



دورة أساسيات الأمن السيبراني

الوصف

يعد الأمن السيبراني في الوقت الحالي أهم عناصر الأمن في الدول المتحضرة و خاصة مع التحول الكامل نحو السيبرانية في كافة جوانب الحياة. و تقوم فكرة الأمن السيبراني على تأمين البنية التحتية المعلوماتية للدول و التي تتمثل في المنشآت الهامة و نظم المعلومات الهامة و منها نظم إدارة الحكومات الإلكترونية و التي تدار بها مؤسسات الدول الحيوية، و كذلك النظم العسكرية و الشرطة و القضائية و الاقتصادية و الصناعية و التجارية و غيرها. و بعد ما يهددها هو تهديد الأمن القومي للدول. لذا قامت العديد من الدول بإعداد الهيئات التي تختص بحماية الأمن السيبراني، و أصبح هذا المفهوم هو "جل إهتمام حكومتنا الرشيدة". فقد سخرت له كافة الإمكانيات و أصبح من معايير قياس تحضر و مدى إمكانيات الدول فيما يتعلق بالجاهزية السيبرانية لمواجهة التهديدات، و الذي يقدم الإتحاد الدولي للإتصالات سنويًا مؤشرًا يتم فيه ترتيب الدول بحسب الجاهزية.

الهدف العام

أن يكون المتدرب في نهاية المقرر قادر على أن يتعرف على قواعد و أسس و عناصر الأمن السيبراني و التهديدات المختلفة التي تهدد مستخدمي نظم المعلومات من العاملين بالمؤسسات المختلفة الصناعية و الاقتصادية، و المؤسسات ذات الطبيعة الحساسة و التي تمس بالأمن القومي، و توضيح جوانب الحماية القانونية للأمن السيبراني و محاوره، و فهم ماهية هجمات الفدية و تحليلها و كيفية إرتكابها و أشهر أنواعها. بالإضافة إلى توضيح الجهود الدولية لحماية الدول و المؤسسات الحيوية من الهجمات السيبرانية، و كذلك تدريب المشاركين على قواعد الأمن السيبراني، و كيفية التعامل مع نظم المعلومات في المؤسسات الحرجة ذات الصلة بالأمن القومي و المؤسسات الصناعية و الحيوية.

الاهداف التفصيلية

أن يكون المتدرب في نهاية المقرر قادر على أن

- يعرف الأمن السيبراني و المعرفة بقواعد و أسس الأمن السيبراني للبنية التحتية الحرجة و الحماية القانونية له
- يذكر المخاطر السيبرانية و كيفية الوقاية منها
- يتعرف على أصول و قواعد استخدام نظم المعلومات المؤسسية
- يتقن التعامل مع القواعد الدولية لحماية الأمن السيبراني
- يحدد المخاطر التي تهدد الأمن السيبراني و قواعد استخدام نظم المعلومات المؤسسية
- يتقن التعامل مع القواعد الدولية و الوطنية لحماية الأمن السيبراني و المؤسسات المختصة بحمايته



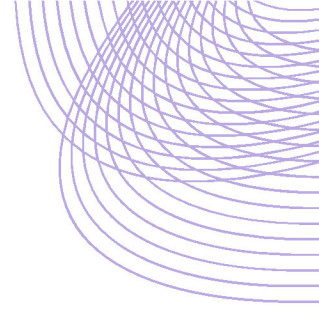
الوقت المتوقع لإتمام الحقيبة التدريبية:-

يتم التدريب على مهارات هذه الحقيبة التدريبية لجميع المتدربين وذلك في (15) ساعة تدريبية يتم توزيعها كالتالي

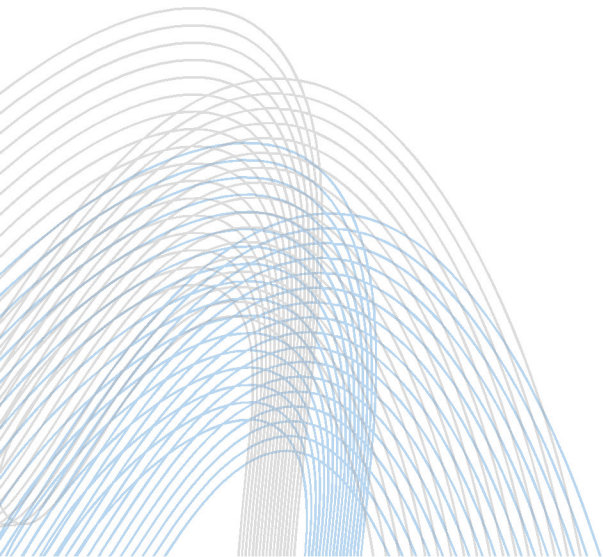
م	الموضوع	عدد الساعات
1	الأمن السيبراني	2
2	دراسات تحليلية لأشهر الهجمات السيبرانية	3
3	فيروسات الفدية	3
4	الجهود الدولية و الوطنية لحماية الأمن السيبراني	3
5	قواعد الأمن السيبراني في المؤسسات	4
	مجموع الساعات	15 ساعة

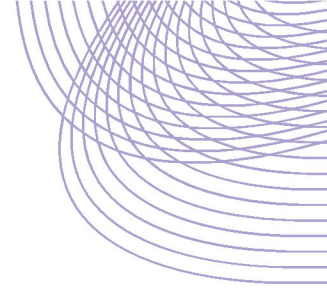


الأمن السيبراني		الأولى	
		أهداف الوحدة	
أن يكون المتدرب في نهاية الوحدة قادراً على أن : 1- يوضح العناصر الأساسية للأمن السيبراني 2- يُعرّف الأمن السيبراني 3- يذكر الجوانب القانونية لحماية الأمن السيبراني 4- يبين عناصر أمن المعلومات 5- يعرف أهمية الأمن السيبراني 6- يوضح أهداف الأمن السيبراني 7- يبين الفرق بين أمن المعلومات والأمن السيبراني			
م	عنوان الدرس	عدد الدقائق	اسلوب تقديم الموضوع
1	مفهوم الأمن السيبراني	20 دقيقة	متزامن
2	التعريف بالأمن السيبراني و محاوره و الحماية القانونية له	30 دقيقة	متزامن
3	العناصر الأساسية للأمن السيبراني	30 دقيقة	متزامن
4	الجوانب القانونية لحماية الأمن السيبراني	30 دقيقة	متزامن

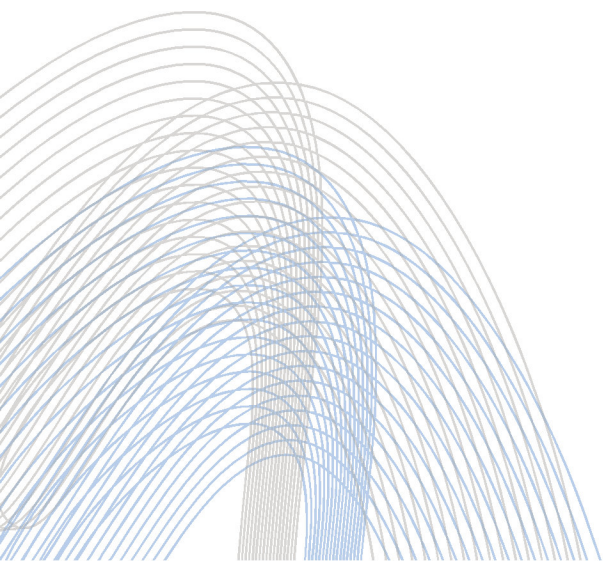


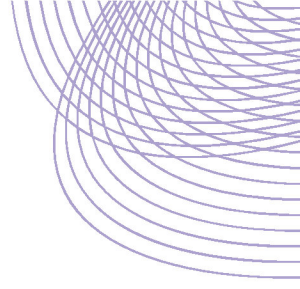
دراسات تحليلية لأشهر الهجمات السيبرانية			الثانية
أن يكون المتدرب في نهاية الوحدة قادراً على أن : 1. يوضح أشهر الهجمات السيبرانية 2. يعرّف الهجمات السيبرانية 3. يذكر كيفية التصدي للهجمات السيبرانية 4. يبين مدى أهمية الدراسات التحليلية للهجمات السيبرانية 5. يوضح أهداف الدراسات التحليلية للهجمات السيبرانية 6. يشعر بدور الدراسات التحليلية للهجوم السيبراني			أهداف الوحدة
اسلوب تقديم الموضوع	عدد الدقائق	عنوان الدرس	م
متزامن	60 دقيقة	دراسة تحليلية لهجمات أرامكو السيبرانية	1
متزامن	50 دقيقة	دراسة تحليلية لهجمات أستونيا السيبرانية و الآثار المترتبة عليها	2
متزامن	60 دقيقة	دراسة تحليلية لهجمات مختلفة في مختلف أنحاء العالم	3
متزامن	60 دقيقة	تحليل لأهم المواقع الإحصائية للهجمات السيبرانية	4



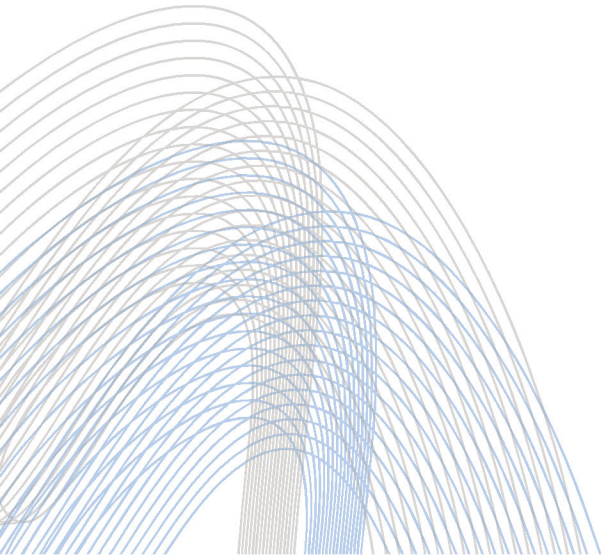


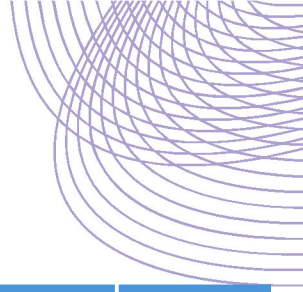
فيروسات الفدية		الثالثة	
أهداف الوحدة		أن يكون المتدرب في نهاية الوحدة قادراً على أن : 1- يوضح تعريف فيروسات الفدية 2- يُعرّف آلية عمل فيروسات الفدية 3- يبين الهدف من الهجمات المرتكبة بفيروسات الفدية 4- يوضح كيفية التعامل مع الهجمات 5- يبين الطرق المستخدمة للوقاية من الفيروسات	
م	عنوان الدرس	عدد الدقائق	اسلوب تقديم الموضوع
1	التعريف بفيروسات الفدية	45 دقيقة	متزامن
2	آلية عمل فيروسات الفدية و الهدف من الهجمات المرتكبة بها	50 دقيقة	متزامن
3	هجمات فيروسات الفدية و كيفية عملها و إستراتيجية التعامل معها	45 دقيقة	متزامن
4	كيفية التعامل مع الهجمات و الوقاية منها	60 دقيقة	متزامن





الجهود الدولية و الوطنية لحماية الأمن السيبراني			الرابعة
أن يكون المتدرب في نهاية الوحدة قادراً على أن : 1- يتعرف علي الحماية الدولية للأمن السيبراني 2- يتعرف علي قواعد الحروب السيبرانية 3- يوضح الطرق المستخدمة لحماية البيانات 4- يتعرف علي جهود الانترنت في حماية الأمن السيبراني			أهداف الوحدة
م	عنوان الدرس	عدد الدقائق	اسلوب تقديم الموضوع
1	الحماية الدولية للأمن السيبراني و تنظيم قواعد الحروب السيبرانية (لجنة تالين للأمن السيبراني)	50 دقيقة	متزامن
2	دور الإتحاد الدولي للإتصالات في تقييم الجاهزية السيبرانية للتعامل مع الهجمات السيبرانية	50 دقيقة	متزامن
3	جهود الإنترنت في حماية الأمن السيبراني	50 دقيقة	متزامن





قواعد الأمن السبيري في المؤسسات			الخامسة
أن يكون المتدرب في نهاية الوحدة قادراً على أن :			أهداف الوحدة
1. يوضح الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات 2. يتعرف علي مهنددات المن السبيري في المؤسسات الصناعية والحيوية 3. يبين مدي خطورة الهجمات الموجهة لنظم المعلومات 4. يتعرف علي قواعد الاستخدام الآمن لنظم المعلومات في المؤسسات			
م	عنوان الدرس	عدد الدقائق	اسلوب تقديم الموضوع
1	الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات	50 دقيقة	متزامن
2	مهنددات الأمن السبيري في المؤسسات الصناعية و الحيوية	60 دقيقة	متزامن
3	الحروب السبيرية و الهجمات الموجهة لنظم المعلومات	55 دقيقة	متزامن
4	قواعد الإستخدام الآمن لنظم المعلومات في المؤسسات	45 دقيقة	متزامن

