

الكتاب الرابع

الأمن السيبراني

وحماية شبكات المعلومات

من الفيروسات

محتويات الفهرس

٧	المقدمة
٩	الفصل الأول: الفيروسات فيروسات الحاسوب (كنموذج)
٢٣	الفصل الثاني: الفيروسات وأمنية المعلومات على الشبكات اللاسلكية
٥١	الفصل الثالث: الأمن السيبراني للحاسوب
٦٧	الفصل الرابع: مضاد الفيروسات السيبرانية الخطيرة
٨٧	الفصل الخامس: مضادات الفيروسات (أفاست كنموذج)
١٢٩	الفصل السادس: سمات برامج الفيروسات المتقدمة
١٥١	الفصل السابع: الانترنت تعريفه، بدايته، وأشهر جرائمه
١٦٩	الفصل الثامن: اعدادات الحماية المضمنة
١٩٩	الفصل التاسع: كيفية تفعيل شاشة - توقف مضاد الفيروسات أفاست!
٢١٣	قائمة المراجع

المقدمة

عادة ما توظف مجموعة متنوعة من الاستراتيجيات. تشمل الفحص المستند على الكشف عن نماذج معروفة من البرمجيات الخبيثة في كود قابل للتنفيذ ومع ذلك يمكن للمستخدم أن يكون مصابا ببرمجيات خبيثة جديدة التي لا يوجد لها حتى الآن توقيع. لمواجهة هذا الذي يسمى تهديدات اليوم صفر، يمكن استخدام الاستدلال. وهو أحد أنواع النهج الإرشادي الذي يستند إلى التوقعات العامة للتعرف على الفيروسات الجديدة. تختلف أشكال الفيروسات الموجودة يتم اكتشافها بالبحث عن أكواد البرمجيات الخبيثة المعروفة في الملفات. بعض برامج الحماية من الفيروسات ويمكنها أيضا التنبؤ بما سوف يحدث تفعل إذا فتح الملف بمحاكاتها في صندوق رمل وتحليل ما تقوم به لمعرفة ما إذا كانت تنفذ أية إجراءات ضارة. إذا نفذت هذا، يمكن أن يعني هذا أن الملف ضار.