€TRAINING

الأمن السيبراني

الأمن السيبراني

مقدمة عن البرنامج التدريبي:

في عالم يتزايد فيه الاعتماد على التكنولوجيا، أصبح الأمن السيبراني ضرورة ملحة. يهدف هذا البرنامج إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لحماية أنظمة مؤسساتهم وبياناتهم من التهديدات المتزايدة، وتمكينهم من اتخاذ القرارات الصحيحة لحمايتها. حيث يقدم فهم شامل لمبادئ الأمن السيبراني وأفضل الممارسات المتبعة لمواجهته.

أهداف البرنامج التدريبي:

في نهاية البرنامج سيكون المشاركون قادرين على:

- فهم مفهوم الأمن السيبراني وأهميته.
- تحليل التهديدات والتحديات التي تواجه الأمن السيبراني.
- تقييم الجهود الدولية والوطنية لحماية الأمن السيبراني.
- التعرف على آلية عمل فيروسات الفدية واستراتيجيات التعامل معها.
- وضع قواعد وإجراءات الأمن السيبراني في المؤسسات وتعزيز الوعي بالمخاطر.

الفئات المستهدفة:

- محترفو ومحللو الأمن السيبراني.
- مديرو تكنولوجيا المعلومات.
- المهندسون الشبكيون ومطورو النظم والبرمجيات.
- الموظفون العاملون في قطاعات البنوك والمالية المعرضة لمخاطر أمنية.
- القادة التنفيذيون المهتمون بسياسات الأمان السيبراني.
- الموظفون في القطاعات الحكومية المعنية بأمن المعلومات.
- ضباط أمن المعلومات في القطاع الشرطي و العسكري.

محاورالبرنامج 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 العصر الحديث.
- التهديدات والتحديات التي تواجه الأمن السيبراني.
- الاستراتيجيات المتبعة لتعزيز الأمن السيبراني.

الوحدة الثانية:

دراسة تحليلية لأشهر الهجمات السيبرانية:

- دراسة تحليلية لهجمات مختلفة في مختلف أنحاء العالم.
- تحليل لأهم المواقع الإحصائية للهجمات السيبرانية.

- أسباب وتداعيات الهجمات السيبرانية.
- الدروس المستفادة من الهجمات السيبرانية.

الوحدة الثالثة:

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.
- الأمن السيبراني في دولة الإمارات العربية المتحدة.
- السياسات الوطنية لحماية الأمن السيبراني.
- أهمية التعاون الدولي في مجال الأمن السيبراني.

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 فيروسات الفدية.
- التدابير الوقائية ضد فيروسات الفدية.

الوحدة الخامسة:

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.
- تطوير سياسات وإجراءات الأمن السيبراني في المؤسسات.
- أسس تدريب الموظفين على الأمن السيبراني والتوعية بالمخاطر.