€TRAINING

الامن السيبراني

الامن السيبراني

مقدمة عن البرنامج التدريبي:

يهدف هذا البرنامج إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لتعزيز الأمن السيبراني في مؤسساتهم. حيث يتناول أحدث التهديدات والتقنيات المستخدمة في حماية المعلومات، مما يساعد المشاركين على فهم كيفية تأمين الأنظمة والبيانات ضد الهجمات السيبرانية.

أهداف البرنامج التدريبي:

في نهاية البرنامج سيكون المشاركون قادرين على:

- فهم محاور الأمن السيبراني و التهديدات التي تكتنفه و كيفية التعامل معها.
- معرفة الآليات الدولية و الوطنية لحماية الأمن السيبراني.
- تحديد الهجمات السيبرانية و كيفية القيام بها و نقاط الضعف و القوة في نظم المعلومات.
- فهم هجمات فيروسات الفدية و كيفية التعامل معها.
- تطوير سياسات وإجراءات الأمن السيبراني.

الفئات المستهدفة:

- ضباط الشرطة العاملين في مجال البحث الجنائي و تحليل المعلومات.
- أعضاء النيابة العامة و القضاة.
- موظفو القطاع الحكومي و الخاص.
- ضباط أمن المعلومات في القطاع الشرطي و العسكري.
- المحامون.
- مسؤولو الأمن في المؤسسات و الشركات.

محاور البرنامج التدريبي:

الوحدة الأولى:

التعريف بالأمن السيبراني ومحاوره والحماية القانونية له:

- مفهوم الأمن السيبراني.
- العناصر الأساسية للأمن السيبراني.
- الجوانب القانونية لحماية الأمن السيبراني.
- أهمية الأمن السيبراني في حماية المؤسسات.
- التهديدات السيبرانية وتأثيرها على الأمن القومي.

الوحدة الثانية:

قواعد الأمن السيبراني في المؤسسات:

- الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات.
- مهددات الأمن السيبراني في المؤسسات الصناعية والحيوية.
- الحروب السيبرانية والهجمات الموجهة لنظم المعلومات.
- قواعد الاستخدام الآمن لنظم المعلومات في المؤسسات.

- أهمية التوعية والتدريب في تعزيز الأمن السيبراني.

الوحدة الرابعة:

أدوات الأمن السيبراني:

- التعريف بالأدوات الشائعة للأمن السيبراني.
- استخدام برامج مكافحة الفيروسات والبرامج الخبيثة.
- أدوات تحليل الشبكات وكشف التهديدات.
- تطبيقات التشفير لحماية البيانات.
- تقييم فعالية الأدوات المستخدمة.

الوحدة الرابعة:

هجمات فيروسات الفدية وكيفية عملها واستراتيجية التعامل معها:

- التعريف بفيروسات الفدية.
- آلية عمل فيروسات الفدية والهدف من الهجمات المرتكبة بها.
- أشهر هجمات فيروسات الفدية والآثار المترتبة عليها.
- كيفية التعامل مع الهجمات والوقاية منها.
- استراتيجيات استجابة المؤسسات لهجمات الفدية.

الوحدة الخامسة:

الجهود الدولية والوطنية لحماية الأمن السيبراني:

- الحماية الدولية للأمن السيبراني وتنظيم قواعد الحروب السيبرانية لجنة تالين للأمن السيبراني.
- دور الاتحاد الدولي للاتصالات في تقييم الجاهزية السيبرانية للتعامل مع الهجمات السيبرانية.
- جهود الإنتربول في حماية الأمن السيبراني.
- دور التعاون الدولي في مواجهة التهديدات السيبرانية.

الوحدة السادسة:

تقييم الجاهزية السيبرانية:

- أدوات تقييم الجاهزية السيبرانية.
- تحليل نتائج تقييم الجاهزية السيبرانية.
- دور التقييم الدوري في تعزيز الأمن السيبراني.
- كيفية تحسين جاهزية المؤسسات لمواجهة التهديدات السيبرانية.
- أهمية الاستجابة السريعة للحوادث السيبرانية.

الوحدة السابعة:

الحماية المتقدمة للشبكات:

- تقنيات الحماية المتقدمة للشبكات.
- إدارة الوصول والسيطرة على المعلومات.
- حماية البيانات أثناء النقل.
- أهمية التشفير في حماية المعلومات.
- تطوير استراتيجيات الحماية للشبكات الداخلية.

الوحدة الثامنة:

تطوير سياسات وإجراءات الأمن السيبراني:

- كيفية تطوير سياسات الأمن السيبراني.
- إجراءات التعامل مع الحوادث السيبرانية.
- آليات المراجعة والتحديث المستمر للسياسات.
- دور السياسات والإجراءات في تعزيز ثقافة الأمن السيبراني.
- تحديات تنفيذ سياسات الأمن السيبراني في المؤسسات.

الوحدة التاسعة:

التعامل مع الحوادث السيبرانية:

- أنواع الحوادث السيبرانية.
- الخطوات المتبعة في التحقيق في الحوادث.
- استعادة النظام بعد الحوادث.
- توثيق الحوادث والإبلاغ عنها.
- تطوير خطط الطوارئ والاستجابة للحوادث السيبرانية.

الوحدة العاشرة:

إدارة المخاطر السيبرانية:

- مفهوم إدارة المخاطر السيبرانية.
- تحليل وتقييم المخاطر السيبرانية.
- استراتيجيات التخفيف من المخاطر.
- دور إدارة المخاطر في تحسين الأمن السيبراني.