پژوهشگاه علوم و فرهنگ اسلامی

شماره ۸۶| یکشنبه ۱۳ دی ماه ۱۳۹۴

اخبار

هشدار پلیس فتا در خصوص آسیب‌های فضای مجازی برای کودکان

پلیس فتا با بیان اینکه والدین در خصوص فعالیت آنلاین کودکان خود توجه بیشتری داشته باشند، گفت: شکارچیان آنلاین در این فضا همیشه به دنبال افرادی هستند که اطلاعات خود را به راحتی ارائه می کنند و کودکان بهترین طعمه برای شکارچیان آنلاین هستند.

پایگاه اطلاع رسانی پلیس فتا : تهدیدات فضای مجازی بسیار بیشتر از فضای حقیقی است، عنوان کرد: در فضای مجازی، امکان برقراری تماس‌های نامناسب کودکان با افرادی که ممکن است قصد سوء استفاده، بهره‌برداری و یا تجاوز به حریم خصوصی آنها را داشته باشند، وجود دارد، لذا تنها گذاشتن کودکان در این فضا خطرناک است. همچنین به خاطر این که امکان ارائه اطلاعات شخصی در شبکه های اجتماعی وجود دارد؛ از این رو، تبدیل شدن کودکان و نوجوانان به عامل و یا هدف زورگیری سایبری دور از انتظار نیست.

پلیس فتا در توصیه به والدین گفت: از کودکان بخواهید تا هر گونه زورگویی سایبری را به سرعت و از طریق گفت و گوی حضوری و یا تلفنی به شما اطلاع دهند، همچنین والدین باید کودکان را نسبت به این مساله آگاه کنند که مخاطبان آنلاین آنها در فضای مجازی لزوما همان افرادی نیستند که ادعا می کنند، چه بسا مجرمانی هستند که تلاش دارند از کودکان سوء استفاده نمایند.

کودکان هرگز نباید بدون نظارت والدین خود با فرد یا افرادی که در دنیای مجازی ارتباط داشته‌اند، در دنیای واقعی ملاقات داشته باشند.

محرمانه نگه داشتن اطلاعات و جزئیات شخصی در فضای مجازی و عدم دسترسی عمومی به آنها را از ضروریات برشمرد و گفت: والدین در این خصوص باید به کودکان خود آموزش دهند که به هیچ عنوان اطلاعات شخصی خود و خانواده را در فضای سایبر منتشر نکنند، ضمن آنکه مانع از به سرقت رفتن اطلاعات مهم و حساس در سیستم های رایانه ای شوند.

پلیس فتا دسترسی به محتوای نامناسب مانند فیلم‌ها، تصاویر، مطالب و نوشته‌های غیراخلاقی، نژادپرستانه، خشونت آمیز و دیگر موارد مضر و خطرناک را یکی دیگر از تهدیدات بالقوه و بالفعل فضای سایبر برای کودکان برشمرد و گفت: والدین برای نظارت بر فعالیت آنلاین کودکان خود می توانند از نرم‌افزارهای ویژه کنترل والدین در مرورگرها، موتورهای جستجو و بسته‌های امنیت اینترنتی برای حضور ایمن کودکان در فضای مجازی استفاده کنند.

پلیس فتا با توجه به اعتیاد اینترنتی به والدین توصیه کرد: والدین نگذارند کودکان روزانه چند ساعت بیشتر با کامپیوتر کار کنند و زمان اتصال آنها به اینترنت محدود باشد.

از باتری لپ تاپ استفاده کنیم یا از برق مستقیم ؟

خیلی از ما برای افزایش طول عمر باتری هایمان نگران بوده و در این باره نهایت دقت را می کنیم. شاید مدت هاست که این سوال در ذهن شما هم وجود دارد: از باتری لپ تاپ استفاده کنیم بهتر است یا از برق مستقیم ؟

کامپیوتر | ۲

آشنایی با ریسک‌های امنیتی گوشی‌های هوشمند

امروز شاهد هستیم که شایع‌ترین وسیله برای دسترسی به اینترنت همین گوشی‌های هوشمند هستند. با توجه به استفاده گسترده و روزافزون از این وسایل ارتباطی، مرور کلی بر ریسک‌ها، فرصت‌ها و توصیه‌های لازم برای استفاده ایمن از گوشی‌های هوشمند ضروری به‌نظر می‌رسد.

امنیت|۵

دستگاه های هوشمند شما چه چیزهایی درباره شما می‌دانند؟

فرقی نمی‌کند از رایانه‌های رومیزی استفاده می‌کنید یا تلفن‌های هوشمند. دستگاه شما حجم قابل‌توجهی از اطلاعات مهم و شخصی شما را در خود نگاهداری می‌کند....

اینفوگرافیک | ۸

از باتری لپ تاپ استفاده کنیم یا از برق مستقیم ؟

خیلی از ما برای افزایش طول عمر باتری هایمان نگران بوده و در این باره نهایت دقت را می کنیم. شاید مدت هاست که این سوال در ذهن شما هم وجود دارد: از باتری لپ تاپ استفاده کنیم بهتر است یا از برق مستقیم ؟؟ چطور از خراب شدن باتری لپ تاپ جلوگیری کنیم؟ طول عمر باتری لپ تاپ چقدر است؟ ادامه مطلب را بخوانید تا به شما بگویم.

طی بررسی‌های انجام شده راه حل‌هایی را به شما ارائه خواهد داد. از آنجایی که لپ تاپ‌ها توسط شرکت‌های مختلفی ساخته شده و هر شرکت سازنده با دیگر شرکت‌ها در استفاده از قطعات و سر هم کردن آنها تفاوت می کند، نمی‌توان برای همه آنها نسخه یکسانی پیچید! مثلا یکی از عواملی که باعث فرسودگی باتری لپ تاپ می‌شود داغ شدن دستگاه است اما شاید یک کمپانی با قرار دادن یک فن خنک کننده داخل لپ تاپ این مشکل را برطرف کرده باشد. همچنین برخی از شرکت‌ها فرایندی را ایجاد کرده‌اند که هنگام اتصال لپ تاپ به برق، باتری از مدار خارج شده و دستگاه از برق استفاده کند. پس این موضوع و دیگر موارد مشابه نمی‌توانند برای همه یکسان باشند. اما یک سری استاندارد ها تقریبا برای همه یکسانند. طبق آن موارد می‌توان راه کار های زیر را پیشنهاد داد:

۱. بهتر است در اولین بار استفاده از باتری لپ تاپ آن را تا انتها مصرف کنید مجدد آن را به طور کامل شارژ کرده و استفاده کنید و این چرخه را چند بار تکرار کرده و بعد باتری را کنار بگذارید. همچنین در تمام دفعاتی که از باتری استفاده می‌کنید همین روش را بکار بگیرید.

۲. برای کنار گذاشتن باتری بعضی می گویند که باتری باید کاملا خالی باشد و در مقابل برخی می گویند که باید کاملا پر باشد اما جالب است بدانید که طبق اطلاعاتی که یک وب سایت متخصص سخت افزار در این زمینه در اختیا ما قرار داده است بهترین روش این است که باتری بین ۳۰ تا ۵۰ درصد شارژ داشته باشد و بعد کنار گذاشته شود.

۳. بهترین دما برای قرار دادن باتری لپ تاپ در آنجا بین ۲۰ تا ۲۵ درجه سانتی گراد است. برخی معتقدند که باید باتری را در یخچال قرار داد اما طبق مطلبی که چندی پیش در مورد آسیب زدن سرما به باتری دستگاه های الکترونیکی (در مدت زمان ماندگاری طولانی در سرما) منتشر کردیم این نظریه کاملا رد می شود . گرما هم به طور جدی به باتری لپ تاپ یا هر وسیله دیگر صدمه می زند (حتی گرمای ناشی از فعالیت زیاد خود لپ تاپ می تواند خطرناک باشد) . پس

بهتر است در حین استفاده از لپ تاپ برای مدت طولانی مثلا زمانی که می خواهید کارهای گرافیکی سنگین انجام دهید یا اینکه می خواهید بازی کنید که در آن صورت لپ تاپ شما داغ خواهد شد بهتر است تا بدون باتری از لپ تاپ استفاده کنید.

۴. در صورتی می توانید باتری را کنار بگذارید که حداقل برای ۱ هفته نخواهید از آن استفاده کنید. بد نیست بدانید اگر فقط برای چند روز بخواهید باتری در بیاورید و مجددا قرار دهید، این کار هم به دستگاه شما آسیب جدی می زند.

۵. اگر لپ تاپ شما به عنوان یک PC برای شما است ، در واقع اگر هر روز در حال استفاده از لپ تاپ هستید و دستگاه شما روی میز کارتان قرار دارد بهتر است باتری را با همان شرایطی که گفتیم کنار بگذارید و کلا از برق مستقیم استفاده کنید . اما نکته مهم در این زمینه استفاده از یک UPS (یک منبع تغذیه جانبی است که قبل از زدن شارژر لپ تاپ مستقیما به برق و به عنوان واسط قرار می گیرد و مثل باتری عمل می کند که اگر برق قطع شود مانع از خاموش شدن دستگاه می شود) است . این کار جدا از جلوگیری از آسیب رسیدن به دستگاه شما ، امنیت لازم برای ذخیره اطلاعاتتان را در لحظه قطع برق فراهم می کند.

۶. اگر در حال استفاده از برق مستقیم هستید باتری لپ تاپ را کنار بگذارید. اما اگر فقط می خواهید تا زمانی که باتری شارژ می شود از دستگاه استفاده کنید مشکلی وجود ندارد . در واقع این نکته در مورد استفاده های طولانی مدت باید رعایت شود.

۷. نکته مهم دیگر در این زمینه این است که نور صفحه را تا جایی که امکان دارد کم کنید تا حجم کمتری از باتری مصرف شود . همچنین از برنامه هایی که در حال استفاده از آنها نیستید خارج شوید . باز بودن برنامه های بدون استفاده به تعداد زیاد به دلیل درگیر کردن پردازنده لپ تاپ مصرف باتری را تا حد زیادی افزایش می دهد.

۸. نکته آخر در این زمینه داشتن یک باتری یدک است تا در هنگام نیاز سریعا آن را عوض کنید.

۹. جمع بندی :پیشنهاد می کنم برای افزایش طول عمر باتری لپ تاپ موارد زیر را بخاطر داشته باشید:

۱۰. تا زمانی که واقعا به باتری نیاز ندارید آن را جدا کرده و از برق مستقیم استفاده کنید؛ زیرا هر باتری بسته به نوع آن دارای طول عمر مشخصی در حدود چند هزار ساعت است که با هربار استفاده، از عمر آن کاسته می شود.

۱۱. در هنگام استفاده لپ تاپ با باتری، آن را روی حالت Power Saver قرار دهید؛ برای اینکار روی آیکن باتری کنار ساعت کلیک و گزینه Power Saver را برگزینید تا نور صفحه و مدت زمان روشن بودن آن برای صرفه جویی در مصرف باتری تنظیم شود.

۱۲.حتما نرم افزارهای اضافی را ببندید؛ زیرا آنها باعث افزایش میزان استفاده از هارد، رم و cpu لپ تاپ شده و مصرف باتری را بالا می برند.

۱۳.دقت کنید مکان قرارگیری لپ تاپ بگونه ای نباشد که در ناحیه باتری حرارت زیاد شود.

آشنایی با ریسک‌های امنیتی گوشی‌های هوشمند

امروز شاهد هستیم که شایع‌ترین وسیله برای دسترسی به اینترنت همین گوشی‌های هوشمند هستند. با توجه به استفاده گسترده و روزافزون از این وسایل ارتباطی، مرور کلی بر ریسک‌ها، فرصت‌ها و توصیه‌های لازم برای استفاده ایمن از گوشی‌های هوشمند ضروری به‌نظر می‌رسد.

ریسک‌های امنیتی به ترتیب اولویت عبارتند از:

۱. افشای اطلاعات گوشی هوشمند در نتیجه گم‌کردن یا سرقت؛

گوشی‌های هوشمند به‌سرقت‌رفته یا گم‌شده کاملا مستعد لو رفتن اطلاعات صاحب خود هستند، به‌خصوص اگر حافظه یا رسانه‌های جداشدنی محافظت نشده باشد. در چنین وضعیتی هکر یا مهاجم اجازه خواهد داشت تا به داده‌های ذخیره‌شده روی آن دسترسی داشته باشد؛ بنابراین اولین اولویت برای محافظت از اطلاعات شخصی و محرمانه،حفاظت فیزیکی از گوشی هوشمند است.

۲. افشای ناخواسته اطلاعات گوشی هوشمند؛

کسانی که از گوشی‌های هوشمند استفاده می‌کنند، همیشه از تمام قابلیت‌های برنامه گوشی‌های هوشمند آگاه نیستند. ممکن است آنها نسبت به اجرای یک برنامه کاربردی با صراحت رضایت دهند، غافل از اینکه ممکن است آن برنامه کاربردی در حال جمع‌آوری، انتشار و ردیابی اطلاعات شخصی باشد. به‌عنوان مثال، استفاده از برنامه‌های کاربردی ناوبری وسایل حمل‌ونقل روی گوشی هوشمند ممکن است موجب افشای اطلاعات باارزشی شود.

جمع‌آوری و پردازش خودکار تمام داده‌های شخصی دردسترس در گوشی‌های هوشمند کار آسانی نیست. از این‌رو شیوه سارقان اطلاعات دیجیتال به این شکل است که با طراحی برنامه‌های کاربردی موبایل، استفاده‌کننده‌ها از گوشی‌های هوشمند را ترغیب به استفاده از برنامه کاربردی خود می‌کنند. با اجرای چنین برنامه‌هایی که نقش طعمه را بازی می‌کنند، در هر مرحله و با کسب رضایت کاربر و بدون نیاز به مجوز دسترسی دیگر، بخشی از داده‌های روی گوشی هوشمند را به‌دست می‌آورند. به‌عنوان مثال، برخی از تصاویر قابلیت ثبت موقعیت مکانی را نیز دارند. با دادن امکان دسترسی به

برنامه‌های اشتراک عکس، عملا امکان دریافت اطلاعات مکانی به مهاجم داده می‌شود. استفاده از شبکه‌های اجتماعی هم در گوشی‌های هوشمند به‌صورت ناخواسته به افشای بخشی از اطلاعات شخصی منجر می‌شود. میزان آشنایی کاربر از تنظیمات حریم خصوصی در اکثر نرم‌افزارهای ارتباطات اجتماعی اینترنتی نقشی تعیین‌کننده در میزان افشای اطلاعات وی خواهد داشت.

۳. افشای اطلاعات گوشی که از رده خارج نشده است؛

برای جلوگیری از سرقت هویت مردم و سازمان‌ها، دیسک‌های سخت کامپیوتر را قبل از انهدام کاملا پاک می‌کنند. اما این فرایند پاک‌سازی برای گوشی‌های هوشمند هنوز رخ نداده است، درحالی‌که به مرور زمان گوشی‌های بیشتری در حال بازیافت هستند.

برای نمونه، در مطالعه‌ای که به تازگی انجام شده، تعدادی تلفن همراه دست دوم از eBay خریداری شد و از ۲۶ گوشی هوشمند خریداری‌شده، چهار مورد حاوی اطلاعاتی بود که با استفاده از آن مالک می‌توانست شناسایی شود. هفت مورد شامل اطلاعات کافی برای شناسایی کارفرمای مالک بود؛ ضمن اینکه تیم تحقیقاتی موفق به ردیابی یک تلفن هوشمند مربوط به یک مدیر ارشد فروش یک شرکت شده بود که شامل کلی از اطلاعات شخصی وی بود.

۴. حملات فیشینگ؛

هکرها با استفاده از برنامه‌های جعلی، ایمیل و پیام‌هایی ارسال می‌کنند که به‌نظر می‌رسد واقعی باشند. آنها به‌واسطه این پیام‌های جعلی قادرند اطلاعات حساس کاربر مانند کلمات عبور و شماره کارت اعتباری را به‌دست آورند.

حملات فیشینگ یک تهدید شناخته‌شده برای کاربران رایانه‌های شخصی سنتی است. حملات فیشینگ در واقع پلتفرم مستقلی دارد، به همین دلیل به‌هیچ‌وجه نیازی به نصب برنامه یا اجرای کد روی دستگاه کاربر ندارند و تغییری بر عملکرد گوشی قربانی از نظر سرعت پردازش نخواهند داشت، از این‌رو شناسایی خودکار آنها دشوار است. دلایلی وجود دارد که نشان‌دهنده اهمیت خطر فیشینگ برای کاربران گوشی‌های هوشمند است. گوشی‌های هوشمند به نسبت رایانه‌های شخصی، صفحه‌نمایش کوچک‌تری دارند، از این‌رو هکرها می‌توانند به‌راحتی اعتماد کاربران را با فریب آنها نشانه رفته و اطلاعات مطلوب خود را کسب کنند. همچنین گوشی‌های هوشمند کانال‌های اضافی برای فیشینگ ارایه می‌کنند. برای مثال کاربران ممکن است در مورد پیام‌های SMS فیشینگ (SMiShing) کمتر محتاط باشند.

۵. جاسوس‌افزارهای موبایل؛

همچون رایانه‌های شخصی، گوشی‌های هوشمند هم مستعد آلوده‌شدن به جاسوس‌افزارها هستند. با فراگیر شدن استفاده از سیستم‌عامل‌های موبایل همچون اندروید، جاسوس‌افزارهایی برای آنها توسعه‌یافته که بی‌هدف به استخراج اطلاعات

موجود در آنها می‌پردازند. مطالعات نشان می‌دهد که از هر پنج برنامه کاربردی اندروید، یکی درخواست دسترسی به اطلاعات محرمانه یا حساس گوشی را دارند. اطلاعاتی چون مکان، دفترچه تلفن، دسترسی به اینترنت و... . همچنین مرورگرهای اینترنت به‌منظور تکمیل خودکار فیلدها، برخی اطلاعات را کش می‌کنند. آلوده‌شدن برنامه کاربردی موبایل به جاسوس‌افزار، اطلاعات محرمانه و حساس را در معرض خطر قرار می‌دهد. دسترسی به داده‌های کش‌شده توسط جاسوس‌افزار هم می‌تواند موجب افشای اطلاعات شخصی شود.

علاوه بر چالش‌های امنیتی بررسی‌شده، خطرات دیگری هم در کمین استفاده‌کننده‌های گوشی‌های هوشمند هستند. نقاط دسترسی WiFi جعلی یکی از ترفندهای هکرها برای دسترسی به جریان ارتباطات داده‌ای گوشی‌های هوشمند است. بدافزارهای مالی هم یکی از دغدغه‌های همیشگی برای گوشی‌های هوشمند است.چالش دیگری هم در شبکه‌های تلفن همراه وجود دارد که به نسبت بقیه مشکلات، ارتباط کمتری با استفاده‌کننده‌های گوشی‌های هوشمند دارد، اما به هر حال آنها را هم تحت تاثیر قرار می‌دهد. فرستادن پیام‌های تصادفی سیل‌آسا روی شبکه تلفن همراه و درگیر کردن منابع پردازشی و ارتباطی با هدف ایجاد وقفه در سرویس‌های موبایل ترفندی است که هکرها برای از کار انداختن شبکه‌های تلفن همراه به‌کار می‌برند. این نوع حملات سایبری به لحاظ جغرافیایی می‌توانند دامنه وسیع‌تری به خود اختصاص دهند. شبکه قدرتمند و پایای تلفن همراه که زیرساخت امنیتی آن به‌درستی فراهم شده باشد، می‌تواند به‌خوبی در مقابل چنین حملاتی پایدار بماند. این چالش امنیتی بیشتر از گوشی‌های قدیمی موبایل، گوشی‌های هوشمند را تحت تاثیر قرار می‌دهد؛ چراکه ماژول‌های ارتباطی این گوشی‌ها متنوع‌تر و آسیب‌پذیرتر خواهد بود. بهترین راهکار مواجه با این مشکل، انتخاب صحیح اپراتور تلفن همراه است.با توجه به توضیحات ارایه‌شده، می‌توان عمده مشکلات و آسیب‌پذیری‌های گوشی‌های هوشمند را در ۲ قالب کلی در نظر گرفت؛ دغدغه‌های امنیتی نرم‌افزاری و سخت‌افزاری. از یک جنبه، چالش‌های امنیتی سخت‌افزاری با محافظت فیزیکی از گوشی هوشمند مرتبط هستند و با رعایت اصول نگهداری صحیح و گم نکردن گوشی می‌توانند رفع شوند. از این جنبه، توجه جدی به پاک‌سازی کامل اطلاعات شخصی هنگام از رده خارج‌کردن گوشی هوشمند هم ضروری خواهد بود. جنبه دیگر، بحث برنامه‌های کاربردی موبایل مورد استفاده و اطمینان از آلوده نشدن آنها به بدافزارهای مختلف موبایل است که با رعایت نکات ذکر شده می‌توان از بروز بخش عمده‌ای از این مشکلات نرم‌افزاری جلوگیری کرد.


دستگاه شما چه چیزهایی دربارهٔ شما می داند؟
فرقی نمی کند که از رایانه استفاده می کنید یا تلفن همراه. دستگاه شما حجم قابل توجهی از اطلاعات مهم و شخصی شما را در خود ذخیره می کند. وجود این اطلاعات در هنگام وقوع حملات سایبری خطرناک بوده و شما را آسیب پذیر می کند.
تلفن هوشمند
تبلت‌های اندرویدی
مکینتاش
ویندوز
اطلاعات شخصی و امنیتی مهم
دانلود اطلاعات فرم های مالیاتی
شماره های کارت های اعتباری
ذخیره توسط مرورگرها
دانلود رسیدهای تراکنش کارت اعتباری
کلمه های عبور
ذخیره توسط مرورگرها
ذخیره در فایل سیستم
پیام و پیامک ها
لاگ پیام های ارسالی در دستگاه ذخیره می شود.
تماس های تلفنی
لاگ تماس ها در دستگاه ذخیره می شود.
نام ها و آدرس ها
ذخیره توسط مرورگرها
در دفترچه تماس ویندوز
در Address Book
در Contact manager
سایت های اخیراً بازدید شده
کش مرورگر
تاریخچه مرورگر
کوکی ها
مکان هایی که اخیراً حضور داشته اید
اپلیکیشن های مدیریت و ناوبری تصاویر
موقعیت جغرافیایی فعلی
خواندن اطلاعات سیستم موقعیت یاب (GPS)
دفترچه تلفن
در دفترچه تماس ویندوز
در Address Book
در Contact manager
فایل اخیراً استفاده شده
ذخیره به صورت لیست در سیستم عامل
اپلیکیشن ها لیست فایل های مربوط به خود را ذخیره می کنند.
فایل های حذف شده
تا زمانی که در فضای ذخیره سازی فیزیکی اطلاعات تازه ای درج نشده است، تمامی فایل های حذف شده از سیستم قابل بازیابی هستند.
اطلاعات حساب های بانکی
دانلود اطلاعات حساب های بانکی
اطلاع از مجموعه اطلاعاتی که در دستگاه شما ذخیره می شوند اولین گام در حافظت و حفظ امنیت آنها محسوب می شود.
آمار و اطلاعات جرائم سایبری
درصد کاربران ایالات متحده که متوجه قربانی شدن خود در فضای مجازی نشده اند:
۲
درصد کاربران ایالات متحده که عقیده دارند مجرمین سایبری به دادگاه کشیده نخواهند شد:
۷۸
درصد کاربران ایالات متحده که حداقل یک بار قربانی جرایم رایانه شده اند:
۷۳
قربانیان ایمیل های آلوده ای در هر روز:
۲۰۰۰
ایمیل های آلوده ای که هر روز ارسال می شود.
۷۵ میلیون
متوسط ضرر مالی قربانیان جرایم رایانه در هر ماه:
۱۲۸ دلار