

قائمة المحتويات

13.....	تمهيد
15.....	المقدمة
19.....	الفصل الأول: مدخل في الأمن السيبراني
21.....	1. المفاهيم الأساسية للأمن السيبراني
26.....	2. إدارة الهويات والوصول (Identity and access management, IAM)
27.....	لماذا تعد إدارة الهوية والوصول مهمة؟
28.....	المكونات الرئيسية لـ IAM
30.....	تحديات أمن IAM
31.....	فوائد إدارة الهوية والوصول (IAM)
31.....	تقنيات وأدوات IAM
34.....	وظائف IAM الأساسية
35.....	مخاطر IAM
36.....	خريطة طريق إدارة الوصول
38.....	الخاتمة
38.....	أسئلة المراجعة
39.....	الفصل الثاني: أمن نظم تكنولوجيا المعلومات
42.....	المقدمة
42.....	أهداف الأمان
43.....	الهجمات Attacks
46.....	الخدمات والتقنيات Services and techniques
52.....	جوانب أخرى للأمن
53.....	جدران الحماية
56.....	الخاتمة
57.....	أسئلة للمراجعة
59.....	الفصل الثالث: أمن وحماية الشبكات
62.....	المقدمة

64.....	مفهوم الشبكات
64.....	أهمية الشبكات
65.....	مكونات الشبكة
68.....	أنواع خطوط التوصيل الرقمية
68.....	1. لنموذج OSI:
70.....	2. نموذج TCP/IP
73.....	أنواع الهجمات التي تتعرض لها كل طبقة في نموذج Osi
76.....	تأمين الشبكات
77.....	دوافع الهجوم على شبكات المعلومات:
79.....	Hacking اختراق
80.....	ملفات التجسس Spyware
82.....	طرق تحقيق أمان الشبكة
83.....	أنواع جدران الحماية
85.....	كيف يساهم جدار الحماية في أمان الشبكة؟
89.....	الخاتمة
89.....	أسئلة المراجعة
91.....	الفصل الرابع: تكنولوجيا وأمان الحوسبة السحابية
94.....	مقدمة
95.....	الخدمة السحابية
96.....	خصائص البنية الأساسية للحوسبة السحابية
102.....	أمن السحابة
104.....	نماذج خدمات الحوسبة السحابية
109.....	نماذج نشر الحوسبة السحابية
110.....	تأمين السحابة
111.....	طريق عمل أمان السحابة
113.....	ما يجعل أمن السحابة مختلف؟
114.....	المخاطر الأمنية السحابية
115.....	أهمية أمان السحابة
117.....	كيفية تأمين السحابة
120.....	التخزين السحابي ومشاركة الملفات

120.....	التحقق من إمكانات الأمان لدى موفر السحابة.....
121.....	حلول أمان السحابة المختلطة.....
122.....	حلول أمان السحابة للشركات الصغيرة والمتوسطة.....
123.....	حلول أمان السحابة للمؤسسات.....
124.....	الخاتمة.....
125.....	أسئلة المراجعة.....
127.....	الفصل الخامس: التشفير.....
130.....	المقدمة.....
131.....	أطر التشفير.....
132.....	أهم مصطلحات التشفير.....
133.....	أنواع التشفير:.....
133.....	التشفير المتماثل (Symmetric Encryption):.....
134.....	التشفير غير المتماثل (Asymmetric Encryption).....
135.....	الخوارزميات الشهيرة.....
137.....	التجزئة: (Hashing).....
140.....	التوقيع الرقمي.....
142.....	التشفير الكمي (Quantum cryptography).....
144.....	إخفاء المعلومات (Steganography).....
145.....	أشهر الهجمات التشفير:.....
148.....	الخاتمة.....
148.....	أسئلة المراجعة.....
149.....	الفصل السادس: الهندسة الاجتماعية.....
152.....	المقدمة.....
152.....	الهندسة الاجتماعية.....
153.....	عمل الهندسة الاجتماعية.....
153.....	مثال على للهندسة الاجتماعية.....
155.....	أكبر هجمات الهندسة الاجتماعية في التاريخ.....
158.....	مبادئ التأثير والتلاعب في الهندسة الاجتماعية.....
158.....	المبدأ الأول: المعاملة بالمثل (Reciprocity).....
160.....	المبدأ الثاني: الالتزام (Obligation).....

المبدأ الثالث: التنازل (Concession)	161
المبدأ الرابع: الندرة (Scarcity)	163
المبدأ الخامس: السلطة (Authority)	164
المبدأ السادس: الاتساق والالتزام (Consistency and Commitment)	166
المبدأ السابع: الإعجاب (Liking)	167
المبدأ الثامن: الإثبات الاجتماعي في التأثير مقابل التلاعب (Social Proof)	169
التأثير مقارنة بالتلاعب (Influence vs. Manipulation)	170
التفكير كالمهندس الاجتماعي	172
أنواع الهجمات الشائعة:	175
أمثلة على رسائل التصيد الاحتيالي:	176
الخاتمة	184
أسئلة المراجعة	184
الفصل السابع: استجابة الحوادث وإدارة المخاطر	185
المقدمة	188
الاستجابة للحوادث	188
الحوادث الأمنية المتعارف عليها	189
تخطيط الاستجابة للحوادث	191
مراحل استجابة الحوادث الرئيسي	192
أهمية استجابة الحوادث	195
الأدوات والتقنيات المستخدمة في الاستجابة للحوادث	196
التحديات في استجابة الحوادث:	198
إدارة المخاطر السيبرانية	198
تأطير المخاطر	200
تقييم المخاطر	201
الاستجابة للمخاطر	202
الخاتمة	206
اسئلة المراجعة	206
قائمة المراجع	207

تمهيد

يعيش العالم أمام تحديات كبيرة نتيجة التطور التقني في عصرنا الحالي وتعاملات مالية ومصرفية واجتماعية وتعليمية ضخمة وغيرها الكثير، وهذا عبء ضخم على مطوري هذه التقنيات من متابعة وتقديم الخدمات والحماية الالكترونية، لذا الكثير من المتخصصين والمهتمين ذهبوا في اتجاه اختصاص دقيق وهو أمن المعلومات والشبكات وهذا سهل علينا ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الإلكترونية التي تستهدف الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية.

الأمن السيبراني ضروري جدا في وقت ظهرت فيه الثورة التكنولوجية الهائلة والتطور المتسارع في إنتاج كل ما هو جديد من صناعات مثل الذكاء الاصطناعي والبيانات الضخمة التي تنتجها وسائل التواصل الاجتماعي يوميا، وهذا يحتاج إلى حمايتها وتأمينها بشتى الوسائل كالتشفير وبرامج حماية أجهزة المتابعة.

أوضح في هذا الكتاب ميزات وخصائص الأمن السيبراني وبعض المفاهيم الأساسية التي يجب أن يكون القارئ على دراية تامة فيها قبل الدخول إلى الفضاء السيبراني، حيث من المتوقع أن الحاجة إلى متخصصين في الأمن السيبراني في زيادة مستمرة، نظرا للتطور التكنولوجي المتسارع والنشط وكمية البيانات والمعلومات الضخمة التي نحصل عليها من استخدام شبكات الإنترنت ونظم تكنولوجيا المعلومات والتي بصدها نحن بحاجة إلى حماية في هذا العالم المظلم المليء بالمخاطر، أقدم أيضا النصائح حول كيفية حماية هويتك الشخصية عبر الإنترنت وبياناتك، ثم نتطرق إلى التعرف على أنواع المهاجمين (Hacker)، من هم؟ وماذا يريدون؟ سنتوصل إلى أهمية أن يتمتع المختصون في الأمن السيبراني بالمهارات نفسها التي يتمتع بها المهاجمون السيبرانيون. يجب على محترفي الأمن السيبراني العمل ضمن حدود القانون المحلي والوطني والدولي، كما يجب على المتخصصين في الأمن السيبراني أيضاً استخدام مهاراتهم بشكل أخلاقي. وأخيراً، يوضح هذا الفصل باختصار الهجمات السيبرانية ولماذا تحتاج الدول والحكومات إلى متخصصين في الأمن السيبراني للمساعدة في حماية مواطنهم وبنيتهم الأساسية؟

المقدمة

الإنترنت هو من بين أهم اختراعات القرن الحادي والعشرين التي أثرت على حياتنا، واليوم تجاوز الإنترنت كل الحواجز وغيّر الطريقة التي نستخدمها للتحدث ولعب الألعاب والعمل والتسوق وتكوين صداقات والاستماع إلى الموسيقى ومشاهدة الأفلام وطلب الطعام ودفع الفواتير... الخ. سمّ ما شئت، ولدينا تطبيق لذلك، فلقد سهّل حياتنا بجعلها مريحة، لقد ولت الأيام التي كان يتعين علينا فيها الوقوف في طوابير طويلة لدفع فواتير الهاتف والكهرباء، الآن يمكننا دفعها بنقرة زر من منزلنا أو مكتبنا، لقد وصلت التكنولوجيا إلى حد أننا لا نحتاج حتى إلى جهاز كمبيوتر لاستخدام الإنترنت، ولدينا هواتف ذكية وأجهزة كمبيوتر محمولة متصلة بالإنترنت... الخ، والتي يمكننا من خلالها البقاء على اتصال بأصدقائنا وعائلتنا ومكتبنا على مدار الساعة طوال أيام الأسبوع. لم يبسط الإنترنت حياتنا فحسب؛ بل جعل العديد من الأشياء في متناول الطبقة المتوسطة من خلال جعلها فعالة من حيث التكلفة. ولم يمض وقت طويل قبل أن نصل إلى مرحلة نركز فيها على عداد الثواني أثناء إجراء مكالمات هاتفية محلية أو حتى دولية، فلقد كانت المكالمات مكلفة للغاية، وكانت المكالمات الدولية والإقليمية تستخدم لنقل الرسائل العاجلة فقط، أما بقية الاتصالات الروتينية فكانت تتم باستخدام الرسائل لأنها كانت رخيصة نسبياً.

لذا أصبحت التكنولوجيا وشبكة الإنترنت جزءاً لا يتجزأ من حياتنا اليومية، حيث تشير التحليلات لأحدث البيانات من الاتحاد الدولي للاتصالات وجمعية GSMA إنتليجنس ويوروستات ومختلف الجهات الحكومية المحلية إلى أن هناك نمو في مستخدمي الإنترنت في العالم بنسبة 1.8٪ خلال الأشهر الاثني عشر الماضية، حيث ارتفع العدد الإجمالي العالمي إلى 5.35 مليار في بداية عام 2024، وقد وصلت إحصائيات من شهر أكتوبر 2024، أن عدد مستخدمي الإنترنت في جميع أنحاء العالم 5.52 مليار، وهو ما يعادل 67.5% من سكان العالم. ومن هذا الإجمالي، كان 5.22 مليار، أو 63.8% من سكان العالم، من مستخدمي