€TRAINING

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

26 - 30 يناير 2020

المنامة (البحرين)

Crowne Plaza

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

رمز الدورة: P434 تاريخ الإنعقاد: 26 - 30 يناير 2020 دولة الإنعقاد: المنامة (البحرين) - Plaza Crowne التكلفة: 2500 يورو

مقدمة عن الدورة التدريبية:

الجريمة الإلكترونية هي أكبر خطر الآن من أي وقت مضى بسبب العدد الهائل من المتصلين من الناس بالأجهزة الالكترونية، ولكن ما هي بالضبط؟ باختصار، هي ببساطة الجريمة المتعلقة بسرقة البيانات الشخصية أو انتهاك حقوق الملكية أو التزوير أو لها علاقة المواد الإباحية المتعلقة بالأطفال أو المطاردة الإلكترونية، والجرائم الإلكترونية تغطي مجموعة واسعة من الهجمات المختلفة وتعرفها بإيجاز بأنها "أي جريمة ترتكب باستخدام شبكة حاسوبية أو جهاز حاسوبي، وهناك شكل شائع من أنواع الجرائم الإلكترونية وهو التصيد الاحتيالي، حيث يتلقى الضحية البريد الإلكتروني المفترض أن يكون مشروع مع وصلة يؤدي إلى موقع معادية على شبكة الإنترنت. بمجرد النقر على الرابط، يمكن بعد ذلك إصابة جهاز الكمبيوتر بالفيروس، وهناك نوع من الجرائم الالكترونية تكون أكثر خطورة بكثير وتغطي أشياء مثل التحرش بالمضايقات وتهريب الأطفال، والابتزاز، والتلاعب في سوق الأوراق المالية، والتجسس المعقد للشركات، والتخطيط.

أهداف الدورة التدريبية:

- تعريف المشاركين بالقضايا التقنية والقانونية والاجتماعية المتعلقة بالجريمة الالكترونية.
- مناقشة تشغيل أجهزة الكمبيوتر والانترنت، ومعالجة أصول الجريمة الإلكترونية ومدى انتشارها، والاستجابات من النظم القانونية للمجرمين الالكترونيين، والأثر الاجتماعي للجرائم الالكترونية.
- تحليل مسببات الجرائم السيبرانية من وجهات النظر الثقافية، والثقافات، والاجتماعية.

المستفيدون من الدورة التدريبية:

في نهاية دورة الجرائم الإلكترونية والأدلة الجنائية الإلكترونية سيكون المشاركين قد تعرفوا على:

- أنواع الجرائم الإلكترونية التي تتعلق بسرقة أو معالجة البيانات أو الخدمات عن طريق القرصنة أو الفيروسات وسرقة الهوية والاحتيال على المصارف أو التجارة الإلكترونية.
- وصف انتشار الجرائم الالكترونية في الدول.
- تحديد الطرق والتقنيات التي يشيع استخدامها من قبل المجرمين الالكترونيين.
- التمييز بين مختلف أنواع الجرائم السيبرانية فيما يتعلق بدوافع وأساليب تشغيل المجرمين، وأنواع الضحايا أو الأهداف، والمجالات المكانية والزمنية والقانونية التي تنفذ فيها.
- تحليل القضايا الدولية مثل الإرهاب الالكتروني، والحرب الإلكترونية، والاتجار بالبشر.
- دراسة قدرة نظريات علم الجريمة الحالية على تفسير الجرائم الالكترونية.
- شرح التحديات القضائية التي تواجهها الدول عند الاستجابة للجريمة الالكترونية.

المحتوى العلمي للدورة التدريبية:

- الكمبيوتر وأساسيات الإنترنت
- أجهزة الكمبيوتر والبرمجيات
- البنية التحتية والاستخدام
- التكوين القانوني للجريمة الالكترونية
- تعريف الجرائم الالكترونية
- تصنيف الجرائم الالكترونية
- جرائم الحاسوب
- الجرائم التي يسهلها الحاسوب
- الجرائم المدعومة بالكمبيوتر
- انتشار وتواتر الجرائم الالكترونية
- تصنيف الهاكرز
- التقنيات المستخدمة من قبل المتسللين

- الرسائل غير المرغوب فيها، والتصيد الاحتيالي، والقشط
- مقدمة لسلامة البيانات
- إشارات التحذير الالكترونية
- رصد وحماية البرمجيات
- نصائح لتجنب الفيروسات الخبيثة
- الحقيقة حول المحتوى عبر الإنترنت
- سرقة الهوية
- برامج التجسس والبرمجيات الخبيثة
- قانون حماية خصوصية الأشخاص على الانترنت
- سياسة الخصوصية
- سلامة الشبكات الاجتماعية
- قواعد إضافية لسلامة الشبكات على الإنترنت