امنیت در زندگی آنلاین

نویسنده: حسین سهلانی

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 سهلانی

به سفارش :

سازمان 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
مشاورطرح: علی محمد رجبی
ناظر و مجری طرح: شرکت فناوران توسعه امن ناجی
آدرس سایت: ceop.ir
شمارگان: ۱۰۰۰جلد
قیمت: ۲۲۰۰۰تومان
شابک:۹-۵۱-۶۰۹۴-۶۰۰-۹۷۸
چاپ: سیمین پرداز کامه ۹-۶۶۴۸۱۶۳۸

نشانی: خیابان انقلاب، خیابان فخر رازی، خیابان نظری، کوچه فرزانه، پلاک ۱، واحد۱۳
تلفن :۹-۶۶۴۸۱۶۳۸

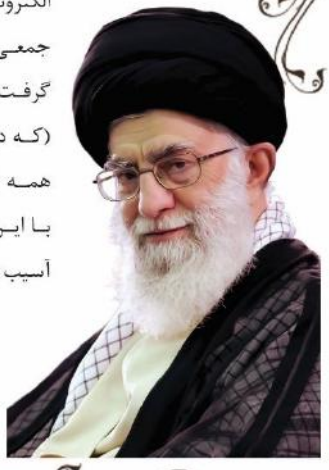
انتشارات عترت نو

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: ۹-۵۱-۶۰۹۴-۶۰۰-۹۷۸
وضعیت فهرست‌نویسی : فیپا
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 : QA۷۶/۷۶/و۹س۹ ۱۳۹۷
رده بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی ۵۲۵۱۰۳۹

بسم الله الرحمن الرحیم

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 به‌وسیلهٔ ابزارهای ارتباط‌جمعی 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 ارتباط‌جمعی با این وسعت بود که فرزندان ما در معرض این‌همه 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. به‌دنبال این امر، حفاظت از فرزندان دربرابر آفت‌های فضای مجازی به یکی از معضلات مهم والدین تبدیل شده است. به‌همین‌دلیل، شرکت‌های مختلف سعی کرده‌اند برای تأمین امنیت فرزندان در فضای مجازی، نرم‌افزارهایی بسازند. بااین‌حال، فراوان مشاهده شده که والدین نمی‌توانند امنیت لازم را برای فرزندان خود مهیا کنند و درنتیجه، دچار مشکلاتی می‌شوند.

کودکان ازآنجاکه از خطرات فضای مجازی باخبر نیستند، احتمال آسیب‌دیدنشان به‌نسبت بزرگ‌سالان بیشتر است. برهمین‌اساس، باید یکی از وظایف اصلی والدین را حفاظت از کودکان دربرابر 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 به‌بهترین نحو برایشان روشن کرد.

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

فهرست مطالب

فهرست اشکال

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، به‌نسبت والدین از فضای مجازی و رایانه و اموری ازاین‌دست آگاهی بیشتری دارند. بنابراین، اگر والدین دانششان را به‌روز کنند و اطلاعاتشان را به میزان مطلوب برسانند، راهنمایی‌هایی که دراین‌زمینه به فرزندانشان می‌کنند، مؤثرتر خواهد بود.

اهمیت دانش و آگاهی رسانه‌ای والدین به‌قدری است که با تمام نکاتی که برای مراقبت از فرزندان لازم است، برابری می‌کند. به‌عبارت دیگر، هیچ‌چیز جای آموزش والدین را نمی‌گیرد و والدین برای آموزش‌دادن فرزندانشان نیازمند دانش و آگاهی‌اند. نهایتاً والدین‌اند که باید بر فرزندان نظارت کنند. به‌همین‌دلیل، اگر میزان سواد رسانه‌ای‌شان با فرزندانشان اختلاف فاحشی داشته باشد، به‌خوبی از عهدهٔ این کار برنمی‌آیند.

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 این‌قبیل آسیب‌ها و به‌حداقل‌رساندنشان 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 هشداری 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 صفحهٔ خانگی[1] یا موتور جست‌وجو، بی‌دلیل عوض شده باشد.
- ✓ اگر ضمیمه‌ها[2] یا ابزارهای[3] 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 کاملِ 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

[1] Home page
[2] extensions
[3] toolbar

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

بهترین راهکار برای تهیهٔ نسخهٔ پشتیبان، ایجاد دو نسخهٔ هم‌زمان است: نسخهٔ اول بر روی فضای ابری (استفاده از سرویسی که به‌طور خودکار عملیات پشتیبان‌گیری را انجام می‌دهد) و نسخهٔ 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

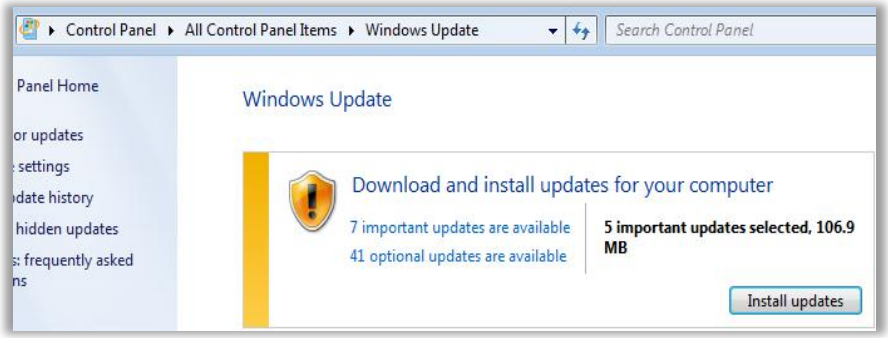
۳. برای حذف باج‌افزار یا دیگر نرم‌افزارهای مخربی که روی کامپیوتر نصب شده، با نرم‌افزار امنیتی مناسب و به‌روز، روزی یک بار کل سیستم را اسکن کنید.

۴. اگر کامپیوترتان ازطریق 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.

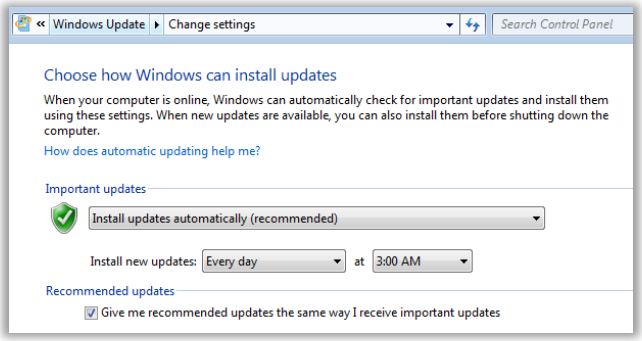
۶. نرم‌افزارهای خود را به‌روز نگه دارید. هر بار که نرم‌افزاری ازسوی شرکت سازنده‌اش به‌روزرسانی می‌شود، علاوه بر ارتقای قابلیت‌ها و تغییر جزئیات، راه‌های نفوذ در آن نیز

محدودتر می‌شود و درنتیجه، 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:



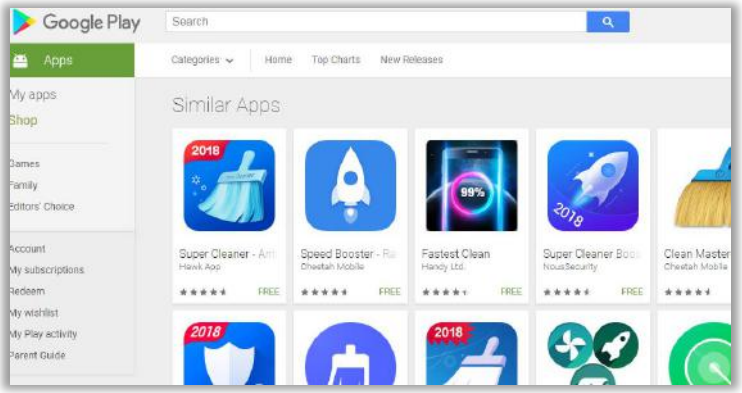
شکل (۳) فعال کردن گزینه انتخاب به‌روزرسانی خودکار

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

شکل (۴) اطلاع‌رسانی در کافه‌بازار دربارهٔ 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 کی‌لاگرها

امروزه یکی از معمول‌ترین ابزارهای دادوستد 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 دامنهٔ

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

الف. آدرس صفحهٔ پرداخت باید صرفاً آدرس یکی از درگاه‌های پرداخت موردتأیید و تحت دامنهٔ شاپرک باشد[1]؛ مثلاً: بِه‌پرداخت ملت: https://bpm.shaparak.ir

ب. حرف s در https به‌معنی امن‌بودن سایت است.

پ. هنگام ورود به سایت از وجود نماد اعتماد الکترونیکی مطمئن شوید. مثلاً در سایت دیجی‌کالا، با کلیک بر روی  نماد وارد صفحهٔ زیر می‌شوید که نشان می‌دهد این سایت معتبر است:

شکل (۷) مشخصات سایت دیجی‌کالا در سایت نماد الکترونیک

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

علاوه‌براین، خود این درگاه‌ها نیز به کاربران پیشنهاد می‌کنند برای واردکردن رمز و اطلاعات امنیتی حساب‌های خود، از صفحه‌کلیدی مجازی که اعداد و حروف روی آن به‌کمک موس انتخاب می‌شوند، استفاده کنند؛ زیرا هکرها با استفاده از اطلاعاتی که هنگام کار با صفحه‌کلید عادی در اختیارشان قرار می‌گیرد، به‌راحتی 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 کی‌لاگرها است. در شکل زیر نمونه‌ای از صفحه‌کلیدهای مجازی نشان داده شده است:

شکل (۸) نمونه‌ای از صفحه‌کلیدهای مجازی در درگاه‌های بانکی

راه‌های مقابله با ایمیل فیشینگ

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

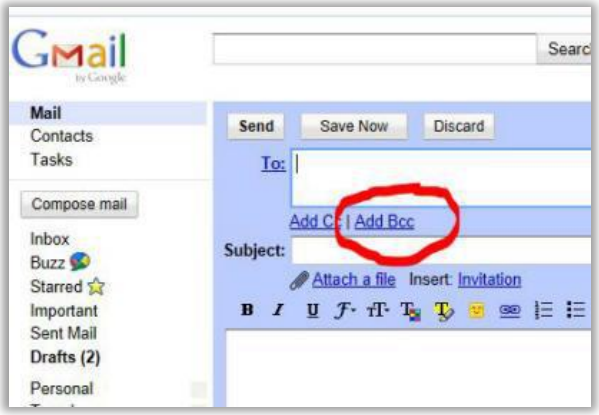
راه‌اندازی و رمز عبور آن‌ها در صورت فراموشی با ایمیل بازیابی می‌شود. همچنین مکاتبات بانکی و اداری با ایمیل صورت می‌گیرد. پس واضح است که کلاهبرداران به ایمیل توجه خاصی می‌کنند. برای درآمان‌ماندن از چنین حملاتی لازم است نکات زیر را رعایت کنید (نک: انجمن خانواده و اینترنت):

- ✓ 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

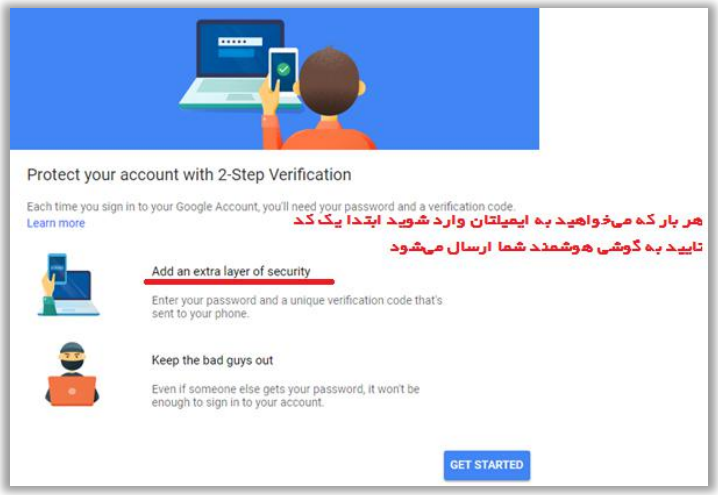
- ✓ ایمیل‌هایی را که به پوشهٔ اسپم منتقل می‌شود، با وسواس بررسی کنید و درصورتی‌که فرستنده را نمی‌شناسید، هرگز بازشان نکنید.
- ✓ از قابلیت BCC سرویس‌های ایمیل استفاده کنید. با این کار امکان مخفی‌ماندن آدرس ایمیل از دید کلاهبرداران فراهم می‌شود. ایمیل‌های فورواردی معمولاً

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



شکل (۱۰) قابلیت پنهان‌کردن 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 سرویس‌دهندهٔ ایمیل خود جست‌وجو کنید. برای مثال، در Gmail به تصویر زیر می‌رسید:



شکل (۱۱) استفاده از ورود دومرحله ای در Gmail

به‌کمک 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.

ناشناس‌بودن 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 این‌قبیل 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 دوستتان 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 دربرابر 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.
- ✓ بلاک‌کردن و حذف‌کردن و گزارش به پلیس، راهکار خوبی برای درآمان‌ماندن از مزاحمت سایبری است.

مقابله با آثار مخرب برخی بازی‌های رایانه‌ای

مقابله با آثار مخرب برخی بازی‌های رایانه‌ای

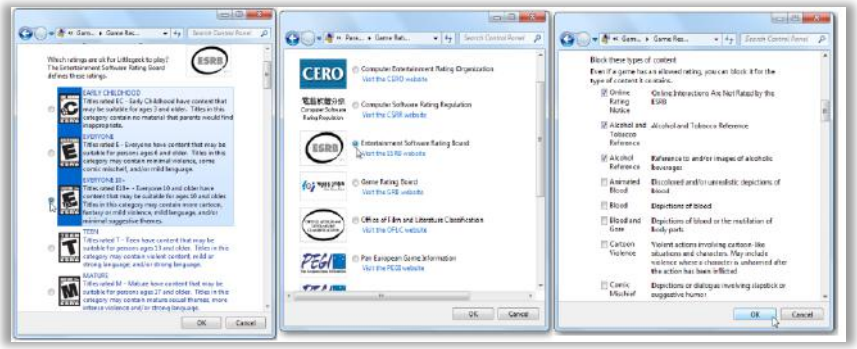
بازی‌های رایانه‌ای به‌رغم تمام مزایایی که دارند، آثار مخربی از خود به‌جا می‌گذارند. توجه به رده‌بندی سنی بازی‌های رایانه‌ای برای والدین امری ضروری است. در تمام کشورها، حتی کشورهایی که در صف اول تولید و طراحی بازی‌های رایانه‌ای هستند، توجه ویژه‌ای به این امر می‌شود؛ به این صورت که براساس ملاک‌های مشخصی درزمینهٔ 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.[1]

شکل (۱۲) نظام رده بندی سنی ESRB

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

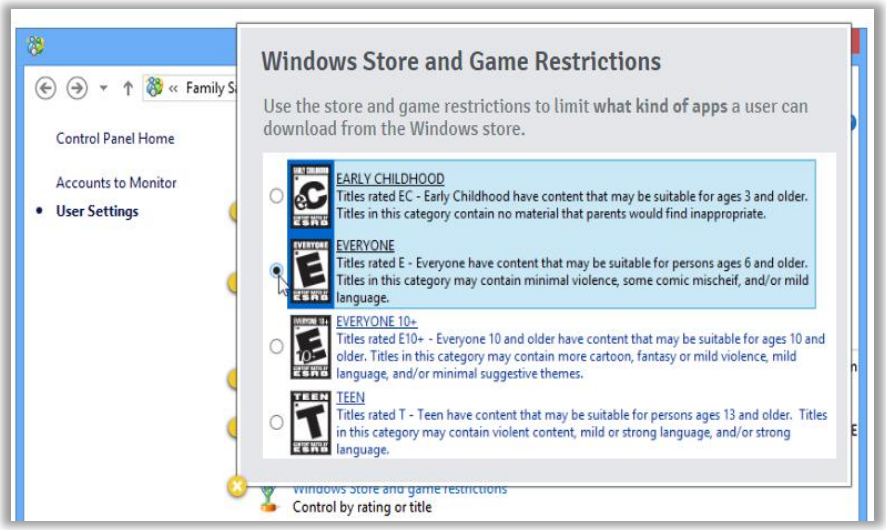
۱. اطلاعات کامل دربارهٔ نظام‌های رده‌بندی سنی بازی‌ها در کتاب *هم‌بازی‌های عصر دیجیتال* آمده است.

در ویندوز ۷ به بعد، در قسمت Parental control گزینه‌ای به‌نام Game Rating System اضافه شده است که ازطریق آن می‌توان ردهٔ 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 نحوهٔ 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 خاموش‌کردن 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 بقیهٔ 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 استفادهٔ صحیح از فضای مجازی باید بتوانیم به‌کمک ابزارهای کارآمد، خود و خانوادهٔ خود را دربرابر آسیب‌های موجود مصون کنیم.

درخواست‌های خانواده‌ها در کشورهای پیشرفته، شرکت‌های تولید نرم‌افزار را تشویق کرد تا فیلترهایی برای نرم‌افزارهای خود تعبیه کنند و به‌این‌ترتیب، برای دسترسی به محتوا در خانه، محدودیت‌هایی در نظر بگیرند. برخی از این شرکت‌ها حتی نرم‌افزارهای مجزایی برای این منظور طراحی کردند. همهٔ این راهکارها برای پالایش و ممانعت از نشر محتوایی است که به‌زعم والدین، سلامت و امنیت خانواده و فرزندان را به خطر می‌اندازد. با این راهکارها می‌توان ازطرفی دسترسی به سایت‌ها و بازی‌ها و برنامه‌ها را محدود یا مقید به زمان معین کرد و ازطرف 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 به‌موقعی بگیرند. به‌همین‌دلیل، این راهکارها بیشتر با نام روش‌های «کنترل والدین»[1] شناخته می‌شوند.

راهکارهای پالایش محتوا در خانه را به‌طور کلی می‌توان بر روی سیستم‌عامل دستگاه کامپیوتر و مرورگرها و تجهیزات شبکهٔ خانگی و گوشی‌های هوشمند موبایل اجرا کرد. بعضی از این راهکارها از قبل در سیستم وجود دارد و فقط کافی است دراین‌باره 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 به‌کمک 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.

گزینهٔ کنترل والدین در سیستم‌عامل‌های ویندوز

گزینه‌های کنترلی در ویندوز ۷

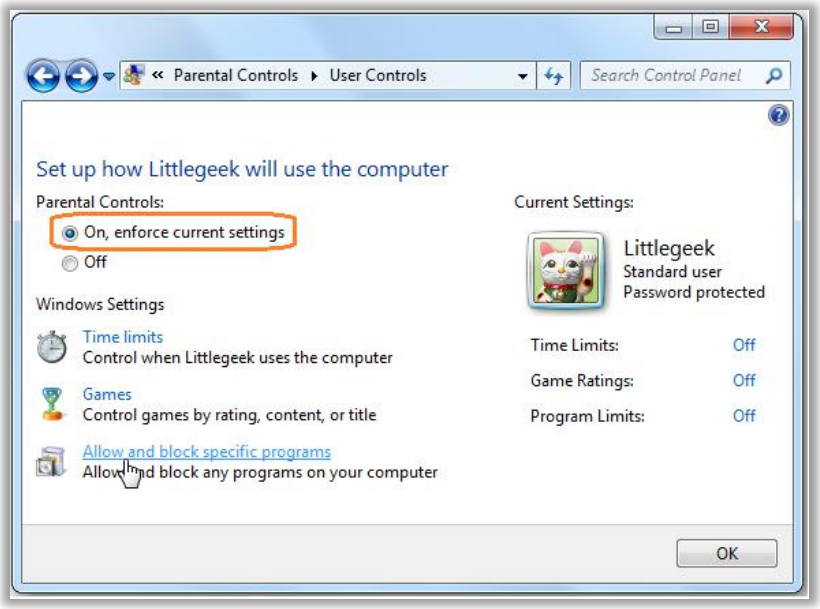
در ویندوز ۷ گزینه‌ای وجود دارد که مسیر فعال‌کردن آن به‌طور خلاصه به‌شکل زیر است (Burgess, 2010):

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

برای دسترسی به این گزینه همچنین می‌توانیم Parental Control را در نوار جست‌وجوی صفحهٔ کنترل‌پنل وارد کنیم. این گزینه فقط برای یکی از کاربرهای کامپیوتر فعال می‌شود. بنابراین قبل‌ازاین باید یک حساب کاربری جداگانه برای فرزندمان تعریف کنیم. برای فعال‌کردن گزینهٔ «کنترل والدین» مانند شکل ۱۵ عمل می‌کنیم.

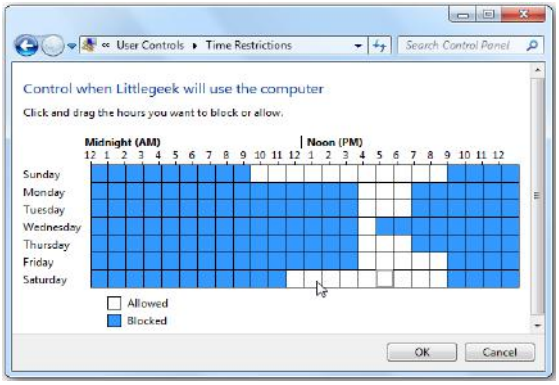
شکل (۱۵) انتخاب گزینهٔ کنترل والدین برای کاربر مشخص

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



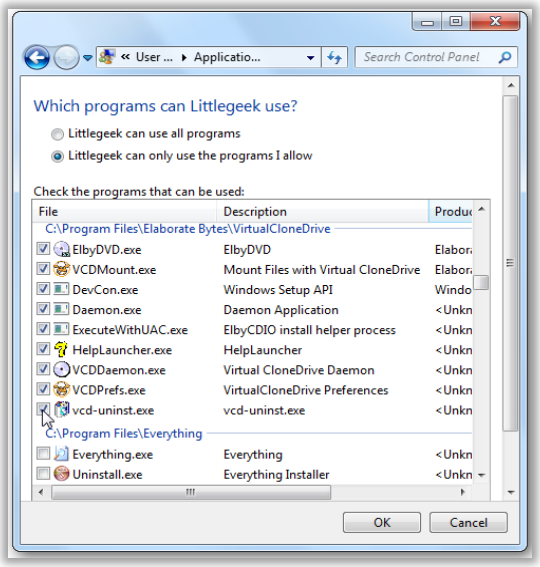
شکل (۱۶) فعال‌کردن گزینه‌های کنترل والدین

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.



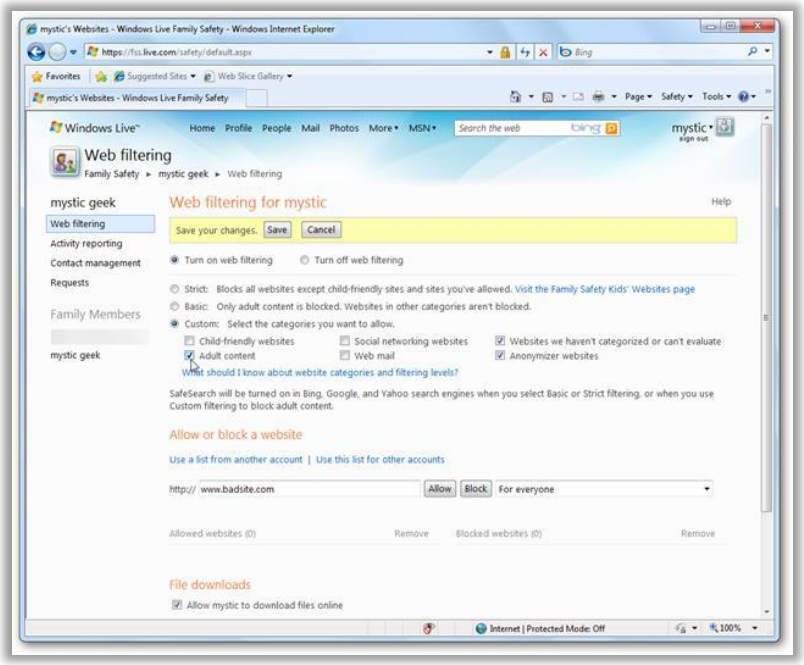
شکل (۱۷) تنظیم مدت‌زمان استفاده کاربر از کامپیوتر

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



شکل (۱۸) تنظیم برنامه‌های مجاز برای استفادهٔ کاربر

اگر بخواهیم کنترل‌های بیشتری مانند پالایش صفحات وب را در ویندوز ۷ اعمال کنیم، می‌توانیم برنامهٔ 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. به‌کمک 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) برنامهٔ Live Family Safety

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

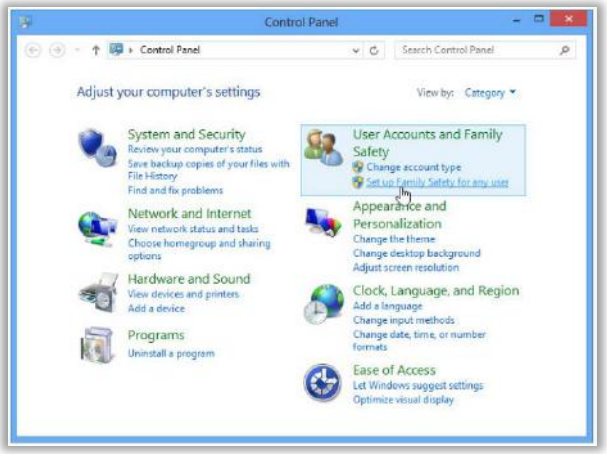
شکل (۲۰) نحوهٔ مواجههٔ فرزند با سایت‌های ممنوع‌شده

گزینه‌های کنترلی در ویندوز ۸

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

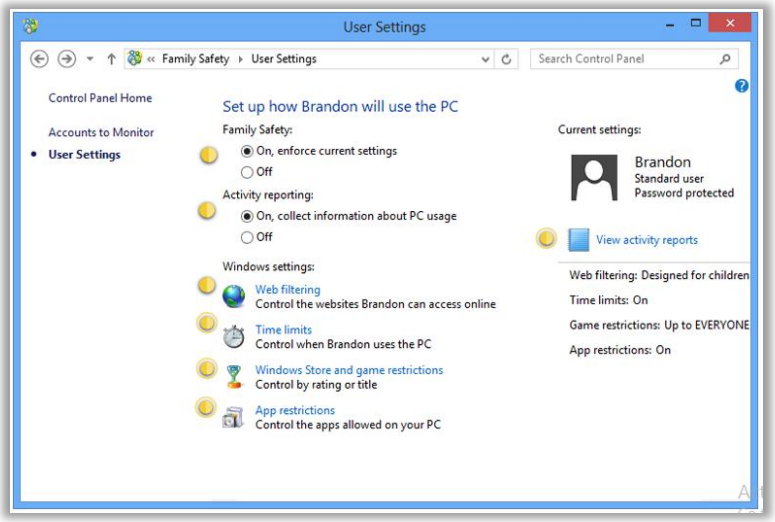
شکل (۲۱) تعریف یک کاربر کودک در ویندوز ۸

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 صفحهٔ Control Panel و در گروه User Account and Family Safety، این کاربر را مطابق شکل‌های ۲۲ انتخاب می‌کنیم.



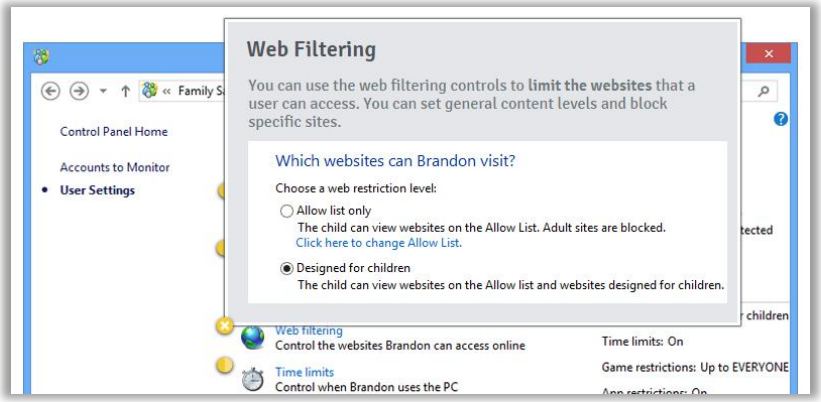
شکل (۲۲) انتخاب کاربر برای ایجاد محدودیت

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



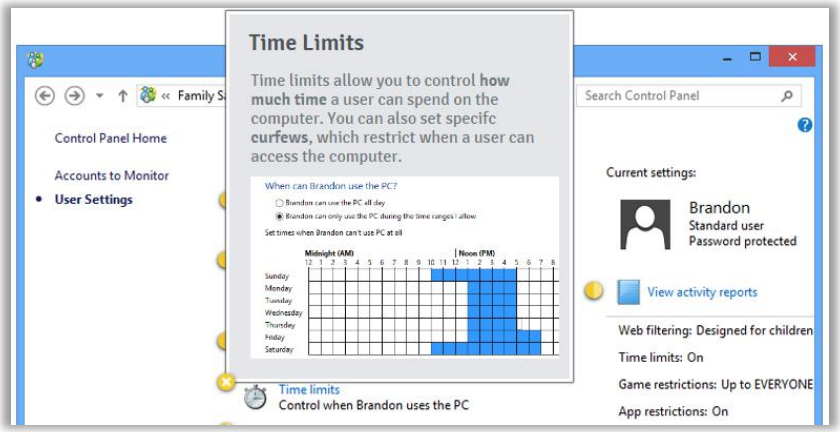
شکل (۲۳) تنظیمات Family Safety برای کاربر کودک

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



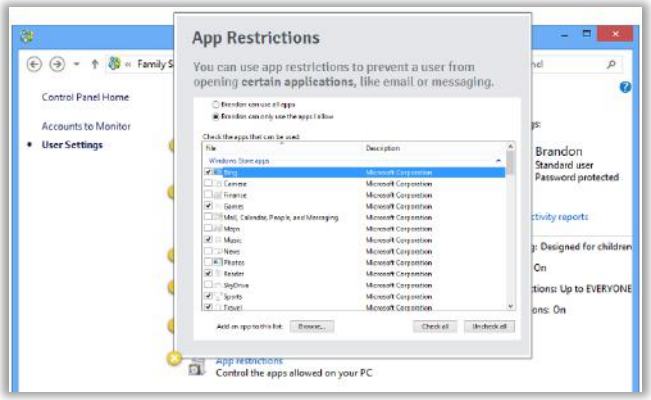
شکل (۲۴) تنظیم وب‌سایت‌های قابل‌مشاهده برای کودک

در تنظیمات Time Limit می‌توانیم ساعات مجاز استفادهٔ 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 نحوهٔ دسترسی کاربر را به برنامه‌های کاربردی مانند ایمیل، تعیین کنیم (GCF, 2017).



شکل (۲۶) نحوهٔ دسترسی کاربر کودک به برنامه‌ها

گزینه‌های کنترلی در ویندوز ۱۰

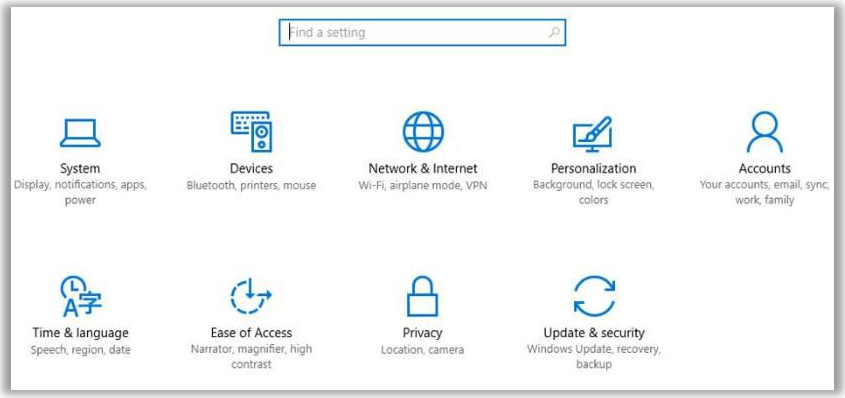
کنترل والدین در ویندوز ۱۰ به‌شکلی ارتقا داده شده که سرپرست (یا فرد بزرگ‌سال) می‌تواند از هر دستگاه دیگری (با سیستم‌عامل ویندوز) بر رفتار فرزند خود نظارت کند. برای این منظور، سرپرست باید بتواند با حساب کاربری مایکروسافت (شامل نام کاربری و کلمهٔ عبور) که قبلاً آن را ایجاد کرده، از دستگاه خود وارد شود و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

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

بنابراین، مهم‌ترین مرحلهٔ 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:

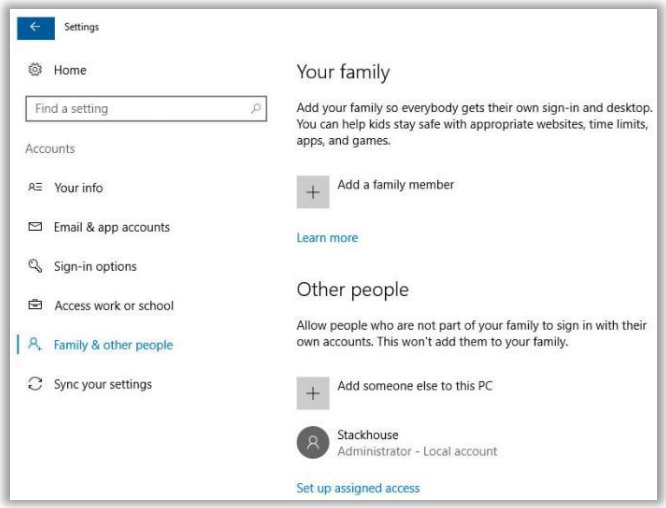


شکل (۲۷) تنظیمات ویندوز ۱۰

شکل زیر Windows Settings-> Accounts را نمایش می‌دهد:

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

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



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

دراین مرحله مطابق شکل زیر، کاربری با مشخصهٔ 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.

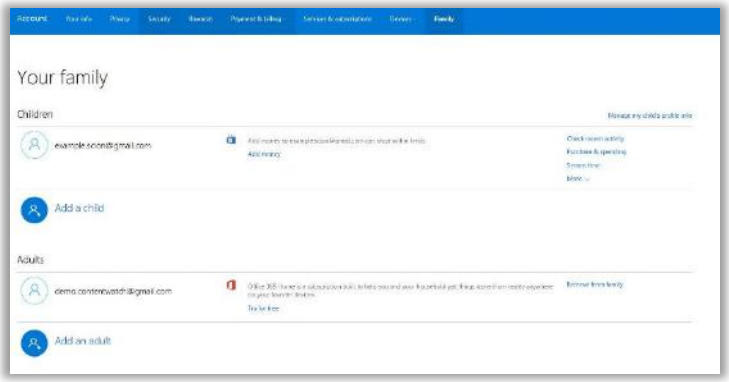
شکل (۳۰) تنظیات ویندوز ۱۰ برای تعریف کاربران (۳)

اگر تابه‌حال حساب کاربری مایکروسافت نساخته باشیم، به‌کمک 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 به‌عنوان بزرگ‌سال (یا سرپرست) شناخته شده و می‌تواند تنظیمات مدنظر را به‌روش زیر برای کودک انجام دهد:

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

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



شکل (۳۱) کنترل والدین مایکروسافت

ازطریق 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.

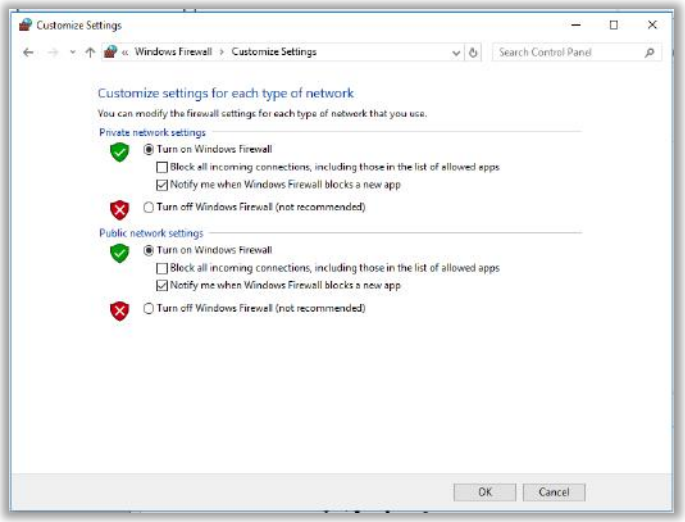
ضعف ویندوز ۱۰ برای فیلترکردن وب‌سایت‌ها این است که محتوایی که کاربران تولید می‌کنند (مثل کامنت‌ها یا پست‌های شبکه‌های اجتماعی) در لیست سیاه فیلتر قرار نمی‌گیرد. به‌علاوه، این فیلترها فقط در مرورگرهای مایکروسافت، یعنی Internert Explorer(IE) و Microsoft Edge، قرار می‌گیرد و در مرورگرهای دیگر، مانند کروم 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 درنتیجه، آن را ممنوع می‌کند یا اجازهٔ ورود به کامپیوتر را به آن

می‌دهد. دیوار آتش می‌تواند دسترسی‌ها را به‌طور جداگانه برای شبکهٔ خانگی و شبکهٔ عمومی تنظیم کند. برای مثال، می‌تواند ارتباطات ورودی را در شبکهٔ امن خانگی مجاز و در شبکهٔ 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 شبکهٔ اینترنت متصل می‌شدند، به‌طور متوسط بعد از ۴ دقیقه آسیب می‌دیدند و قربانی حملهٔ کرم‌ها می‌شدند.

دیوار آتش در زمان اجرای سیستم‌عامل ویندوز، به‌طور پیش‌فرض در پنجرهٔ Control Panel روشن است (مانند شکل زیر) و هنگام برقراری ارتباطات، به کاربر هشداری را نشان می‌دهد؛ به‌این‌ترتیب، درصورتی‌که کاربر اجازه بدهد، ارتباط برقرار می‌شود.



شکل (۳۲) تنطیمات دیوار آتش در ویندوز

در شکل بالا می‌توان گزینهٔ زیر را هم تیک زد:

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

این گزینه امنیت رایانهٔ 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 به‌صورت پیش‌فرض در سیستم‌عامل ویندوز تعریف شده است. درعین‌حال، کاربر می‌تواند در تنظیمات پیشرفته به این گزینه دسترسی پیدا کند.

گزینهٔ کنترل والدین در سیستم‌عامل‌های گوشی‌های هوشمند

در سیستم‌عامل 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 غیرفعال‌کردن آن پیدا کنند (Knorr, 2016).

گزینه‌های کنترلی در گوشی آیفون

در گوشی‌های آیفون که با سیستم‌عامل 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؛ به‌طوری که اگر برنامهٔ دیگری را باز کرد، گوشی خاموش شود. به‌طور خلاصه مسیر استفاده از این قابلیت به‌صورت زیر است (Cell Phone, 2016):

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

در تبلت‌های آیپد نیز ابتدا به‌روش زیر می‌توانیم کلمهٔ عبوری برای خود انتخاب کنیم:

General->Passcode lock

در این‌قبیل دستگاه‌ها نیز، درست مثل گوشی‌های آیفون، می‌توانیم با استفاده از کلید Guided Access کودک را به استفاده از برنامه‌ای خاص محدود کنیم. همچنین می‌توانیم ازطریق 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 صفحهٔ گوشی ظاهر نشود یا کارکرد بعضی برنامه‌ها را محدود کنیم. برای مثال، می‌توانیم از این طریق واردشدن به بازی با چند کاربر یا امکان تغییر در برنامه‌های موجود یا دسترسی به بعضی از محتواها را محدود یا ممنوع کنیم (Character, 2016).

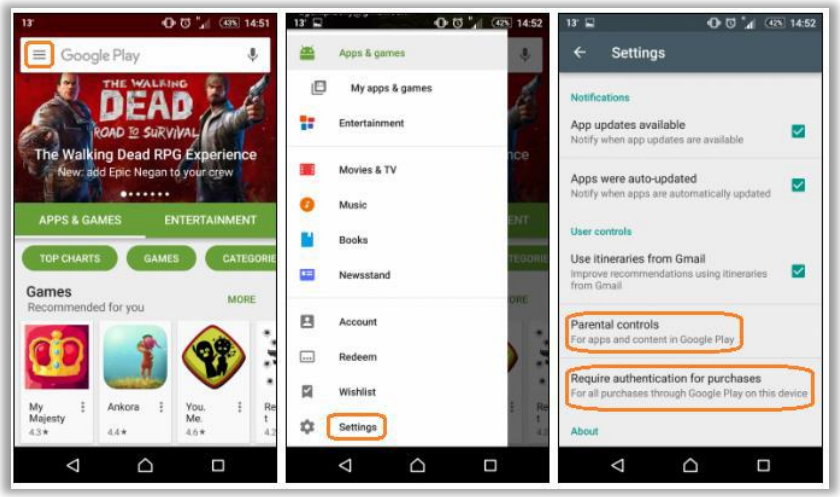
گزینه‌های کنترلی در گوشی‌های اندرویدی

در گوشی‌هایی که سیستم‌عاملشان اندروید است نیز سازکارهایی پیش‌بینی شده است. اگر بخواهید گوشی اندرویدی خود را گاهی به فرزندتان هم بدهید، می‌توانید از منوی «تنظیمات» محیطی امن را برای او فراهم سازید. در قسمت Settings ازطریق فعال‌کردن گزینهٔ Guest mode برنامه‌های کاربردی مناسب را برایش مشخص کنید. به‌این‌ترتیب، فقط اجازهٔ دسترسی به آن‌ها را خواهد داشت و وارد منوی مخصوص خود خواهد شد.

شکل (۳۳) تنظیمات حالت Guest برای اندروید

در ابتدا با واردکردن کلمهٔ عبور وارد تنظیمات این حالت می‌شوید. سپس مشخص می‌کنید اخطارها[1] 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.

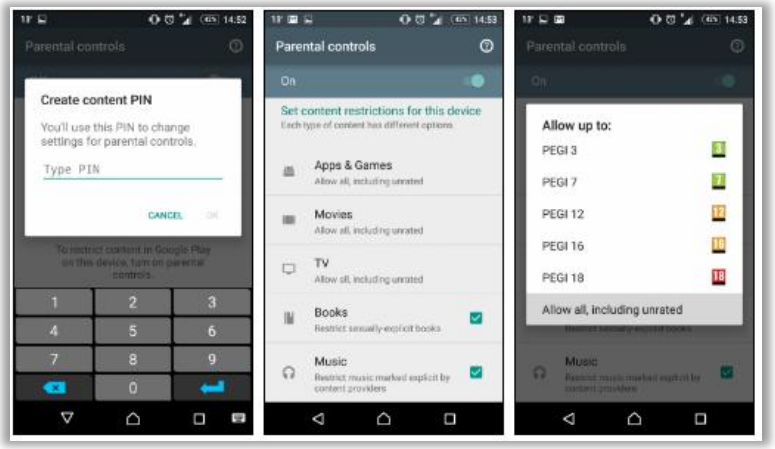
یکی دیگر از تمهیدات نظارتی اندروید در فروشگاه Play Store دیده می‌شود. با انتخاب Settings در این نرم‌افزار می‌توانید گزینهٔ Parental control و همچنین گزینهٔ Require authentication for purchases را فعال کنید. مراحل این کار در شکل زیر با مستطیل‌های قرمزرنگ نشان داده شده است.



شکل (۳۴) منوهای فعال‌سازی کنترل والدین

[1] notifications

با فعال‌کردن گزینهٔ «کنترل والدین» می‌توان ردهٔ سنی نرم‌افزارهایی را که در این فروشگاه نشان داده می‌شود، مطابق شکل زیر تعیین کرد.

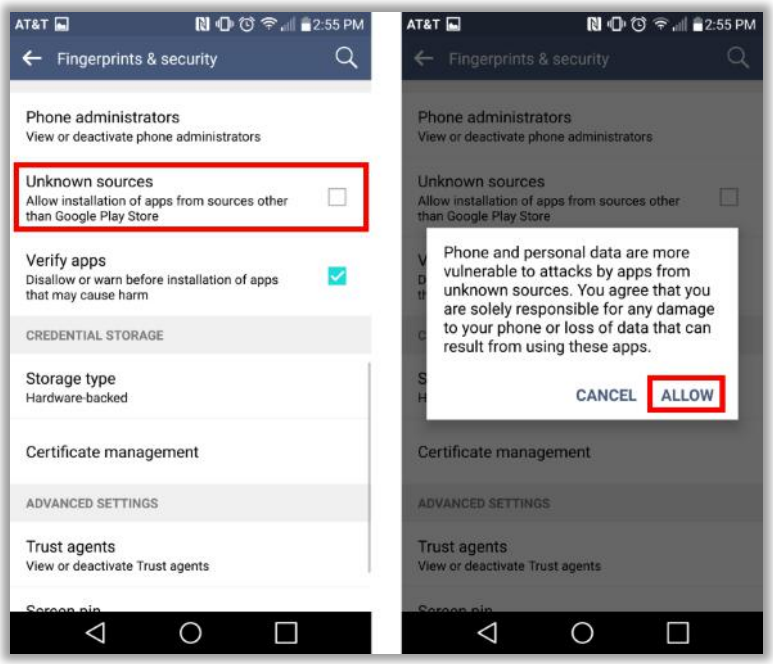


شکل (۳۵) تعیین ردهٔ سنی در برنامه‌های اندرویدی

رده‌های سنی پایین‌تر به‌معنی اعمال محدودیت بیشتر است. گزینهٔ 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 گزینهٔ «اجازهٔ 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 به‌نام Family Care طراحی شده است. برای استفاده از این نرم‌افزار در زمانی که فرزند دستگاه جداگانه‌ای دارد، دستگاه او با دستگاه والدین ازطریق QR Code جفت می‌شود. به‌وسیلهٔ این نرم‌افزار والدین می‌توانند زمان استفاده از دستگاه یا هریک از برنامه‌ها را برای فرزند خود تعیین کنند. همچنین نصب‌کردن برنامهٔ جدید یا دانلودکردن موسیقی جدید تنها با اجازهٔ والدین انجام خواهد شد. با معین‌کردن زمان استفاده، کودک نمی‌تواند برای مثال در ساعت خواب یا ساعتی که مربوط به مدرسه است، از دستگاه خود استفاده کند (MICHEL, 2016).

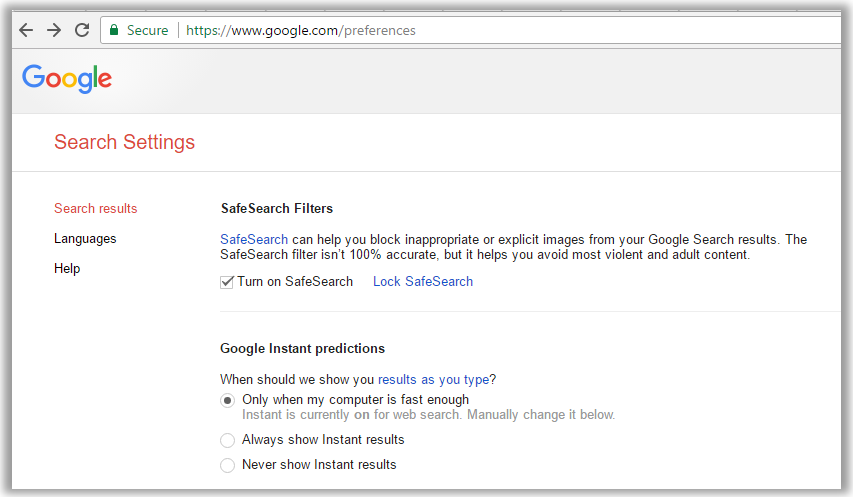
نظارت به‌کمک مرورگرها و موتورهای جست‌وجو

برای‌اینکه والدین بتوانند فعالیت فرزندان خود را کنترل کنند، سازندگان نرم‌افزارهای مرورگر و موتورهای جست‌وجو، تنظیماتی را مهیا کرده و در اختیار آن‌ها قرار داده‌اند. به‌این‌ترتیب، راه‌هایی برای مسدودکردن 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 همهٔ آن‌ها فعال کنیم. البته این ابزار برای کنترل فرزندان بزرگ‌تر که با جزئیات نرم‌افزارها آشنا هستند، مناسب نیست.

گزینه‌های کنترلی در موتور جست‌وجوی گوگل

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

گزینهٔ 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 ذخیرهٔ وضعیت جدید باید بر روی آن کلیک کرد.



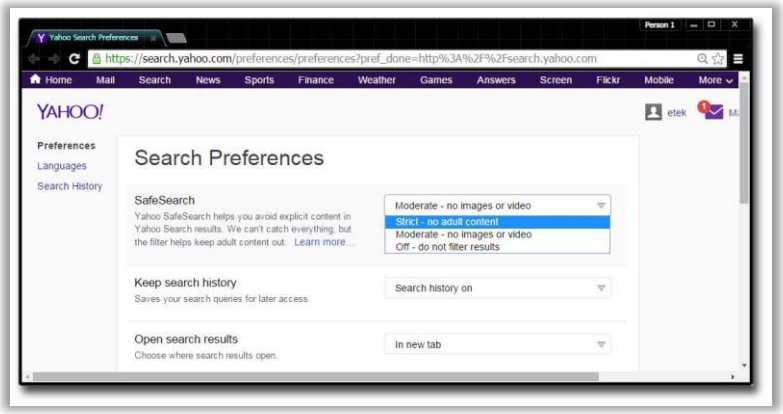
شکل (۳۷) تنظیم گزینهٔ جست‌وجوی امن در موتور جست‌وجوی گوگل

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

گزینه‌های کنترلی در موتور جست‌وجوی یاهو

برای دسترسی به گزینه کنترل والدین در موتور جست‌وجوی یاهو هم می‌توان به سایت http://search.yahoo.com/preferences مراجعه کرد. گزینهٔ 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.

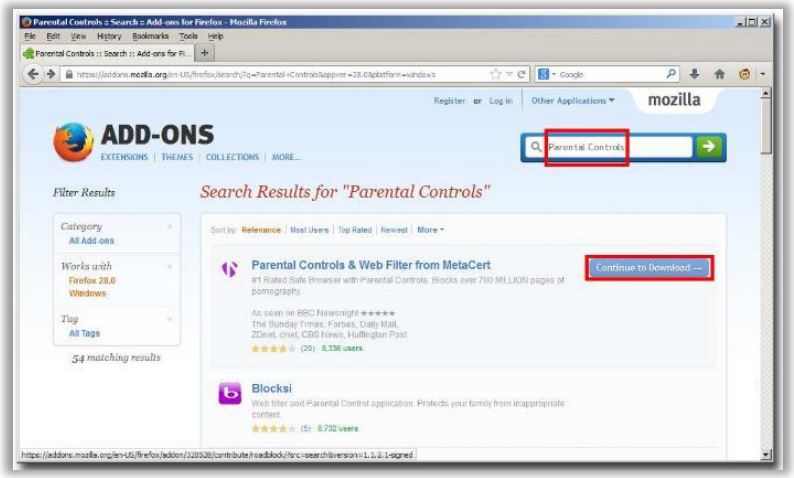


شکل (۳۸) گزینهٔ کنترلی موتور جست‌وجوی یاهو

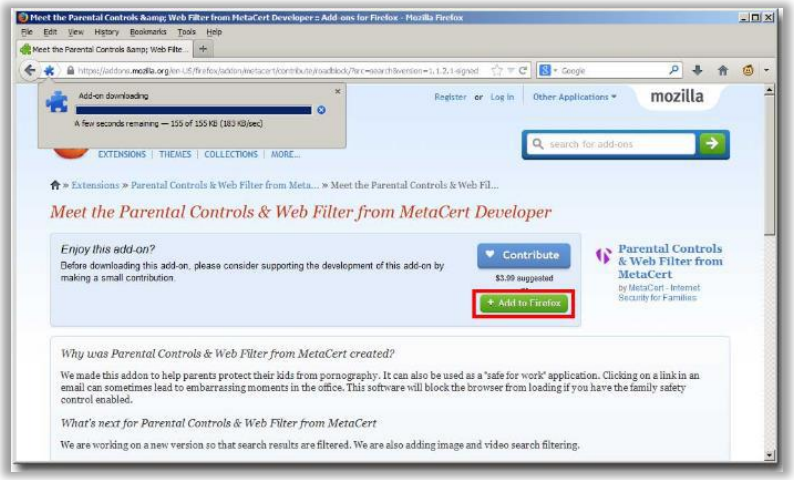
گزینه‌های کنترلی در مرورگر فایرفاکس

در مرورگر فایرفاکس ابتدا وارد سایت Firefox Add-on[1] می‌شویم و در قسمت جست‌وجوی آن، parental control را جست‌وجو می‌کنیم. در مرحلهٔ بعد می‌توانیم هریک از افزونه‌هایی را که با این عنوان نمایش داده می‌شود، انتخاب و به مرورگر خود اضافه کنیم. در شکل‌های زیر مستطیل‌های قرمزرنگ، کلیدهایی است که مسیر اجرای این کار را نشان می‌دهد (محمود، ۱۳۹۴).

[1] https://addons.mozilla.org/en-US/firefox/



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

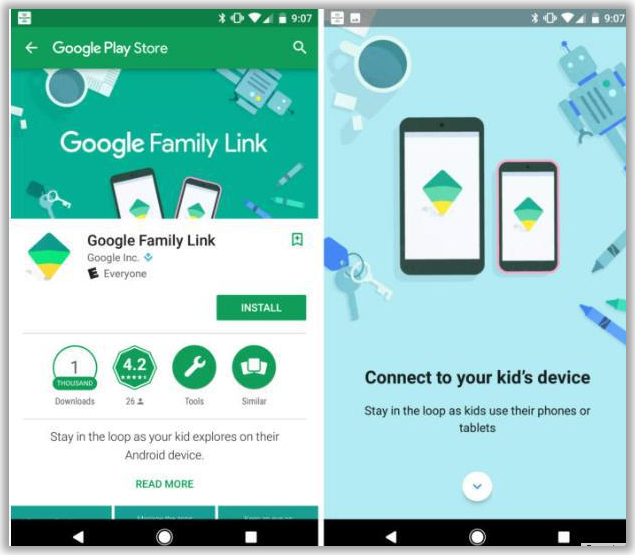


شکل (۴۰) کلیدهای کنترل والدین در مرورگر فایرفاکس (۲)

گزینه‌های کنترلی در مرورگر کروم

مرورگر کروم برای فعال‌سازی قابلیت نظارت بر فرزندان زیر ۱۳ سال، از والدین می‌خواهد ازطریق برنامهٔ 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 ژانویهٔ 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. به‌این‌ترتیب، 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. به‌همین‌دلیل، برای نظارت بر وب‌گردی فرزندان با این مرورگر، باید از نرم‌افزارهایی که در ادامه معرفی شده و نیز افزونه‌های مسدودکردن سایت‌ها استفاده کرد.

گزینه‌های کنترلی در مرورگر سافاری[1]

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

برای اعمال محدودیت، ابتدا به بخش زیر بروید:

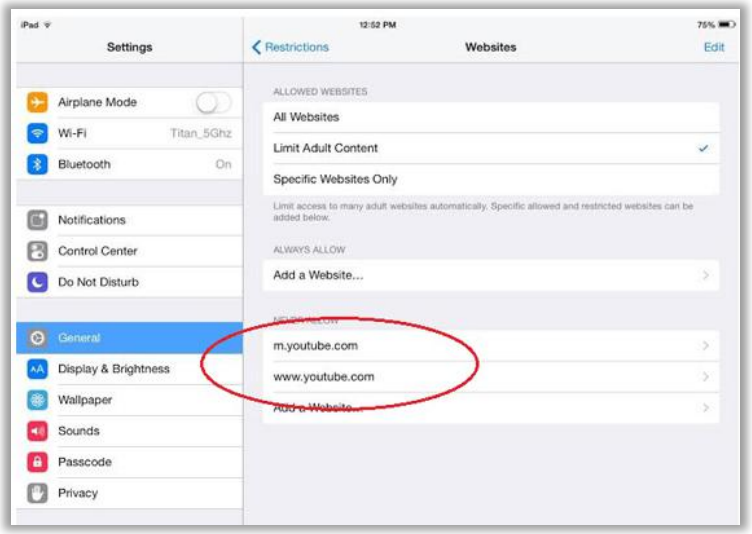
Settings> General>Restrictions

در اینجا پس از واردکردن کد تأیید چهاررقمی می‌توانید فهرست سایت‌هایی را که مناسب فرزندتان نیست یا فهرست سایت‌هایی را که ترجیح می‌دهید فرزندتان فقط از آن‌ها بازدید کند، وارد کنید. از این قسمت همچنین می‌توانید گزینهٔ مسدودکردن سایت‌های بزرگ‌سال را انتخاب کنید:

شکل (۴۲) دستیابی به گزینهٔ کنترلی در مرورگر سافاری

[1] 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 محدودکردن بازدید از صفحات وب توسط والدین در مروگر سافاری

افزونه‌ها

راهکار دیگری که برای حفاظت از فرزندان دربرابر 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 مروگر خود نصب کنید. این کار بسیار ساده است. سپس باید با راست‌کلیک روی آن یا انتخاب گزینهٔ Options بسته به مرورگر، تنظیمات آن را به‌دلخواه خود تغییر دهید.

برای مشاهدهٔ افزونه‌های مروگر کروم خود در گوشهٔ سمت راست بالا روی علامت سه‌نقطه 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.

افزونهٔ مدیریت زمان Nanny

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

شکل (۴۴) افزونهٔ کنترل والدین Nanny

افزونهٔ ضدپورن[1]

این افزونه برای مسدودسازی سایت‌های غیراخلاقی است. پس از نصب آن، سایت‌های مستهجن به‌صورت خودکار مسدود می‌شوند. می‌توانید سایت‌هایی را هم که ازنظر شما مناسب نیستند، به تنظیمات آن اضافه کنید. از دیگر قابلیت‌های این افزونه گذاشتن کلمهٔ عبور بر روی تنظیمات است که هیچ‌کس نمی‌تواند تغییری در آن ایجاد کند.

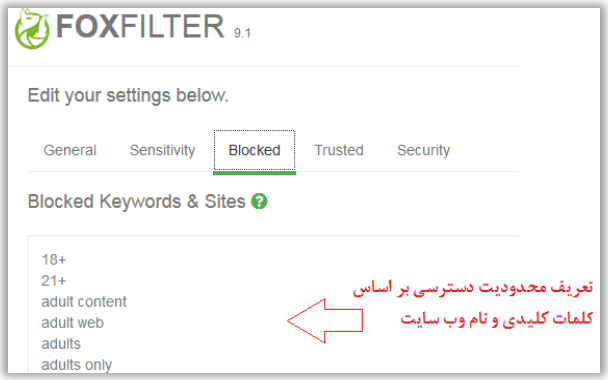
یکی از ویژگی‌های این افزونه مدیریت فیلترینگ به‌صورت ابری است؛ یعنی دسترسی به وب‌سایت‌های ممنوع زیر نظر هزاران وب‌سایت بر روی فضای ابری کنترل می‌شود.

شکل (۴۵) تنظیمات افزونهٔ ضدپورن فایرفاکس

افزونهٔ فیلتر فایرفاکس[2]

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

[1] Anti-Porn Pro
[2] FoxFilter



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

حفاظت با انتخاب کلمهٔ 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 سادهٔ 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 0f 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”

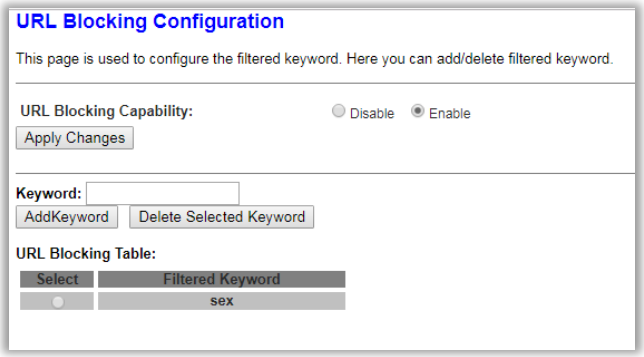
- هرازگاهی رمز عبورهای خود را تغییر دهید و در مدت‌زمان طولانی از یک رمز عبور استفاده نکنید.
- در رمز عبور، از اطلاعات شناسنامه‌ای یا شماره‌موبایل یا نام فرزندان خود استفاده نکنید.
- از یک رمز برای چند حساب کاربری (مانند ایمیل و حساب کاربری در شبکه‌های مجازی) استفاده نکنید.

علاوه بر موارد یادشده، می‌توان از نرم‌افزارهای مدیریتی رمز عبور برای ساده‌ترشدن 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 ازطریق تجهیزات شبکهٔ 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 به‌سراغ گزینه‌های access control و filter می‌رویم. در قسمت بازشده می‌توانیم فهرستی از سایت‌های نامطلوب را که نمی‌خواهیم به آن‌ها دسترسی داشته باشیم، درج می‌کنیم. به‌این‌ترتیب، دسترسی به سایت‌هایی که در فهرست درج شده، برای تمام دستگاه‌های موجود در شبکهٔ خانگی، ناممکن می‌شود (Donnell, 2016).



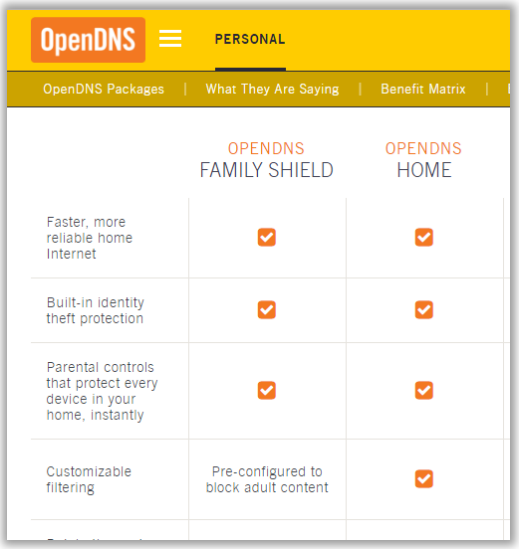
شکل (۴۷) تنظیمات مودم برای فیلترشدن سایت‌های خاص

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

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

بعضی از مودم‌های خانگی قابلیتی به‌نام «کنترل والدین» دارند که باید در هنگام راه‌اندازی دستگاه، فعال شود. با فعال‌شدن 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).

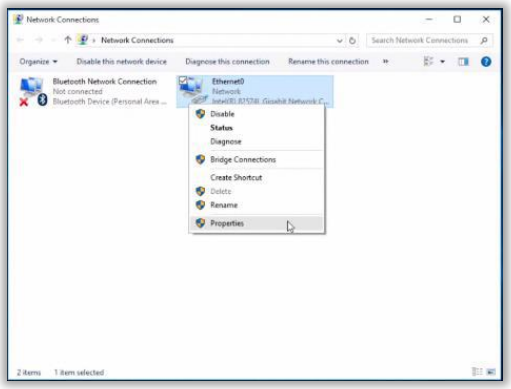
سرویس OpenDNS (که ازجمله سرویس‌های شرکت آمریکایی Cisco است) یکی از سرویس‌های متداول با کاربردهای مختلف است که بدون نصب هیچ نرم‌افزاری و به‌منظور فیلترکردن محتوای نامناسب، روی شبکه خانگی، کامپیوتر شخصی، گوشی هوشمند یا سرورها استفاده می‌شود. با استفاده از این سرویس، سایت‌های مجاز یا whitelist در شبکهٔ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



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

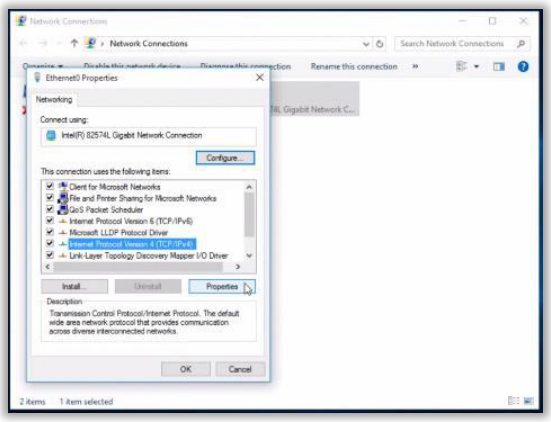
البته این لیست برای همهٔ افراد خانواده یکی است و امکان تعریف سطوح مختلف برای افراد، به‌طور جداگانه وجود ندارد. برای مثال، روش فعال‌کردن آن بر روی کامپیوتر به‌شکل زیر است:

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

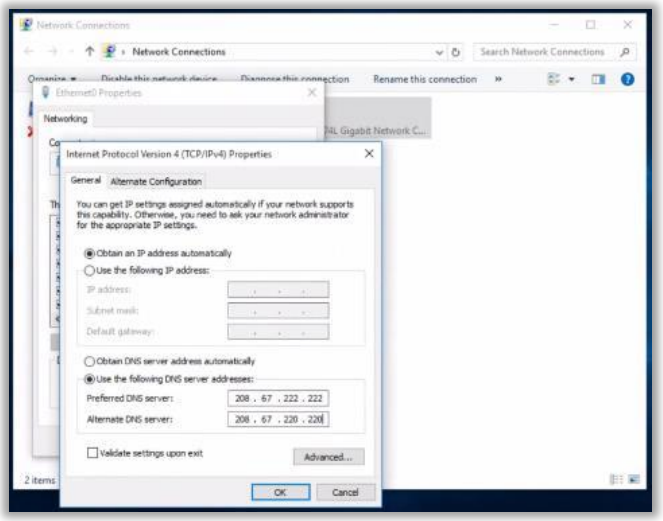


شکل (۵۰) تنظیمات استفاده از سرور OpenDNS

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) تنظمیات استفاده از سرور OpenDNS



شکل (۵۲) تنظیمات استفاده از سرور OpenDNS

نظارت والدین به‌کمک نرم‌افزارهای ضدویروس

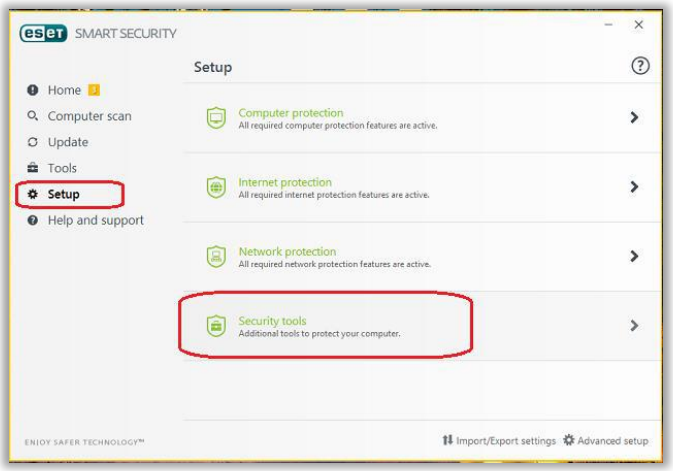
نرم‌افزارهای ضدویروس نیز امکاناتی برای کنترل والدین به مشتریان عرضه کرده‌اند.

نرم‌افزار 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. به‌این‌ترتیب، وب‌گردی فرزندمان 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 گزینهٔ کنترل والدین آنتی‌ویروس نود ۳۲ (یا ESET) را به‌شکل زیر فعال می‌کنیم:

Setup -> Security tools -> Parental control

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

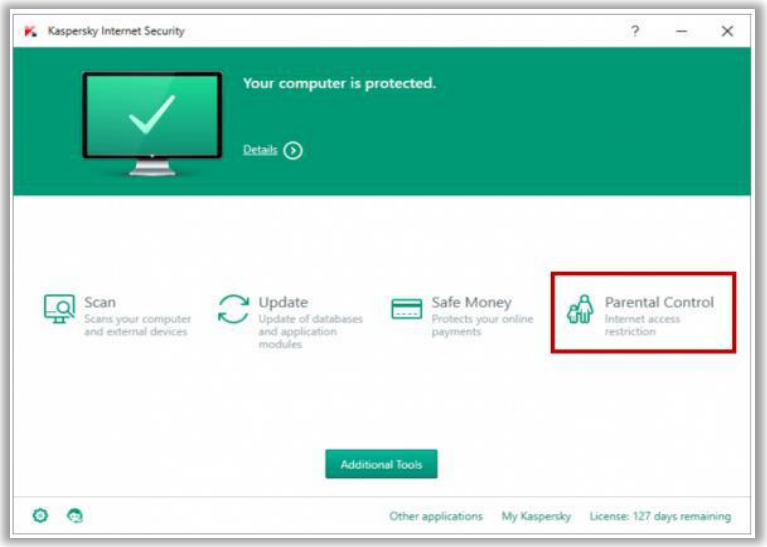


شکل (۵۳) مرحله‌ای از تنظیمات کنترل والدین در نود ۳۲

نرم‌افزار Kaspersky

نرم‌افزار آنتی‌ویروس معروف Kaspersky نیز راه‌حل‌هایی برای این موضوع در نظر گرفته است. گزینهٔ parental control می‌تواند محدودیت‌هایی در دسترسی به صفحات اینترنت ایجاد کند. همچنین با فعال‌سازی Control Web Browsing می‌توانیم گزارش کاملی از وب‌گردی کاربر تهیه و مشاهده کنیم. برای فعال‌سازی parental control باید در صفحهٔ Kaspersky Internet Security آیکون parental control را انتخاب کنیم. از گزینه‌هایی که برای محدودیت دسترسی به اینترنت در این نرم‌افزار قرار داده شده، می‌توان برای روزهای کاری[1] یا تعطیلات پایان هفته[2] استفاده کرد. گزینهٔ دیگری نیز در این نرم‌افزار وجود دارد که می‌تواند دسترسی به تعدادی وب‌سایت خاص را مسدود کند. این وب‌سایت‌ها یا به‌صورت جدولی از آدرس‌هایی است که از محتوای آن‌ها آگاهی داریم یا براساس دسته‌بندی پیشنهادی خود نرم‌افزار[3] مسدود می‌شود (یزدانی، ۱۳۹۵). شکل زیر اولین مرحله از مراحل بالا را نشان می‌دهد.

[1] Restrict access on weekday
[2] Restrict access on weekends
[3] 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، به‌ترتیب زیر عمل می‌کنیم.

Kaspersky Internet Security-> Parental Control-> Configure restrict-> انتخاب حساب کاربری -> Application

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 به‌کمک

قابلیت محدودکردن برنامه‌ها در نرم‌افزار Kaspersky می‌توانیم برنامه‌های خاصی را در لیست برنامه‌ها تیک بزنیم تا از دسترس 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 ازطریق این نرم‌افزار می‌شود انتقال اطلاعات خصوصی مانند شماره‌تلفن و شماره‌کارت اعتباری را محدود کرد. این نرم‌افزار قابلیت دیگری نیز به‌نام «کنترل والدین پیشرفته» دارد که ازطریق آن می‌توان بر فعالیت‌های آنلاین کودکان کاملاً نظارت کرد و به‌طور مؤثری محتواهای نامناسب را مسدود نمود. به‌این‌ترتیب، از تمام اعضای خانواده دربرابر مجرمان اینترنتی حفاظت می‌شود (کی پاد، ۱۳۹۷).

برنامهٔ Bitdefender

در برنامهٔ 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. صفحهٔ تنظیمات کنترل والدین این نرم‌افزار، به‌شکل زیر باز می‌شود:

Bitdefender window: privacy->Parental Control->Configure

در این صفحه به‌وسیلهٔ 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، تعیین‌کردن کلمه‌ای کلیدی مانند porn است. با این کار، مشاهدهٔ صفحات وب یا پست الکترونیکی یا پیام فوری‌ای که شامل این کلمه باشد، برای حساب کاربریِ مشخص‌شده 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 بقیهٔ برنامه‌های آنتی‌ویروس هم (مانند آویرا یا f-secure) چنین قابلیت‌هایی پیش‌بینی شده؛ هرچند در آن‌ها توضیحات مفصلی دراین‌باره داده نشده است. بنابراین، پیدا است سازندگان نرم‌افزارهای ضدویروس از اهمیت این قابلیت نرم‌افزاری غافل نبوده‌اند.

نظارت به‌کمک 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 برای‌اینکه 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 پیشرفتهٔ جهان که خود از طراحان اولیهٔ اینترنت‌اند، بسیار موردتوجه است. به‌دلیل متنوع‌بودن 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. به‌همین‌دلیل، بسیاری از کشورها برای کمک به خانواده‌ها و فرهنگ‌سازی دراین‌زمینه، 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 محدودهٔ سنی برای فرزندان
- مشاهدهٔ محتوایی که فرزندان دیده‌اند
- امکان تعیین زمان استفاده
- مکان‌یابی فرد
- ارائهٔ گزارش
- امکان اعمال تنظیمات دلخواه و تغییر رمز عبور اصلی
- هدایت کاربر به‌سمت 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 مشخص‌شده 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 پیشرفتهٔ 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 باتوجه‌به 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 آنلاینِ کاربر گزارش‌هایی می‌دهد (kidlogger, n.d.).

کیدلاگر به شما کمک می‌کند تا بدانید:

+ فرزندتان چه مدت با کامپیوتر یا موبایل کار کرده است.
+ از چه نرم‌افزارهایی استفاده کرده است.
+ از چه وب‌سایت‌هایی بازدید کرده است.
+ با چه کسی ازطریق 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. نسخهٔ رایگان کیدلاگر را فقط در یک دستگاه می‌توان استفاده کرد؛ درحالی‌که نسخه‌های غیررایگان را می‌شود در چندین دستگاه و با قابلیت‌های بیشتر استفاده کرد.

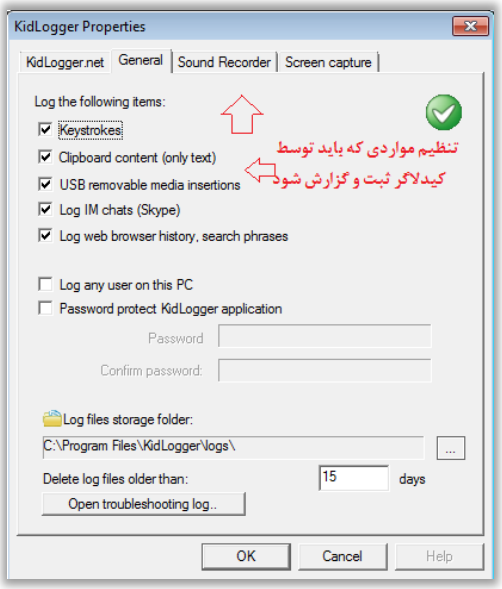
پس از دریافت نسخهٔ مدنظر این برنامه از سایت kidlogger.net مانند بقیهٔ برنامه‌های نصبی ویندوز، آن را نصب می‌کنیم.

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:



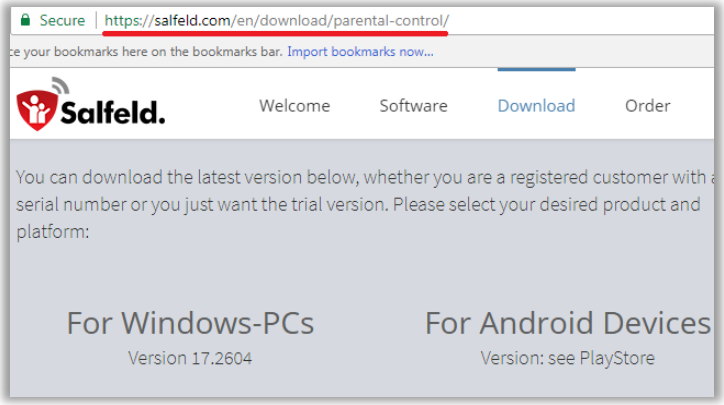
شکل (۵۸) پنل کنترلی در نرم‌افزار Kid Logger

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

نرم‌افزار Salfeld Child Cotrol

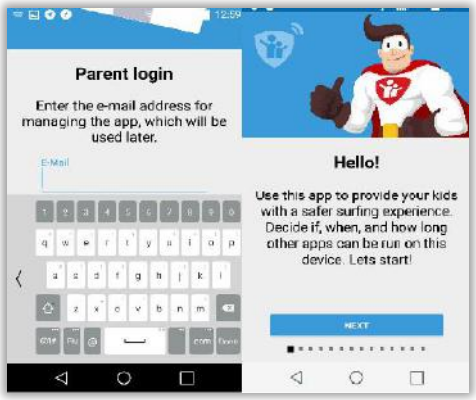
با استفاده از این نرم‌افزار آلمانی به‌راحتی بگومگوهای خود با فرزندتان را برای خاموش‌کردن رایانه یا تبلت خاتمه می‌دهید و رایانه و تبلت رأس ساعت مقرر خاموش می‌شود. نرم‌افزار Salfeld Child Control راهکار مناسبی برای جلوگیری از غرق‌شدن فرزندتان در دنیای رایانه و موبایل است (Salfeld, n.d.).

نسخهٔ موبایلی و رایگان این نرم‌افزار در فروشگاه‌های Google Play و iOS موجود است. برای دریافت نسخهٔ ویندوز ازطریق سایت آن اقدام کنید.



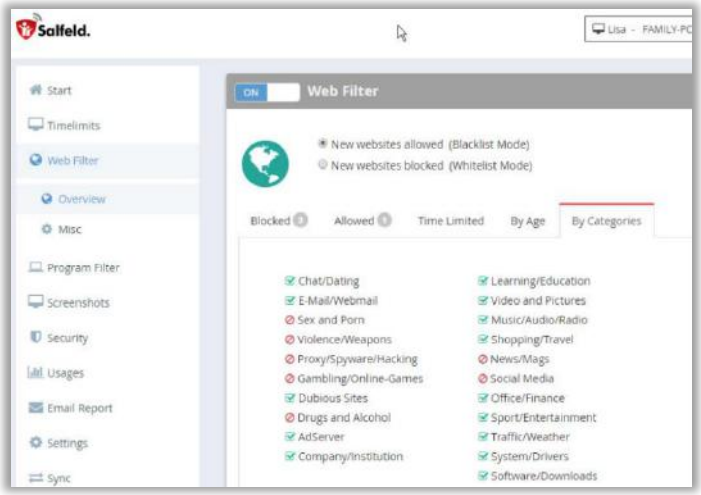
شکل (۵۹) دریافت نرم‌افزار از سایت salfeld

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



شکل (۶۰) یکی از مراحل راه‌اندازی نرم‌افزار 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 اجازهٔ 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 اجازهٔ دسترسی به چند سایت خاص را بدهید.



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

نرم‌افزار NQ Family Guardian[1]

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

[1] NQ Family Guardian

موقعیت مکانی فرزندشان و نحوهٔ استفاده او از گوشی همراه را مدیریت کنند. با نصب این نرم‌افزار روی گوشی فرزند خود، به نحوهٔ وب‌گردی و برنامه‌های نصب‌شده، عکس‌ها، تماس‌ها و پیامک‌هایش دسترسی دارید. یکی از قابلیت‌های خوب این نرم‌افزار تعریف منطقهٔ امن برای فرزندان است. با این قابلیت، در صورت احساس ناامنی، فرزندتان ازطریق لمس دکمهٔ SOS می‌تواند شما را از بروز مشکل مطلع سازد.

شکل (۶۲) دکمه کمک در نرم‌افزار NQ Family Guardian

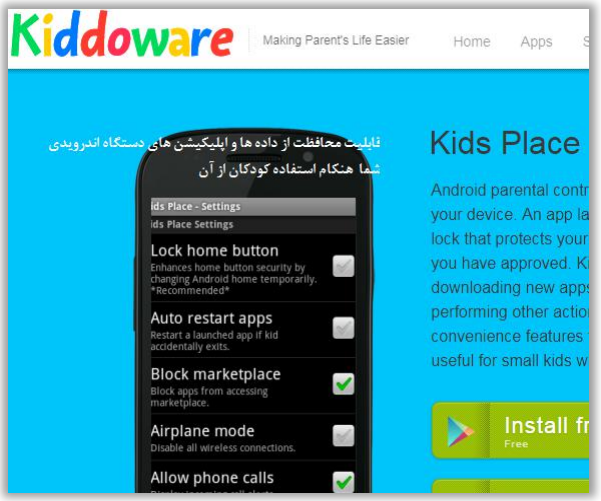
والدین ابتدا این نرم‌افزار را از گوگل‌پلی بر روی گوشی خود نصب می‌کنند و در سایت https://family.nq.com یک حساب کاربری می‌سازند. بعد ازطریق اسکن‌کردن QR Code زیر به گوشی فرزندشان دسترسی پیدا می‌کنند و از امکانات نظارتی خوب این نرم‌افزار استفاده می‌کنند.

شکل (۶۳) فعال‌سازی قابلیت‌های نرم‌افزار NQ Family Guardian

نرم‌افزار کیدز پِلِیس[1]

اگر بخواهید برای مدتی وسیلهٔ 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 همهٔ کارهایی که برای شما هزینه دارد، جلوگیری می‌کند.

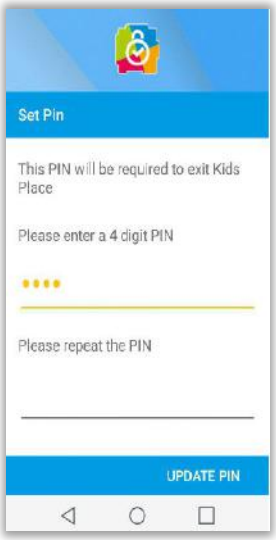
[1] Kids Place



شکل (۶۴) نرم‌افزار Kids Place

نسخهٔ پیشرفتهٔ این نرم‌افزار که غیررایگان است، علاوه بر زمان‌بندی استفاده از گوشی و هر نرم‌افزاری روی آن، قابلیت اجرا در پس‌زمینه را دارد. این ویژگی دربرابر شیطنت فرزندان بزرگ‌تر که نرم‌افزارهای نظارتی را به‌محض تشخیص uninstall می‌کنند، قابلیت خوبی است (googleplay, n.d.).

خوشبختانه این نرم‌افزار در فروشگاه بازار موجود است و نصب آن به‌راحتی انجام می‌شود. در ابتدا از شما یک کد چهاررقمی می‌خواهد تا بعداً به‌راحتی از حالت kids خارج شوید یا تنظیمات را تغییر دهید.

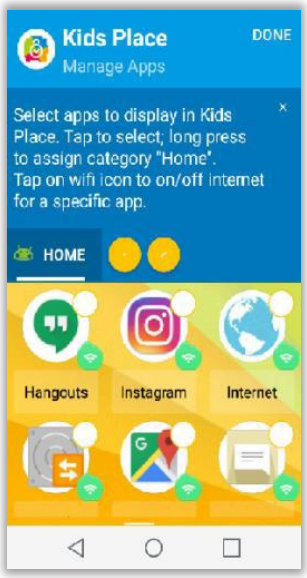


شکل (۶۵) تنظیم پین کد برای نرم‌افزار Kids Place

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 مشاهدهٔ بقیهٔ برنامه‌های کاربردی روی گوشی‌تان مجوز بدهید.

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

در گام بعدی وارد صفحهٔ 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 صفحهٔ فرزندتان می‌شوید و ازطریق چرخ‌دندهٔ تنظیمات و پس از واردکردن رمز عبوری که در ابتدا مشخص کرده‌اید، می‌توانید نظارت بیشتری را اعمال کنید:



گفتنی است بیشتر قابلیت‌های این برنامه ازطریق 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 واردشدن به سایت familyguard.ir ازطریق تب «ثبت‌نام و دانلود نرم‌افزار» وارد صفحهٔ خرید شوید و نرم‌افزار را دانلود کنید (فمیلی گارد، ۱۳۹۶).

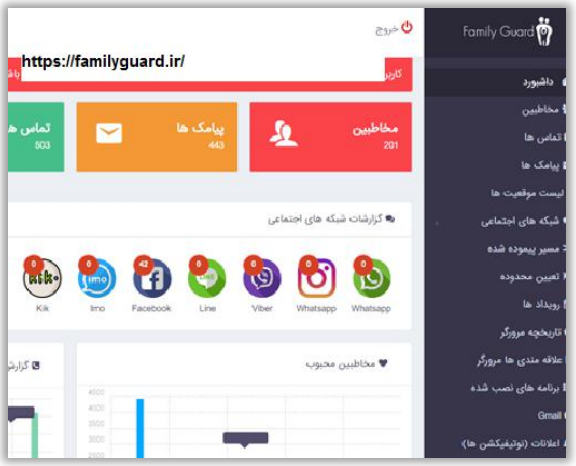
شکل (۶۷) منوی دانلود و ثبت‌نام نرم‌افزار فمیلی گارد

با استفاده از این برنامه:

- ✓ می‌توانیم گزارش تماس‌های ورودی و خروجی شامل نام مخاطب، شمارهٔ تماس و مدت‌زمان مکالمه و همچنین گزارش تماس‌هایی که به‌صورت دستی حذف شده‌اند، را داشته باشیم یا حتی آن‌ها 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 شبکه‌های اجتماعی همچون اینستاگرام، تلگرام، ایمو، واتس‌اپ و... مدیریت و در صورت لزوم، دسترسی آن‌ها را محدود کنیم.
- ✓ در هر لحظه از موقعیت عزیزان خود آگاه شویم و در کنار آن‌ها حضور پیدا کنیم و در صورت ورود به مناطق مجاز یا غیرمجاز تعیین‌شده، 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 برنامهٔ فمیلی گارد

سامانهٔ مراقبت از خانواده SFP[1]

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

[1] 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) صفحهٔ 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. به‌این‌ترتیب، دیگر فرزندتان به قسمت‌های دیگر گوشی دسترسی ندارد و می‌توانید با خیال آسوده گوشی را به او بدهید. این برنامه علاوه بر امکانات نظارتی، پس‌زمینهٔ کودکانه و کتاب داستان‌های تصویری و صوتی کودکانه هم دارد. این برنامه در نرم‌افزار بازار موجود است.

شکل (۷۰) نمایی از برنامهٔ کنترل فرزند شقایق

برای نصب این نرم‌افزار ابتدا از فروشگاه بازار، آن را دانلود کنید. سپس در صفحات زیر رمز عبور را وارد و نرم‌افزارهایی را که برای فرزند خود مناسب می‌دانید، مشخص کنید.

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

پس از اینکه ساعات استفاده از گوشی را مشخص می‌کنید، اگر فرزندتان خارج از ساعات مشخص‌شده به‌سراغ گوشی برود، سمت راست شکل زیر برایش نشان داده می‌شود.

شکل (۷۲) تنظیم ساعات استفاده از گوشی

برنامه ParentKit (iOS)

این برنامه نحوهٔ دسترسی به مرورگر و دیگر برنامه‌ها را براساس سن افراد مدیریت می‌کند و قابلیت‌هایی مثل ممانعت از نصب برنامهٔ جدید، خرید برنامه، دسترسی به مراکز بازی و محدودکردن محتوایی مثل موزیک و ویدئو را دارد. می‌توانید در زمان درس‌خواندن 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) برنامهٔ کنترلی ParentKit

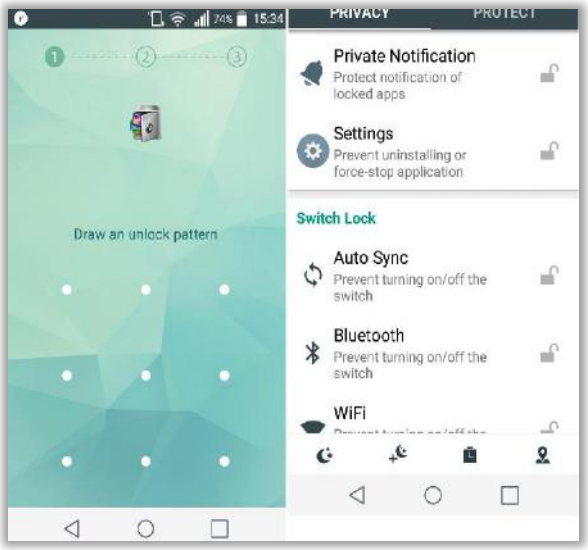
قفل‌کنندهٔ نرم‌افزار[1]

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

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

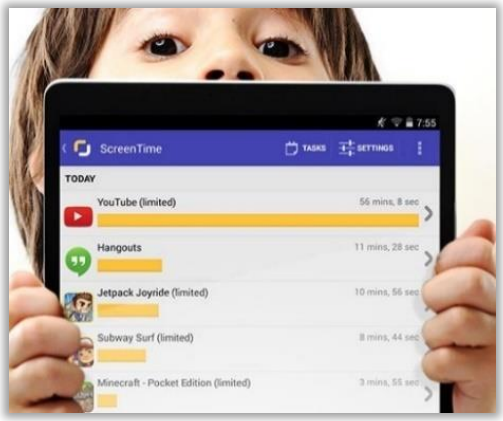
[1] AppLock

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



شکل (۷۴) نمایی از مراحل نصب و تنظیمات AppLock

برنامه Screen Time Parental Control

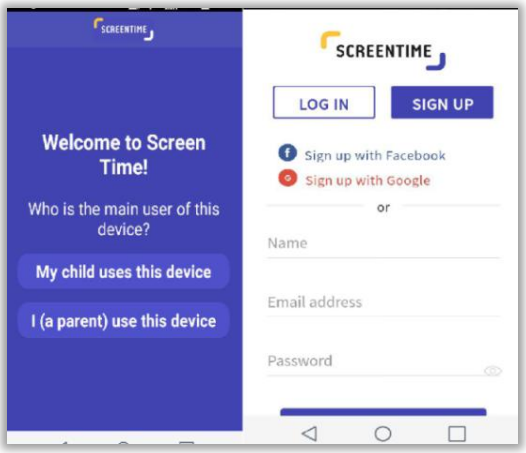


این برنامه را که در فروشگاه google play به‌صورت رایگان در دسترس است، می‌توان روی تمام سیستم‌عامل‌های اندروید و iOS نصب کرد. موارد زیر از جمله قابلیت‌های این نرم‌افزار است:

- ✓ محدودیت زمانی روزانه
- ✓ کنترل ساعت خواب: مسدودکردن بازی‌ها در زمان خواب (اما امکان استفاده از برنامه‌های مرتبط با خواندن وجود دارد)، مسدودکردن تمام برنامه‌ها در زمان خواب
- ✓ کنترل زمان مدرسه: مسدودکردن شبکه‌های اجتماعی و بازی‌ها (اما برنامه‌های آموزشی در ساعات مدرسه در دسترس است)
- ✓ مسدودکردن دستگاه فرزندان از راه دور، دادن پاداش به فرزندان برای انجام‌دادن وظایف و کارهای روزمره
- ✓ مسدودکردن برنامه‌های خاص به‌طور کامل و دریافت هشدار در زمان نصب برنامهٔ جدید توسط فرزند

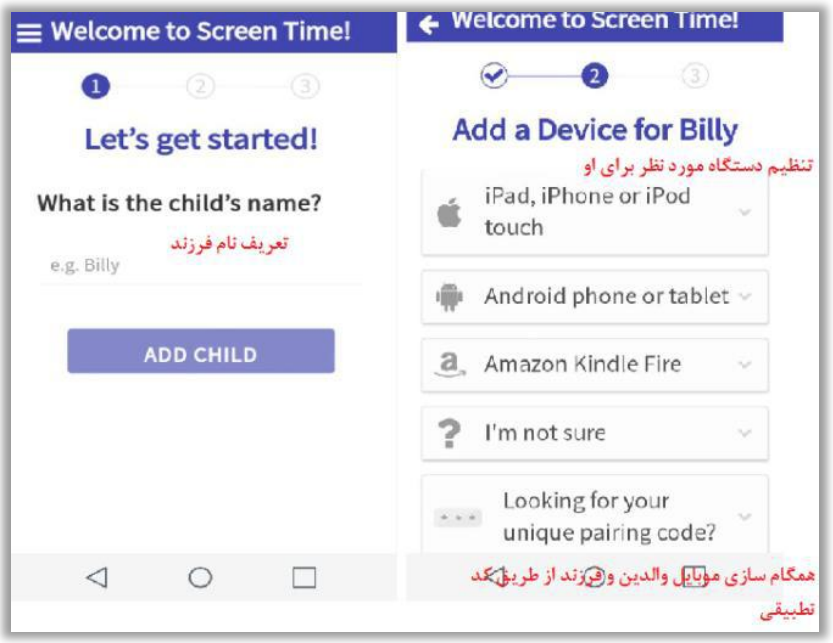
- ✓ نیاز به واردکردن کلمهٔ عبور تعیین‌شده توسط والدین برای حذف برنامه (پژوهشگاه ارتباطات و فناوری اطلاعات، ۱۳۹۶)

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 ثبت‌نام دستگاه فرزند خود و جفت‌کردن آن با موبایل خود ازطریق کد تطبیقی می‌شوید:



شکل (۷۶) صفحه تنظیمات Screen Time Parental Control

سپس ازطریق 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.

سیم‌کارت‌های کنترل‌شده

سیم‌کارت کنترل‌شده، 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 به‌راحتی نمی‌توانند کنترل‌های اعمال‌شده 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 مجموعهٔ 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. به‌این‌ترتیب، 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 مجموعهٔ دانش‌آموزان ایرانی طراحی شده است. این سیم‌کارت ضمن برآوردن تمام نیازهای مکالمه و

پیامک دانش‌آموزان، 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 توسعه‌یافتهٔ 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 اطلاعات‌اند. این اطلاعات حتی اگر به دست شرکت‌های تجاری و اطلاعاتی نیفتد و از آن سوءاستفاده نکنند، لقمهٔ 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 (boult, 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.commonsensemedia.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.commonsensemedia.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 Sequrity 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.symantec.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 ذکری.

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