانات، وورش العمل التفاعلية، من فهم تأثير سلوكهم الرقمي على أمنهم الشخصي والمؤسسي. تتضمن المنهجية مقاطع فيديو توضيحية وأنشطة جماعية لتعزيز الوعي وبناء عادات رقمية آمنة. سيتم التركيز على الجانب التطبيقي للحماية، من تأمين الحسابات إلى استخدام أدوات التشفير. يقدم BIG BEN Training Center هذه الدورة لتمكين الأفراد والمؤسسات من التحكم في مصيرهم الرقمي وحماية أصولهم الأكثر قيمة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الهوية الرقمية والخصوصية

- مفهوم الهوية الرقمية وبصمتك الرقمية.
- أهمية الخصوصية على الإنترنت.
- التهديدات الشائعة للهوية الرقمية (سرقة الهوية، الاحتيال).
- الفرق بين البيانات الشخصية والبيانات الحساسة.
- أخلاقيات استخدام الإنترنت والخصوصية.
- تأثير انتهاك البيانات على الأفراد والمؤسسات.
- حقوقك الرقمية وقوانين حماية البيانات.

الوحدة الثانية: تأمين الحسابات وكلمات المرور

- إنشاء كلمات مرور قوية وآمنة.
- استخدام المصادقة متعددة العوامل (MFA).
- إدارة كلمات المرور بشكل فعال.
- حماية الحسابات على منصات التواصل الاجتماعي والبريد الإلكتروني.
- التعامل مع رسائل التصيد الاحتيالي (Phishing).
- التعرف على علامات الاختراق.
- التعامل مع اختراق الحساب.

الوحدة الثالثة: حماية البيانات على الإنترنت

- مخاطر مشاركة المعلومات الشخصية على الإنترنت.
- تأمين البيانات أثناء التسوق الإلكتروني.
- استخدام شبكات Wi-Fi العامة بأمان.
- تشفير البيانات على الأجهزة الشخصية.
- أمان التصفح وأدوات حظر التتبع.
- التعامل الآمن مع رسائل البريد الإلكتروني والمرفقات.
- حماية الخصوصية على محركات البحث.

الوحدة الرابعة: حماية الأجهزة الشخصية والشبكات

- أمن الأجهزة المحمولة (الهواتف، الأجهزة اللوحية).
- حماية أجهزة الكمبيوتر من البرامج الضارة والفيروسات.
- تأمين الشبكة المنزلية (الراوتر).
- التعامل مع البرامج الضارة (Malware) وفيروس الفدية (Ransomware).
- أهمية تحديث البرامج وأنظمة التشغيل.
- النسخ الاحتياطي للبيانات بشكل دوري.
- استخدام أدوات الحماية الأمنية.

الوحدة الخامسة: الخصوصية في المؤسسات والتعامل مع الحوادث

- سياسات حماية البيانات في المؤسسات.
- مسؤولية الموظف في حماية البيانات.
- التعرف على حوادث انتهاك البيانات.
- وضع خطة للاستجابة للحوادث الأمنية.
- الإبلاغ الفوري عن أي انتهاك للخصوصية.
- الالتزام باللوائح القانونية لحماية البيانات.
- مستقبل الهوية الرقمية والخصوصية.

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 ظل التطور المتسارع للذكاء الاصطناعي والبيانات الضخمة، كيف يمكن للأفراد والمؤسسات أن يبتكرون استراتيجيات لحماية هوياتهم الرقمية لا تقتصر على معالجة التهديدات الحالية، بل تتوقع انتهاكات الخصوصية المستقبلية، وتُنشئ درعًا رقميًا مرنًا يُمكنهم من التحكم الكامل في بصمتهم الرقمية والحفاظ على أمنهم الشخصي؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل والعملي على حماية الهوية الرقمية والخصوصية، مما يوفر محتوى مصممًا خصيصًا ليناسب الأفراد وموظفي المؤسسات على حد سواء. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لحماية البيانات الشخصية وأمن الحسابات. تقدم الدورة دراسات حالة واقعية لحوادث سرقة الهوية، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز على الجانب السلوكي للأمن، وتشجيع المشاركين على اتخاذ قرارات واعية ومسؤولة. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء مجتمع واعٍ رقميًا قادر على حماية نفسه ومؤسسته من التهديدات المتزايدة.