

€ TRAINING

الأدلة الجنائية داخل الجرائم الإلكترونية



الأدلة الجنائية داخل الجرائم الإلكترونية

مقدمة عن البرنامج التدريبي:

تعتبر الجريمة الإلكترونية في الوقت الحاضر هي أكبر خطراً من أي وقت مضى بسبب العدد الهائل من المتصلين من الناس بالأجهزة الإلكترونية، وهناك شكل شائع من أنواع الجرائم الإلكترونية سيتم خلال هذا البرنامج عرض ما هو التصيد الاحتيالي وكيفية التعامل مع أهم الحالات، 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 والابتزاز، والتلاعب في سوق الأوراق المالية، والتجسس المعقد للشركات، والتخطيط.

أهداف البرنامج التدريبي:

في نهاية البرنامج سيكون المشاركون قادرين على:

- معرفة القضايا التقنية والقانونية والاجتماعية المتعلقة بالجريمة الإلكترونية.
- تحليل مسببات الجرائم السيبرانية من وجهات النظر الثقافية، والثقافات، والاجتماعية.
- تحديد الطرق والتقنيات التي يشيع استخدامها من قبل المجرمين الإلكترونيين.
- دراسة قدرة نظريات علم الجريمة الحالية على تفسير الجرائم الإلكترونية.
- شرح التحديات القضائية التي تواجهها الدول عند الاستجابة للجريمة الإلكترونية.

الفئات المستهدفة:

- مدراء الاقسام القانونية في الشركات الخاصة والحكومية.
- رؤساء الاقسام القانونية والتحقيق.
- القضاة والمحامون .
- مدراء الأمن المعلوماتي.
- رؤساء الاقسام الأمنية في الشركات.

محاور البرنامج التدريبي:

الوحدة الأولى:

الكمبيوتر وأساسيات الإنترنت:

- أجهزة الكمبيوتر والبرمجيات.
- البنية التحتية والاستخدام.
- التكوين القانوني للجريمة الإلكترونية.
- تعريف الجرائم الإلكترونية.

الوحدة الثانية:

تصنيف الجرائم الإلكترونية:

- جرائم الحاسوب.
- الجرائم التي يسهلها الحاسوب.
- الجرائم المدعومة بالكمبيوتر.

الوحدة الثالثة:

انتشار وتواتر الجرائم الالكترونية:

- تصنيف الهاكرز.
- التقنيات المستخدمة من قبل المتسللين.
- الرسائل غير المرغوب فيها، والتصيد الاحتيالي، والقشط.
- استراتيجيات سلامة البيانات.

الوحدة الرابعة:

إشارات التحذير الالكترونية:

- رصد وحماية البرمجيات.
- نصائح لتجنب الفيروسات الخبيثة.
- الحقيقة حول المحتوى عبر الإنترنت.
- سرقة الهوية.

الوحدة الخامسة:

برامج التجسس والبرمجيات الخبيثة:

- قانون حماية خصوصية الأشخاص على الانترنت.
- سياسة الخصوصية.
- سلامة الشبكات الاجتماعية.
- قواعد إضافية لسلامة الشبكات على الإنترنت.