الدورة التدريبية: الجرائم الإلكترونية والابتزاز الرقمي: الوقاية والتعامل القانوني



08 - 12 نوفمبر 2026
عمان
3800 € (للشخص الواحد)
Ref: #LEG9523_395106

مقدمة الدورة التدريبية / لمحة عامة:

يقدم BIG BEN Training Center هذه الدورة التدريبية المتخصصة في مجال الجرائم الإلكترونية والابتزاز الرقمي، مع التركيز على الوقاية والتعامل القانوني مع هذه الظواهر المتزايدة التعقيد. في عصر التحول الرقمي، أصبح الأفراد والمؤسسات عرضة بشكل متزايد للتهديدات السيبرانية التي تتطور باستمرار، مما يستدعي فهمًا عميقًا لأنواع الجرائم الإلكترونية، وآلياتها، وكيفية حماية البيانات والمعلومات الحساسة. تهدف هذه الدورة إلى تزويد المشاركين بالمعرفة اللازمة للتعرف على أساليب الابتزاز الرقمي والاحتيال الإلكتروني، وتطبيق استراتيجيات الوقاية الفعالة، والتعامل مع التداعيات القانونية لهذه الجرائم. تستلهم الدورة من أعمال خبراء مثل البروفيسور بيتر نوي (Peter Neumann) من مركز ستانفورد لأبحاث الأمن السيبراني، الذي أسهم في تحليل نقاط الضعف في الأنظمة وتطوير منهجيات الأمن السيبراني. ستغطي الدورة الجوانب التقنية والقانونية للجرائم السيبرانية، بما في ذلك التشريعات المحلية والدولية ذات الصلة، وإجراءات الإبلاغ والتحقيق، ودور الأدلة الرقمية في الإثبات. هذه الدورة ضرورية لكل من يسعى لتعزيز أمنه الرقمي وحماية نفسه ومؤسسته من التهديدات المتجددة في الفضاء السيبراني.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- المتخصصون في الأمن السيبراني.
- المستشارون القانونيون والمحامون.
- موظفو أقسام تقنية المعلومات.
- مديرو المخاطر والامتثال.
- الأفراد المهتمون بحماية بياناتهم الشخصية.
- القيادات الإدارية في الشركات والمؤسسات.
- مسؤولو حماية البيانات.

القطاعات والصناعات المستهدفة:

- القطاع المصرفي والمالي.
- القطاع الحكومي والهيئات الرقابية.
- شركات الاتصالات وتقنية المعلومات.
- المؤسسات التعليمية والصحية.
- الشركات التجارية والإلكترونية.
- مكاتب المحاماة والاستشارات القانونية.
- قطاع الإعلام والنشر الرقمي.

الأقسام المؤسسية المستهدفة:

- إدارات الأمن السيبراني.
- الإدارات القانونية.
- إدارات تقنية المعلومات.
- إدارات المخاطر والامتثال.
- إدارات الموارد البشرية.
- إدارات التدقيق الداخلي.
- أقسام حماية البيانات والخصوصية.

أهداف الدورة التدريبية:

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

- تحديد أنواع الجرائم الإلكترونية الشائعة وأساليبها.
- فهم آليات الابتزاز الرقمي وكيفية انتشاره.
- تطبيق استراتيجيات الوقاية والحماية من التهديدات السيبرانية.
- التعرف على التشريعات والقوانين المتعلقة بالجرائم الإلكترونية.
- معرفة الإجراءات القانونية المتبعة في التعامل مع الابتزاز الرقمي.
- فهم دور الأدلة الرقمية في التحقيقات الجنائية.
- تطوير خطط استجابة فعالة للحوادث السيبرانية.
- حماية البيانات الشخصية وبيانات المؤسسة من الاختراق.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة منهجية تدريبية متكاملة تجمع بين الشرح النظري المفصل والتطبيقات العملية المباشرة لمواجهة تحديات الجرائم الإلكترونية. تبدأ المنهجية بعرض شامل للمفاهيم الأساسية للجرائم السيبرانية وأساليبها، مع تحليل دقيق لدراسات حالة واقعية توضح كيفية وقوع هذه الجرائم وتداعياتها. سيتم التركيز على الجلسات التفاعلية التي تتيح للمشاركين طرح الأسئلة وتبادل الخبرات، إضافة إلى ورش عمل تطبيقية تتناول سيناريوهات عملية للتعامل مع الابتزاز الرقمي والاختراقات الأمنية. سيتعلم المشاركون كيفية تطبيق أدوات وتقنيات الوقاية، وفهم الإجراءات القانونية اللازمة للإبلاغ عن الجرائم وجمع الأدلة الرقمية. كما ستقدم الدورة تغذية راجعة مستمرة لضمان استيعاب المفاهيم وتطوير المهارات. تهدف هذه المنهجية إلى تزويد المشاركين بالقدرة على حماية أنفسهم ومؤسساتهم بفعالية من التهديدات الرقمية المتجددة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مفهوم الجرائم الإلكترونية وأنواعها.

- تعريف الجريمة الإلكترونية وخصائصها.
- تصنيف الجرائم الإلكترونية (الاختراق، الاحتيال، الابتزاز، سرقة الهوية).
- الفرق بين الجرائم الإلكترونية والجرائم التقليدية.
- دوافع مرتكبي الجرائم الإلكترونية.
- أمثلة على الجرائم الإلكترونية الشائعة عالميًا ومحليًا.
- التطور التاريخي للجرائم الإلكترونية.
- التحديات التي تواجه مكافحة الجرائم الإلكترونية.

الوحدة الثانية: الابتزاز الرقمي: آلياته وضحاياه.

- مفهوم الابتزاز الرقمي وأشكاله.
- كيف تتم عمليات الابتزاز الرقمي (التصيد، البرمجيات الخبيثة).
- تأثير الابتزاز الرقمي على الأفراد والمؤسسات.
- التعرف على مؤشرات الابتزاز الرقمي.
- حماية البيانات الشخصية والمعلومات الحساسة.
- دور وسائل التواصل الاجتماعي في الابتزاز.
- قصص واقعية عن الابتزاز الرقمي.

الوحدة الثالثة: استراتيجيات الوقاية والحماية الرقمية.

- أفضل الممارسات للأمن السيبراني الشخصي والمؤسسي.
- استخدام كلمات مرور قوية والمصادقة متعددة العوامل.
- تحديث البرامج والأنظمة بانتظام.
- النسخ الاحتياطي للبيانات والمعلومات.
- الوعي بمخاطر الروابط المشبوهة والبريد الإلكتروني الاحتيالي.
- حماية الأجهزة المحمولة والشبكات اللاسلكية.
- بناء ثقافة أمن سيبراني قوية في المؤسسات.

الوحدة الرابعة: الإطار القانوني للتعامل مع الجرائم الإلكترونية.

- القوانين والتشريعات المحلية والدولية لمكافحة الجرائم الإلكترونية.
- دور الجهات الحكومية في مكافحة الجرائم السيبرانية.
- إجراءات الإبلاغ عن الجرائم الإلكترونية.
- حقوق الضحايا في قضايا الابتزاز الرقمي.
- التعاون الدولي في مكافحة الجريمة السيبرانية.
- العقوبات القانونية المترتبة على الجرائم الإلكترونية.
- التحديات القانونية في إثبات الجرائم الرقمية.

الوحدة الخامسة: التحقيق الجنائي الرقمي والأدلة الإلكترونية.

- مفهوم التحقيق الجنائي الرقمي ومراحله.
- جمع الأدلة الرقمية وحفظها بطريقة قانونية.
- تحليل الأدلة الرقمية واستخلاص المعلومات.
- تقارير الخبرة الفنية في القضايا الإلكترونية.
- دور الأدلة الرقمية في إثبات الجرائم.
- التحديات التقنية والقانونية في التعامل مع الأدلة الرقمية.
- دراسات حالة عملية في التحقيق الرقمي.

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 للتقنيات الرقمية، كيف يمكن للأطر القانونية والتشريعية أن تواكب التحديات الجديدة التي تفرضها الجرائم الإلكترونية، مع الحفاظ على التوازن بين حماية الأمن الرقمي وحقوق الأفراد في الخصوصية والحرية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتقديم رؤية شاملة وعملية في مجال الجرائم الإلكترونية والابتزاز الرقمي، مع التركيز على الجانبين الوقائي والقانوني، مما يجعلها مختلفة عن الدورات التي تركز على جانب واحد فقط. نحن لا نكتفي بشرح المفاهيم النظرية، بل نوفر للمشاركين الأدوات والتقنيات العملية اللازمة لحماية أنفسهم ومؤسساتهم. ما يميزنا هو دمج الأمثلة الواقعية ودراسات الحالة التي توضح كيفية وقوع هذه الجرائم وكيفية التعامل معها بفعالية. كما تركز الدورة على الجوانب القانونية الدقيقة، بما في ذلك التشريعات الحالية وإجراءات الإبلاغ وجمع الأدلة الرقمية، وهو أمر حيوي للمتخصصين في هذا المجال. تهدف الدورة إلى تزويد المشاركين بفهم عميق للمخاطر السيبرانية وكيفية الاستجابة لها بفعالية، مما يجعلهم قادرين على حماية أصولهم الرقمية واتخاذ القرارات القانونية الصائبة في مواجهة هذه التهديدات المتزايدة.