

۵۱ نکته‌ی سودمند درباره‌ی حملات سایبری

نویسنده: سید علی موسوی



آشناسازان کتاب و نوشتن

سرشناسه: موسوی، سیدعلی، ۱۳۶۴ مرداد -
عنوان و نام پدیدآور: ۵۱ نکته‌ی سودمند درباره‌ی حملات سایبری / نویسنده سیدعلی موسوی.
موضوعات: نشر: تهران: نسل روشن، ۱۳۹۶.
مشخصات ظاهری: ۷۵ ص.

شابک: ۹۷۸-۶۰۰-۸۷۵۲-۱۵-۸

وضعیت فهرست نویسی: فیبا
عنوان گسترده: راه و نکته‌ی سودمند درباره‌ی حملات سایبری.

موضوع: شبکه‌های رایجیوتری -- تدابیر ایمنی

موضوع: Computer networks -- Security measures

موضوع: فضای مجازی -- تدابیر ایمنی

موضوع: Cyberspace -- Security measures

موضوع: جرایم کامپیوتری -- پیشگیری

موضوع: Computer crimes -- Prevention

موضوع: شرکت‌ها -- تدابیر ایمنی

موضوع: Corporations -- Security measures

رده بندی کنگره: ۱۳۹۶ پ ۹/۲/۴۳

رده بندی دیویی: ۶۵۸/۴۷۸

شماره کتابشناسی ملی: ۴۷۶۴۹۶۲

۵۱ نکته‌ی سودمند درباره‌ی حملات سایبری

نام کتاب:

انتشارات نسل روشن

ناشر:

سید علی موسوی

نویسنده:

علیرضا زمانی

صفحه‌آرایی و طراحی جلد:

حمزه‌ای

چاپخانه صحافی:

اول ۱۳۹۶

نوبت چاپ:

۱۰۰۰ نسخه

شمارگان:

۷۰,۰۰۰ ریال

قیمت:

۹۷۸-۶۰۰-۸۷۵۲-۱۵-۸

شابک:

WWW.NASLEROSHAN.IR

تهران - میدان انقلاب، مابین خیابان فخررازی و خیابان دانشگاه، خیابان شهید نظری

پلاک ۶۱ - طبقه چهارم واحد ۴۴. تلفن: ۶۶۹۵۳۱۲۶

به نام خدا

انسان مثال گیاهی است که خشک شده و از بین می‌رود و تمام زیبایی‌های انسان نیز همچون گلی است که پژمرده می‌شود.

آری؛ گیاه خشک و پژمرده می‌شود و انسان نیز مانند گیاه از بین می‌رود اما آثارها، کلام، آثار و آثار او باقی می‌ماند.

انتشارات نسل روشن در تلاش است تا با ایجاد یک بستر مناسب در حمایت از مولفان، هم‌نشینان، نگاری ایده‌ها، آثار و افکار آن‌ها و با انتشار کتابی ارزشمند که از سطح علمی مطلوبی برخوردار باشد به وظیفه‌ی انسانی و اعتقادی خویش عمل کند تا بتواند اثری سازنده را به عنوان میراثی ناچیز برای نسل روشن باقی گذارد.

هر روز اخبار جدیدی در مورد حملات و تهدیدات رایانه‌ای منتشر می‌شود. این تهدیدات شامل ویروس‌های جدید و یا انواع هک و نفوذ در سیستم‌های رایانه‌ای است. در این کتاب به چند نکته که در رابطه با امنیت رایانه اهمیت اساسی دارند به صورت مختصر پرداخته می‌شود. یک کاربر یا مدیر در صورت رعایت این نکات می‌تواند از حد زیادی از حفظ امنیت سیستم رایانه‌ای خود مطمئن باشد.

سیدعلی موسوی

dr.ali.moosavi2000@gmail.com

- ۱ - مشخصه های حملات سایبری و تاریخچه ی آن ها
- ۲ - طهی بین امنیت سایبری و افراد معتبری که از فضای سایبری استفاده می کنند
- ۱ - دلیلی برای استفاده از اینترنت به عنوان بستری برای انجام حملات
- ۴ - در ۱ خرس بود بازار های هک به عنوان مشوقی برای جرایم سایبری
- ۵ - وسعت به حد و ۱ ره برای شروع حملات سایبری: هیچ چیز امن نیست
- ۶ - فعالترین کشور ها در زمینه ی آنها
- ۷ - مشهور ترین گروه ها ۱ ری در ادوار زمانی
- ۸ - نکاتی مهم برای دانستن در زمینه ی ب پذیری سایبری
- ۹ - رایج ترین جرایم سایبری به همراه توضیح آنها
- ۱۰ - انواع مهاجمین سایبری از دیدگاه های مختلف
- ۱۱ - انواع حملات سایبری و شناخت آنها
- ۱۲ - نمونه هایی از جرایم سایبری و کسب اطلاعات برای حفظ امنیت
- ۱۳ - نشانه های اولیه برای آن که بفهمید شاید مورد حمله ی سایبری قرار گرفته باشید
- ۱۴ - نشانه های قطعی برای پی بردن به این که به یک سیستم نفوذ شده است
- ۱۵ - راه های نسبتا ساده ای که هکرها با استفاده از آنها به اطلاعات شما دسترسی پیدا می کنند
- ۱۶ - روش هایی نسبتا ساده که با آنها می توان از بسیاری از حملات جلوگیری کرد
- ۱۷ - راه های کاهش خطر وب سایت ها
- ۱۸ - پوشش امنیتی ناقصی که توسط آنتی ویروس های متداول ارائه می شود

- ۴۲ - راه‌های برای مراقبت و جلوگیری از وقوع حملات سایبری
- ۴۳ - بدافزار: انتشار، انواع و راه‌های جلوگیری
- ۴۴ - پنهان‌سازی: راه‌های پنهان شده برای حفظ امنیت
- ۴۵ - باج‌افزار: تاریخچه، انواع و سرگذشت آن در طول زمان
- ۴۶ - دسته‌بندی باج‌افزارها بر اساس مدت و پیچیدگی
- ۴۷ - چگونه از خودتان در مقابل حملات باج‌افزار محافظت کنید؟
- ۴۸ - راه‌حل‌های پیشنهادی برای زمانی که تحت حمله‌ای باج‌افزاری قرار گرفته‌اید
- ۴۹ - شرکت‌ها چرا و چگونه پول را به عنوان باج به باج‌افزارها می‌دهند؟
- ۵۰ - هدف از حمله‌ای باج‌افزاری به مؤسسات عمومی
- ۵۱ - باج‌افزار: سلاحی برای نابودی اقتصاد
- ۵۲ - افزایش حملات سایبری ای که تجارت‌های نوپا را هدف قرار می‌دهند.
- ۵۳ - دفاع موثر: دانستن گستره‌ی تهدیدات
- ۵۴ - ابزارهایی که توسط هکرها به کار گرفته می‌شوند و روش‌های مقابله‌ای با آن‌ها
- ۵۵ - تکنیک‌هایی که به طور معمول توسط مجرمان سایبری به کار گرفته می‌شوند و راه‌های
گیری از آن‌ها
- ۵۶ - چگونه با تهدیدات داخلی (در زمینه‌ی جرایم سایبری) مقابله کنیم؟
- ۵۷ - چگونه حملات سازماندهی شده را محدود کنیم؟
- ۵۸ - استفاده از مهندسی اجتماعی به عنوان روشی برای آغاز حملات سایبری

- ۳۶ - تهدیداتی که متوجه افراد می‌شود و خودشان در آن مقصرند
- ۳۷ - راه‌هایی برای کم رنگ کردن نقش انسانی در حملات سایبری
- ۳۸ - اعضای گروه های هکری
- ۳۹ - بهترین سیستم عامل برای مجرمان سایبری
- ۴۰ - راه‌هایی برای ردیابی هک‌هایی که پشت حملات سایبری هستند.
- ۴۱ - سنجش میزان امنیت پس از صورت گرفتن حمله سایبری: پیشگیری
- ۴۲ - اندازه گیری امنیت در حین صورت گرفتن حمله‌ی سایبری: مدیریت رخداد
- ۴۳ - اندازه گیری امنیت پس از صورت گرفته حمله‌ی سایبری: مدیریت نتایج و آثار
- ۴۴ - آزادی در فضای مجازی، در زمانه‌ی ترس از آن
- ۴۵ - بررسی حملات هوشمند سایبری در ابعاد سترده: جمع‌بندی احتمالی‌ای که با آن اتفاق می‌افتد.
- ۴۶ - تلاش جهانی برای جلوگیری از حملات سایبری
- ۴۷ - نقش مجازات در کاهش جرایم سایبری
- ۴۸ - کافی نبودن قانون برای متوقف کردن مجرمان سایبری (سهایی بدون کمک)
- ۴۹ - پیش نیازهای اعتلای آگاهی در برابر تهدیدات
- ۵۰ - دنیای امروز ما...
- ۵۱ - افزایش توانایی دولت‌ها در مقابله‌ی با جرایم سایبری

■ مقدمه

در این کتاب ۵۱ نکته‌ی سودمند موجود است که با استفاده از آن‌ها می‌توانید بفهمید که چگونه از رایانه‌های خود محافظت کنید و چه نشانه‌هایی به شما می‌گویند که ممکن است اطلاعات شما تحت نفوذ قرار گرفته باشند. مطالعه‌ی این کتاب برای افراد و صاحبان تجارت ضروریست. تهدیدات سایبری دائماً در حال رشد هستند و اهدانی که پشت آنهاست نیز روز به روز تغییر می‌کند. جوانان نیز به صورت روزافزون در این جنایات و جرایم سایبری نقش پررنگ‌تری ایفا می‌کنند. تمام انواع تحولات در خطر حملات سایبری قرار دارند و این در حالی است که آن‌ها راه محافظت از خودشان آمادگی‌های لازم را ندارند و این گونه حملات سایبری به فشارهای روحی و نیز ضررهای مالی می‌انجامند. با گذشت سال‌ها، فرآیند هک کردن - که طبق عادت آن‌ها را جرایمی تحت عنوان کلاه‌نویسی و... می‌خوانیم - به طور کلی تغییر کرده است. علاوه بر این، کرها با بکارگیری بد افزارها، به صورت رو به افزایشی از مهندسان امنیت برای دستیابی به اهدافشان استفاده می‌کنند. بنابراین افزایش داه‌ی در زمینه‌ی روش‌ها و نتایج حملات سایبری امری ضروری می‌باشد.