

€ TRAINING

إدارة التحقيقات في جرائم الإنترنت الإلكتروني

16 - 20 ديسمبر 2024
لندن (المملكة المتحدة)



إدارة التحقيقات في جرائم الإبتزاز الإلكتروني

رمز الدورة: Q792 تاريخ الإنعقاد: 16 - 20 ديسمبر 2024 دولة الإنعقاد: لندن (المملكة المتحدة) - التكلفة: 5850 يورو

مقدمة البرنامج التدريبي:

يهدف هذا البرنامج إلى تعزيز مهارات المشاركين في إدارة التحقيقات في جرائم الإبتزاز الإلكتروني، مع التركيز على استراتيجيات جمع الأدلة الرقمية، التحليل القانوني، وأساليب التحقيق الفعّالة. حيث سيغطي الأدوات والتقنيات الحديثة للتعامل مع هذه الجرائم وتحقيق النجاح في مكافحة الإبتزاز الإلكتروني من خلال تطبيق أفضل الممارسات في التحقيقات.

أهداف البرنامج التدريبي:

في نهاية البرنامج، سيكون المشاركون قادرين على:

- فهم الأنواع المختلفة لجريمة الإبتزاز الإلكتروني وأساليب تنفيذها.
- تطبيق الأدوات القانونية والتقنية في التحقيقات المتعلقة بالإبتزاز الإلكتروني.
- جمع وتحليل الأدلة الرقمية بفعالية خلال التحقيقات.
- تطوير استراتيجيات فعّالة للتعامل مع المبتزين والوقاية من الجريمة.
- بناء قدرات فرق التحقيق وتعزيز التنسيق بين الجهات الأمنية لمكافحة الإبتزاز الإلكتروني.

الفئات المستهدفة:

- المحققون في الجرائم الإلكترونية.
- ضباط الشرطة المختصون بالتحقيقات الجنائية.
- محامو الدفاع والادعاء.
- مستشارو الأمن السيبراني.
- مدراء التحقيقات في الجهات الحكومية والمؤسسات الأمنية.

محاور البرنامج التدريبي:

الوحدة الأولى:

مفهوم الإبتزاز الإلكتروني وأشكال الجريمة:

- تعريف جريمة الإبتزاز الإلكتروني وأسبابها.
- تصنيف الجرائم حسب نوع الضحية أفراد، مؤسسات، حكومات.
- أساليب الإبتزاز وفقًا لهدف المبتز مال، سمعة، معلومات حساسة.
- الأدوات والتقنيات المستخدمة في تنفيذ الإبتزاز الإلكتروني.
- تأثير الإبتزاز الإلكتروني على الأفراد والمجتمعات.

الوحدة الثانية:

الجوانب القانونية في جرائم الإبتزاز الإلكتروني:

- أركان جريمة الإبتزاز الإلكتروني في القوانين المحلية والدولية.
- الفرق بين الإبتزاز التقليدي والإلكتروني من الناحية القانونية.
- تحديد المسؤوليات القانونية للأطراف المتورطة في الجريمة.
- العقوبات القانونية المرتبطة بالإبتزاز الإلكتروني.
- حماية حقوق الضحايا من الناحية القانونية ودور الدعم القانوني.

الوحدة الثالثة:

التحقيق في جرائم الإبتزاز الإلكتروني:

- تقنيات جمع الأدلة الرقمية وتحليلها في سياق الإبتزاز الإلكتروني.
- التعامل مع البلاغات وطرق تقديم الدعم للضحايا.
- استخدام الأدوات التقنية للتعرف على هوية المبتزين.
- تقنيات التحقيق في الجرائم متعددة الجنسيات.
- أساليب التحقيق في حالات الإبتزاز عبر وسائل التواصل الاجتماعي.

الوحدة الرابعة:

استراتيجيات التعامل مع المبتزين والوقاية من الجريمة:

- استراتيجيات التحقيق في حالات الإبتزاز عبر البريد الإلكتروني والاختراقات.
- كيفية التعامل مع المبتزين عبر برامج المراسلة ووسائل التواصل الاجتماعي.
- الوقاية من الوقوع ضحية للإبتزاز الإلكتروني من خلال التوعية التقنية.
- بناء استراتيجيات دفاعية لحماية البيانات الشخصية من الإبتزاز.
- دور التعاون بين الأجهزة الأمنية لتقوية جهود مكافحة الإبتزاز الإلكتروني.

الوحدة الخامسة:

التدابير الوقائية والتحسين المستمر في التحقيقات:

- تحسين استراتيجيات التحقيق في جرائم الإبتزاز الإلكتروني.
- كيفية استخدام الذكاء الاصطناعي والبيانات الكبيرة في تحليل وتحقيق الجرائم الإلكترونية.
- تعزيز التعاون بين الجهات المحلية والدولية في مكافحة الإبتزاز الإلكتروني.
- تطبيق أساليب التعلم المستمر للمحققين والفرق الأمنية.
- بناء ثقافة أمان سيبراني لحماية الأفراد والمؤسسات من الإبتزاز الإلكتروني.