

امنیت در زندگی آنلاین

نویسنده: حسین سهلانی





سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

این کتاب در پروژه "صیانت از کودکان و خانواده در اینترنت" به سفارش معاونت امنیت فضای تولید و تبادل اطلاعات با همکاری پلیس فتا ناجا تهیه شده است.

امنیت در زندگی آنلاین

حسین سملانی

به سفارش :

ساختمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات



ناشر: عترت نو

تألیف: حسین سهلانی

ویرایش محتوایی: لیلا سهیلی آزاد

تصویرساز: مژگان کمیجانی

ویراستاری: محمد یوسفی

مشاور طرح: علی محمد رجبی

ناظر و مجری طرح: شرکت فناوران توسعه امن

ناجی

آدرس سایت: ceop.ir

شمارگان: ۱۰۰۰ جلد

قیمت: ۲۲۰۰۰ تومان

شابک: ۹۷۸-۶۰۰-۶۰۹۴-۵۱-۹

چاپ: سیمین پرداز کامه ۹-۶۶۴۸۱۶۳۸

نشانی: خیابان انقلاب، خیابان فخر رازی، خیابان

نظری، کوچه فرزانه، پلاک ۱، واحد ۱۳

تلفن: ۹-۶۶۴۸۱۶۳۸



سرشناسه: سهلانی، حسین، ۱۳۶۵

عنوان و نام پدیدآور: امنیت در زندگی آنلاین / حسین

سهلانی؛ ویراستاری محمد یوسفی؛ به سفارش سازمان فناوری

اطلاعات، معاونت امنیت فضای تولید و تبادل اطلاعات

مشخصات نشر: تهران، عترت نو، ۱۳۹۷.

مشخصات ظاهری: ۱۰۷ص: مصور(رنگی).

شابک: ۹۷۸-۶۰۰-۶۰۹۴-۵۱-۹

وضعیت فهرستنویسی: فیبا

یادداشت: کتابنامه.

موضوع: ویروس‌های کامپیوتر

موضوع: Computer Viruses

موضوع: شبکه‌های کامپیوتری - تدابیر ایمنی

موضوع: Computer networks - Security measures

موضوع: کامپیوترها - ایمنی اطلاعات

موضوع: Computer security

موضوع: فضای مجازی - تدابیر ایمنی

موضوع: Cyberspace - security measures

شناسه افزوده: سازمان فناوری اطلاعات، معاونت

امنیت فضای تولید و تبادل اطلاعات

رده بندی کنگره: ۱۳۹۷ س ۹/۷۶/۷۶ Q4۷۶

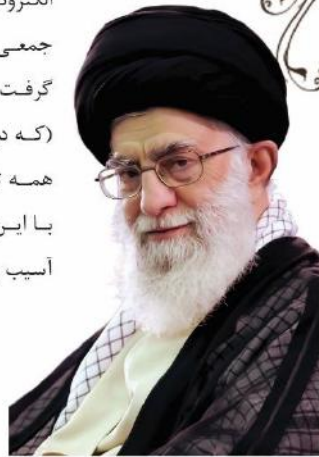
رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۵۲۵۱۰۳۹

بسم رب العلمین

شیطان، امروز از راه اینترنت و ماهواره و روش‌های ارتباطی مدرن و فوق‌مدرن سراغ فرزندان می‌آید. حرف‌های مدرنی هم دارد. سخت‌افزارش را مدرن کرده. نرم‌افزار مدرن هم دارد. شبهه‌آفرینی دارد. اخلال در عقیده دارد. ایجاد تشویش در ذهن دارد. تزریق ناامیدی دارد. ایجاد اختلاف دارد. امروز نشر افکار باطل به وسیله ابزارهای ارتباط جمعی فراوان مثل رادیو، تلویزیون، اینترنت و انواع و اقسام روش‌های الکترونیکی انجام می‌گیرد و با وجود وسایل ارتباط جمعی گوناگون، باید مواظبت از فرزندان خود را جدی گرفت و نباید آن‌ها را با دوران کودکی و نوجوانی خود (که در آن دوران نه اینترنت بود، نه ماهواره، نه این همه تبلیغات گوناگون بود و نه وسایل ارتباط جمعی با این وسعت بود که فرزندان ما در معرض این همه آسیب باشند) مقایسه کرد.

بخشی از سخنان مقام معظم رهبری



پیشگفتار

رشد روزافزون تکنولوژی، بین نسل گذشته (پدر و مادرها) و نسل جدید (فرزندان) شکافی عمیق ایجاد کرده است. به دنبال این امر، حفاظت از فرزندان در برابر آفت‌های فضای مجازی به یکی از معضلات مهم والدین تبدیل شده است. به همین دلیل، شرکت‌های مختلف سعی کرده‌اند برای تأمین امنیت فرزندان در فضای مجازی، نرم‌افزارهایی بسازند. باین حال، فراوان مشاهده شده که والدین نمی‌توانند امنیت لازم را برای فرزندان خود مهیا کنند و در نتیجه، دچار مشکلاتی می‌شوند.

کودکان از آنجاکه از خطرات فضای مجازی با خبر نیستند، احتمال آسیب دیدنشان به نسبت بزرگسالان بیشتر است. بر همین اساس، باید یکی از وظایف اصلی والدین را حفاظت از کودکان در برابر آفت‌های این فضا دانست. برای داشتن فضای مجازی ایمن، لازم است تا زمانی که کودکان به سن تشخیص می‌رسند، بر رفتارهای آن‌ها در فضای مجازی نظارتی جدی و آگاهانه داشت و خطرات موجود در این فضا را به بهترین نحو برایشان روشن کرد.

در این کتاب سعی شده است این‌گونه خطرات و روش‌های مقابلهٔ صحیح با آن‌ها به شکلی کارآمد بیان شود؛ به طوری که والدین با جزئیات مربوط به این حوزه آشنا شوند و آگاهانه خود و فرزندانشان را در برابر این قبیل خطرات مصون نگه دارند.

فهرست مطالب

مقدمه	۱۴
تهدیدات نرم افزاری	۱۵
راه های مقابله با بدافزارها و باج افزارها	۱۶
راه های مقابله با کی لاگرها	۲۰
راه های مقابله با ایمیل فیشینگ	۲۲
روش های جلوگیری از مزاحمت های سایبری	۲۷
مقابله با آثار مخرب برخی بازی های رایانه ای	۳۰
روش هایی برای حفظ امنیت خانواده در فضای مجازی	۳۴
کنترل و نظارت به کمک سیستم عامل ها	۳۵
گزینه کنترل والدین در سیستم عامل های ویندوز	۳۵
محافظت با دیوار آتش در سیستم عامل ویندوز	۴۹
گزینه کنترل والدین در سیستم عامل های گوشی های هوشمند	۵۱
نظارت به کمک مرور گر ها و موتورهای جستجو	۵۶
گزینه های کنترلی در موتور جستجوی گوگل	۵۶
گزینه های کنترلی در موتور جستجوی یاهو	۵۷

گزینه‌های کنترلی در مرورگر کروم	۶۰
گزینه‌های کنترلی در مرورگر سافاری	۶۱
افزونه‌ها.....	۶۲
حفاظت با انتخاب کلمه عبور مناسب	۶۵
کنترل ازطریق تجهیزات شبکه خانگی	۶۷
نظارت والدین به کمک نرم‌افزارهای ضدویروس.....	۷۲
نرم‌افزار نود ۳۲	۷۳
نرم‌افزار Kaspersky	۷۴
نرم‌افزار eScan	۷۶
برنامه Bitdefender	۷۶
نظارت به کمک نرم‌افزارهای کنترلی در رایانه یا گوشی هوشمند	۷۸
نرم‌افزار کیدلاگر	۸۰
نرم‌افزار Salfeld Child Cotrol	۸۳
نرم‌افزار NQ Family Guardian.....	۸۵
نرم‌افزار کیدز پلیس	۸۷
نرم‌افزار فمیلی گارد.....	۹۱
سامانه مراقبت از خانواده SFP	۹۳
برنامه کنترل فرزند شقایق	۹۵
برنامه ParentKit (iOS)	۹۸
قفل کننده نرم‌افزار	۹۸

۱۰۰..... Screen Time Parental Control برنامه

۱۰۳.....سیم کارت‌های کنترل شده

۱۰۴.....امنیت تجهیزات هوشمند خانگی

فهرست اشکال

- شکل (۱) ابزار تهیه نسخه پشتیبان ۱۷
- شکل (۲) دانلود آخرین به‌روزرسانی‌ها برای ویندوز ۷ ۱۸
- شکل (۳) فعال کردن گزینه انتخاب به‌روزرسانی خودکار ۱۸
- شکل (۴) اطلاع‌رسانی در کافه‌بازار درباره آخرین به‌روزرسانی برنامه‌ها ۱۹
- شکل (۵) آنتی‌ویروس‌های ایرانی در فروشگاه اندرویدی بازار ۲۰
- شکل (۶) آنتی‌ویروس‌های موجود در فروشگاه Google Play ۲۰
- شکل (۷) مشخصات سایت دیجی‌کالا در سایت نماد الکترونیک ۲۱
- شکل (۸) نمونه‌ای از صفحه کلیدهای مجازی در درگاه‌های بانکی ۲۲
- شکل (۹) نمونه‌ای از آدرس جعلی و صحیح بانک پاسارگاد ۲۳
- شکل (۱۰) قابلیت پنهان کردن آدرس در Gmail ۲۴
- شکل (۱۱) استفاده از ورود دومرحله‌ای در Gmail ۲۵
- شکل (۱۲) نظام رده‌بندی سنی ESRB ۳۰
- شکل (۱۳) تنظیمات سنی بازی‌ها در ویندوز ۷ از منوی Control Panel ۳۱
- شکل (۱۴) تنظیمات رده‌بندی سنی بازی در ویندوز ۸ ۳۲
- شکل (۱۵) انتخاب گزینه کنترل والدین برای کاربر مشخص ۳۶
- شکل (۱۶) فعال کردن گزینه‌های کنترل والدین ۳۷
- شکل (۱۷) تنظیم مدت‌زمان استفاده کاربر از کامپیوتر ۳۸
- شکل (۱۸) تنظیم برنامه‌های مجاز برای استفاده کاربر ۳۸
- شکل (۱۹) برنامه Live Family Safety ۳۹

شکل (۲۰) نحوه مواجههٔ فرزند با سایت‌های ممنوع‌شده	۴۰
شکل (۲۱) تعریف یک کاربر کودک در ویندوز ۸	۴۰
شکل (۲۲) انتخاب کاربر برای ایجاد محدودیت	۴۱
شکل (۲۳) تنظیمات Family Safety برای کاربر کودک	۴۲
شکل (۲۴) تنظیم وب‌سایت‌های قابل‌مشاهده برای کودک	۴۳
شکل (۲۵) تنظیمات زمان استفاده از رایانه برای کودک	۴۳
شکل (۲۶) نحوهٔ دسترسی کاربر کودک به برنامه‌ها	۴۴
شکل (۲۷) تنظیمات ویندوز ۱۰	۴۵
شکل (۲۸) تنظیمات ویندوز ۱۰ برای تعریف کاربران (۱)	۴۶
شکل (۲۹) تنظیمات ویندوز ۱۰ برای تعریف کاربران (۲)	۴۷
شکل (۳۰) تنظیمات ویندوز ۱۰ برای تعریف کاربران (۳)	۴۸
شکل (۳۱) کنترل والدین مایکروسافت	۴۹
شکل (۳۲) تنظیمات دیوار آتش در ویندوز	۵۰
شکل (۳۳) تنظیمات حالت Guest برای اندروید	۵۲
شکل (۳۴) منوهای فعال‌سازی کنترل والدین	۵۳
شکل (۳۵) تعیین ردهٔ سنی در برنامه‌های اندرویدی	۵۴
شکل (۳۶) محدودکردن دانلود از منابع ناشناس	۵۵
شکل (۳۷) تنظیم گزینهٔ جست‌وجوی امن در موتور جست‌وجوی گوگل	۵۷
شکل (۳۸) گزینهٔ کنترلی موتور جست‌وجوی یاهو	۵۸
شکل (۳۹) کلیدهای کنترل والدین در مرورگر فایرفاکس (۱)	۵۹
شکل (۴۰) کلیدهای کنترل والدین در مرورگر فایرفاکس (۲)	۵۹
شکل (۴۱) نرم‌افزار کنترل والدین Family Link	۶۰
شکل (۴۲) دستیابی به گزینهٔ کنترلی در مرورگر سافاری	۶۱
شکل (۴۳) قابلیت محدودکردن بازدید از صفحات وب توسط والدین در مرورگر سافاری	۶۲

- شکل (۴۴) افزونه کنترل والدین Nanny ۶۴
- شکل (۴۵) تنظیمات افزونه ضدپورن فایرفاکس ۶۴
- شکل (۴۶) تنظیمات افزونه فاکس فیلتر بر اساس URL و کلمات کلیدی ۶۵
- شکل (۴۷) تنظیمات مودم برای فیلترشدن سایت‌های خاص ۶۸
- شکل (۴۸) اینترنت امن برای کودکان با روترهای کنترل والدین ۶۹
- شکل (۴۹) نمایی از سایت OpenDNS و قابلیت کنترل والدین ۷۰
- شکل (۵۰) تنظیمات استفاده از سرور OpenDNS ۷۱
- شکل (۵۱) تنظیمات استفاده از سرور OpenDNS ۷۱
- شکل (۵۲) تنظیمات استفاده از سرور OpenDNS ۷۲
- شکل (۵۳) مرحله‌ای از تنظیمات کنترل والدین در نود ۳۲ ۷۳
- شکل (۵۴) بخشی از اجرای مراحل کنترل والدین در Kaspersky ۷۵
- شکل (۵۵) تعریف پروفایل برای کودک در نرم‌افزار BitDefender ۷۷
- شکل (۵۶) آغاز نصب Kidlogger نسخه ویندوز ۷ ۸۱
- شکل (۵۷) تنظیمات اولیه در Kidlogger ۸۲
- شکل (۵۸) پنل کنترلی در نرم‌افزار Kid Logger ۸۳
- شکل (۵۹) دریافت نرم‌افزار از سایت salfeld ۸۴
- شکل (۶۰) یکی از مراحل راه‌اندازی نرم‌افزار Salfeld برای اندروید ۸۴
- شکل (۶۱) تنظیمات بخش محدودیت دسترسی در وب با Salfeld ۸۵
- شکل (۶۲) دکمه کمک در نرم‌افزار NQ Family Guardian ۸۶
- شکل (۶۳) فعال‌سازی قابلیت‌های نرم‌افزار NQ Family Guardian ۸۷
- شکل (۶۴) نرم‌افزار Kids Place ۸۸
- شکل (۶۵) تنظیم پین کد برای نرم‌افزار Kids Place ۸۹
- شکل (۶۶) منوی App Usage access در اندروید برای اجازه مشاهده برنامه‌های دیگر ۹۰
- شکل (۶۷) منوی دانلود و ثبت‌نام نرم‌افزار فمیلی گارد ۹۲

شکل (۶۸) قسمتی از داشبورد برنامه فمیلی گارد	۹۳
شکل (۶۹) صفحه ثبت نام برنامه SFP	۹۵
شکل (۷۰) نمایی از برنامه کنترل فرزند شقایق	۹۶
شکل (۷۱) نمایی از مراحل نصب برنامه کنترل فرزند شقایق	۹۷
شکل (۷۲) تنظیم ساعات استفاده از گوشی	۹۷
شکل (۷۳) برنامه کنترلی ParentKit	۹۸
شکل (۷۴) نمایی از مراحل نصب و تنظیمات AppLock	۹۹
شکل (۷۵) تعریف حساب کاربری در Screen Time Parental Control	۱۰۱
شکل (۷۶) صفحه تنظیمات Screen Time Parental Control	۱۰۲



راه‌های مقابله با
بدافزارها و باج‌افزارها



مقدمه

برای مواجهه با هر مشکل، آگاهی از جنبه‌های مختلف آن ضروری است. کودکان و نوجوانان امروز که از کودکی با فناوری‌های مدرن بزرگ می‌شوند، به نسبت والدین از فضای مجازی و رایانه و اموری از این دست آگاهی بیشتری دارند. بنابراین، اگر والدین دانششان را به‌روز کنند و اطلاعاتشان را به میزان مطلوب برسانند، راهنمایی‌هایی که در این زمینه به فرزندانشان می‌کنند، مؤثرتر خواهد بود.

اهمیت دانش و آگاهی رسانه‌ای والدین به قدری است که با تمام نکاتی که برای مراقبت از فرزندان لازم است، برابری می‌کند. به عبارت دیگر، هیچ‌چیز جای آموزش والدین را نمی‌گیرد و والدین برای آموزش دادن فرزندانشان نیازمند دانش و آگاهی‌اند. نهایتاً والدین‌اند که باید بر فرزندان نظارت کنند. به همین دلیل، اگر میزان سواد رسانه‌ای‌شان با فرزندانشان اختلاف فاحشی داشته باشد، به‌خوبی از عهده این کار بر نمی‌آیند.

تا زمانی که فضای مجازی وجود دارد، خطرات و آسیب‌های مرتبط با آن هم وجود دارد. این خطرات بسیار متنوع است؛ از بدافزارهایی که به‌طرق مختلف سیستم‌ها را آلوده می‌کنند یا از افراد اخاذی می‌کنند گرفته تا کسانی که با سرقت هویت و اطلاعات خصوصی، امنیت خانواده‌ها و فرزندان را به خطر می‌اندازند. برای رهایی از این قبیل آسیب‌ها و به حداقل رساندنشان باید راه‌های مقابله با آن‌ها را بشناسیم.

تهدیدات نرم‌افزاری

همزمان با رشد و توسعه نرم‌افزارهای کاربردی و مفید نوع دیگری از نرم‌افزارها با هدف تخریب، سوء استفاده و جاسوسی اطلاعات کاربران گسترش یافتند. این برنامه‌های خرابکار انواع مختلفی دارند برخی مثل یک ویروس خود را تکثیر می‌کند، دسته‌ای مثل کرم، از نقاط آسیب‌پذیر وارد شبکه شده و آهسته آهسته به رایانه‌های دیگر می‌خزند، گروهی دیگر مثل اسب تروای قدیمی با چهره‌ای دوستانه وارد می‌شوند و سپس سیستم را نابود می‌کنند، برخی هم باج افزارند یعنی ابتدا رایانه قربانی یا فایل‌های او را قفل می‌کنند و سپس در ازای دسترسی مجدد، باج می‌خواهند.

کلکسیون تهدیدات نرم‌افزاری به همین‌ها محدود نمی‌شود؛ برنامه‌هایی هستند که کارشان سوء استفاده از اطلاعات محرمانه و خصوصی است مثل کی‌لاگرها که حرکت کلیدهای کیبورد را با هدف دسترسی به رمز عبور و اطلاعات حساس کاربران ثبت می‌کنند و یا انواع روش‌های فیشینگ که با تکیه بر اعتماد کاربر و خطاهای تشخیصی و با کمک جعل و بازسازی صفحات وب، او را فریب می‌دهند. امروزه تکنیک‌های بد افزارنویسی بسیار پیچیده شده است و شناسایی و تشخیص آنها دانش و تسلط بالایی را می‌طلبد، اما با استفاده از برنامه‌های بازدارنده می‌توان تا حدود زیادی سد راه این حملات شد. این برنامه‌های حفاظتی از دو طریق کلی با انواع نرم‌افزارهای مخرب مقابله می‌کنند:

(Symantec Corporation World Headquarters, 2016)

۱. جلوگیری از ورود و نصب بدافزار
 ۲. تشخیص و پاک‌سازی بدافزارهایی که سیستم را آلوده کرده‌اند
- از کجا بفهمیم گوشی یا تبلت یا رایانه، گرفتار بدافزار شده است؟ هریک از علائم زیر هشدار است که نشان می‌دهد بدافزار به سیستم راه پیدا کرده است:
- ✓ اگر عملکرد سیستم کند شده باشد.

- ✓ اگر برخی از فایل‌های سیستمی و غیرسیستمی پاک شده باشد.
 - ✓ اگر از فایل و پوشه‌ها کپی‌های بی‌دلیل ایجاد شود.
 - ✓ اگر فایل‌ها و پوشه‌ها پنهان شده باشد.
 - ✓ اگر صفحه‌خانگی^۱ یا موتور جست‌وجو، بی‌دلیل عوض شده باشد.
 - ✓ اگر ضمیمه‌ها^۲ یا ابزارهای^۳ ناشناسی به مرورگر اضافه شده باشد.
 - ✓ اگر مرورگر صفحات ناشناسی را باز کند.
- این تغییرات ممکن است به‌وسیلهٔ بدافزار در سیستم ایجاد شده باشد. این‌گونه بدافزارها ممکن است ازطریق دانلود فایل، بازکردن ایمیل آلوده، استفاده از حافظهٔ خارجی آلوده یا ازطریق گشت‌وگذار در وبگاه‌های ناامن وارد سیستم شده باشند. در ادامه با برخی از روش‌های محافظتی و برنامه‌های بازدارنده آشنا می‌شویم.

راه‌های مقابله با بدافزارها و باج افزارها

بدافزارها ممکن است بسیار خطرناک و نگران‌کننده باشند. باوجوداین، اگر برای مقابله با آن‌ها آماده باشیم، واقعاً جای نگرانی نیست. با رعایت دقیق و کامل چند توصیهٔ زیر می‌توان تا حد زیادی از ورود بدافزارها پیشگیری کرد یا در صورت ورود آن‌ها به سیستم، آسیب‌ها را به حداقل رساند (Symantec Corporation World Headquarters, 2016).

۱. برنامه‌های غیرلازم را از رایانهٔ خود پاک کنید.
۲. به‌طور منظم از اطلاعات خود نسخهٔ پشتیبان تهیه کنید. به‌این‌ترتیب، اگر سیستم شما دچار آلودگی شد، آسیبی که می‌بینید، به حداقل می‌رسد. امن‌ترین روش برای حفظ اطلاعات از هرگونه گزند، استفادهٔ درست و مطمئن از ابزارهای پشتیبان‌گیری است. گرفتن

^۱ Home page

^۲ extensions

^۳ toolbar

نسخه پشتیبان به این معنی است که اطلاعات، برای همیشه از آسیب باج‌افزارها در امان می‌ماند.

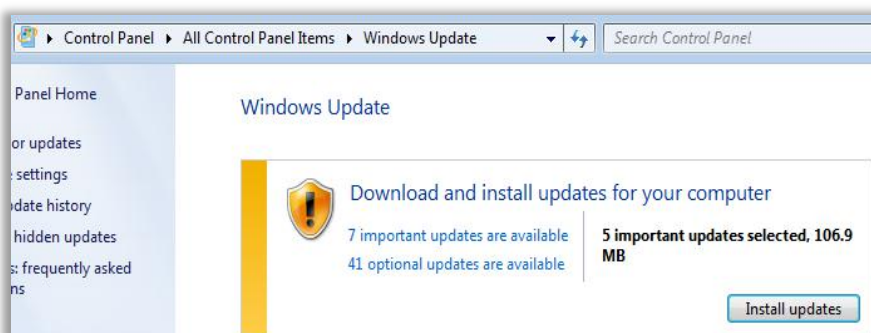
بهترین راهکار برای تهیه نسخه پشتیبان، ایجاد دو نسخه هم‌زمان است: نسخه اول بر روی فضای ابری (استفاده از سرویسی که به‌طور خودکار عملیات پشتیبان‌گیری را انجام می‌دهد) و نسخه دوم بر روی حافظه‌ای فیزیکی (مانند هارد اکسترنال، فلش، لپ‌تاپ و...). حتماً پس از تمام‌شدن مراحل پشتیبان‌گیری، این ابزارها را از دستگاه خود جدا کنید.



شکل (۱) ابزار تهیه نسخه پشتیبان

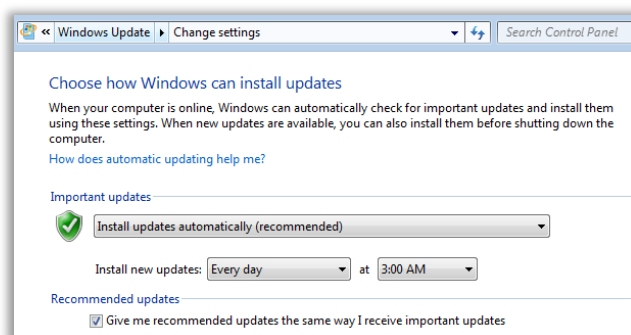
۳. برای حذف باج‌افزار یا دیگر نرم‌افزارهای مخربی که روی کامپیوتر نصب شده، با نرم‌افزار امنیتی مناسب و به‌روز، روزی یک بار کل سیستم را اسکن کنید.
۴. اگر کامپیوترتان از طریق باج‌افزار قفل شده، حتماً از یک منبع مطمئن کمک بگیرید و به‌هیچ‌وجه پولی واریز نکنید؛ چراکه حتی اگر با این کار، آن‌ها قفل کامپیوترتان را باز کنند، ممکن است پس از مدتی دوباره کامپیوتر را قفل کنند و از شما باج بگیرند.
۵. نرم‌افزارهای موردنیاز خود را از سایت‌ها و عرضه‌کنندگان معتبر دریافت کنید.
۶. نرم‌افزارهای خود را به‌روز نگه دارید. هر بار که نرم‌افزاری ازسوی شرکت سازنده‌اش به‌روزرسانی می‌شود، علاوه بر ارتقای قابلیت‌ها و تغییر جزئیات، راه‌های نفوذ در آن نیز

محدودتر می‌شود و در نتیجه، نرم‌افزار مقاوم‌تر می‌شود. مثلاً برای به‌روزرسانی سیستم‌عامل ویندوز، گزینهٔ windows Update را در Control Panel پیدا کنید:



شکل (۲) دانلود آخرین به‌روزرسانی‌ها برای ویندوز ۷

علاوه‌براین، می‌توانید انتخاب کنید که سیستم‌عامل شما به‌طور خودکار آخرین به‌روزرسانی‌ها را دریافت کند و Update شود:



شکل (۳) فعال کردن گزینه انتخاب به‌روزرسانی خودکار

برای به‌روزرسانی برنامه‌های موبایلتان، از فروشگاه‌های معروف اپلیکیشن موبایلی مثل Bazaar و Google Play Store استفاده کنید. در فروشگاه اندرویدی کافه‌بازار هم می‌توانید از طریق منوی تنظیمات (همان چرخ‌دنده بالای صفحه اصلی) عمل کنید:

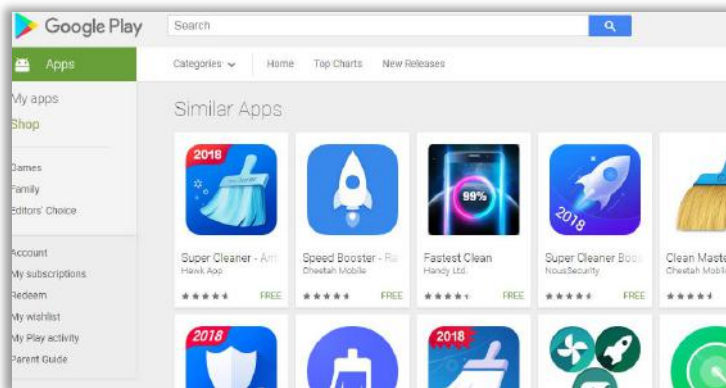


شکل (۴) اطلاع‌رسانی در کافه‌بازار درباره آخرین به‌روزرسانی برنامه‌ها

۷. از یک آنتی‌ویروس معتبر و مطمئن استفاده کنید. آنتی‌ویروس‌های رایگان و مناسبی مثل Avira، Avast، Bit Defender و... برای سیستم‌عامل‌های ویندوز و مک وجود دارد. برای گوشی‌های هوشمند خود از آنتی‌ویروس‌های عرضه‌شده در فروشگاه‌های مجازی معتبر مثل Bazaar یا Google play کمک بگیرید.



شکل (۵) آنتی‌ویروس‌های ایرانی در فروشگاه اندرویدی بازار



شکل (۶) آنتی‌ویروس‌های موجود در فروشگاه Google Play

راه‌های مقابله با کی‌لاکرها

امروزه یکی از معمول‌ترین ابزارهای دلدوستد کالا و خدمات، اینترنت است. در این فضا، پرداخت‌ها به‌صورت الکترونیکی انجام می‌گیرد. سایت‌های معتبر فروشگاهی کشور و سازمان‌های خدماتی دولتی و غیردولتی ایران از درگاه‌های پرداخت امن تحت دامنه


«شاپرک» استفاده می‌کنند تا از اطلاعات محرمانه مالی مشتریانشان حفاظت کنند. راستی، شما هنگام خرید اینترنتی به نکات امنیتی زیر دقت می‌کنید؟

الف. آدرس صفحه پرداخت باید صرفاً آدرس یکی از درگاه‌های پرداخت مورد تأیید و

تحت دامنه شاپرک باشد؛ مثلاً: به پرداخت ملت: <https://bpm.shaparak.ir>

ب. حرف s در https به معنی امن بودن سایت است.

پ. هنگام ورود به سایت از وجود نماد اعتماد الکترونیکی مطمئن شوید. مثلاً در سایت

دیجی کالا، با کلیک بر روی  نماد وارد صفحه زیر می‌شوید که نشان می‌دهد این سایت معتبر است:



شکل (۷) مشخصات سایت دیجی کالا در سایت نماد الکترونیک

۱. شرکت‌های معتبر پرداخت تحت دامنه شاپرک <https://shaparak.ir/content?id=287>

علاوه بر این، خود این دستگاه‌ها نیز به کاربران پیشنهاد می‌کنند برای وارد کردن رمز و اطلاعات امنیتی حساب‌های خود، از صفحه‌کلیدی مجازی که اعداد و حروف روی آن به کمک موس انتخاب می‌شوند، استفاده کنند؛ زیرا هکرها با استفاده از اطلاعاتی که هنگام کار با صفحه‌کلید عادی در اختیارشان قرار می‌گیرد، به راحتی می‌توانند از حساب افراد سوءاستفاده کنند؛ اما اگر از صفحه‌کلید مجازی استفاده شود، چنین امکانی نخواهند داشت. این از مهم‌ترین و مؤثرترین راه‌های مقابله با کی‌لاکرها است. در شکل زیر نمونه‌ای از صفحه‌کلیدهای مجازی نشان داده شده است:



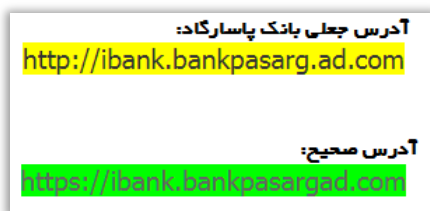
شکل (۸) نمونه‌ای از صفحه‌کلیدهای مجازی در دستگاه‌های بانکی

راه‌های مقابله با ایمیل فیشینگ

راه‌های مختلفی برای جلب اعتماد افراد و سرقت اطلاعات آن‌ها وجود دارد. یکی از این راه‌ها کلاهبرداری از طریق ایمیل است که به آن «ایمیل فیشینگ» می‌گویند. ایمیل محل نگهداری اطلاعات مهم کاربران است. بسیاری از حساب‌های شبکه‌های اجتماعی با ایمیل

راه‌اندازی و رمز عبور آن‌ها در صورت فراموشی با ایمیل بازیابی می‌شود. همچنین مکاتبات بانکی و اداری با ایمیل صورت می‌گیرد. پس واضح است که کلاهبرداران به ایمیل توجه خاصی می‌کنند. برای درآمان‌ماندن از چنین حملاتی لازم است نکات زیر را رعایت کنید (نک: انجمن خانواده و اینترنت):

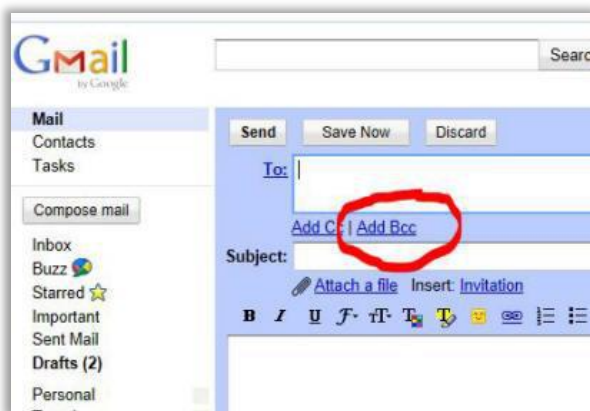
- ✓ آدرس ایمیل خود را در اختیار سایت یا اشخاص ناشناس قرار ندهید.
- ✓ پس از پایان کار با ایمیل، Sign out کنید؛ مخصوصاً وقتی از کافی‌نت‌ها یا شبکه‌های عمومی استفاده می‌کنید.
- ✓ حداقل سه ایمیل داشته باشید: یکی برای امور شخصی و مهم، یکی برای راه‌اندازی حساب‌های شبکه‌های اجتماعی، یکی برای وب‌گردی و کارهای متفرقه.
- ✓ همیشه به آدرس ایمیل‌های دریافتی توجه کنید. حتی اختلافات جزئی را نادیده نگیرید.



شکل (۹) نمونه‌ای از آدرس جعلی و صحیح بانک پاسارگاد

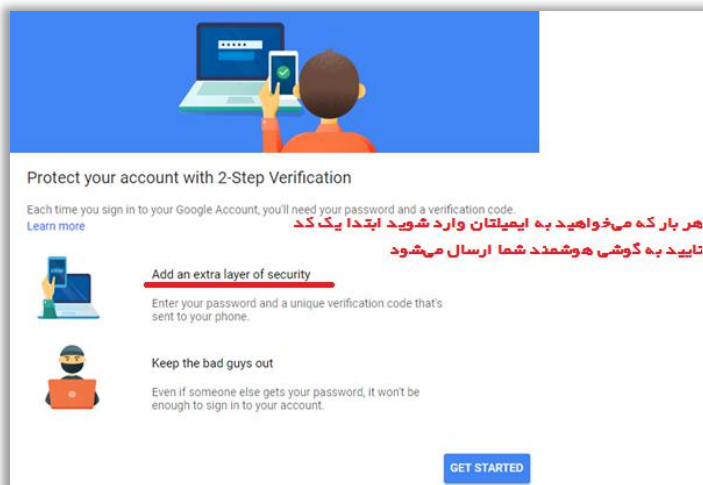
- ✓ ایمیل‌هایی را که به پوشه اسپم منتقل می‌شود، با وسواس بررسی کنید و در صورتی که فرستنده را نمی‌شناسید، هرگز بازشان نکنید.
- ✓ از قابلیت BCC سرویس‌های ایمیل استفاده کنید. با این کار امکان مخفی‌ماندن آدرس ایمیل از دید کلاهبرداران فراهم می‌شود. ایمیل‌های فورواردی معمولاً

فهرست بلندی از آدرس‌های ایمیل در خود دارد که به درد کلاهبرداری می‌خورد که ایمیل‌های حاوی بدافزار توزیع می‌کنند.



شکل (۱۰) قابلیت پنهان کردن آدرس در Gmail

- ✓ از قابلیت‌های آنتی‌فیشینگ نرم‌افزارهای محافظتی استفاده کنید. معمولاً امکانات خوبی برای شناسایی ایمیل‌های ناشناس دارند.
- ✓ از امکان ورود دومرحله‌ای به ایمیل‌ها استفاده کنید. عبارت Two Step Verification را در سرویس‌دهنده ایمیل خود جست‌وجو کنید. برای مثال، در Gmail به تصویر زیر می‌رسید:



شکل (۱۱) استفاده از ورود دومرحله ای در Gmail

به کمک این قابلیت، هر بار که می‌خواهید به ایمیل خود وارد شوید، کد تأییدی بر روی گوشی هوشمند خود دریافت می‌کنید و از ورودهای غیرمجاز به ایمیلتان جلوگیری می‌شود.



روش‌های جلوگیری از
مزاحمت‌های سایبری

روش‌های جلوگیری از مزاحمت‌های سایبری

شبکه‌های اجتماعی مثل تلگرام و فیس‌بوک راهی آسان و کم‌زحمت برای آشنایی با افراد جدید است. والدین باید آسیب‌ها و خطرات این سایت‌ها و شبکه‌های اجتماعی را جدی بگیرند و دورادور بر عملکرد فرزندان خود نظارت کنند.

ناشناس بودن افراد در این فضاها یکی از ویژگی‌های منحصربه‌فرد و درعین‌حال خطرناک آن است. افراد ناباب می‌توانند خود را به هر شکلی که بخواهند، معرفی کنند و هر هویتی برای خود بسازند. سوءاستفاده‌کنندگان جنسی و کودک‌آزاران می‌توانند با استفاده از هویت‌های جذاب و جعلی، کودکان و نوجوانان را که هنوز اطلاعات درست و دقیقی از این قبیل روابط ندارند، فریب دهند و حتی آن‌ها را به ملاقات حضوری تشویق کنند. امروزه «مزاحمت سایبری» یا Cyberbullying اصطلاحی شناخته‌شده است که معنایش «استفاده از تکنولوژی برای آزار و اذیت، تهدید، یا هدف‌گرفتن دیگری» است. متأسفانه بیشتر قربانیان این نوع مزاحمت، جوانان و نوجوانان هستند (گرداب، ۱۳۹۴).



خوب است نکات زیر را برای جلوگیری از مزاحمت سایبری در نظر داشته باشیم:

- ✓ در شبکه‌های اجتماعی وقتی درخواست دوستی برایتان ارسال می‌شود، با استفاده از سؤال‌هایی که فقط خودتان می‌دانید، مطمئن شوید طرف مقابل واقعاً همان دوست شماست.
- ✓ اگر به پیام‌های دوستان شک کردید، تلفنی با او تماس بگیرید یا اگر امکانش نبود، سؤال‌های مشخصی از او بپرسید که مطمئنید جوابش را می‌داند (نصیری، ۱۳۹۴).

- ✓ اسرار شخصی و شغلی و مالی خود را در شبکه‌های اجتماعی منتشر نکنید.
- ✓ اطلاعات بسیار خصوصی را که شما را در برابر خانواده یا همکارانتان خجالت‌زده می‌کند، منتشر نکنید.
- ✓ ممکن است سارقان هویت، از تصاویر و فایل‌های شخصی شما سوءاستفاده کنند. هرگز آن‌ها را در شبکه‌های اجتماعی منتشر نکنید.
- ✓ بلاک کردن و حذف کردن و گزارش به پلیس، راهکار خوبی برای درآمان ماندن از مزاحمت سایبری است.

مقابله با آثار مخرب برخی
بازی های رایانه ای



مقابله با آثار مخرب برخی بازی‌های رایانه‌ای

بازی‌های رایانه‌ای به‌رغم مزایایی که دارند، آثار مخربی از خود به‌جا می‌گذارند. توجه به رده‌بندی سنی بازی‌های رایانه‌ای برای والدین امری ضروری است. در تمام کشورها، حتی کشورهایی که در صف اول تولید و طراحی بازی‌های رایانه‌ای هستند، توجه ویژه‌ای به این امر می‌شود؛ به این صورت که براساس ملاک‌های مشخصی در زمینه محتوا و داستان، بازی‌ها را دسته‌بندی می‌کنند تا خانواده‌ها بدانند فرزندان‌شان در بازی با چه نوع فعالیت‌ها و فضاهایی مواجه‌اند. بیشتر بازی‌های خارجی که در کشور ما مرسوم است، از تولیدات شرکت‌های بازی‌سازی آمریکایی است که از نظام رده‌بندی سنی ESRB استفاده می‌کنند. البته تولیدات داخلی براساس نظام «اسرا» برچسب‌گذاری می‌شود.^۱



شکل (۱۲) نظام رده‌بندی سنی ESRB

در این زمینه، نکته درخورتوجه برای والدین، مباحث امنیتی در رده‌بندی سنی است. وقتی کودک وارد فضای بازی‌های بزرگسالان می‌شود، در معرض کلاهبرداری و سوءاستفاده قرار می‌گیرد؛ مواردی از قبیل جعل هویت و سرقت اطلاعات خصوصی و خانوادگی و در ساده‌ترین حالت، کلاهبرداری مالی در هنگام خرید درون‌برنامه‌ای.

۱. اطلاعات کامل درباره نظام‌های رده‌بندی سنی بازی‌ها در کتاب هم‌بازی‌های عصر دیجیتال آمده است.

مقابله با آثار مخرب برخی بازی‌های رایانه‌ای

در ویندوز ۷ به بعد، در قسمت Parental control گزینه‌ای به نام Game Rating System اضافه شده است که از طریق آن می‌توان رده سنی بازی‌ها و نیز دسته‌بندی‌های محتوایی مربوط را تنظیم کرد.



شکل (۱۳) تنظیمات سنی بازی‌ها در ویندوز ۷ از منوی Control Panel

در ویندوز ۸ هم با استفاده از تنظیمات Windows Store and Game Restrictions می‌توان تعیین کرد که کاربر چه نوع برنامه‌هایی را دانلود کند. شکل زیر نحوه دسترسی به این منو را نشان می‌دهد.



شکل (۱۴) تنظیمات رده‌بندی سنی بازی در ویندوز ۸

در کنسول‌های Xbox و PS هم گزینه‌هایی برای امنیت و حریم خصوصی تعبیه شده است؛ مثل خاموش کردن مکان‌نما و دوربین سیستم (Microsoft, n.d). مایکروسافت قابلیت یکپارچه‌سازی تنظیمات کاربر را در تمام دستگاه‌های ساخت این شرکت فراهم کرده است؛ یعنی اگر کودکی یک بار با یک حساب کاربری وارد شود، تنظیمات و محدودیت‌هایی که برایش تعریف می‌شود، در بقیه دستگاه‌ها و سیستم‌عامل‌های مایکروسافت نیز عمل می‌کند. البته در کشور ما این قابلیت فعال نیست.



روش‌هایی برای حفظ امنیت
خانواده در فضای مجازی



روش‌هایی برای حفظ امنیت خانواده در فضای مجازی

برای استفاده صحیح از فضای مجازی باید بتوانیم به کمک ابزارهای کارآمد، خود و خانواده خود را در برابر آسیب‌های موجود مصون کنیم.

درخواست‌های خانواده‌ها در کشورهای پیشرفته، شرکت‌های تولید نرم‌افزار را تشویق کرد تا فیلترهایی برای نرم‌افزارهای خود تعبیه کنند و به این ترتیب، برای دسترسی به محتوا در خانه، محدودیت‌هایی در نظر بگیرند. برخی از این شرکت‌ها حتی نرم‌افزارهای مجزایی برای این منظور طراحی کردند. همه این راهکارها برای پالایش و ممانعت از نشر محتوایی است که به زعم والدین، سلامت و امنیت خانواده و فرزندان را به خطر می‌اندازد. با این راهکارها می‌توان از طرفی دسترسی به سایت‌ها و بازی‌ها و برنامه‌ها را محدود یا مقید به زمان معین کرد و از طرف دیگر با تولید گزارش‌های لحظه‌ای یا روزانه از رفتار و عملکرد کاربران در شبکه، به والدین کمک کرد تا از رفتار فرزند خود آگاه شوند و تصمیمات درست و به موقعی بگیرند. به همین دلیل، این راهکارها بیشتر با نام روش‌های «کنترل والدین»¹ شناخته می‌شوند.

راهکارهای پالایش محتوا در خانه را به طور کلی می‌توان بر روی سیستم‌عامل دستگاه کامپیوتر و مرورگرها و تجهیزات شبکه خانگی و گوشی‌های هوشمند موبایل اجرا کرد. بعضی از این راهکارها از قبل در سیستم وجود دارد و فقط کافی است در این باره آگاهی و آموزش داده شود؛ اما برای بعضی دیگر از آن‌ها باید نرم‌افزار یا تجهیزات اضافی خریداری شود. در ادامه، درخصوص هریک از این راهکارها توضیحات بیشتری آمده است.

¹ Parental Control



کنترل و نظارت به کمک سیستم‌عامل‌ها

در سیستم‌عامل‌های مختلف گزینه‌هایی با عنوان «کنترل والدین» قرار داده شده است. این گزینه‌ها همان راهکارهای مدیریت و نظارت در خانه است که والدین می‌توانند آن‌ها را در سیستم‌های کامپیوتری و گوشی‌های هوشمند خود فعال کنند.

گزینه کنترل والدین در سیستم‌عامل‌های ویندوز

گزینه‌های کنترلی در ویندوز ۷

در ویندوز ۷ گزینه‌ای وجود دارد که مسیر فعال کردن آن به‌طور خلاصه به‌شکل زیر است (Burgess, 2010):

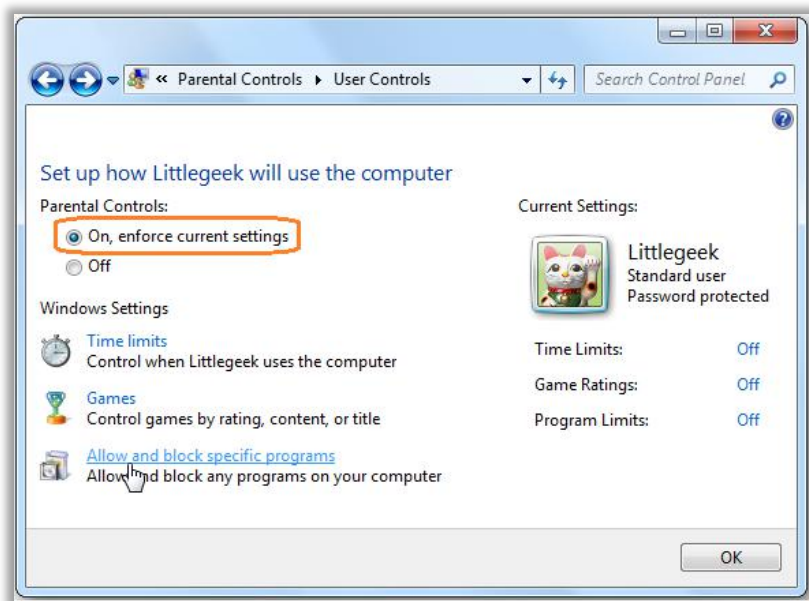
Control Panel->Internet Options->Content->Parental Control

برای دسترسی به این گزینه همچنین می‌توانیم Parental Control را در نوار جست‌وجوی صفحه کنترل پنل وارد کنیم. این گزینه فقط برای یکی از کاربرهای کامپیوتر فعال می‌شود. بنابراین قبل از این باید یک حساب کاربری جداگانه برای فرزندانم تعریف کنیم. برای فعال کردن گزینه «کنترل والدین» مانند شکل ۱۵ عمل می‌کنیم.



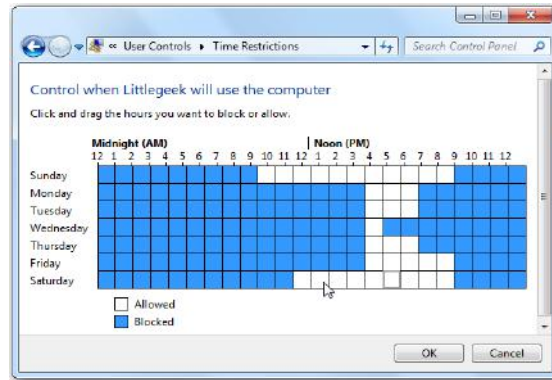
شکل (۱۵) انتخاب گزینه کنترل والدین برای کاربر مشخص

گاهی در زمان انتخاب کاربر، ویندوز پیغام مهمی می‌دهد و می‌گوید که در این سیستم، کاربران دیگری وجود دارند که فاقد کلمه عبور هستند. با وجود این کاربران، تنظیمات کنترلی بی‌فایده می‌شود و همه می‌توانند به‌سادگی از طریق این کاربران، وارد سیستم شوند. به این دلیل، در این مرحله سیستم ما را راهنمایی می‌کند که برای همه کاربران کلمه عبور بگذاریم و سپس گزینه کنترل والدین را مانند شکل زیر برای کاربر معینی فعال کنیم.



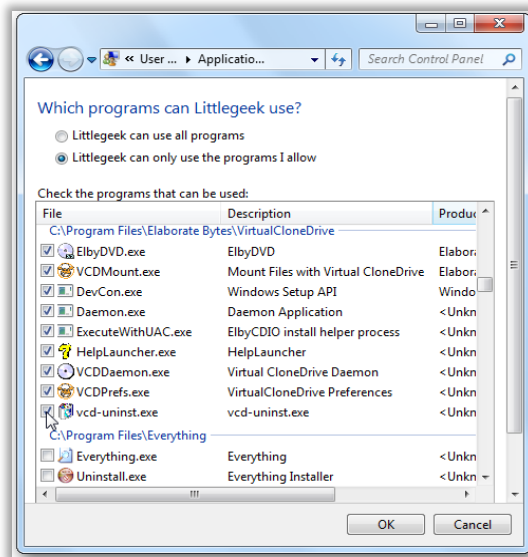
شکل (۱۶) فعال کردن گزینه‌های کنترل والدین

در قسمتی دیگر از ویندوز ۷ می‌توان ساعت مجاز استفاده از بازی‌ها و برنامه‌ها را تنظیم کرد. برای تنظیم ساعت‌های مجاز در روزهای هفته، از جدولی مانند زیر استفاده می‌شود.



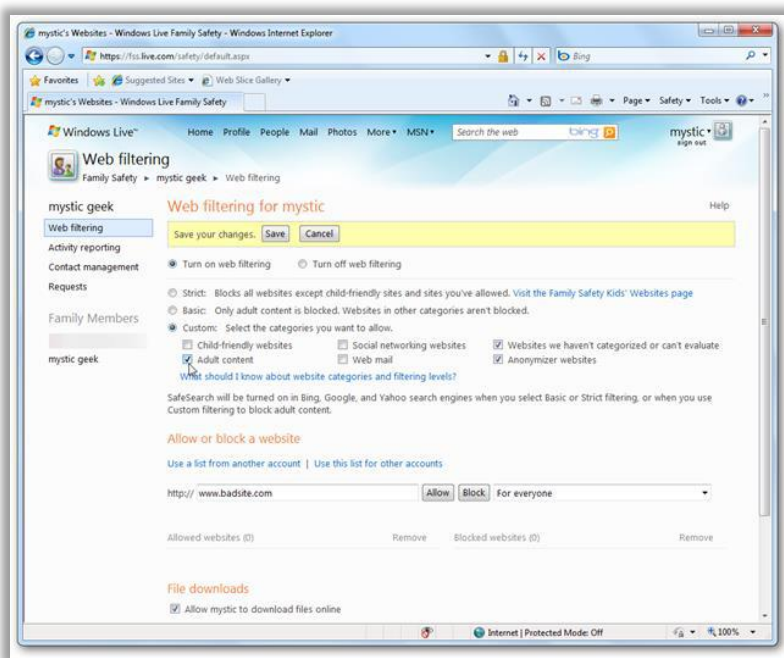
شکل (۱۷) تنظیم مدت زمان استفاده کاربر از کامپیوتر

درنهایت، تنظیم برنامه‌های مجاز نیز به کمک جدولی مانند شکل زیر انجام می‌شود:



شکل (۱۸) تنظیم برنامه‌های مجاز برای استفاده کاربر

اگر بخواهیم کنترل‌های بیشتری مانند پالایش صفحات وب را در ویندوز ۷ اعمال کنیم، می‌توانیم برنامه Live Family Safety را که بخشی از Window Live Essentials suite است، اجرا کنیم. ویندوز این بسته را برای اعمال نظارت قوی‌تر والدین در نظر گرفته است. به کمک این برنامه می‌توانیم دسترسی به سایت‌های معینی را مانند شکل زیر ممنوع کنیم و همچنین گزارشی از وب‌گردی فرزندان خود به دست آوریم (Burgess, 2010):



شکل (۱۹) برنامه Live Family Safety

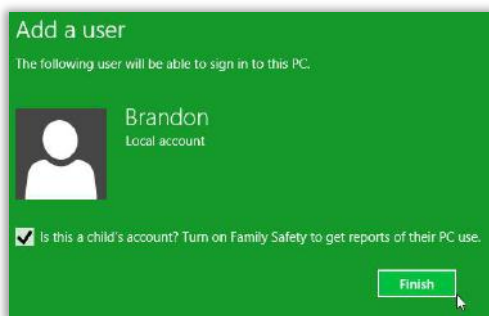
شکل زیر نحوه برخورد نرم‌افزار فوق را در مواجهه با سایت‌های ممنوع‌شده برای کودک نشان می‌دهد.



شکل (۲۰) نحوه مواجهه فرزند با سایت‌های ممنوع‌شده

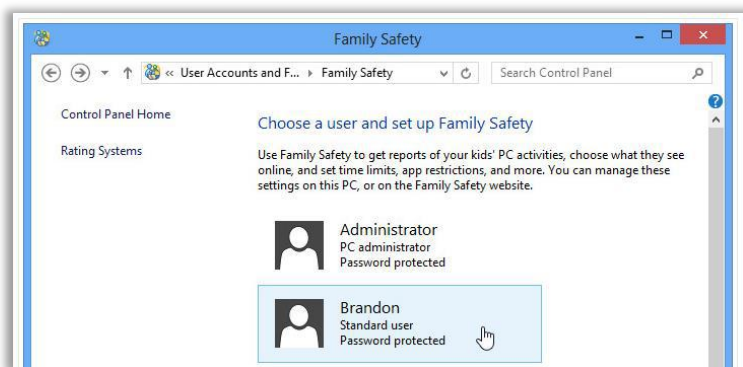
گزینه‌های کنترلی در ویندوز ۸

در سیستم‌عامل ویندوز ۸ هم برای اعمال کنترل والدین، اولین اقدام، ایجاد یک کاربر جدید با حساب کاربری است. کاربر جدید را می‌توانیم از طریق Settings و Control Panel مانند شکل زیر ایجاد کنیم.



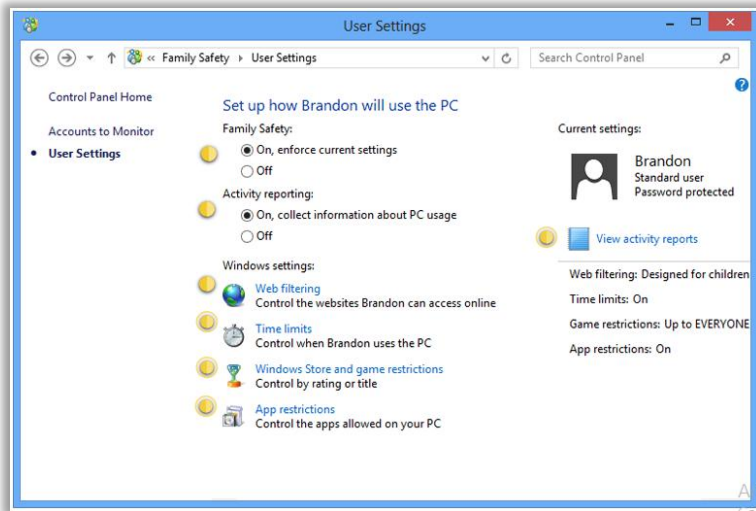
شکل (۲۱) تعریف یک کاربر کودک در ویندوز ۸

همان‌طور که در شکل دیده می‌شود، با تیک‌زدن عبارت زیر تصویر کاربر، اعلام می‌کنیم که کاربر، یک کودک است و می‌خواهیم از قابلیت Family Safety برای او استفاده کنیم. سپس در صفحه Control Panel و در گروه User Account and Family Safety، این کاربر را مطابق شکل‌های ۲۲ انتخاب می‌کنیم.



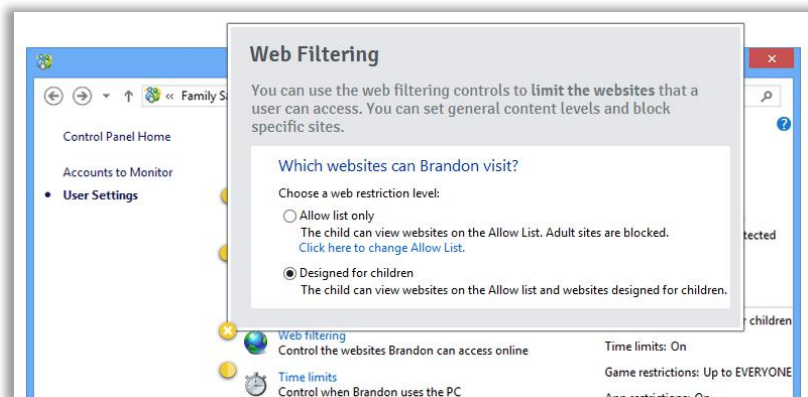
شکل (۲۲) انتخاب کاربر برای ایجاد محدودیت

اولین تنظیمات کاربر، روشن کردن ویژگی Family Safety و همچنین دریافت گزارش از رفتار کاربر است که در شکل زیر نشان داده شده است.



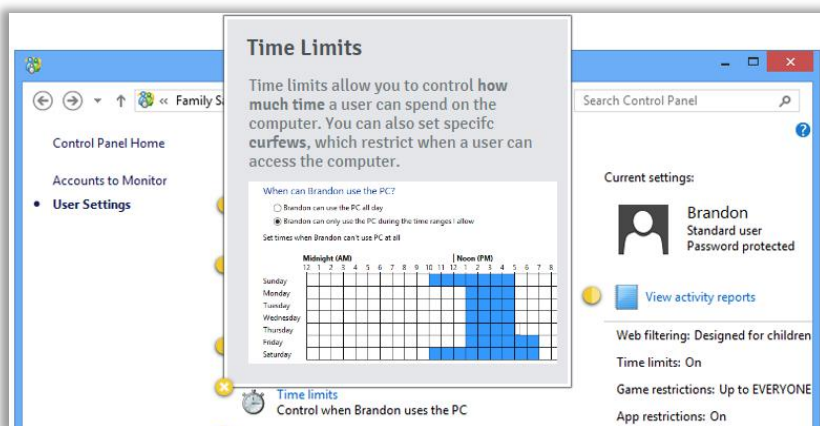
شکل (۲۳) تنظیمات Family Safety برای کاربر کودک

در تنظیمات Web filtering می‌توانیم به‌دلخواه خود، مشاهده صفحات وب را به فهرستی مشخص‌شده، محدود کنیم؛ درست مثل شکل زیر.



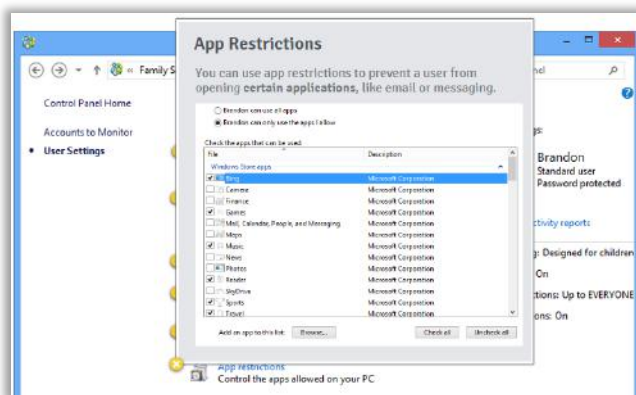
شکل (۲۴) تنظیم وبسایت‌های قابل مشاهده برای کودک

در تنظیمات Time Limit می‌توانیم ساعات مجاز استفاده کاربر را در هریک از روزهای هفته مطابق شکل زیر معین کنیم.



شکل (۲۵) تنظیمات زمان استفاده از رایانه برای کودک

و بالاخره در تنظیمات App Restrictions مطابق شکل زیر می‌توانیم نحوه دسترسی کاربر را به برنامه‌های کاربردی مانند ایمیل، تعیین کنیم (GCF, 2017).



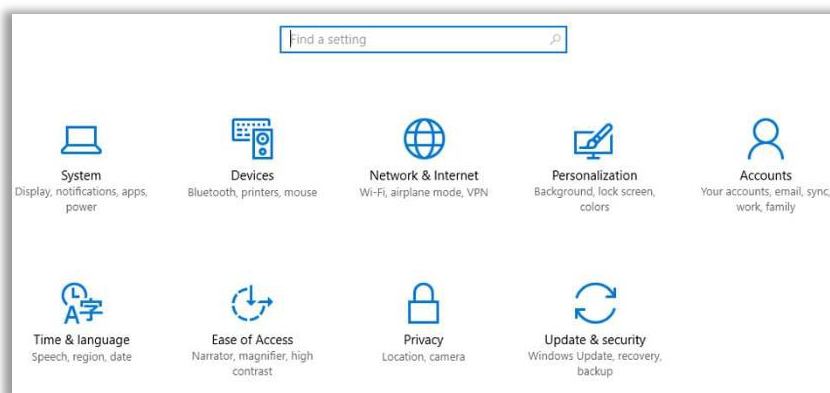
شکل (۲۶) نحوه دسترسی کاربر کودک به برنامه‌ها

گزینه‌های کنترلی در ویندوز ۱۰

کنترل والدین در ویندوز ۱۰ به‌شکلی ارتقا داده شده که سرپرست (یا فرد بزرگ‌سال) می‌تواند از هر دستگاه دیگری (با سیستم‌عامل ویندوز) بر رفتار فرزند خود نظارت کند. برای این منظور، سرپرست باید بتواند با حساب کاربری میکروسافت (شامل نام کاربری و کلمه عبور) که قبلاً آن را ایجاد کرده، از دستگاه خود وارد شود و بر رفتار کودک نظارت کند.

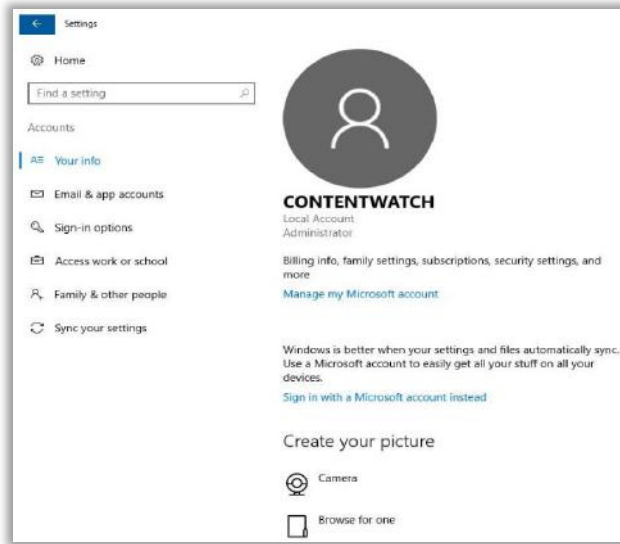
ویژگی مهم حساب کاربری میکروسافت این است که برای وارد شدن به همه نرم‌افزارهای میکروسافت (مانند Skype, office, windows, outlook, Xbox) می‌توان از آن استفاده کرد. به عبارت دیگر، اگر فرزند ما با حساب کاربری‌اش وارد هریک از نرم‌افزارهای ذکر شده بشود، با همان تنظیمات و محدودیت‌هایی روبه‌رو خواهد شد که در ویندوز ۱۰ برایش اعمال شده است.

بنابراین، مهم‌ترین مرحله ایجاد تنظیمات کنترل والدین در ویندوز ۱۰، ایجاد حساب کاربری مایکروسافت و ایجاد دو کاربر با مشخصات کودک (child) و بزرگسال (adult) است. به‌طور خلاصه مسیری که باید طی شود به‌ترتیب زیر است (Net Nanny, 2017):
Windows Settings-> Accounts-> Family & other people-> Add a family member
در ادامه جزئیات این مسیر به‌صورت گام‌به‌گام با تصاویر نمایش داده شده است. شکل زیر Windows Settings را نمایش می‌دهد:



شکل (۲۷) تنظیمات ویندوز ۱۰

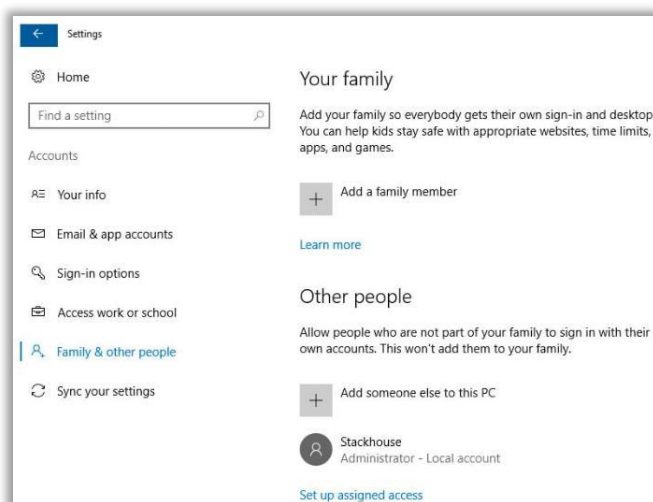
شکل زیر Windows Settings-> Accounts را نمایش می‌دهد:



شکل (۲۸) تنظیمات ویندوز ۱۰ برای تعریف کاربران (۱)

شکل زیر Windows Settings-> Accounts->Add a family member را نمایش

می‌دهد:



شکل (۲۹) تنظیمات ویندوز ۱۰ برای تعریف کاربران (۲)

در این مرحله مطابق شکل زیر، کاربری با مشخصه child انتخاب و آدرس ایمیلی را که با حساب کاربری مایکروسافت یکی شده، وارد می‌کنیم. با این کار، پیغام دعوتی به ایمیل فرستاده می‌شود که باید آن را تأیید کنیم.

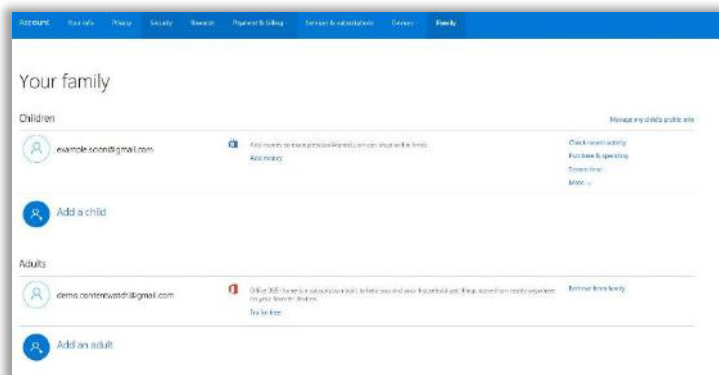


شکل (۳۰) تنظیمات ویندوز ۱۰ برای تعریف کاربران (۳)

اگر تا به حال حساب کاربری مایکروسافت نساخته باشیم، به کمک لینکی که در زیر نوار آدرس ایمیل در شکل بالا دیده می‌شود، می‌توانیم آن را ایجاد کنیم. تا این مرحله حساب کاربری کودک فعال شده و حساب کاربری قبلی به عنوان بزرگسال (یا سرپرست) شناخته شده و می‌تواند تنظیمات مدنظر را به روش زیر برای کودک انجام دهد:

Windows Settings-> Accounts -> Family & other people->Manage family settings online

در گام بعد، در مرورگر، صفحه «کنترل والدین مایکروسافت» مانند شکل زیر باز می‌شود. گزینه‌های سمت راست قابلیت‌های کنترل را نشان می‌دهد.



شکل (۳۱) کنترل والدین مایکروسافت

از طریق این گزینه‌ها می‌توان گزارش فعالیت‌های کودک را مشاهده کرد؛ وبسایت‌ها، برنامه‌ها و بازی‌های نامناسب را ممنوع کرد؛ زمان‌بندی استفاده از سیستم را اعمال کرد و در صورت لزوم، بر عملیات خریدی که کودک در بازارهای اینترنتی انجام می‌دهد، نظارت کرد.

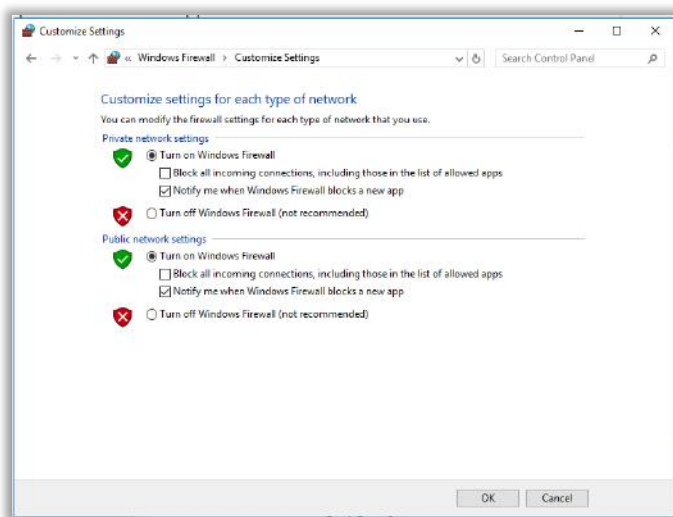
ضعف ویندوز ۱۰ برای فیلترکردن وبسایت‌ها این است که محتوایی که کاربران تولید می‌کنند (مثل کامنت‌ها یا پست‌های شبکه‌های اجتماعی) در لیست سیاه فیلتر قرار نمی‌گیرد. به‌علاوه، این فیلترها فقط در مرورگرهای مایکروسافت، یعنی Internet Explorer و Microsoft Edge، قرار می‌گیرد و در مرورگرهای دیگر، مانند کروم و فایرفاکس، نمی‌توان آن را اجرا کرد.

محافظت با دیوار آتش در سیستم‌عامل ویندوز

دیوار آتش نرم‌افزار یا سخت‌افزاری است که اطلاعات واردشده از اینترنت یا شبکه را بررسی می‌کند و در نتیجه، آن را ممنوع می‌کند یا اجازه ورود به کامپیوتر را به آن

می‌دهد. دیوار آتش می‌تواند دسترسی‌ها را به‌طور جداگانه برای شبکه خانگی و شبکه عمومی تنظیم کند. برای مثال، می‌تواند ارتباطات ورودی را در شبکه امن خانگی مجاز و در شبکه عمومی بیرونی ممنوع کند. همچنین می‌تواند ارتباطات شبکه‌ای را با سرویس‌های آسیب‌پذیر ممنوع یا کنترل کند. در سیستم‌عامل ویندوز و لینوکس، دیوار آتش به‌طور پیش‌فرض وجود دارد و می‌تواند از ورود بدافزارها به کامپیوتر جلوگیری کند و نیز مانع ارسال آن‌ها از سیستم به کامپیوترهای دیگر شود. قبلاً وقتی سیستم‌عامل‌های ویندوز بدون داشتن دیوار آتش مستقیماً به شبکه اینترنت متصل می‌شدند، به‌طور متوسط بعد از ۴ دقیقه آسیب می‌دیدند و قربانی حمله کرم‌ها می‌شدند.

دیوار آتش در زمان اجرای سیستم‌عامل ویندوز، به‌طور پیش‌فرض در پنجره Control Panel روشن است (مانند شکل زیر) و هنگام برقراری ارتباطات، به کاربر هشدار را نشان می‌دهد؛ به این ترتیب، در صورتی که کاربر اجازه بدهد، ارتباط برقرار می‌شود.



شکل (۳۲) تنظیمات دیوار آتش در ویندوز

در شکل بالا می‌توان گزینه زیر را هم تیک زد:

Block all incoming connections, including those in the list of allowed apps

این گزینه امنیت رایانه ما را بیشتر می‌کند و برای مواقعی که می‌خواهیم به شبکه‌ای عمومی مانند هتل یا فرودگاه یا کافی‌شاپ وصل شویم، مناسب است. فهرست برنامه‌های مجاز در این گزینه (allowed apps) نیز به صورت پیش فرض در سیستم عامل ویندوز تعریف شده است. در عین حال، کاربر می‌تواند در تنظیمات پیشرفته به این گزینه دسترسی پیدا کند.

گزینه کنترل والدین در سیستم عامل‌های گوشی‌های هوشمند

در سیستم عامل بعضی از گوشی‌های هوشمند و تبلت‌ها، گزینه‌هایی برای کنترل والدین قرار داده شده است. استفاده از این کنترل‌ها عموماً برای فرزندان کوچک‌تر مناسب است؛ زیرا بچه‌های بزرگ‌تر می‌توانند راه‌هایی برای غیرفعال کردن آن پیدا کنند (Knorr, 2016).

گزینه‌های کنترلی در گوشی آیفون

در گوشی‌های آیفون که با سیستم عامل iOS کار می‌کند، گزینه‌هایی برای کنترل والدین وجود دارد. برای مثال، با استفاده از کلید Guided Access می‌توانیم فرزند خود را به استفاده از برنامه‌ای خاص محدود کنیم؛ به طوری که اگر برنامه دیگری را باز کرد، گوشی خاموش شود. به طور خلاصه مسیر استفاده از این قابلیت به صورت زیر است (Cell Phone, 2016):

Settings-> General-> Accessibility-> Learning-> Guided Access

در تبلت‌های آیفون نیز ابتدا به روش زیر می‌توانیم کلمه عبوری برای خود انتخاب کنیم:

General->Passcode lock

در این قبیل دستگاه‌ها نیز، درست مثل گوشی‌های آیفون، می‌توانیم با استفاده از کلید Guided Access کودک را به استفاده از برنامه‌ای خاص محدود کنیم. همچنین می‌توانیم از طریق Restrictionها به‌روش زیر محدودیت‌هایی ایجاد کنیم:

Settings -> General -> passcode-protected

با این محدودیت‌ها می‌توانیم بعضی نرم‌افزارها را مخفی کنیم؛ به‌طوری که نماد مربوط به آن روی صفحه گوشی ظاهر نشود یا کارکرد بعضی برنامه‌ها را محدود کنیم. برای مثال، می‌توانیم از این طریق وارد شدن به بازی با چند کاربر یا امکان تغییر در برنامه‌های موجود یا دسترسی به بعضی از محتواها را محدود یا ممنوع کنیم (Character, 2016).

گزینه‌های کنترلی در گوشی‌های اندرویدی

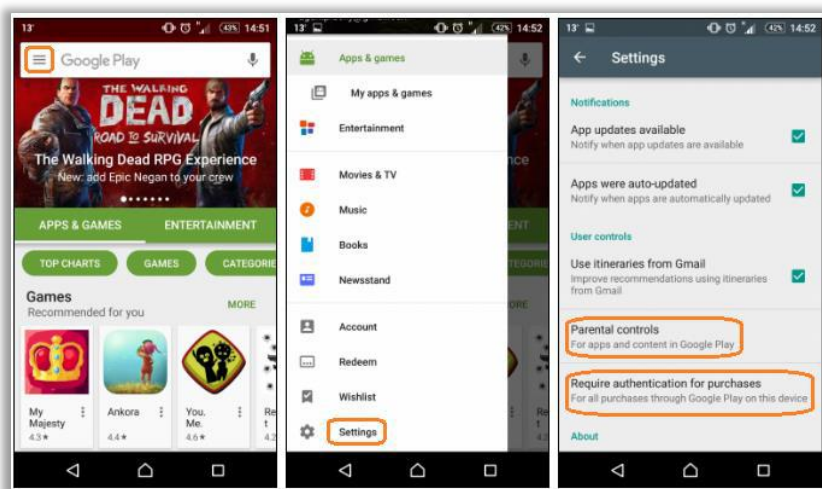
در گوشی‌هایی که سیستم‌عاملشان اندروید است نیز سازکارهایی پیش‌بینی شده است. اگر بخواهید گوشی اندرویدی خود را گاهی به فرزندان هم بدهید، می‌توانید از منوی «تنظیمات» محیطی امن را برای او فراهم سازید. در قسمت Settings از طریق فعال کردن گزینه Guest mode برنامه‌های کاربردی مناسب را برایش مشخص کنید. به این ترتیب، فقط اجازه دسترسی به آن‌ها را خواهد داشت و وارد منوی مخصوص خود خواهد شد.



شکل (۳۳) تنظیمات حالت Guest برای اندروید

در ابتدا با وارد کردن کلمه عبور وارد تنظیمات این حالت می‌شوید. سپس مشخص می‌کنید اخطارها^۱ برای این حالت فعال یا غیرفعال باشد. بعد برنامه‌های کاربردی و در آخر پس‌زمینه کاربر را انتخاب می‌کنید. دیگر می‌توانید گوشی خود را با خیال راحت به فرزندتان بدهید.

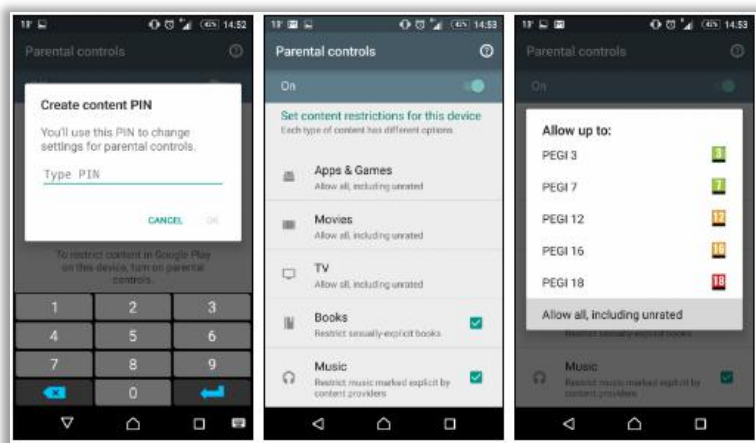
یکی دیگر از تمهیدات نظارتی اندروید در فروشگاه Play Store دیده می‌شود. با انتخاب Settings در این نرم‌افزار می‌توانید گزینه Parental control و همچنین گزینه Require authentication for purchases را فعال کنید. مراحل این کار در شکل زیر با مستطیل‌های قرمز رنگ نشان داده شده است.



شکل (۳۴) نمونه‌ای فعال‌سازی کنترل والدین

^۱ notifications

با فعال کردن گزینه «کنترل والدین» می‌توان رده سنی نرم‌افزارهایی را که در این فروشگاه نشان داده می‌شود، مطابق شکل زیر تعیین کرد.

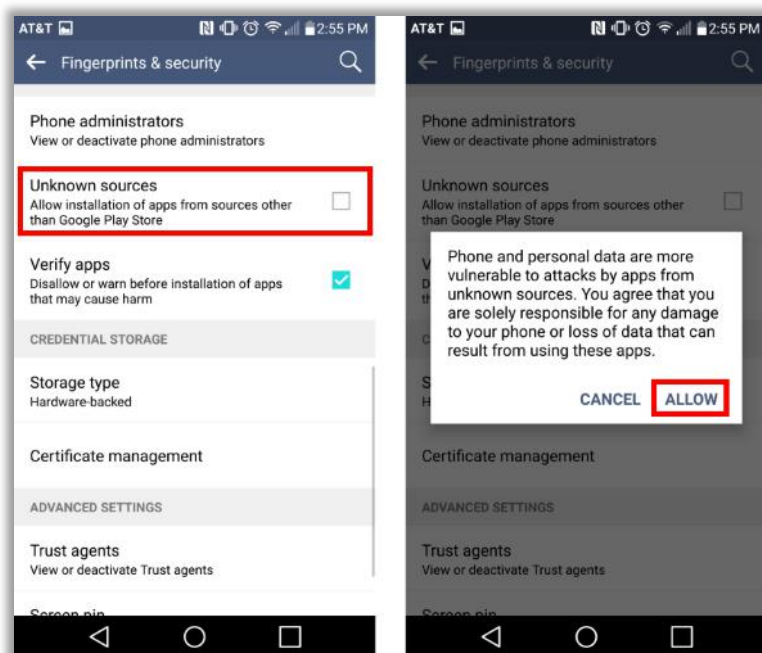


شکل (۳۵) تعیین رده سنی در برنامه‌های اندرویدی

رده‌های سنی پایین‌تر به معنی اعمال محدودیت بیشتر است. گزینه Require authentication for purchases هم امکان خرید برنامه‌های مختلف را محدود و منوط به اجازه و نظارت والدین می‌کند.

برای کنترل دانلود برنامه‌ها از جایی غیر از Play Store نیز می‌توان از روش زیر در گوشی‌های اندروید استفاده کرد و گزینه «اجازه دانلود از منابع ناشناخته» را غیرفعال کرد (Cruickshank, 2016).

Settings->General-> Security -> unknown sources



شکل (۳۶) محدودکردن دانلود از منابع ناشناس

در گوشی‌های سامسونگ، برای نظارت والدین بر فرزندان، نرم‌افزاری به نام Family Care طراحی شده است. برای استفاده از این نرم‌افزار در زمانی که فرزند دستگاه جداگانه‌ای دارد، دستگاه او با دستگاه والدین از طریق QR Code جفت می‌شود. به وسیله این نرم‌افزار والدین می‌توانند زمان استفاده از دستگاه یا هریک از برنامه‌ها را برای فرزند خود تعیین کنند. همچنین نصب کردن برنامه جدید یا دانلود کردن موسیقی جدید تنها با اجازه والدین انجام خواهد شد. با معین کردن زمان استفاده، کودک نمی‌تواند برای مثال در ساعت خواب یا ساعتی که مربوط به مدرسه است، از دستگاه خود استفاده کند (MICHEL, 2016).



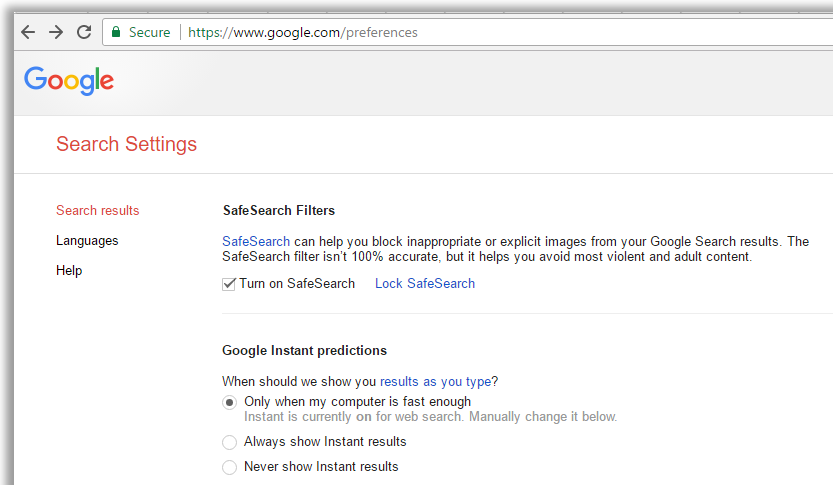
نظارت به کمک مرورگرها و موتورهای جستجو

برای اینکه والدین بتوانند فعالیت فرزندان خود را کنترل کنند، سازندگان نرم افزارهای مرورگر و موتورهای جستجو، تنظیماتی را مهیا کرده و در اختیار آن‌ها قرار داده‌اند. به این ترتیب، راه‌هایی برای مسدود کردن سایت‌های نامطلوب یا تعریف لیست سایت‌های مجاز ایجاد شده است. باید در نظر داشت که اگر بیش از یک مرورگر در سیستم خود داریم، باید فیلترها را در همه آن‌ها فعال کنیم. البته این ابزار برای کنترل فرزندان بزرگ‌تر که با جزئیات نرم افزارها آشنا هستند، مناسب نیست.

گزینه‌های کنترلی در موتور جستجوی گوگل

برای اجرای تنظیمات کنترلی در موتور جستجوی گوگل، می‌توان به آدرس <https://www.google.com/preferences> مراجعه کرد و گزینه SafeSearch را مانند شکل زیر فعال کرد.

گزینه Lock SafeSearch فیلتر سخت‌گیرانه‌ای است که هم برای متن و هم برای تصاویر اعمال می‌شود؛ هرچند هیچ فیلتری صددرصدی نیست. در پایین صفحه، کلید save قرار دارد که پس از انتخاب تنظیمات، برای ذخیره وضعیت جدید باید بر روی آن کلیک کرد.



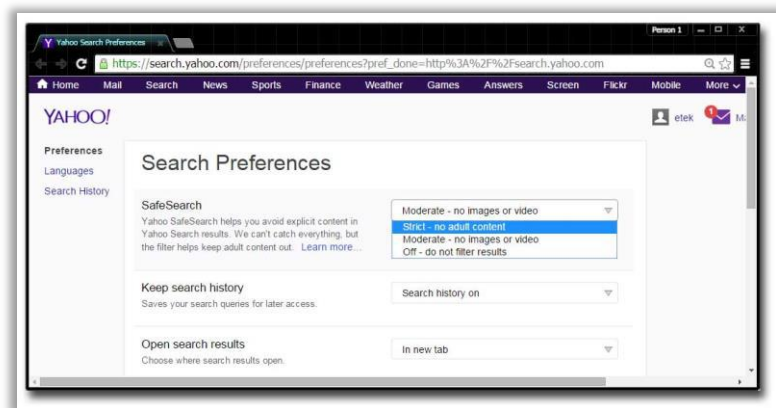
شکل (۳۷) تنظیم گزینه جستجوی امن در موتور جستجوی گوگل

برای دیدن تاریخچه سایت‌های بازدید شده می‌توان به History در تنظیمات مرورگر مراجعه کرد یا از کلید میان‌بر Ctrl+H استفاده کرد. همچنین در صفحه <https://www.google.com/preferences> بخش‌هایی از تاریخچه را می‌توان دید. تاریخچه‌ای که در این صفحه نگهداری می‌شود، حتی در صورتی که لیست History در مرورگر پاک شده باشد، قابل مشاهده است.

گزینه‌های کنترلی در موتور جستجوی یاهو

برای دسترسی به گزینه کنترل والدین در موتور جستجوی یاهو هم می‌توان به سایت <http://search.yahoo.com/preferences> مراجعه کرد. گزینه SafeSearch در این صفحه را می‌توان در سه حالت تنظیم کرد. در حالت Off هیچ محدودیتی اعمال نمی‌شود. در حالت میانه (Moderate) محدودیتی برای تصاویر یا ویدئو در نظر گرفته

می‌شود. در حالت سخت‌گیرانه (Strict) محتواهای مختص بزرگسالان برای فرزندان ممنوع می‌شود.



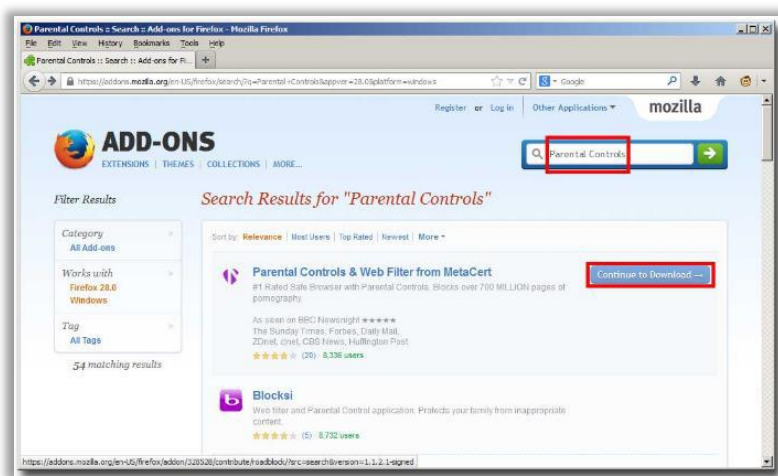
شکل (۳۸) گزینه کنترل موتور جستجوی یاهو

گزینه‌های کنترلی در مرورگر فایرفاکس

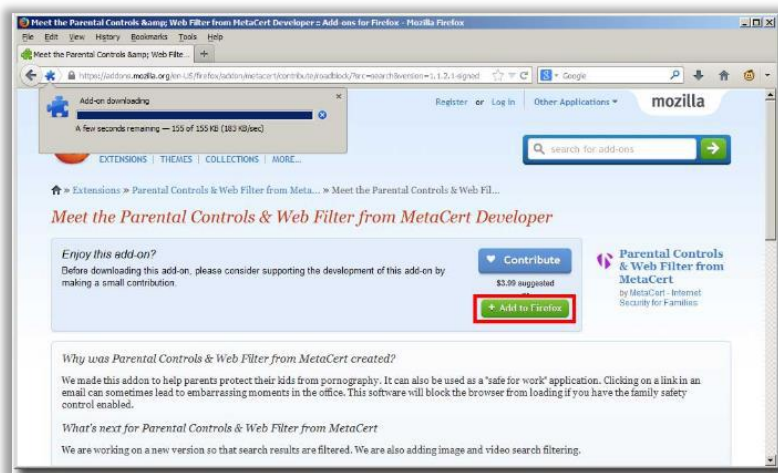
در مرورگر فایرفاکس ابتدا سایت 'Firefox Add-on' می‌شویم و در قسمت جستجوی آن، parental control را جستجو می‌کنیم. در مرحله بعد می‌توانیم هریک از افزونه‌هایی را که با این عنوان نمایش داده می‌شود، انتخاب و به مرورگر خود اضافه کنیم. در شکل‌های زیر مستطیل‌های قرمز رنگ، کلیدهایی است که مسیر اجرای این کار را نشان می‌دهد (محمود، ۱۳۹۴).

¹ <https://addons.mozilla.org/en-US/firefox/>

روش‌هایی برای حفظ امنیت خانواده در فضای مجازی



شکل (۳۹) کلیدهای کنترل والدین در مرورگر فایرفاکس (۱)



شکل (۴۰) کلیدهای کنترل والدین در مرورگر فایرفاکس (۲)

گزینه‌های کنترلی در مرورگر کروم

مرورگر کروم برای فعال‌سازی قابلیت نظارت بر فرزندان زیر ۱۳ سال، از والدین می‌خواهد از طریق برنامه Family Link برای فرزندان خود که از گوشی‌های اندرویدی و مرورگر کروم استفاده می‌کنند، حساب کاربری بسازند تا بتوانند فضای سالم و امنی را برایشان فراهم کنند.

گوگل تا قبل از ژانویه ۲۰۱۸ از قابلیت Supervised User برای کنترل والدین استفاده می‌کرد؛ اما این گزینه غیرفعال شده است. برای استفاده از نرم‌افزار Family Link باید گوشی یا تبلت والدین اندروید یا iOS باشد و گوشی یا تبلت فرزندان اندرویدی. همچنین داشتن حساب کاربری گوگل هم لازم است. با نصب این نرم‌افزار، گوشی فرزندان با گوشی والدین جفت می‌شود و در لیست خانواده قرار می‌گیرد. به این ترتیب، والدین می‌توانند محدودیت‌های لازم برای بازدید از وبسایت‌ها را اعمال کنند.



شکل (۴۱) نرم‌افزار کنترل والدین Family Link

متأسفانه فعلاً این نرم‌افزار در کشور ما پشتیبانی نمی‌شود. به همین دلیل، برای نظارت بر وب‌گردی فرزندان با این مرورگر، باید از نرم‌افزارهایی که در ادامه معرفی شده و نیز افزونه‌های مسدود کردن سایت‌ها استفاده کرد.

گزینه‌های کنترلی در مرورگر سافاری^۱

اگر فرزندان گوشی یا تبلت آپید دارد یا مدام از گوشی آیفون شما استفاده می‌کند، باید مراقب محتوایی که از طریق مرورگر مخصوص سیستم‌عامل اپل، یعنی Safari، در دسترس او قرار می‌گیرد، باشید.

برای اعمال محدودیت، ابتدا به بخش زیر بروید:

Settings > General > Restrictions

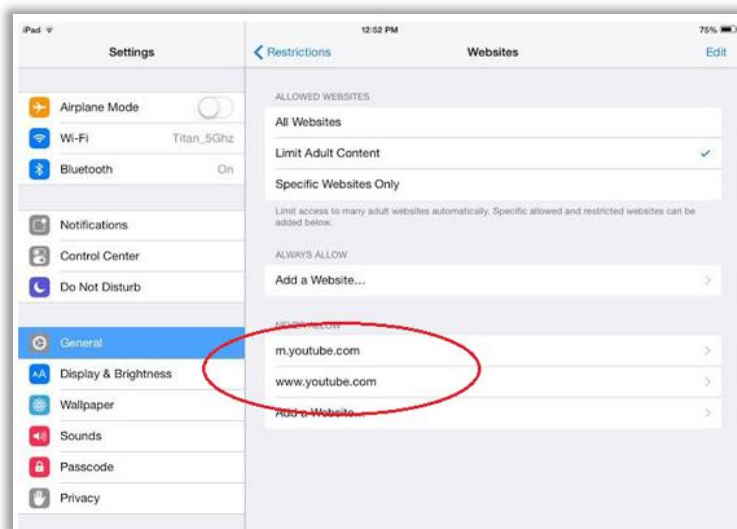
در اینجا پس از وارد کردن کد تأیید چهاررقمی می‌توانید فهرست سایت‌هایی را که مناسب فرزندان نیست یا فهرست سایت‌هایی را که ترجیح می‌دهید فرزندان فقط از آن‌ها بازدید کنند، وارد کنید. از این قسمت همچنین می‌توانید گزینه مسدود کردن سایت‌های بزرگسال را انتخاب کنید:



شکل (۴۲) دستیابی به گزینه کنترلی در مرورگر سافاری

^۱ Safari

همان‌طور که در شکل زیر مشاهده می‌کنید، علاوه بر اینکه دسترسی به سایت‌های بزرگسال مسدود شده، فهرست سایت‌هایی که کودک نباید به آن‌ها دسترسی داشته باشد هم مشخص شده است.



شکل (۴۳) قابلیت محدود کردن بازدید از صفحات وب توسط والدین در مرورگر سافاری

افزونه‌ها

راهکار دیگری که برای حفاظت از فرزندان در برابر تهدیدات فضای مجازی استفاده می‌شود، افزونه‌هاست. افزونه‌ها بسته‌های کوچکی هستند که کارایی مرورگر را بیشتر می‌کنند و قابلیت‌های مختلفی را به آن می‌افزایند. به‌طور کلی، برای کار با افزونه‌ها ابتدا باید آن‌ها را در مرورگر خود نصب کنید. این کار بسیار ساده است. سپس باید با راست کلیک روی آن یا انتخاب گزینه Options بسته به مرورگر، تنظیمات آن را به دلخواه خود تغییر دهید.

برای مشاهده افزونه‌های مرورگر کروم خود در گوشه سمت راست بالا روی علامت سه نقطه کلیک کنید و از قسمت More tools وارد Extentions شوید. در مرورگر فایرفاکس هم از همان قسمت Add-ons یا کلید میان‌بر Ctrl+Shift+L وارد بخش افزونه‌ها شوید.

با استفاده از افزونه‌های نظارت والدین در مرورگرها می‌توانید کارهای مختلفی انجام دهید. در ادامه به برخی از این کارها اشاره می‌شود.

افزونه مدیریت زمان Nanny

این افزونه برای مدیریت زمان فرزندان در دسترسی به سایت‌های موردعلاقه‌شان طراحی شده است. علاوه‌براین، می‌توانید سایت‌هایی را که از نظر شما مناسب نیستند، به تنظیمات آن اضافه کنید یا لیست سایت‌های مجاز برای دسترسی فرزندان را مشخص کنید. این افزونه برای مرورگر کروم و فایرفاکس در دسترس است.



شکل (۴۴) افزونه کنترل والدین Nanny

افزونه ضدپورن^۱

این افزونه برای مسدودسازی سایت‌های غیراخلاقی است. پس از نصب آن، سایت‌های مستهجن به صورت خودکار مسدود می‌شوند. می‌توانید سایت‌هایی را هم که از نظر شما مناسب نیستند، به تنظیمات آن اضافه کنید. از دیگر قابلیت‌های این افزونه گذاشتن کلمه عبور بر روی تنظیمات است که هیچ‌کس نمی‌تواند تغییری در آن ایجاد کند. یکی از ویژگی‌های این افزونه مدیریت فیلترینگ به صورت ابری است؛ یعنی دسترسی به وبسایت‌های ممنوع زیر نظر هزاران وبسایت بر روی فضای ابری کنترل می‌شود.



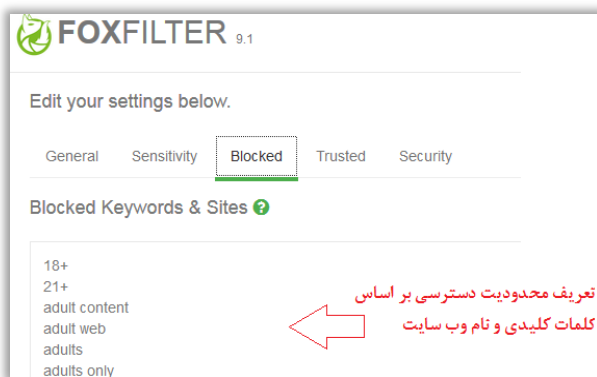
شکل (۴۵) تنظیمات افزونه ضدپورن فایرفاکس

افزونه فیلتر فایرفاکس^۲

این افزونه قبل از ورود کاربر به سایت، محتوای آن را براساس تنظیمات تعریف‌شده یا کلمات کلیدی معینی که به آن داده شده، به سرعت بررسی می‌کند و اگر خطری را شناسایی کند، هشدار می‌دهد. این افزونه برای پدر و مادرهایی که نگران وب‌گردی فرزندان‌شان هستند، بسیار کارآمد است.

^۱ Anti-Porn Pro

^۲ FoxFilter



شکل (۴۶) تنظیمات افزونه فاکس فیلتر بر اساس URL و کلمات کلیدی



حفاظت با انتخاب کلمه عبور مناسب

انتخاب رمز عبور قوی و مناسب از ضروری‌ترین کارها در امنیت فضای مجازی است. رمز عبور قوی و مناسب، رمزی است که حداقل ۸ نویسه داشته باشد و از حروف و اعداد و علائم تشکیل شده باشد. می‌توانید از راهنمای کوتاه زیر برای این منظور استفاده کنید.

- رمز عبوری انتخاب کنید که بتوانید آن را به خاطر بسپارید. مثلاً از حروف اول هریک از کلمات یک جمله استفاده کنید؛ مانند «من در اینترنت با اطمینان قدم برمی‌دارم: MDIBEGBM».
- رمز عبورتان حداقل ۱۲ نویسه داشته باشد.
- از الگوهای ساده صفحه‌کلیدی استفاده نکنید؛ مثل «۱۲۳۴۵» یا «qwerty».
- از حروف بزرگ و کوچک و اعداد استفاده کنید (برای راحتی کار می‌توانید به‌ترتیبی حروف بزرگ و کوچک را تغییر دهید)؛ مانند «AsDfG12».
- از علائم و نمادهای خاص مانند !@#\$%^&* در ترکیب با اعداد و حروف استفاده کنید؛ مانند «!n the n@me Of All@h».



- از افشای رمز عبور خود، حتی برای نزدیک‌ترین دوستانتان، خودداری کنید. از نوشتن رمز عبور خود روی کاغذ و قراردادن آن در جای نامناسب بپرهیزید (مثلاً چسباندن رمز عبور کارت بانکی به کارت بانکی یا قراردادن رمز عبور کامپیوتر زیر صفحه‌کلید).
- از زبان‌های مختلف استفاده کنید؛ مثلاً «Esme man reza ast».
- از صفحه‌کلید انگلیسی استفاده کنید؛ ولی به‌فارسی بنویسید؛ مثلاً در صفحه‌کلید انگلیسی به‌فارسی بنویسید «امنیت سایبری»: «hlkdj shfvd».
- از علائم و اختصارات برای تبدیل عبارات طولانی به جملات پیچیده و کوتاه استفاده کنید؛ مثلاً:

“Are you happy today”: “ru:-)2d@y”

- هرازگاهی رمز عبورهای خود را تغییر دهید و در مدت‌زمان طولانی از یک رمز عبور استفاده نکنید.
 - در رمز عبور، از اطلاعات شناسنامه‌ای یا شماره‌موبایل یا نام فرزندان خود استفاده نکنید.
 - از یک رمز برای چند حساب کاربری (مانند ایمیل و حساب کاربری در شبکه‌های مجازی) استفاده نکنید.
- علاوه بر موارد یادشده، می‌توان از نرم‌افزارهای مدیریتی رمز عبور برای ساده‌تر شدن و درعین‌حال افزایش امنیت نگهداری از رمزهای عبور خود استفاده کرد. نرم‌افزارهای مدیریت رمز عبور برای حساب‌های کاربری ما رمز عبوری قوی و مطمئن می‌سازند و آن را در محیطی امن نگه می‌دارند.



کنترل از طریق تجهیزات شبکه خانگی

در اغلب مودم‌های خانگی می‌توان محدودیت‌هایی برای دسترسی ایجاد کرد و دسترسی به بعضی از سایت‌ها را ممنوع کرد. برای این منظور، ابتدا نشانی 192.168.1.1 را

در مرورگر وارد می‌کنیم و وارد تنظیمات مودم می‌شویم. سپس به سراغ گزینه‌های access control و filter می‌رویم. در قسمت باز شده می‌توانیم فهرستی از سایت‌های نامطلوب را که نمی‌خواهیم به آن‌ها دسترسی داشته باشیم، درج می‌کنیم. به این ترتیب، دسترسی به سایت‌هایی که در فهرست درج شده، برای تمام دستگاه‌های موجود در شبکه خانگی، ناممکن می‌شود (Donnell, 2016).

شکل (۴۷) تنظیمات مودم برای فیلتر شدن سایت‌های خاص

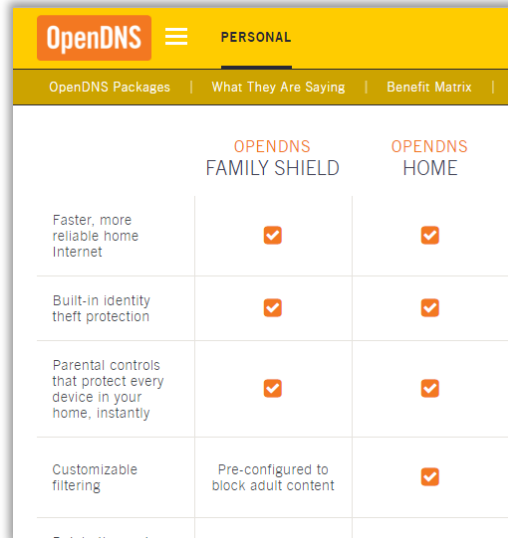
برای حفاظت از کودکان در شبکه خانگی، همچنین می‌توانیم دستگاه مودم جدیدی با قابلیت‌های مورد نیاز خریداری کنیم یا دستگاهی اضافی خریده و در کنار مودم قرار دهیم. برای مثال، netpure دستگاهی است به اندازه یک لیوان معمولی که می‌توان آن را در کنار مودم قرار داد و شبکه wi-fi خانگی را برای تمام دستگاه‌هایی که به آن متصل‌اند، به شکل دلخواه فیلتر کرد و گزارش‌هایی از آن گرفت.



شکل (۴۸) اینترنت امن برای کودکان با روترهای کنترل والدین

بعضی از مودم‌های خانگی قابلیت‌هایی به نام «کنترل والدین» دارند که باید در هنگام راه‌اندازی دستگاه، فعال شود. با فعال شدن این ویژگی، تمام دستگاه‌های داخل خانه تحت کنترل والدین قرار می‌گیرد (Hoffman, 2013). استفاده از این نوع ابزار برای همهٔ سنین مناسب است (Knorr, 2016).

سرویس OpenDNS (که از جمله سرویس‌های شرکت آمریکایی Cisco است) یکی از سرویس‌های متداول با کاربردهای مختلف است که بدون نصب هیچ نرم‌افزاری و به‌منظور فیلترکردن محتوای نامناسب، روی شبکه خانگی، کامپیوتر شخصی، گوشی هوشمند یا سرورها استفاده می‌شود. با استفاده از این سرویس، سایت‌های مجاز یا whitelist در شبکهٔ خانگی تعریف می‌شود.

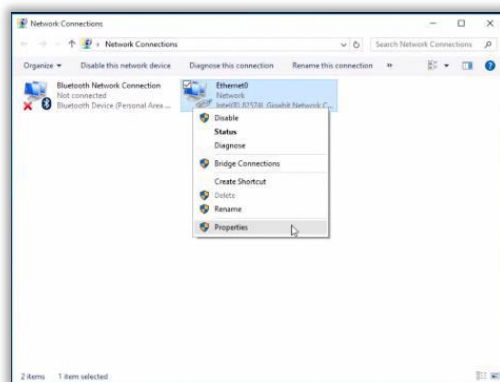


PERSONAL		
OpenDNS Packages	What They Are Saying	Benefit Matrix
	OPENDNS FAMILY SHIELD	OPENDNS HOME
Faster, more reliable home Internet	✓	✓
Built-in identity theft protection	✓	✓
Parental controls that protect every device in your home, instantly	✓	✓
Customizable filtering	Pre-configured to block adult content	✓

شکل (۴۹) نمایی از سایت OpenDNS و قابلیت کنترل والدین

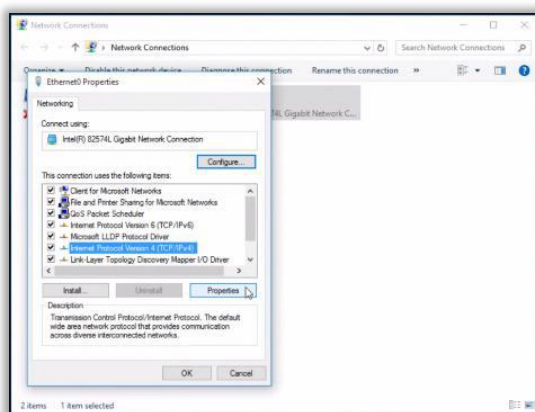
البته این لیست برای همه افراد خانواده یکی است و امکان تعریف سطوح مختلف برای افراد، به‌طور جداگانه وجود ندارد. برای مثال، روش فعال کردن آن بر روی کامپیوتر به‌شکل زیر است:

بر روی واسط شبکه‌ای که در کامپیوتر استفاده می‌کنیم، گزینه properties را باز می‌کنیم.

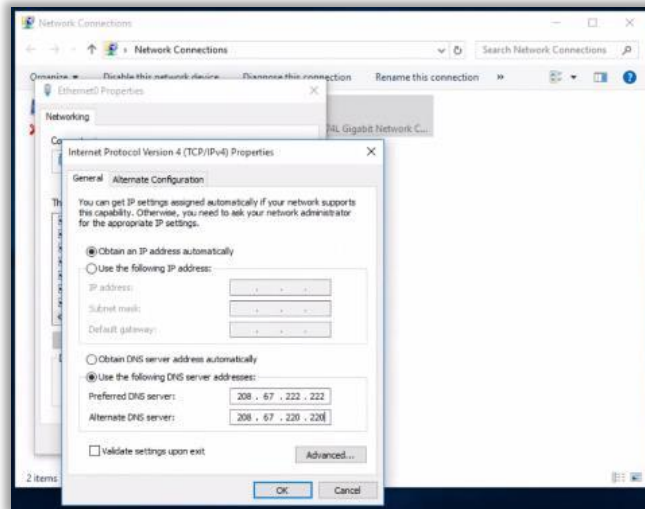


شکل (۵۰) تنظیمات استفاده از سرور OpenDNS

سپس (مطابق شکل‌های زیر) وارد مشخصات TCP/IP می‌شویم و آدرس DNS را برابر مقادیر 208.67.222.222 و 208.67.220.220 قرار می‌دهیم (OpenDNS, 2017).



شکل (۵۱) تنظیمات استفاده از سرور OpenDNS



شکل (۵۲) تنظیمات استفاده از سرور OpenDNS



نظارت والدین به کمک نرم افزارهای ضد ویروس

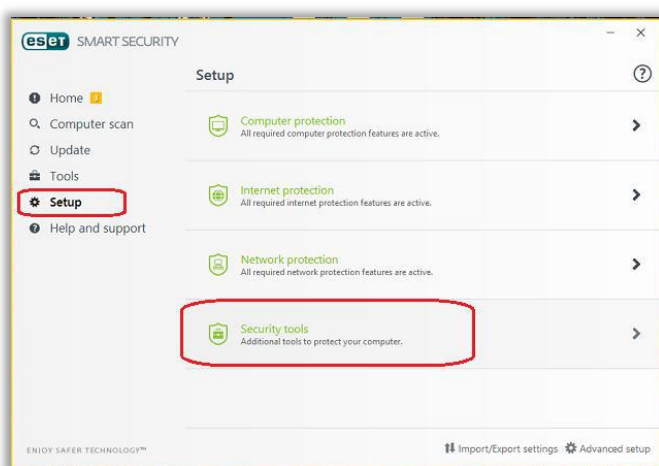
نرم افزارهای ضد ویروس نیز امکاناتی برای کنترل والدین به مشتریان عرضه کرده اند.

نرم افزار نود ۳۲

با امکان parental control در آنتی‌ویروس نود ۳۲ می‌توانیم فعالیت آنلاین فرزندان خود را کنترل و دسترسی آن‌ها به محتوای نامناسب را محدود کنیم. به این ترتیب، وب‌گردی فرزندان امن‌تر خواهد بود. برای استفاده از قابلیت parental control در آنتی‌ویروس نود ۳۲ باید حداقل دو حساب کاربری داشته باشیم: یکی مخصوص والدین و دیگری مخصوص فرزند. سپس گزینه کنترل والدین آنتی‌ویروس نود ۳۲ (یا ESET) را به شکل زیر فعال می‌کنیم:

Setup -> Security tools -> Parental control

در صفحه Parental control با انتخاب حساب کاربری‌ای که برای فرزندمان ساخته‌ایم، وارد تنظیمات می‌شویم. شکل ۵۳ اولین مرحله این عملیات را نشان می‌دهد (زارع‌پور، ۱۳۹۵).



شکل (۵۳) مرحله‌ای از تنظیمات کنترل والدین در نود ۳۲

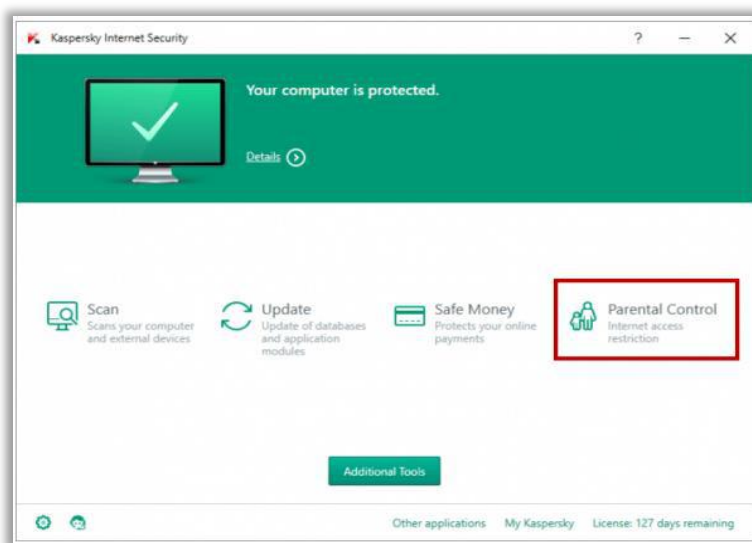
نرم افزار Kaspersky

نرم افزار آنتی ویروس معروف Kaspersky نیز راه حل هایی برای این موضوع در نظر گرفته است. گزینه parental control می تواند محدودیت هایی در دسترسی به صفحات اینترنت ایجاد کند. همچنین با فعال سازی Control Web Browsing می توانیم گزارش کاملی از وب گردی کاربر تهیه و مشاهده کنیم. برای فعال سازی parental control باید در صفحه Kaspersky Internet Security آیکون parental control را انتخاب کنیم. از گزینه هایی که برای محدودیت دسترسی به اینترنت در این نرم افزار قرار داده شده، می توان برای روزهای کاری^۱ یا تعطیلات پایان هفته^۲ استفاده کرد. گزینه دیگری نیز در این نرم افزار وجود دارد که می تواند دسترسی به تعدادی وبسایت خاص را مسدود کند. این وبسایت ها یا به صورت جدولی از آدرس هایی است که از محتوای آن ها آگاهی داریم یا براساس دسته بندی پیشنهادی خود نرم افزار^۳ مسدود می شود (یزدانی، ۱۳۹۵). شکل زیر اولین مرحله از مراحل بالا را نشان می دهد.

^۱ Restrict access on weekday

^۲ Restrict access on weekends

^۳ Adult websites



شکل (۵۴) بخشی از اجرای مراحل کنترل والدین در Kaspersky

قابلیت دیگری که در نرم‌افزار Kaspersky در نظر گرفته شده، محدودکردن دسترسی به بازی‌ها برای فرزندان و بزرگ‌ترهاست. برای محدودکردن دسترسی به بازی‌هایی که مناسب سن فرزندان نیست، به ترتیب زیر عمل می‌کنیم.

Kaspersky Internet Security-> Parental Control-> Configure restrict->

Application-> انتخاب حساب کاربری

در این مرحله دو گزینه برای محدودکردن بازی برای کودکان و بزرگسالان به‌طور جداگانه در نظر گرفته شده است. پس از انتخاب یکی از این گزینه‌ها، لیست بازی‌های موجود در سیستم دیده می‌شود که در کنار هریک از آن‌ها جایی برای تیک‌زدن وجود دارد. بازی‌های تیک‌خورده بازی‌های مجاز هستند (یزدانی، ۱۳۹۵). همچنین به کمک

قابلیت محدود کردن برنامه‌ها در نرم‌افزار Kaspersky می‌توانیم برنامه‌های خاصی را در لیست برنامه‌ها تیک بزنیم تا از دسترسی کاربر خارج شود (یزدانی، ۱۳۹۵). جالب اینکه برای استفاده از Kaspersky در گوشی‌های اندروید هم قابلیت نظارت بر محتوای سایت‌ها و برنامه‌های مختلف در نظر گرفته شده و در نسخه‌ای با نام Kaspersky Safe Kids گنجانده شده است. پس از نصب این نرم‌افزار را روی گوشی، دو حالت را می‌توان انتخاب کرد: حالت والدین و حالت کودکان. وقتی دستگاه در حالت والدین قرار می‌گیرد، می‌تواند بر دستگاه کودک نظارت کند (Kaspersky, 2017).

نرم‌افزار eScan

در نرم‌افزار ضدویروس eScan که بر روی کامپیوتر نصب می‌شود، قابلیت «نظارت و کنترل بر فعالیت‌های آنلاین کودکان» گنجانده شده است. این قابلیت به والدین کمک می‌کند از کودکانشان محافظت کنند و دسترسی آن‌ها به برنامه‌های اینترنتی و بازی‌ها و وبسایت‌های غیراخلاقی را کنترل کنند. همچنین از طریق این نرم‌افزار می‌شود انتقال اطلاعات خصوصی مانند شماره‌تلفن و شماره کارت اعتباری را محدود کرد. این نرم‌افزار قابلیت دیگری نیز به نام «کنترل والدین پیشرفته» دارد که از طریق آن می‌توان بر فعالیت‌های آنلاین کودکان کاملاً نظارت کرد و به‌طور مؤثری محتواهای نامناسب را مسدود نمود. به‌این‌ترتیب، از تمام اعضای خانواده در برابر مجرمان اینترنتی حفاظت می‌شود (کی پاد، ۱۳۹۷).

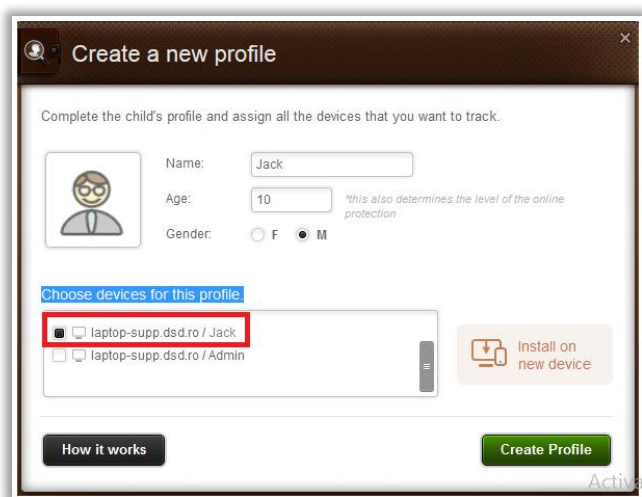
برنامه Bitdefender

در برنامه Bitdefender ویژگی کنترل والدین برای کنترل دسترسی کاربران به اینترنت و برنامه‌های کاربردی قرار داده شده است. برای دسترسی به این ویژگی، باید محصولات کامل‌تر Internet Security 2015 یا Total Security 2015 را روی کامپیوتری که فرزندان استفاده می‌کنند، نصب کنیم و سپس مراحل فعال‌سازی ویژگی کنترل والدین را گام‌به‌گام پیش ببریم. در گام اول باید حساب کاربری محدودشده‌ای روی کامپیوتر برای فرزندان

ایجاد کنیم. در گام دوم باید با حساب کاربری administrator وارد سیستم شویم. فقط با این حساب کاربری می‌توانیم تنظیمات کنترل والدین را انجام دهیم. صفحه تنظیمات کنترل والدین این نرم‌افزار، به شکل زیر باز می‌شود:

Bitdefender window: privacy->Parental Control->Configure

در این صفحه به وسیله کلید Add child پروفایلی مانند شکل ۵۵ برای فرزند ایجاد می‌کنیم.



شکل (۵۵) تعریف پروفایل برای کودک در نرم‌افزار BitDefender

با فشردن کلید Create Profile، پروفایل تکمیل می‌شود و می‌توانیم برای آن محدودیت‌های دلخواه‌مان را اعمال کنیم. برای مثال، می‌توانیم صفحات مربوط به بازی‌های برخط یا بازی‌های کامپیوتری را ممنوع یا دسترسی به اینترنت را در زمان‌هایی مانند آخر هفته محدود کنیم. قابلیت دیگری که در این محدودیت‌ها وجود دارد، تعیین کردن کلمه‌ای کلیدی مانند porn است. با این کار، مشاهده صفحات وب یا پست الکترونیکی یا پیام فوری‌ای که شامل این کلمه باشد، برای حساب کاربری مشخص شده غیرممکن می‌شود. همچنین این کاربر نمی‌تواند پیامی فوری یا پست الکترونیکی‌ای را که حاوی این کلمه باشد، ارسال کند (Bitdefender, 2017).

گفتنی است که در بقیه برنامه‌های آنتی‌ویروس هم (مانند آویرا یا f-secure) چنین قابلیت‌هایی پیش‌بینی شده؛ هرچند در آن‌ها توضیحات مفصلی در این باره داده نشده است. بنابراین، پیدا است سازندگان نرم‌افزارهای ضدویروس از اهمیت این قابلیت نرم‌افزاری غافل نبوده‌اند.



نظارت به کمک نرم‌افزارهای کنترلی در رایانه یا گوشی هوشمند

آنچه کودکان و نوجوانان در فضای مجازی می‌بینند، از دید والدین مخفی می‌ماند؛ مگر اینکه با استفاده از ابزارهای تکنولوژیک این نقص را برطرف کنیم.

علاوه بر راهکارهایی که پیش‌تر به آن‌ها اشاره شد، نرم‌افزارهای دیگری وجود دارد برای اینکه خانواده‌ها بهتر و دقیق‌تر بتوانند فعالیت‌های اینترنتی فرزندان خود را مدیریت کنند؛ نرم‌افزارهایی که مشخصاً برای این منظور طراحی شده است.

نرم‌افزارهای فیلترینگ خانگی نوعی نظارت اختیاری و مستقل هر خانواده بر فعالیت‌های اینترنتی فرزندان است و با مفهوم فیلترینگ دولتی که براساس خط‌مشی دولت‌ها صورت می‌گیرد، تفاوت دارد (تبیان، ۱۳۹۱).

این نرم‌افزارها در بسیاری از کشورهای پیشرفته جهان که خود از طراحان اولیه اینترنت‌اند، بسیار مورد توجه است. به دلیل متنوع بودن موضوعات و محتواهای اینترنتی، در بسیاری مواقع مطالب و تصاویری که در اینترنت منتشر می‌شود، حتی اگر از فیلتر دولتی و قانونی مرسوم هم عبور کند، برای تمام گروه‌های سنی مناسب نیست. به همین دلیل، بسیاری از کشورها برای کمک به خانواده‌ها و فرهنگ‌سازی در این زمینه، براساس ارزش‌های فرهنگی و اخلاقی و بومی، نرم‌افزارهایی نظارتی طراحی کرده و در اختیار عموم قرار داده‌اند. معمولاً این نرم‌افزارها شامل امکانات زیر است:

- امکان انتخاب محدوده سنی برای فرزندان
- مشاهده محتوایی که فرزندان دیده‌اند
- امکان تعیین زمان استفاده
- مکان‌یابی فرد
- ارائه گزارش
- امکان اعمال تنظیمات دلخواه و تغییر رمز عبور اصلی
- هدایت کاربر به سمت سایت‌های مفید

این نرم‌افزارها می‌توانند به دو روش بر فعالیت فرزندان در فضای مجازی نظارت کنند: یکی فعالانه و دیگری غیرفعالانه. در روش فعالانه، دسترسی فرزندان به محتواهایی مشخص شده محدود می‌شود. در روش غیرفعالانه، صرفاً گزارشی از فعالیت‌های فرزندان در

فضای مجازی به والدین داده می‌شود. برخی از این نرم‌افزارها فقط مخصوص گوشی‌های هوشمند و تبلت‌هاست و برخی نیز با نسخه‌های متنوع، با همه نوع دستگاه و رایانه‌ای سازگار است. البته غالباً استفاده از قابلیت‌های اختصاصی و پیشرفته این نرم‌افزارها نیازمند پرداخت هزینه است.

مراحل نصب این نرم‌افزارها اغلب شبیه به هم است؛ به این ترتیب که در هریک باید حساب کاربری و رمز عبوری تعیین کرد و سپس بسته به سلیقه و خواست خانواده و کاربر، تنظیماتی را اعمال کرد.

در زیر نمونه‌هایی از این نرم‌افزارها معرفی می‌شود. والدین می‌توانند برحسب نیاز خود و باتوجه به قابلیت‌ها، نرم‌افزار دلخواهشان را بیابند و تهیه کنند (ITSN, ۱۳۹۴).

نرم‌افزار کیدلاگر

کیدلاگر بیش از آنکه نرم‌افزاری پیشگیری‌کننده باشد، یک لاگر یا ثبت‌کننده است و فقط درخصوص فعالیت‌های آنلاین کاربر گزارش‌هایی می‌دهد (kidlogger, n.d.). کیدلاگر به شما کمک می‌کند تا بدانید:

- + فرزندان چه مدت با کامپیوتر یا موبایل کار کرده است.
- + از چه نرم‌افزارهایی استفاده کرده است.
- + از چه وبسایت‌هایی بازدید کرده است.
- + با چه کسی از طریق تلفن، پیامک، Skype یا فیس‌بوک ارتباط داشته است.
- + در چه مکان‌هایی بوده است.
- + چه عکس‌هایی گرفته است.
- + به دوستانش چه نوشته است.

این نرم‌افزار را می‌توان بر روی کامپیوتر، موبایل و تبلت با سیستم‌عامل‌های مختلف نصب کرد. نسخه رایگان کیدلاگر را فقط در یک دستگاه می‌توان استفاده کرد؛ درحالی‌که نسخه‌های غیررایگان را می‌شود در چندین دستگاه و با قابلیت‌های بیشتر استفاده کرد.

پس از دریافت نسخهٔ مدنظر این برنامه از سایت kidlogger.net مانند بقیهٔ برنامه‌های نصبی ویندوز، آن را نصب می‌کنیم.



شکل (۵۶) آغاز نصب Kidlogger نسخهٔ ویندوز ۷

پس از نصب کیدلاگر، از شما دربارهٔ نام کاربری‌ای که می‌خواهید بر فعالیت‌هایش نظارت شود، سؤال می‌شود:



شکل (۵۷) تنظیمات اولیه در Kidlogger

با انتخاب کلید Connect to kidlogger.net accout وارد منوی زیر می‌شوید و پس از ثبت حساب کاربری خود در این سایت، از گزارش‌های مختلف آن استفاده می‌کنید:



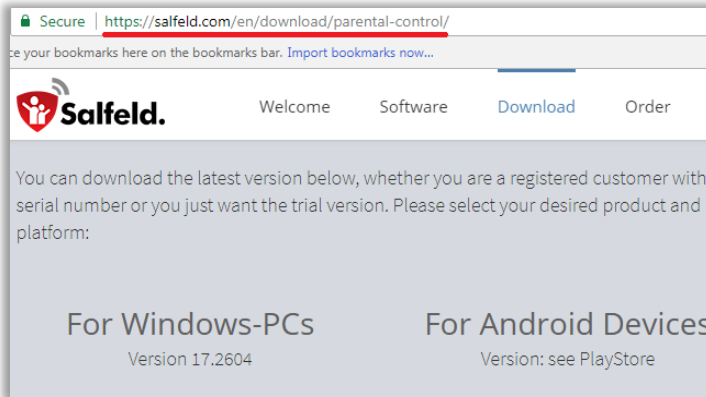
شکل (۵۸) پنل کنترلی در نرم‌افزار Kid Logger

تقریباً مشابه همین عملیات برای نصب kidlogger در گوشی‌های هوشمند تکرار می‌شود. توجه کنید که نسخه رایگان این نرم‌افزار فقط قابلیت نظارت بر یک دستگاه را دارد.

نرم‌افزار Salfeld Child Cotrol

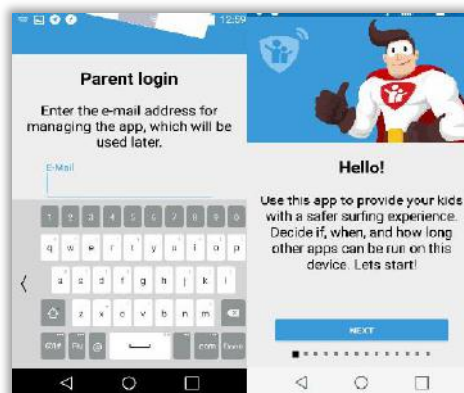
با استفاده از این نرم‌افزار آلمانی به راحتی بگومگوهای خود با فرزندان را برای خاموش کردن رایانه یا تبلت خاتمه می‌دهید و رایانه و تبلت رأس ساعت مقرر خاموش می‌شود. نرم‌افزار Salfeld Child Control راهکار مناسبی برای جلوگیری از غرق شدن فرزندان در دنیای رایانه و موبایل است (Salfeld, n.d.).

نسخه موبایلی و رایگان این نرم افزار در فروشگاه های Google Play و iOS موجود است. برای دریافت نسخه ویندوز از طریق سایت آن اقدام کنید.



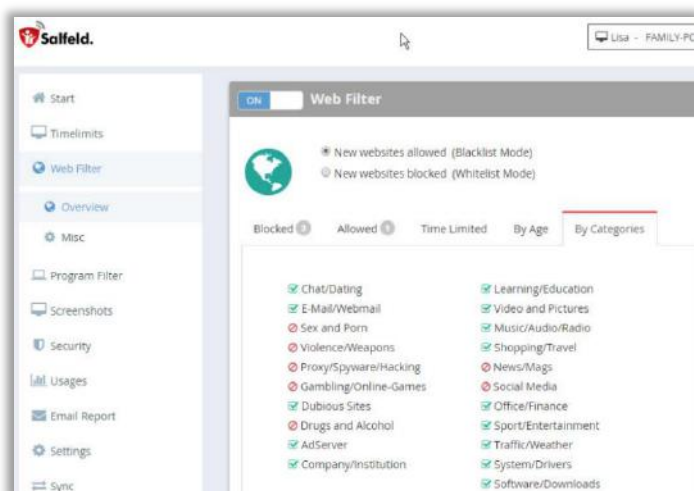
شکل (۵۹) دریافت نرم افزار از سایت salfeld

پس از وارد کردن آدرس ایمیل معتبر و رمز عبور، از شما سؤال می شود که دستگاه فعلی مال شماست یا فرزندتان. سپس بسته به پاسخ، مراحل خاصی دنبال می شود.



شکل (۶۰) یکی از مراحل راه اندازی نرم افزار Salfeld برای اندروید

با این نرم‌افزار می‌توانید محدودیت‌های مدنظر خود را ایجاد کنید و با خیال راحت به کودکان اجازه دهید از رایانه استفاده کنند. این نرم‌افزار می‌تواند دسترسی به فولدرها، فایل‌ها، نرم‌افزارها، بازی‌ها و... را محدود کند یا فقط در ساعت‌های خاصی اجازه کار با رایانه را بدهد. همچنین با این نرم‌افزار می‌توانید مطابق شکل زیر دسترسی به اینترنت را محدود یا بعضی از سایت‌ها را فیلتر کنید یا اینکه فقط اجازه دسترسی به چند سایت خاص را بدهید.



شکل (۶۱) تنظیمات بخش محدودیت دسترسی در وب با Salfeld

نرم‌افزار NQ Family Guardian^۱

این نرم‌افزار مناسب زمانی است که فرزند شما به سنی رسیده که می‌تواند گوشی همراه داشته باشد. در چنین حالتی، با نرم‌افزار NQ Family Guardian، والدین می‌توانند

^۱ NQ Family Guardian

موقعیت مکانی فرزندشان و نحوه استفاده او از گوشی همراه را مدیریت کنند. با نصب این نرم افزار روی گوشی فرزند خود، به نحوه وب گردی و برنامه های نصب شده، عکس ها، تماس ها و پیامک هایش دسترسی دارید. یکی از قابلیت های خوب این نرم افزار تعریف منطقه امن برای فرزندان است. با این قابلیت، در صورت احساس ناامنی، فرزندان از طریق لمس دکمه SOS می تواند شما را از بروز مشکل مطلع سازد.



شکل (۶۲) دکمه کمک در نرم افزار NQ Family Guardian

والدین ابتدا این نرم افزار را از گوگل پلی بر روی گوشی خود نصب می کنند و در سایت <https://family.nq.com> یک حساب کاربری می سازند. بعد از طریق اسکن کردن QR Code زیر به گوشی فرزندشان دسترسی پیدا می کنند و از امکانات نظارتی خوب این نرم افزار استفاده می کنند.

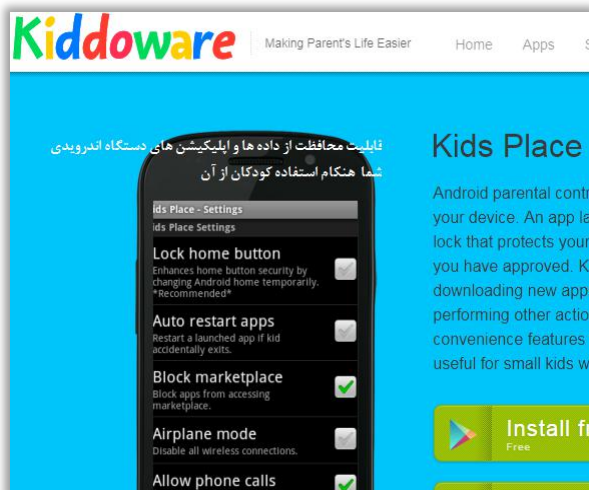


شکل (۶۳) فعال‌سازی قابلیت‌های نرم‌افزار NQ Family Guardian

نرم‌افزار کیدز پلیس^۱

اگر بخواهید برای مدتی وسیله خود را در اختیار فرزندتان قرار دهید، این نرم‌افزار قابلیت‌های کارآمدی دارد و علاوه بر محافظت از داده‌ها و نرم‌افزارهایی که برایشان دسترسی محدود تعریف کرده‌اید، از تماس صوتی و نصب و خرید نرم‌افزار و همه کارهایی که برای شما هزینه دارد، جلوگیری می‌کند.

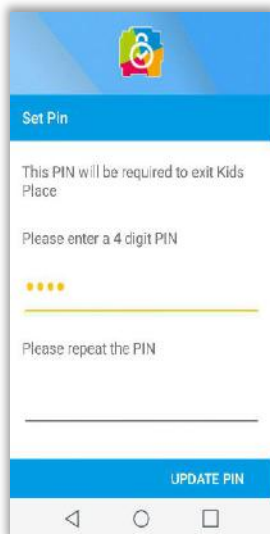
¹ Kids Place



شکل (۶۴) نرم افزار Kids Place

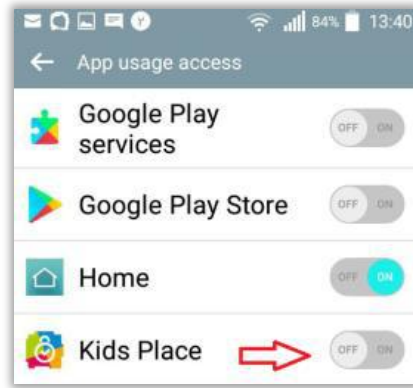
نسخه پیشرفته این نرم افزار که غیررایگان است، علاوه بر زمان بندی استفاده از گوشی و هر نرم افزاری روی آن، قابلیت اجرا در پس زمینه را دارد. این ویژگی در برابر شیطنیت فرزندان بزرگتر که نرم افزارهای نظارتی را به محض تشخیص uninstall می کنند، قابلیت خوبی است (googleplay, n.d.).

خوشبختانه این نرم افزار در فروشگاه بازار موجود است و نصب آن به راحتی انجام می شود. در ابتدا از شما یک کد چهاررقمی می خواهد تا بعداً به راحتی از حالت kids خارج شوید یا تنظیمات را تغییر دهید.



شکل (۶۵) تنظیم پین کد برای نرم‌افزار Kids Place

سپس آدرس ایمیل را برای بازیابی این کد درخواست می‌کند. بعد از آن مطابق با اغلب نرم‌افزارهای کنترل والدین از شما می‌خواهد که به این نرم‌افزار برای مشاهده بقیه برنامه‌های کاربردی روی گوشی‌تان مجوز بدهید.



شکل (۶۶) منوی App Usage access در اندروید برای اجازه مشاهده برنامه‌های دیگر توسط Kids Place

در گام بعدی وارد صفحه مدیریت نرم‌افزار می‌شوید و برنامه‌های مدنظر خود را انتخاب می‌کنید. در این قسمت حتی می‌توانید با لمس علامت WiFi در کنار برنامه‌ها، دسترسی به اینترنت را مسدود کنید. سپس وارد صفحه فرزندان می‌شوید و از طریق چرخ‌دنده تنظیمات و پس از وارد کردن رمز عبوری که در ابتدا مشخص کرده‌اید، می‌توانید نظارت بیشتری را اعمال کنید:



گفتنی است بیشتر قابلیت‌های این برنامه از طریق خرید درون‌برنامه‌ای فعال می‌شود.

نرم‌افزار فمیلی گارد

فمیلی گارد یک نرم‌افزار موبایل با نصب و فعال‌سازی بسیار ساده است که به والدین امکان کنترل و مدیریت فعالیت فرزندان در شبکه‌های مجازی موبایلی را می‌دهد. دقت کنید که این برنامه پس از نصب و فعال‌سازی پنهان می‌شود. رابط کاربری فمیلی گارد آسان بوده و نصب آن با کمترین سطح دانش فنی، برای والدین قابل انجام است. پس از وارد شدن به سایت familyguard.ir از طریق تب «ثبت‌نام و دانلود نرم‌افزار» وارد صفحه خرید شوید و نرم‌افزار را دانلود کنید (فمیلی گارد، ۱۳۹۶).

شکل (۶۷) منوی دانلود و ثبت نام نرم افزار فمیلی گارد

با استفاده از این برنامه:

- ✓ می توانیم گزارش تماس های ورودی و خروجی شامل نام مخاطب، شماره تماس و مدت زمان مکالمه و همچنین گزارش تماس هایی که به صورت دستی حذف شده اند، را داشته باشیم یا حتی آن ها را مسدود کنیم.
- ✓ از مکاتبات پیامکی فرزندان خود با دوستان و دیگران آگاهی یابیم و در صورت نیاز، برخی از مخاطبان را مسدود کنیم.
- ✓ ارتباطات فرزندان خود را در شبکه های اجتماعی همچون اینستاگرام، تلگرام، ایمو، واتس اپ و... مدیریت و در صورت لزوم، دسترسی آن ها را محدود کنیم.
- ✓ در هر لحظه از موقعیت عزیزان خود آگاه شویم و در کنار آن ها حضور پیدا کنیم و در صورت ورود به مناطق مجاز یا غیرمجاز تعیین شده، فوراً مطلع شویم.

- ✓ وبسایت‌های را که بازدید کرده‌اند، کنترل کنیم و دسترسی آنان به مطالب غیراخلاقی را مسدود کنیم.
- ✓ فهرستی کامل از برنامه‌های نصب‌شده بر روی گوشی فرزند خود داشته باشیم و از وجود برنامه‌های نامناسب آگاه شویم (فمیلی گارد، ۱۳۹۶).
- برای استفاده از این نرم‌افزار می‌توانیم تعرفه‌های یک‌ماهه، سه‌ماهه، شش‌ماهه یا یک‌ساله را به‌شکل اینترنتی پرداخت و نرم‌افزار را تهیه کنیم.



شکل (۶۸) قسمتی از داشبورد برنامه فمیلی گارد

سامانه مراقبت از خانواده^۱ SFP

یکی از نرم‌افزارهای موبایلی ایرانی که فرزندان را از آسیب‌های ناشی از مشاهده محتوای نامناسب در شبکه‌های اجتماعی، سایت‌ها و نرم‌افزارها محافظت و دسترسی‌شان

^۱ SuperFamilyProtector

را مسدود می‌کند، سامانهٔ مراقبت از خانواده یا Super Family Protector است. قابلیت‌های این نرم‌افزار در شکل زیر لیست شده است:



این نرم‌افزار از وبسایت و امکانات پشتیبانی مطلوبی برخوردار است و می‌توان برای بازه‌های زمانی مشخصی آن را شارژ و از امکاناتش استفاده کرد. برای نصب و استفاده از این نرم‌افزار از تب «ثبت‌نام و دانلود» در سایت superfamilyprotector.com وارد صفحهٔ زیر می‌شوید و پس از خرید شارژ، نرم‌افزار را روی گوشی هوشمند دریافت می‌کنید.

شکل (۶۹) صفحه ثبت‌نام برنامه SFP

برنامک کنترل فرزند شقایق

این نرم‌افزار ایرانی به شما این امکان را می‌دهد که مشخص کنید فرزند خردسالتان چه روز و ساعاتی با گوشی‌تان کار کند. همچنین می‌توانید عکس‌ها و فیلم‌ها و برنامه‌ها و بازی‌ها و مخاطبان موردتأییدتان را برایش انتخاب کنید تا فقط به آن‌ها دسترسی داشته باشد. به این ترتیب، دیگر فرزندان به قسمت‌های دیگر گوشی دسترسی ندارد و می‌توانید با خیال آسوده گوشی را به او بدهید. این برنامه علاوه بر امکانات نظارتی، پس‌زمینه کودکانه و کتاب داستان‌های تصویری و صوتی کودکانه هم دارد. این برنامه در نرم‌افزار بازار موجود است.



شکل (۷۰) نمایی از برنامه کنترل فرزند شقایق

برای نصب این نرم افزار ابتدا از فروشگاه بازار، آن را دانلود کنید. سپس در صفحات زیر رمز عبور را وارد و نرم افزارهایی را که برای فرزند خود مناسب می دانید، مشخص کنید.



شکل (۷۱) نمایی از مراحل نصب برنامه کنترل فرزند شقایق

پس از اینکه ساعات استفاده از گوشی را مشخص می‌کنید، اگر فرزندان خارج از ساعات مشخص شده به سراغ گوشی بروند، سمت راست شکل زیر برایشان نشان داده می‌شود.



شکل (۷۲) تنظیم ساعات استفاده از گوشی

برنامه ParentKit (iOS)

این برنامه نحوه دسترسی به مرورگر و دیگر برنامه‌ها را براساس سن افراد مدیریت می‌کند و قابلیت‌هایی مثل ممانعت از نصب برنامه جدید، خرید برنامه، دسترسی به مراکز بازی و محدود کردن محتوایی مثل موزیک و ویدئو را دارد. می‌توانید در زمان درس خواندن بچه‌ها، دسترسی به مرورگر را آزاد کنید و زمان خواب تمام برنامه‌ها را ببندید. این نرم‌افزار را می‌توان از فروشگاه App store دانلود کرد.



شکل (۷۳) برنامه کنترلی ParentKit

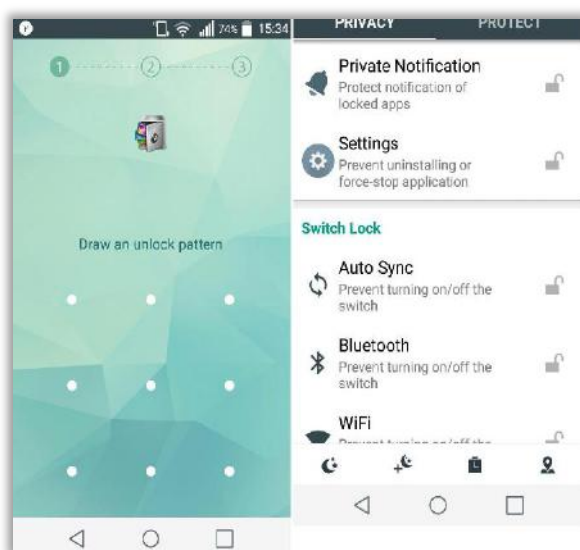
قفل‌کننده نرم‌افزار^۱

این برنامه یکی از محبوب‌ترین برنامه‌های اندرویدی است که کارش قفل کردن است. قفل کردن فایل‌ها و نرم‌افزارها و همچنین کنترل عکس‌ها و فیلم‌های داخل گالری و پنهان کردن آن‌ها، از قابلیت‌های این برنامه است. البته همیشه با وارد کردن رمز خود می‌توانید آن‌ها را از حالت قفل خارج کنید.

پس از نصب AppLock از طریق بازار، ابتدا یک الگوی باز کردن قفل به نرم‌افزار می‌دهید. سپس یک ایمیل امن برایش تعریف می‌کنید و بعد از آن

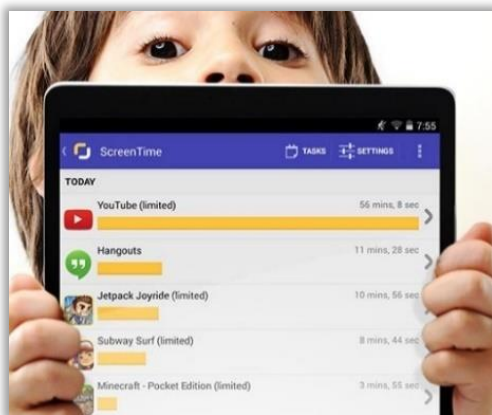
^۱ AppLock

می‌توانید تمام بخش‌های گوشی خود را، اعم از نرم‌افزارها و تماس و تنظیمات و WiFi و Bluetooth، قفل کنید.



شکل (۷۴) نمایی از مراحل نصب و تنظیمات AppLock

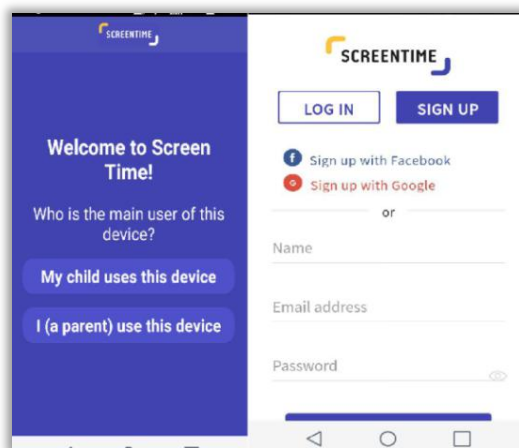
برنامه Screen Time Parental Control



این برنامه را که در فروشگاه google play به صورت رایگان در دسترس است، می توان روی تمام سیستم عامل های اندروید و iOS نصب کرد. موارد زیر از جمله قابلیت های این نرم افزار است:

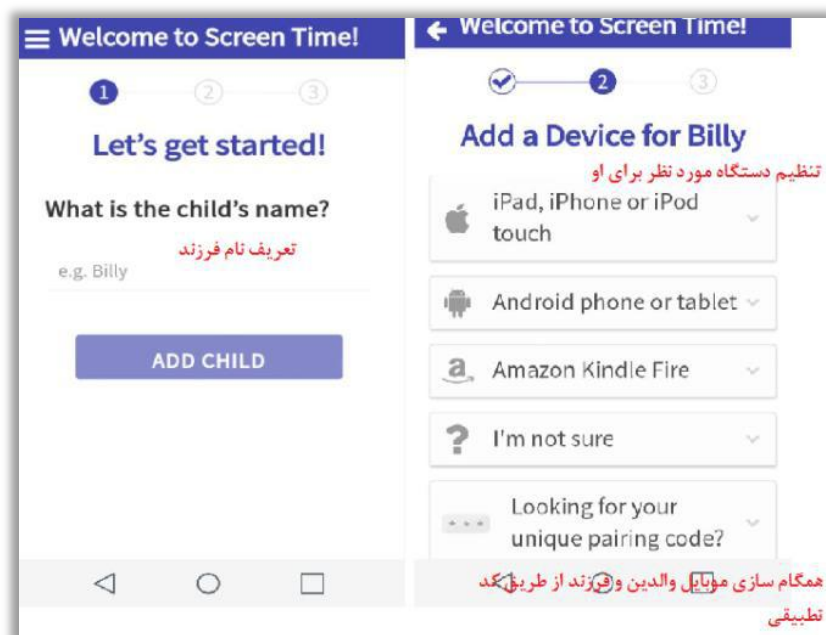
- ✓ محدودیت زمانی روزانه
- ✓ کنترل ساعت خواب: مسدود کردن بازی ها در زمان خواب (اما امکان استفاده از برنامه های مرتبط با خواندن وجود دارد)، مسدود کردن تمام برنامه ها در زمان خواب
- ✓ کنترل زمان مدرسه: مسدود کردن شبکه های اجتماعی و بازی ها (اما برنامه های آموزشی در ساعات مدرسه در دسترس است)
- ✓ مسدود کردن دستگاه فرزندان از راه دور، دادن پاداش به فرزندان برای انجام دادن وظایف و کارهای روزمره
- ✓ مسدود کردن برنامه های خاص به طور کامل و دریافت هشدار در زمان نصب برنامه جدید توسط فرزند

- ✓ نیاز به وارد کردن کلمه عبور تعیین شده توسط والدین برای حذف برنامه (پژوهشگاه ارتباطات و فناوری اطلاعات، ۱۳۹۶)
- در هنگام نصب، ابتدا باید مشخص کنید دستگاه متعلق به شماست یا فرزندتان. سپس یک حساب کاربری ایجاد کنید:



شکل (۷۵) تعریف حساب کاربری در Screen Time Parental Control

- پس از تعریف حساب کاربری، وارد مراحل تنظیم و ثبت نام دستگاه فرزند خود و جفت کردن آن با موبایل خود از طریق کد تطبیقی می‌شوید:



شکل (۷۶) صفحه تنظیمات Screen Time Parental Control

سپس از طریق تنظیمات نرم‌افزار می‌توانید بر فعالیت‌های او نظارت کنید و بر روی گوشی خود گزارش‌ها را دریافت کنید. به نظر می‌رسد این نرم‌افزار تا حدودی برای برقراری ارتباط با وبسایت اصلی screentimelabs.com و تعریف حساب کاربری در کشور ما با مشکل مواجه است.



سیم کارت‌های کنترل شده

سیم کارت کنترل شده، سیم‌کارتی است که اپراتور آن، تنظیماتی را برای کنترل والدین بر روی آن اعمال می‌کند. این سرویس در مقایسه با راهکارها و گزینه‌هایی که بر روی گوشی با عنوان «کنترل والدین» وجود دارد، از مزیت بیشتری برخوردار است؛ چراکه تنظیم گزینه‌های کنترلی برای والدین آسان نیست و نیازمند اطلاعات و تحقیق است. علاوه‌براین، فرزندان به راحتی نمی‌توانند کنترل‌های اعمال شده در این سیم‌کارت‌ها را دور بزنند یا تغییری در تنظیمات آن ایجاد کنند. این نوع سیم‌کارت‌ها هم در داخل و هم در خارج از کشور به متقاضیان عرضه می‌شوند. نمونه‌های داخلی آن، محصول مجموعه درسا و انارستان است.

در سیم‌کارت درسا، والد (در حال حاضر پدر خانواده) دو سیم‌کارت دارد که یکی از آن‌ها برای خودش است و دیگری را به سیم‌کارت درسایی تبدیل می‌کند. به این ترتیب، دو سیم‌کارت با یکدیگر ارتباط برقرار می‌کنند و سیم‌کارت دوم (سیم‌کارت فرزند) به یک سیم‌کارت قابل نظارت توسط والد تبدیل می‌شود. سیم‌کارت انارستان، سیم‌کارتی اعتباری است که برای مجموعه دانش‌آموزان ایرانی طراحی شده است. این سیم‌کارت ضمن برآوردن تمام نیازهای مکالمه و

پیامک دانش آموزان، امکان استفاده از فضای اینترنتی سالم و امن متناسب با سن آنها را فراهم می‌کند.

سیم‌کارت‌های امن نه‌تنها در ایران، بلکه در بسیاری از کشورهای توسعه‌یافته جهان کاربرد دارد؛ مثلاً انگلیس، آلمان و آفریقای جنوبی با همکاری اپراتورهای موبایل، خدمات خوبی را به خانواده‌ها می‌دهند.

امنیت تجهیزات هوشمند خانگی

با ورود تجهیزات هوشمند به زندگی مدرن، امنیت انسان تا حد زیادی به خطر افتاده است؛ زیرا در اطراف ما دستگاه‌هایی مدام مشغول ثبت و ضبط اطلاعاتند. این اطلاعات حتی اگر به دست شرکت‌های تجاری و اطلاعاتی نیفتد و از آن سوءاستفاده نکنند، لقمه خوبی برای سارقان اینترنتی است. با این‌همه، از کاربرد این تجهیزات ناگزیریم. اما بهتر است با راهکارهای محافظت از حریم شخصی و اطلاعات خود به‌درستی آشنا باشیم تا عوارض و خطرات این تجهیزات را کاهش دهیم.



در مواقعی که با دوربین رایانه یا لپ‌تاپ خود کاری ندارید، می‌توانید با برچسب، روی دوربین را بپوشانید. برچسب‌های کشویی محصولات بهتری هستند. بعضی از محافظ‌ها یا کیف‌های تبلت هم نوعی زائده دارند که روی دوربین قرار می‌گیرد (boul, 2016).

همهٔ این تجهیزات قابلیت تغییر تنظیمات امنیتی و اطلاعات پیش‌فرض کاربر را دارند. تلویزیون‌های هوشمند معمولاً برای کنترل اتصال به اینترنت از کاربر سؤال می‌کنند. حتی به کاربر اطلاع می‌دهند که میکروفون یا دوربین تلویزیون فعال است و کاربر می‌تواند آن‌را در صورت تمایل غیرفعال کند. بسیاری از آن‌ها هم برای دریافت رمز عبور و اطلاعات حساس کاربر از صفحه‌کلید امن استفاده می‌کنند.

نرم‌افزارهایی را که از آن‌ها استفاده نمی‌کنید، غیرفعال کنید. همواره سیستم‌عامل دستگاه‌های هوشمند خود را به‌روز کنید. بسیاری از شکاف‌های امنیتی در این دستگاه‌ها را متخصصان تشخیص می‌دهند و در نسخه‌های جدیدتر برطرف می‌کنند (Faern, 2016).

فهرست منابع

1. Bitdefender, 2017, <https://www.bitdefender.com/support/how-to-configure-parental-control-1164.html>
2. Burgess. Brian, 2010, How To Use Parental Controls in Windows 7, <https://www.howtogeek.com/howto/10524/how-to-use-parental-controls-in-windows-7/>
3. Cell Phone Parenting, 2016, <https://www.common sense media.org/cell-phone-parenting/how-do-i-set-parental-controls-on-the-iphone>
4. Cellphone safety, n.d, Disable the internet on a SIM card on South African networks only, <http://www.cellphonesafety.co.za/how-to-disable-the-internet.html>
5. Character Strengths and Life Skills, 2016, <https://www.common sense media.org/screen-time/how-do-i-lock-down-my-kids-ipad>
6. Googleplay, nd, Kids Place - Parental Control & Child Lock, Retrived from https://play.google.com/store/apps/details?id=com.kiddoware.kidsplace&hl=en_GB
7. GCF, 2017, Windows 8:Managing User Accounts and Parental Controls, <https://www.gcflearnfree.org/windows8/managing-user-accounts-and-parental-controls/1/>
8. iNet Guardian, 2017 (About iNet Guardian Children's safety in an online world) , Retrived from <https://inetguardian.co.uk/about at 12/23/2017>
9. Kaspersky, 2017, product & service, <http://support.kaspersky.com/us/9570#block2>

10. Kidlogger, nd, Do You Know What Your Kids Are Doing Online?, Retrived from <http://kidlogger.net/> at 23/12/2017
 11. 15. MICHEL G, 2016, Exclusive: Family Care will be Samsung's own parental control app for Galaxy users, <https://www.sammobile.com/2016/11/15/exclusive-family-care-will-be-samsungs-own-parental-control-app-for-galaxy-users/>
 12. Microsoft, n.d, Xbox camera and privacy, <https://privacy.microsoft.com/en-US/xbox-camera-and-privacy>
 13. Net Nanny, 2017, How To Set Parental Controls for Windows 10, <https://www.netnanny.com/blog/how-to-set-parental-controls-for-windows-10/>
 14. OpenDNS. 2017, Internet Security for your home or small business, Retrived from <https://www.opendns.com/home-internet-security/>
 15. Sachin Shetty, 2005, "Introduction to Spyware Keyloggers", <https://www.svmantec.com/connect/articles/introduction-spyware-keyloggers>
 16. Salfeld, nd, Parental Control for Windows and Android, Retrived from <https://salfeld.com/en/software/parental-control/> at 12/23/2017
 17. Symantec Corporation World Headquarters, 2016, "Internet Security Threat Report", V. 21.
۱۸. پژوهشگاه ارتباطات و فناوری اطلاعات، ۱۳۹۶، ابزارهای کنترل والدین، وزارت ارتباطات و فناوری اطلاعات پیوست ۴، ۵۲۷۶۸ pdf.orig
۱۹. تبیان، ۱۳۹۱، فیلترینگ خانگی، بازیابی شده در ۹۶/۹/۲۷ از <http://94.232.175.51/222330/>
۲۰. کهوند محمد، ۱۳۹۵، «شبکهٔ عنکبوتی: روش‌های جذب، نفوذ و تأثیرگذاری در فضای مجازی»، معاونت تبلیغ و آموزش‌های کاربردی حوزه‌های علمیه، قم، انتشارات ذکرى.
۲۱. گرداب، ۱۳۹۴، تأثیر اینترنت بر بلوغ زودرس کودکان، بازیابی‌شده در ۹۶/۹/۲۷ از <http://gerdab.ir/fa/news/14527/>
۲۲. نصیری، امیررضا، ۱۳۹۴، حملهٔ فیشینگ (Phishing) چیست و نحوهٔ جلوگیری، بازیابی‌شده در ۹۶/۹/۲۷ از <http://bytegate.ir/حمله-فیشینگ>



فناوران توسعه امن ناجی
Naji Secure Development
Technologist co