

مبانی امنیت در اینترنت

تألیف: عرفان باسیمی نژاد

اکرم آزادی سوابله



سرشناسنامه	: یاسمی نژاد، عرفان، ۱۳۶۵-
عنوان و نام پدیدآور	: مبانی امنیت در اینترنت/ عرفان یاسمی نژاد، اکرم آزادی سرابله.
مشخصات نشر	: تهران: نیروی انتظامی جمهوری اسلامی ایران، پلیس فتا، ۱۳۹۲.
مشخصات ظاهری	: ۴۸۲ ص. مصور.
شابک	: ۹۷۸-۶۰۰-۹۳۴۰۱-۲-۵
وضعیت فهرست نویسی	: فیپا
موضوع	: اینترنت—تدابیر ایمنی
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: کامپیوترها -- ایمنی اطلاعات
موضوع	: پایگاه‌های اطلاعاتی -- امنیت
شناسه افزوده	: آزادی سرابله، اکرم - ۱۳۶۵
شناسه افزوده	: نیروی انتظامی جمهوری اسلامی ایران، پلیس فتا
رده‌بندی کنگره	: ۱۳۹۲ م ۲/ی ۵۹/۵۱۰۵ TK
رده‌بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۳۲۴۶۶۶۲



نام کتاب	: امنیت در اینترنت
ناشر	: پلیس فتا
مولفان	: عرفان یاسمی نژاد، اکرم آزادی سرابله
ویراستار	: علی نیک‌نفس
نظارت	: محسن خداپرست
چاپ اول	: ۱۳۹۲
تیراژ	: ۱۰۰۰ جلد
لیتوگرافی، چاپ و صحافی	: چاپ و نشر حدیث کوثر
قیمت	: ۱۹۰۰۰۰ ریال
شابک	: ۹۷۸-۶۰۰-۹۳۴۰۱-۲-۵
ISBN	: 978-600-93401-2-5

فهرست مطالب

۱۷	۱- آشنایی با مهمترین تهدیدهای امنیتی
۲۰	۱-۱ ویروس
۲۱	۲-۱ کرم
۲۲	۱-۲ سازندگان کرم چرا آنها را می‌سازند؟ آیا دلیل مالی نیز برای این کار دارند؟
۲۳	۲-۲-۱ فرشته کرم‌ها، کرم‌هایی با اهداف خوب
۲۳	۳-۱ تروجان یا اسب تروا
۲۴	۱-۳-۱ اهداف و عملکرد
۲۵	۲-۳-۱ انتقال و نصب
۲۷	۳-۳-۱ اگر به تروجان آلوده شدید
۲۷	۴-۳-۱ شیوع تروجان‌ها
۲۸	۴-۱ اسپم
۲۸	۱-۴-۱ دسته‌بندی اسپم‌ها
۳۰	۲-۴-۱ راهکارهایی برای جلوگیری از دریافت ایمیل‌های اسپم
۳۱	۵-۱ اسپای ورها، دزد اطلاعات شما هستند
۳۲	۱-۵-۱ انواع اسپای ورها
۳۲	۲-۵-۱ راه‌های نفوذ اسپای‌ورها
۳۳	۳-۵-۱ نشانه‌های وجود جاسوس‌افزار در کامپیوتر
۳۵	۴-۵-۱ مشکلات
۳۵	۶-۱ آدورها، تبلیغات بازرگانی ناخواسته‌ی دنیای کامپیوتر
۳۶	۷-۱ روت‌کیت‌ها
۳۶	۸-۱ حقه‌بازی اینترنتی یا Spoofing چیست؟
۳۶	۹-۱ کلاهبرداری ایمیلی
۳۶	۱۰-۱ کلاهبرداری وب‌سایتی
۳۷	۱۱-۱ کلیک دزدی یا Clickjacking چیست؟
۳۸	۱-۱۱-۱ چطور متوجه یک صفحه مشکوک شویم؟
۳۹	۲-۱۱-۱ راه مقابله

۴۰	۱۲-۱ حملات اکس اس اس
۴۰	۱۳-۱ آنتی‌ویروس‌های جعلی و Ransomware
۴۲	۱-۱۳-۱ چگونه از خودمان در برابر این برنامه‌ها محافظت کنیم؟
۴۲	۱۴-۱ کلاهبرداری از طریق SMS یا Smishing
۴۳	۱۵-۱ BlueBugging
۴۳	۱۶-۱ Pod luring
۴۳	۱۷-۱ Sidejacking
۴۳	۱۸-۱ Black Hat
۴۴	۱۹-۱ White hat
۴۴	۲۰-۱ Script Kiddy
۴۴	۲۱-۱ Social Engineering (مهندسی اجتماعی)
۴۴	۲۲-۱ Crapware
۴۵	۲۳-۱ کامپیوتر زامبی چیست و چگونه عمل می‌کند؟
۴۵	۱-۲۳-۱ هک کردن کامپیوتر
۴۶	۲-۲۳-۱ توزیع هرزنامه‌ها (اسپم)
۴۸	۳-۲۳-۱ زامبی یا هر نام دیگری
۴۸	۴-۲۳-۱ حملات عدم سرویس‌دهی توزیع شده (DDoS)
۵۰	۵-۲۳-۱ کلاهبرداری در کلیک (Click Fraud)
۵۱	۶-۲۳-۱ چگونه زامبی نشویم؟
۵۴	۲- انتخاب رمز عبور مناسب و سؤالات امنیتی
۵۵	۱-۲ چگونه کلمات عبور بهتری بسازیم؟
۵۸	۲-۲ چه عواملی یک پسورد را در مقابل حملات، قدرتمند می‌سازد؟
۵۹	۳-۲ ساختن یک پسورد قوی که بتوان به یاد آورد
۶۰	۴-۲ الگوهای خطرناک پسورد که باید از آن اجتناب شود
۶۱	۵-۲ چند نکته برای این که پسورد خود را مخفی نگاه دارید
۶۳	۶-۲ پسورد جدید خود را با Password Checker تست کنید
۷۰	۷-۲ پرکاربردترین کدهای قفل صفحه نمایش موبایل که باید از آنها پرهیز کنیم
۷۱	۸-۲ مدیریت بحران پس از لو رفتن رمز عبور ایمیل
۷۱	۱-۸-۲ ریست/بازیابی رمز ورود

۷۱	۲-۸-۲ فاکتور تأیید هویت را ارتقاء دهید
۷۱	۳-۸-۲ تنظیمات مربوط به ایمیل خود را با تدابیر مناسب مدیریت کنید
۷۲	۴-۸-۲ به نکات ایجاد یک رمز عبور قوی توجه کنید
۷۲	۵-۸-۲ تمام رمز عبورهای مرتبط با آدرس ایمیل خود را عوض کنید
۷۲	۶-۸-۲ از برنامه مدیریت رمزعبور استفاده کنید
۷۳	۷-۸-۲ ایمیل خود را برای یادآوری‌های زمان ثبت‌نام جستجو کنید
۷۳	۸-۸-۲ کلمات عبور همیشه باید از حداقل بیشتر باشد
۷۴	۹-۲ سوالات امنیتی
۷۹	۳- مدیریت رمزهای عبور
۸۲	۱-۳ صندوقچه اسرار برای رمزهای عبور با KeePass
۸۲	۱-۱-۳ آنچه شما بعد از خواندن این متن خواهید دانست
۸۲	۲-۱-۳ چگونه از کی‌پس استفاده کنیم؟
۸۳	۳-۱-۳ چگونگی ساخت بانک اطلاعاتی جدید، برای نگهداری رمزهای عبور
۸۷	۴-۱-۳ چگونگی اضافه کردن رمزعبور به بانک اطلاعاتی کی‌پس
۹۱	۵-۱-۳ چگونه ورودی ساخته شده را ویرایش کنیم؟
۹۲	۶-۱-۳ چگونه رمزعبور تصادفی و امن بسازیم؟
۹۴	۷-۱-۳ چگونگی ورود و خروج نرم‌افزار
۹۵	۸-۱-۳ چگونه رمزعبور اصلی را عوض کنیم؟
۹۵	۹-۱-۳ چگونه از رمزهای عبور ذخیره شده در بانک اطلاعاتی نرم‌افزار استفاده کنیم؟
۹۷	۲-۳ LastPass، نرم‌افزار امن مدیریت پسورد از طریق اینترنت
۹۷	۱-۲-۳ چرا LastPass؟
۱۰۰	۲-۲-۳ افزونه‌های ویژه مرورگرها
۱۰۱	۳-۲-۳ چند تنظیم مفید و مهم
۱۰۲	۴-۲-۳ رمزعبورهای یکبار مصرف یا One-Time Passwords
۱۰۳	۵-۲-۳ یادداشت‌های امن یا Secure Notes
۱۰۳	۶-۲-۳ برنامه ویژه تلفن‌های همراه هوشمند
۱۰۴	۳-۳ PasswordCard دستیار شما در انتخاب رمزهای عبور مطمئن
۱۰۵	۱-۳-۳ چگونه از کارت رمز استفاده کنیم؟

۱۰۷	۴- امنیت در مرورگرهای اینترنتی
۱۱۰	۴-۱ چرا امنیت مرورگر مهم است؟
۱۱۰	۴-۲ چه مرورگری استفاده کنیم؟
۱۱۸	۴-۳ خطرات و راهکارها
۱۱۸	۴-۴ امنیت مرورگر چگونه تهدید می‌شود؟
۱۱۹	۴-۵ افزونه چیست؟
۱۱۹	۴-۶ معرفی چند افزونه امنیتی برای مرورگرها
۱۱۹	۴-۶-۱ Stealther
۱۱۹	۴-۶-۲ Close 'n' Forget
۱۲۰	۴-۶-۳ WOT
۱۲۳	۴-۶-۴ NoScript
۱۲۶	۴-۶-۵ فعال‌سازی قابلیت "Click to Play (FlashBlock)" در گوگل کروم
۱۲۸	۴-۶-۶ Https Everywhere
۱۲۹	۴-۶-۷ Panic
۱۳۰	۴-۶-۸ hideBad
۱۳۰	۴-۶-۹ TabRenamizer / Page Title Eraser
۱۳۱	۴-۶-۱۰ Gish It / tEMPORARYiNBOX / spamavert
۱۳۱	۴-۶-۱۱ BetterPrivacy
۱۳۱	۴-۶-۱۲ Ghostery
۱۳۲	۴-۶-۱۳ JSview
۱۳۲	۴-۷ کوکی چیست و چگونه کار می‌کنند؟
۱۳۲	۴-۷-۱ اساس کار کوکی‌ها
۱۳۴	۴-۷-۲ چگونگی انتقال اطلاعات کوکی
۱۳۵	۴-۷-۳ چگونه وبسایت‌ها از کوکی استفاده می‌کنند؟
۱۳۶	۴-۷-۴ مشکلات کوکی‌ها
۱۳۷	۴-۷-۵ کوکی‌ها در اینترنت: مشکلات حریم خصوصی
۱۳۸	۴-۷-۶ کوکی‌ها و امنیت
۱۳۹	۴-۸ نسخه دروغین فایرفاکس و آپدیت ویندوز
۱۴۰	۴-۹ Do Not Track چیست؟
۱۴۱	۴-۹-۱ چگونه Do Not Track را در مرورگر خود فعال کنم؟

۱۴۱	۲-۹-۴ فعال سازی Do Not Track در مرورگر اینترنت اکسپلورر
۱۴۱	۳-۹-۴ فعال سازی Do Not Track در مرورگر موزیلا فایرفاکس
۱۴۲	۴-۹-۴ فعال سازی Do Not Track در مرورگر گوگل کروم
۱۴۳	۱۰-۴ تست امنیت مرورگر رایانه شما
۱۴۴	۱-۱۰-۴ سرویس browser check موارد زیر را چک می کند
۱۴۴	۱۱-۴ اس اس ال چیست و چرا توجه به آن بسیار مهم است؟
۱۴۵	۱-۱۱-۴ اطلاعات معمولاً کی و کجا دزدیده می شوند؟
۱۴۵	۲-۱۱-۴ اطلاعات در اینترنت چگونه جابه جا می شوند؟
۱۴۶	۳-۱۱-۴ SSL چیست؟
۱۴۶	۴-۱۱-۴ ملزومات ارتباط بر پایه اس اس ال
۱۴۶	۵-۱۱-۴ رمزنگاری
۱۴۷	۶-۱۱-۴ اس اس ال چگونه کار می کند؟
۱۴۸	۷-۱۱-۴ چگونه می توان مطمئن شد، یک سایت از اس اس ال استفاده می کند؟
۱۴۸	۸-۱۱-۴ چگونه اس اس ال ایمیل را فعال کنیم؟
۱۴۹	۹-۱۱-۴ حساب های بانکی
۱۴۹	۱۰-۱۱-۴ هشدارهای امنیتی مرورگرها را جدی بگیرید
۱۵۲	۱۱-۱۱-۴ پیام های مشکل SSL
۱۵۲	۱۲-۱۱-۴ مشخصات سایت
۱۵۳	۱۳-۱۱-۴ ارتباط شما با سایت
۱۵۳	۱۴-۱۱-۴ تاریخچه بازدید از این سایت
۱۵۴	۱۲-۴ مرورگر وب ناشناس که کاملاً خصوصی و ایمن هستند
۱۵۴	۱-۱۲-۴ بسته مرورگر تر (Tor)
۱۵۶	۲-۱۲-۴ اس آر ور آیرن (SRWare Iron)
۱۵۷	۳-۱۲-۴ مرورگرهای وب مانع شده: گوست زیلا (Ghostzilla) و اپراتور
۱۵۷	۱۳-۴ آماری از مرورگرهای استفاده شده توسط کاربران اینترنت در دنیا
۱۶۰	۱-۱۳-۴ آماری از مرورگرهای استفاده شده توسط کاربران ایرانی
۱۶۴	۲-۱۳-۴ آماری از مرورگرهای استفاده شده در موبایل
۱۶۷	۱۵- امنیت ایمیل و چت
۱۶۹	۱-۵ یک ایمیل چگونه ارسال می شود

۱۷۰	۱-۱-۵ بررسی محتوای یک پیام ایمیلی
۱۷۱	۲-۱-۵ هدر
۱۷۱	۳-۱-۵ بخش مقدماتی و پایه
۱۷۲	۴-۱-۵ اطلاعات مسیریابی
۱۷۶	۵-۱-۵ اطلاعات قابل رؤیت هدر
۱۷۷	۶-۱-۵ شیوه شناسایی «هدر جعلی»
۱۷۸	۷-۱-۵ مخ‌گیری اسپمر زرنگ
۱۷۸	۸-۱-۵ متن پیام
۱۸۰	۲-۵ امنیت در ایمیل
۱۸۰	۳-۵ چگونه ارتباطات ایمیلی امن داشته باشیم؟
۱۸۱	۴-۵ امنیت ارتباطات ایمیلی وقتی که از Webmail استفاده می‌کنید
۱۸۱	۵-۵ چگونه ایمیل‌مان را محرمانه نگه داریم؟
۱۸۳	۶-۵ مهاجرت به یک سرویس ایمیل امن‌تر
۱۸۴	۷-۵ راه حل دوم استفاده از سرویس RiseUp
۱۸۵	۸-۵ نکات تکمیلی برای بالا بردن سطح امنیت ایمیل
۱۸۶	۹-۵ توصیه‌های امنیتی گوگل برای سرویس پست الکترونیک جی‌میل
۱۹۳	۱۰-۵ امکان جدید گوگل برای افزایش امنیت حساب کاربران
۱۹۳	۱۰-۱۰-۵ Two-Step Verification چیست؟
۱۹۶	۱۱-۵ از کجا بفهمیم Gmail ما هک شده است؟
۱۹۹	۱۲-۵ اگر واقعاً اکانت شما هک شده باشد، چه باید بکنید؟
۱۹۹	۱۳-۵ راهنمای استفاده از چند حساب کاربری گوگل به‌طور همزمان
۲۰۲	۱۴-۵ ساخت آدرس‌های ایمیل موقت در هات‌میل
۲۰۵	۱۵-۵ چند روش برای امنیت بیشتر و نگارش بهتر ایمیل
۲۱۱	۱۶-۵ امنیت در چت
۲۱۱	۱۷-۵ نرم‌افزارهای پیام‌رسان امن
۲۱۳	۱-۱۷-۵ پیجین: پیام‌رسانی امن، برای چت
۲۱۵	۲-۱۷-۵ چگونگی اضافه‌نمودن یک اکانت به پیجین
۲۲۰	۳-۱۷-۵ شیوه افزودن آی‌دی یک فرد از طریق پیجین
۲۲۲	۴-۱۷-۵ چگونه با افراد لیست خود چت کنیم؟
۲۲۴	۵-۱۷-۵ امنیت چت در پیجین توسط پلاگین OTR

۲۲۴	۶-۱۷-۵ چگونگی راه‌اندازی پلاگین OTR بر روی پيچين
۲۲۵	۷-۱۷-۵ نحوه ساخت کلید رمزنگار
۲۲۷	۸-۱۷-۵ چگونگی ايجاد يك گفتگوی امن و مطمئن
۲۳۲	۹-۱۷-۵ چگونه يك كانكشن (ارتباط) امن داشته باشیم؟
۲۳۳	۶- آنتی‌ویروس‌ها و انتخاب آن‌ها
۲۳۵	۱-۶ خصوصیات یک نرم‌افزار آنتی‌ویروس مناسب
۲۳۵	۱-۱-۶ شناسایی هوشمندانه ویروس‌ها
۲۳۶	۲-۱-۶ به‌روزرسانی
۲۳۶	۳-۱-۶ اسکن اطلاعات ذخیره شده در هارد
۲۳۷	۴-۱-۶ صندوقچه ویروس‌ها یا مکانی برای قرنطینه
۲۳۷	۵-۱-۶ قابلیت‌های اضافی و نکات ضروری
۲۳۷	۶-۱-۶ میزان مصرف رم و پردازنده
۲۳۷	۲-۶ آنتی‌ویروس رایگان یا تجاری؟
۲۳۸	۱-۲-۶ به حرف فروشنده‌ها اعتماد نکنید
۲۳۸	۲-۲-۶ آنتی‌ویروس‌های رایگان پیشنهادی
۲۳۹	۳-۶ شیوه ویروس‌یابی کامپیوتر آلوده توسط لایو سی دی اوبونتو
۲۵۱	۴-۶ چهار آنتی‌ویروس مناسب ویژه لینوکس
۲۵۱	۱-۴-۶ AVAST
۲۵۲	۲-۴-۶ BitDefender
۲۵۳	۳-۴-۶ ClamAV
۲۵۴	۴-۴-۶ AVG
۲۵۵	۵-۶ پنج آنتی‌ویروس برای مک و آیا مک نیازمند آنتی‌ویروس است؟
۲۶۲	۶-۶ بهترین مرجع بررسی آنتی‌ویروس‌ها
۲۶۷	۷- نرم‌افزارهای ضد جاسوس افزار و تبلیغ افزار
۲۷۰	۱-۷ کامپیوتر شما چگونه به جاسوس افزار آلوده می‌گردد؟
۲۷۲	۲-۷ جاسوس افزار چه کارهایی می‌تواند انجام دهد
۲۷۳	۳-۷ قوانین دولتی
۲۷۵	۴-۷ Ad-Aware

- ۲۷۵ ۵-۷ اسپای بات، ایمنی در برابر جاسوس افزارها
- ۲۷۶ ۱-۵-۷ نصب اسپای بات
- ۲۷۷ ۲-۵-۷ تنظیمات اسپای بات هنگام اولین اجرا
- ۲۷۹ ۳-۵-۷ آپدیت اسپای بات
- ۲۸۱ ۴-۵-۷ چگونه سیستم را ایمن کنیم
- ۲۸۲ ۵-۵-۷ اسکن سیستم با اسپای بات
- ۲۸۴ ۶-۵-۷ تی فایمر دائم
- ۲۸۶ ۷-۵-۷ چگونه از ابزار بازیابی استفاده کنیم
- ۲۸۸ ۸-۵-۷ سؤالات رایج
- ۲۸۹ ۶-۷ نسخه پرتابل SuperAntispyware
- ۲۹۰ ۷-۷ نکاتی که برای جلوگیری از نصب جاسوس افزارها لازم است بدانید و رعایت کنید
- ۲۹۱ ۸- دیوار آتش و لزوم استفاده از آن
- ۲۹۳ ۱-۸ مقدمه ای بر فایروال
- ۲۹۵ ۲-۸ ابزار فایروال چه می کند؟
- ۲۹۶ ۳-۸ پیکربندی فایروال
- ۲۹۹ ۴-۸ چرا از حفاظ امنیتی فایروال استفاده می کنیم؟
- ۳۰۲ ۵-۸ پروکسی سرورها و DMZ
- ۳۰۳ ۶-۸ کنترل دیواره ی آتش ویندوز ۷
- ۳۰۵ ۷-۸ کومودو، دیواره آتش کامپیوتر شما
- ۳۰۶ ۱-۷-۸ شروع کار با کومودو
- ۳۰۷ ۲-۷-۸ چگونه اجازه دسترسی را تعریف کنیم
- ۳۱۰ ۳-۷-۸ سؤالات رایج
- ۳۱۱ ۸-۸ ZoneAlarm دیواره آتش کامپیوتر شما
- ۳۱۱ ۱-۸-۸ قابلیت های کلیدی نرم افزار
- ۳۱۳ ۹- مبانی امنیت در سیستم عامل
- ۳۱۶ ۱-۹ چارت پر استفاده ترین سیستم عامل ها در جهان
- ۳۱۷ ۲-۹ چارت پر استفاده ترین سیستم عامل ها در ایران
- ۳۱۹ ۳-۹ به روزرسانی (Update)

۳۲۱	۴-۹ استفاده از آخرین نسخه ویندوز
۳۲۱	۵-۹ قرار دادن رمز عبور بروی حساب‌های کاربری
۳۲۲	۶-۹ اهمیت نظم در ذخیره‌سازی فایل‌ها و فولدرها
۳۲۲	۷-۹ نمایش پسوند فایل‌ها در ویندوز
۳۲۳	۸-۹ تنها نرم‌افزارهای ضروری را نصب کنید
۳۲۴	۹-۹ تنها نرم‌افزارهای ضروری را نصب کنید
۳۲۵	۱۰-۹ از نسخه های ۶۴ بیتی ویندوز استفاده کنید
۳۲۵	۱۱-۹ اهمیت نصب نرم‌افزارهای نابودگر بدافزارها
۳۲۵	۱۲-۹ پاک‌سازی نرم‌افزارهای نصب شده
۳۲۵	۱۳-۹ رمزنگاری اطلاعات سیستم‌عامل
۳۲۶	۱۴-۹ نکته امنیتی برای کاربران سیستم‌عامل اپل Mac OS
۳۳۱	۱- نگه‌داری و پاک کردن اطلاعات به صورت امن
۳۳۴	۱-۱۰ مفهوم حذف فایل‌ها
۳۳۶	۲-۱۰ حذف ایمن و بازنویسی فایل‌ها
۳۳۶	۳-۱۰ اطلاعات خود را رمزگذاری کنید
۳۳۸	۱-۳-۱۰ نکاتی در مورد استفاده درست از رمزگذارها
۳۳۹	۴-۱۰ اطلاعات محرمانه و حساس خود را مخفی کنید
۳۳۹	۵-۱۰ خطر مشخص شدن موقعیت اطلاعات محرمانه
۳۳۹	۶-۱۰ آموزش نرم‌افزار True Crypt
۳۴۴	۱-۶-۱۰ روش استفاده از درایو ساخته شده
۳۴۶	۷-۱۰ پاک‌سازی اطلاعات با ابزار امن
۳۴۶	۸-۱۰ پاک‌سازی فایل‌ها
۳۴۷	۹-۱۰ پاک‌سازی فایل‌های موقت (Temporary)
۳۴۸	۱۰-۱۰ نکاتی برای استفاده صحیح از نرم‌افزارهای پاک‌کننده
۳۴۹	۱۱-۱۰ چگونه ردپاها را با CCleaner پاک کنیم؟
۳۵۰	۱-۱۱-۱۰ تنظیم CCleaner برای حذف امن و مطمئن فایل‌ها
۳۵۱	۲-۱۱-۱۰ چگونگی کار با CCleaner
۳۵۳	۳-۱۱-۱۰ چطور فایل‌های موقتی برنامه‌های نصب شده را پاک کنید؟
۳۵۴	۴-۱۱-۱۰ رجیستری ویندوز

۳۵۴	۵-۱۱-۱۰ چطور رجیستری ویندوز را تعمیر کنیم؟
۳۵۶	۶-۱۱-۱۰ سؤالات متداول
۳۵۷	۱۲-۱۰ روش‌های تخریب فیزیکی دیسک سخت
۳۵۹	۱۱- امنیت در شبکه‌های بی‌سیم
۳۶۱	۱-۱۱ تنظیمات پیش‌فرض
۳۶۱	۲-۱۱ نگهداری اطلاعات
۳۶۲	۳-۱۱ دسترسی غیرمجاز
۳۶۲	۴-۱۱ استفاده از آی‌پی آدرس شما برای فعالیت‌های غیرمجاز
۳۶۲	۵-۱۱ منفعت، بیش از ضرر
۳۶۶	۶-۱۱ اطلاعات کامل شبکه‌ای با yougetsignal
۳۷۰	۷-۱۱ شما هم می‌توانید کلمه عبور شبکه‌های بی‌سیم Wi-Fi را هک کنید
۳۷۰	۱-۷-۱۱ یک آداپتور بی‌سیم
۳۷۰	۲-۷-۱۱ سی دی لای 3 Back Track
۳۷۰	۳-۷-۱۱ یک شبکه Wi-Fi
۳۷۰	۴-۷-۱۱ صبر و طاقت کار با محیط command line
۳۷۶	۵-۷-۱۱ مشکلات احتمالی
۳۷۷	۱۲- امنیت در کامپیوترهای عمومی و سفر
۳۷۹	۱-۱۲ وقتی با لپ‌تاپ/ موبایل خودم از اینترنت در اماکن عمومی استفاده می‌کنم
۳۸۰	۲-۱۲ امنیت در مسیر انتقال اطلاعات
۳۸۱	۳-۱۲ مقدمه‌ای بر شبکه خصوصی مجازی (VPN)
۳۸۱	۱-۳-۱۲ دسته‌بندی VPN براساس رمزنگاری
۳۸۲	۲-۳-۱۲ دسته‌بندی VPN براساس لایه پیاده‌سازی
۳۸۳	۳-۳-۱۲ دسته‌بندی VPN براساس کارکرد تجاری
۳۸۳	۴-۱۲ به اشتراک‌گذاری فایل و پرینتر را غیرفعال کنید
۳۸۳	۵-۱۲ به‌روز بودن سیستم‌عامل
۳۸۳	۶-۱۲ فعال کردن امکان خصوصی‌سازی فایل‌ها در ویندوز
۳۸۴	۷-۱۲ مراقب اینترنت‌های مجانی باشید
۳۸۴	۸-۱۲ امنیت در کامپیوترهای عمومی

۳۸۴	۹-۱۲ چگونه کامپیوترهای عمومی را امن تر کنیم؟
۳۸۵	۱۰-۱۲ کامپیوتری را انتخاب کنید که کمترین مشکل را داشته باشد
۳۸۵	۱۱-۱۲ فایل هایی که در مدت زمان استفاده داندود یا ایجاد کرده اید از کامپیوتر پاک کنید
۳۸۵	۱۲-۱۲ شیوه های تایپ کردن رمزهای عبور
۳۸۵	۱۳-۱۲ پاک سازی اطلاعات
۳۸۶	۱۴-۱۲ خروج از سایت ها، مسنجرها و کلاینت ها را به هیچ عنوان فراموش نکنید
۳۸۶	۱۵-۱۲ از خریدهای اینترنتی و ورود اطلاعات شخصی خود پرهیز کنید
۳۸۶	۱۶-۱۲ پس از اتمام کار کامپیوتر را ری استارت نمایید
۳۸۶	۱۷-۱۲ حافظه فلش / فلش مموری
۳۸۷	۱۸-۱۲ نرم افزارهای پرتابل
۳۸۷	۱۹-۱۲ چت و تلفن امن
۳۸۸	۲۰-۱۲ مخفی کردن هویت
۳۸۸	۲۱-۱۲ سی دی Live لینوکس
۳۸۸	۲۲-۱۲ پاسخ به چند پرسش مهم
۳۹۳	۲۳-۱۲ نکات امنیتی سخت افزاری در سفر
۳۹۵	۱۳- امنیت در شبکه های اجتماعی
۳۹۸	۱-۱۳ مواظب باشید که چه چیزی را به اشتراک می گذارید
۳۹۸	۲-۱۳ دوستان و دوستان دوستان تان را بشناسید و به خاطر داشته باشید
۳۹۸	۳-۱۳ حریم شخصی خود را مشخص کنید
۴۰۰	۴-۱۳ دسترسی افراد را به اکانت فیس بوک تان قطع کنید
۴۰۰	۵-۱۳ سرقت اطلاعات شخصی، فیشینگ و اخاذی
۴۰۱	۶-۱۳ پاک کردن حساب کاربری در سایت ها و شبکه های اجتماعی
۴۰۱	۷-۱۳ فیس بوک
۴۰۲	۸-۱۳ تویتر
۴۰۲	۹-۱۳ فرزند فید
۴۰۲	۱۰-۱۳ آمار استفاده از شبکه های اجتماعی
۴۰۳	۱۱-۱۳ فیس بوک چیست؟
۴۰۴	۱-۱۱-۱۳ چه کارهایی را می توان با فیس بوک انجام داد؟
۴۰۴	۲-۱۱-۱۳ چرا افراد جوان از شبکه های اجتماعی استفاده می کنند؟

۴۰۵	۱۳-۱۱-۳ آیا فیس‌بوک محیطی امن است؟
۴۰۵	۱۳-۱۱-۴ چه خطراتی در فعالیتهای شبکه اجتماعی وجود دارد؟
۴۰۶	۱۳-۱۱-۵ ریسک‌های به خصوص فعالیت در شبکه‌های اجتماعی عبارتند از
۴۰۷	۱۳-۱۱-۶ برای کاربران فیس‌بوک چگونه همانند والدین عمل می‌کنیم؟
۴۰۸	۱۳-۱۱-۷ روش‌هایی جهت نظارت بر فعالیتهای فیس‌بوک فرزندان
۴۰۹	۱۳-۱۱-۸ امنی، حریم و محافظت از اعتبار و شهرت در عصر دیجیتال
۴۱۱	۱۳-۱۱-۹ اعتبار و شهرت خوب و ردپای دیجیتالی
۴۱۲	۱۳-۱۱-۱۰ چگونه تنظیمات سایت فیس‌بوک را برای فرزندان خود بهینه کنیم؟
۴۱۲	۱۳-۱۱-۱۱ همه‌ها باید در مورد ذکر سن و سال خود صادق باشند
۴۱۳	۱۳-۱۱-۱۲ دوستان خود را عاقلانه و خردمندانه انتخاب کنید
۴۱۴	۱۳-۱۱-۱۳ خدمات پیام، صفحه پست‌ها و فید اخبار
۴۱۵	۱۳-۱۱-۱۴ محتویات پروفایل کودک خود را کنترل کنید
۴۱۷	۱۳-۱۱-۱۵ پیگیرندی تنظیمات مربوط به حریم خصوصی در فیس‌بوک
۴۱۸	۱۳-۱۱-۱۶ حفاظت‌های اضافی برای افراد نابالغ
۴۱۸	۱۳-۱۱-۱۷ تنظیم کنترل‌های مربوط به حریم خصوصی
۴۱۹	۱۳-۱۱-۱۸ تنظیمات مربوط به حریم خصوصی پیش‌فرض فیس‌بوک
۴۱۹	۱۳-۱۱-۱۹ شخصی کردن تنظیمات حریم خصوصی
۴۲۲	۱۳-۱۱-۲۰ گزینه شخصی سازی
۴۲۲	۱۳-۱۱-۲۱ کنترل و تعیین افرادی که می‌توانند پست‌های شخصی شما را ببینند
۴۲۳	۱۳-۱۱-۲۲ ایجاد و استفاده از لیست‌ها
۴۲۳	۱۳-۱۱-۲۳ ایجاد یک لیست
۴۲۵	۱۳-۱۱-۲۴ استفاده از قابلیت "گروه‌ها"
۴۲۶	۱۳-۱۱-۲۵ تشکیل یک گروه
۴۲۸	۱۳-۱۱-۲۶ چگونگی مشاهده اعضا گروه خود
۴۲۸	۱۳-۱۱-۲۷ کنترل برنامه‌های کاربردی فیس‌بوک
۴۲۹	۱۳-۱۱-۲۸ محدود کردن برنامه‌های کاربردی شخصی
۴۳۰	۳-۱۱-۲۹ مکان‌های فیس‌بوک: به اشتراک گذاری مکان‌یابی فیس‌بوکی
۴۳۱	۱۳-۱۱-۳۱ غیرفعال کردن قابلیت مکان‌ها در فیس‌بوک
۴۳۱	۳-۱۱-۳۰ مکان‌یابی کاملاً خودکار نیست
۴۳۲	۱۳-۱۱-۳۲ مقررات ویژه برای افراد زیر سن قانونی (زیر ۱۸ سال)

۴۳۲	۱۳-۱۱-۳۳ وارد شدن در فهرست مکان‌ها یا برجسب‌گذاری
۴۳۳	۱۳-۱۱-۳۴ تنظیمات اضافی مربوط به پیکربندی قابلیت مکان‌ها
۴۳۴	۱۳-۱۱-۳۵ گزارش مشکلات ۴۲۵
۴۳۶	۱۳-۱۱-۳۶ جلوگیری از خودکشی و سایر خود آزاری‌ها
۴۳۹	۱۴- امنیت فیزیکی
۴۴۱	۱۴-۱ از قفل‌های مطمئن داخلی برای درهای ورودی اصلی استفاده کنید
۴۴۱	۱۴-۲ در اتاق کامپیوتر همیشه قفل باشد
۴۴۲	۱۴-۳ یک سیستم نظارت و مراقبت دائمی داشته باشید
۴۴۲	۱۴-۴ تمامی ابزارهای در معرض خطر در محل امنی قرار داشته باشند
۴۴۲	۱۴-۵ محیط کاری را فراموش نکنید
۴۴۳	۱۴-۶ کیس کامپیوترتان را قفل کنید
۴۴۳	۱۴-۷ مراقب ابزارهای پرتابل باشید
۴۴۳	۱۴-۸ نگهداری امن نسخه‌های پشتیبان
۴۴۳	۱۴-۹ مراقب دستگاه‌های کیبی و پرینتر باشید
۴۴۴	۱۴-۱۰ از سیستم‌های هشداردهنده استفاده کنید
۴۴۴	۱۴-۱۱ مراقب کلیدهای پتان باشید
۴۴۴	۱۴-۱۲ اطراف دفتر کار
۴۴۷	۱۵- امنیت در موبایل
۴۵۰	۱۵-۱ آمار پراستفاده‌ترین سیستم‌عامل‌ها بر روی موبایل
۴۵۱	۱۵-۲ چگونگی پاک کردن اطلاعات خصوصی از روی تلفن همراه هوشمند
۴۵۲	۱۵-۳ تلفن‌های اندروید
۴۵۲	۱۵-۴ آی فون
۴۵۳	۱۵-۵ موبایل‌های بلک بری
۴۵۳	۱۵-۶ ویندوز فون
۴۵۳	۱۵-۷ مشکل آسیب‌پذیری اطلاعات در اندروید و نحوه‌ی مقابله با آن
۴۵۴	۱۵-۸ چگونه از خودمان در برابر این آسیب محافظت کنیم؟
۴۵۵	۱۵-۹ برنامه امنیتی برتر ویژه اندروید
۴۵۵	۱۵-۱۰ بدافزارها و محافظت در برابر سرقت اطلاعات

۴۵۷	۱۱-۱۵ مدیریت رمزهای عبور
۴۵۸	۱۲-۱۵ نکات امنیتی برای استفاده کودکان از موبایل
۴۵۸	۱۳-۱۵ کنترل‌های مربوط به والدین (Parental Controls) را در دستگاه بررسی کنید
۴۵۸	۱۴-۱۵ فعالیت کودکان را تحت‌نظر داشته باشید
۴۵۹	۱۵-۱۵ مسدودسازی یا ایجاد محدودیت
۴۵۹	۱۶-۱۵ استفاده از برنامه مدیریت زمان
۴۵۹	۱۷-۱۵ مراقب WiFi مجانی باشید
۴۶۰	۱۸-۱۵ نرم‌افزار برای گوشی مفقود شده
۴۶۰	۱۹-۱۵ بعد از گم کردن موبایل مان چه باید بکنیم؟
۴۶۳	۱۶- امنیت در فلش در یوها
۴۶۵	۱-۱۶ فایل‌های پنهان را آشکار کنید
۴۶۶	۱-۱-۱۶ پسوند فایل‌ها را آشکار کنید
۴۶۶	۲-۱-۱۶ فایل‌های سیستمی پنهان را نیز آشکار کنید
۴۶۷	۳-۱-۱۶ من فایل‌های پنهان را نمی‌بینم
۴۶۸	۲-۱۶ چرا ویروس‌ها جلوی نمایش فایل‌های پنهان را می‌گیرند؟
۴۶۹	۳-۱۶ گشت‌وگذار در کول دیسک با استفاده از ویندوز اکسپلورر
۴۷۰	۱-۳-۱۶ Standard Buttons را نمی‌بینم
۴۷۰	۲-۳-۱۶ Folders را نمی‌بینم
۴۷۰	۴-۱۶ فایل‌های بالقوه خطرناک را پاک کنید
۴۷۱	۵-۱۶ با پوشه‌های پنهانی که پاک نمی‌شوند چه کنیم؟
۴۷۱	۶-۱۶ تنظیم کردن AutoPlay
۴۷۲	۷-۱۶ در آخر تصمیم با شما است
۴۷۲	۸-۱۶ حفاظت از فلش دیسک‌ها با استفاده از رمزعبور
۴۷۳	۱-۸-۱۶ نصب برنامه
۴۷۴	۲-۸-۱۶ اجرای برنامه
۴۷۵	۳-۸-۱۶ نصب رمزعبور بر روی درایو
۴۸۱	منابع