

# € TRAINING

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

28 ديسمبر 2020 - 1 يناير 2021  
هونكونغ



## الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

رمز الدورة: P434 تاريخ الإنعقاد: 28 ديسمبر 2020 - 1 يناير 2021 دولة الإنعقاد: هونكونغ - التكلفة: 5500 يورو

### مقدمة عن الدورة التدريبية:

الجريمة الإلكترونية هي أكبر خطر الآن من أي وقت مضى بسبب العدد الهائل من المتصلين من الناس بالأجهزة الإلكترونية، 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 الإلكترونية 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 الإلكترونية.
- مناقشة تشغيل أجهزة الكمبيوتر والانترنت، ومعالجة أصول الجريمة الإلكترونية ومدى انتشارها، والاستجابات من النظم القانونية للمجرمين الإلكترونيين، والأثر الاجتماعي للجرائم الإلكترونية.
- تحليل مسببات الجرائم السيبرانية من وجهات النظر الثقافية، والثقافات، والاجتماعية.

### المستفيدون من الدورة التدريبية:

في نهاية دورة الجرائم الإلكترونية والأدلة الجنائية الإلكترونية سيكون المشاركون 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 الإلكترونية في الدول.
- تحديد الطرق والتقنيات التي يشيع استخدامها من قبل المجرمين الإلكترونيين.
- 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 الإلكتروني، والحرب الإلكترونية، والاتجار بالبشر.
- دراسة قدرة نظريات علم الجريمة الحالية على تفسير الجرائم الإلكترونية.
- شرح التحديات القضائية التي تواجهها الدول عند الاستجابة للجريمة الإلكترونية.

### المحتوى العلمي للدورة التدريبية:

- الكمبيوتر وأساسيات الإنترنت
- أجهزة الكمبيوتر والبرمجيات
- البنية التحتية والاستخدام
- التكوين القانوني للجريمة الإلكترونية
- تعريف الجرائم الإلكترونية
- تصنيف الجرائم الإلكترونية
- جرائم الحاسوب
- الجرائم التي يسهلها الحاسوب
- الجرائم المدعومة بالكمبيوتر
- انتشار وتواتر الجرائم الإلكترونية
- 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