الدورة التدريبية: الجرائم الإلكترونية والابتزاز الرقمي: الوقاية والتعامل القانوني

يونيو ٢٠٢٦ ٠٥ - ٠١

القاهرة - *

(للشخص الواحد) ٤١٠٠ €

Ref: #LEG9523_556409

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مفهوم الجرائم الإلكترونية وأنواعها.

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

الوحدة الثانية: الابتزاز الرقمي: آلياته وضحاياه.

- مفهوم الابتزاز الرقمي وأشكاله.
- الخبيثة). كيف تتم عمليات الابتزاز الرقمي (التصيد، البرمجيات
- 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.

الرقمية. الوحدة الثالثة: استراتيجيات الوقاية والحماية

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

الجرائم الإلكترونية. الوحدة الرابعة: الإطار القانوني للتعامل مع

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

الإلكترونية. الوحدة الخامسة: التحقيق الجنائي الرقمي والأدلة

- 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.
- الرقمية. التحديات التقنية والقانونية في التعامل مع الأدلة
- دراسات حالة عملية في التحقيق الرقمي.

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

الجرائم الإلكترونية، مع للأطر القانونية والتشريعية أن تواكب التحديات في ظل التطور المتسارع للتقنيات الرقمية، كيف يمكن

الأفراد في الخصوصية والحرية؟ الحفاظ على التوازن بين حماية الأمن الرقمي وحقوق الجديدة التي تفرضها

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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