



گروه فناوری //

کارشناسان فعال در حوزه امنیت سایبری راهکارهای مهمی را که می‌تواند امنیت گوشی و اطلاعات شخصی کاربران را بالا ببرد و مانع نفوذ هکرها شود، معرفی کرده‌اند.

با توجه به اهمیت روزافزون حفاظت از اطلاعات شخصی و امنیت سایبری دستگاه‌های الکترونیکی و گوشی‌های هوشمند، امنیت اطلاعات آنها تبدیل به یکی از بزرگترین دغدغه‌های بسیاری از کاربران در فضای مجازی شده است.

به گزارش ایتنا از ایسنا، کارشناسان فعال در حوزه فناوری و امنیت سایبری خطاب به کاربران گوشی‌های هوشمند توصیه کرده‌اند که با رعایت نکات و موارد مختلفی قادر خواهند بود که امنیت اطلاعات شخصی موجود در گوشی‌های هوشمند خود را به میزان قابل توجهی افزایش داده و از نفوذ هکرها و مجرمان سایبری به اطلاعات و حریم خصوصی خود جلوگیری به عمل بیاورند.

در زیر به مهم‌ترین راهکارهای ارتقای سطح امنیت سایبری گوشی‌های اندرویدی که این کارشناسان در جدیدترین گزارش و بررسی‌های خود منتشر کرده‌اند، خواهیم پرداخت:

۱. فعال سازی ورود دو مرحله‌ای

ورود دو مرحله‌ای یکی از نخستین راه‌هایی است که همواره کارشناسان فعال در حوزه امنیت سایبری به کاربران گوشی‌های هوشمند و دارندگان هرگونه حساب کاربری توصیه می‌کنند. این کار با فعال سازی قابلیت ورود دو مرحله‌ای به کاربران این امکان را می‌دهد تا راه نفوذ هکرها به حساب کاربری و اطلاعات شخصی خود در گوشی سد کرده و مانع ورود آذانه آنها به گوشی شوند.

۲. خرید از برندهای معتبر سازنده گوشی‌های اندروید

به گفته متخصصان امنیتی، آن دسته از برندهای

سازنده گوشی‌های اندرویدی که از اعتبار بالایی برخوردارند و همواره نسخه‌های به‌روزرسانی سیستم عامل اندروید را زود به زود و بلافاصله بعد از رونمایی نسخه جدید اندروید، عرضه کرده و در اختیار کاربران قرار می‌دهند، باید برای خریداری گوشی توسط کاربران در اولویت قرار بگیرند.

۳. فعال سازی قفل گوشی با پین کد

با اینکه دیگر کمتر کسی پیدا می‌شود که همچنان از کدهای امنیتی معروف به PIN Code های شرکت سازنده موبایل به هنگام روشن و خاموش کردن گوشی استفاده کند، اما همچنان بسیاری از متخصصان امنیتی بر این باورند که فعال سازی قفل گوشی با این کدهای امنیتی تا حد زیادی قادر است از نفوذ هکرها جلوگیری به عمل بیاورد.

۴. داندلود اپلیکیشن از فروشگاه معتبر گوگل پلی

استور

یکی از توصیه‌های امنیتی که همواره کارشناسان فعال در این حوزه خطاب به کاربران عنوان می‌کنند، آن است که کاربران باید تنها از پلتفرم فروشگاه معتبر گوگل پلی استور اقدام به داندلود، دریافت و نصب اپلیکیشن کنند و به هیچ عنوان از سایر فروشگاه‌های غیر معتبر و محلی که معمولاً در بسیاری از کشورهای جهان وجود دارد، برنامه داندلود نکنند.

۵. از وی پی ان (VPN) استفاده کنید!

در صورتی که در کشوری خارجی هستید و یا امکان استفاده از اینترنت همراه (دیتا) را ندارید و مجبورید برای اتصال به شبکه فضای مجازی و انجام کار اینترنتی خود، به اینترنت وای‌فای عمومی و رایگانی که در اماکن عمومی وجود دارد، متصل شوید بهتر است طبق نظر کارشناسان و متخصصان امنیتی، ابتدا به یک

یکی از توصیه‌های امنیتی که همواره کارشناسان فعال در این حوزه خطاب به کاربران عنوان می‌کنند، آن است که کاربران باید تنها از پلتفرم فروشگاه معتبر گوگل پلی استور اقدام به داندلود، دریافت و نصب اپلیکیشن کنند و به هیچ عنوان از سایر فروشگاه‌های غیر معتبر و محلی که معمولاً در بسیاری از کشورهای جهان وجود دارد، برنامه داندلود نکنند



توصیه‌های کارشناسان

برای ارتقای امنیت اندروید

نرم افزار وی پی ان (VPN) معتبر وصل شده و سپس از خدمات اینترنتی بهره مند شوید.

۶. مدیریت دقیق و به موقع گذرواژه

گذرواژه ورود به گوشی در کنار سایر رمزهای عبور حساب‌های کاربری مختلفی که کاربر از آنها به صورت آنلاین و آفلاین استفاده می‌کند، یکی از راه‌های نفوذ هکرها به حریم خصوصی قربانیان به شمار می‌رود بنابراین کاربران باید توجه ویژه‌ای به مدیریت دقیق و درست گذرواژه‌های مورد استفاده خود داشته باشند و هر از گاهی طبق توصیه کارشناسان و متخصصان امنیتی، آنها را تعویض کرده و به

سایبری گوشی و اطلاعات شما کند.
۸. خاموش و غیر فعال سازی اتصالات گوشی به‌هنگام عدم نیاز
در صورتی که به اینترنت یا بلوتوث نیازی ندارید، تنها می‌اتصالات گوشی همچون اینترنت وای‌فای، دیتا (اینترنت همراه)، بلوتوث و آن‌اف‌سی را قطع کنید بدین ترتیب می‌توانید احتمال و ضریب نفوذ هکرها و مجرمان سایبری را دست کم در مدت زمانی که به آنها از طریق اتصالات گوشی اجازه ورود نمی‌دهید، را به حداقل برسانید.

۹. لغو نصب اپلیکیشن‌های بی‌استفاده در گوشی

در صورتی که شما نیز جز آن



نکات ایمنی مربوط به آن نیز دقت کنند.

۷. نصب و استفاده از نرم افزارهای معتبر آنتی‌ویروس

نصب آنتی‌ویروس‌های معتبری که در فروشگاه‌های آنلاین معتبر و قابل اعتماد همچون گوگل پلی استور وجود دارند و در دسترس کاربران گوشی‌های اندرویدی قرار گرفته اند، می‌تواند تا حد زیادی کمک بسزایی به ارتقای سطح امنیت

مرورگر اینترنت اکسپلورر را دور بیندازید!

به تازگی محققان و کارشناسان امنیتی به کاربران هشدار داده‌اند که مرورگر اینترنت اکسپلورر از رایانه خود به طور کلی حذف کنند.
چندی پیش کارشناسان و پژوهشگران فعال در حوزه امنیت سایبری به کاربران در فضای مجازی اعلام کرده‌اند که به هیچ عنوان از مرورگر اینترنت اکسپلورر (internet explorer) استفاده نکنند چرا که مایکروسافت مدت‌ها قبل اعلام کرده بود که دیگر از این مرورگر اینترنتی پشتیبانی نکرده و برای آن نیز به روزرسانی‌های امنیتی و نرم‌افزاری ارائه نخواهد داد همین امر کافی است تا دلیل محکمی به شمار بیاید تا کاربران دیگر از آن استفاده نکنند.
امنیت سایبری و حفاظت از حریم خصوصی کاربران یکی از مسائلی است که در سال‌های اخیر از اهمیت بیشتر و بسزایی برخوردار شده است. اما حالا به تازگی گزارش‌های منتشر شده از سوی کارشناسان امنیتی نشان می‌دهد که علاوه بر آن که استفاده از مرورگر اینترنت اکسپلورر می‌تواند برای حریم خصوصی کاربران در دسترس‌زا و خطر آفرین باشد و به هکرها اجازه نفوذ و دسترسی به اطلاعات شخصی آنها را بدهد، بلکه حتی عدم استفاده از این مرورگر اینترنتی نیز می‌تواند به همان اندازه برای آنها خطر آفرین و از لحاظ امنیتی مشکل ساز باشد. این کارشناسان بر این باورند که نقص‌های امنیتی و آسیب پذیری‌های موجود در مرورگر مذکور این امکان را به هکرها و مجرمان سایبری می‌دهد تا تمامی داده‌های مورد نظر خود را از رایانه کاربران به سرعت برده و به آنها دسترسی پیدا کنند و برای اهداف و انگیزه‌های شما خود از آنها سو استفاده کنند.

تلفن‌های همراه و افزایش ۱۰ درصدی حواس‌پرتی رانندگان در سال ۲۰۱۸

گروه فناوری //

محققان در پی پژوهشی جدید دریافته‌اند که به شمار رانندگانی که در هنگام رانندگی با تلفن همراه هوشمند خود کار می‌کنند نسبت به سال ۲۰۱۸ میلادی ده درصد افزوده‌شده است.

محققان در پی پژوهشی جدید دریافته‌اند که به شمار رانندگانی که در هنگام رانندگی با تلفن همراه هوشمند خود کار می‌کنند نسبت به سال ۲۰۱۸ میلادی ده درصد افزوده‌شده است.

به گزارش ایتنا به نقل از وب‌سایت خبری تحلیلی cnet، این پژوهش جدید براساس اطلاعات ناشناس از ۱٫۸ میلیون راننده است که در مجموع ۴٫۵ میلیون مایل در جاده را طی کرده‌اند. ای اطلاعات از طریق نرم‌افزار کمپانی Zendrive جمع‌آوری شد که برای نظارت بر رفتار رانندگان و اخطار به آن‌ها در صوت درگیر شدن در فعالیت‌های مخاطره‌آمیز را دارد.

اطلاعات جمع‌آوری‌شده حاکی از آن بود که افراد معناد به تلفن‌های همراه هوشمند (افرادی که بیش از ۱۰ درصد از زمان خود را در حین رانندگی صرف کار با تلفن همراه خود می‌کنند) در ۲۸ درصد از مواقعی که پشت فرمان اتومبیل خود هستند، جاده را نادیده می‌گیرند و به دستگاهشان توجه می‌کنند. اطلاعات Zendrive نشان می‌دهد که فعالیت‌های شایع حین رانندگی شامل صحبت کردن، پیام دادن، استفاده از نرم‌افزارهای جهت‌یاب یا انتخاب موسیقی است.

پژوهشی دیگر که جامعه آماری ۵۰۰ نفر را در برداشت از رانندگان نشان داده که خطرات رانندگی با حواس‌پرت از هیچ‌کس پوشیده نیست. حدود ۸۵ درصد از پاسخگوها اعلام کرده بودند که انجام این کار مشکل‌ساز خواهد بود.
باین‌حال ۴۷ درصد آن‌ها اعتراف کرده بودند که در حدود ۱۰ درصد از زمان خود را در حین رانندگی صرف کار با تلفن همراه هوشمند می‌کنند. البته مطالعه دیگری که از جانب یکی از موسسه‌های بیمه در ایالات متحده انجام شده بود نشان داد که احتمال استفاده از تلفن‌های همراه هوشمند در حین رانندگی نسبت به سال ۲۰۱۴ میلادی به میزان ۵۷ درصد افزایش داشته است. نتیجه‌گیری نهایی حاکی از آن است که شمار افرادی که از خطرات استفاده از تلفن همراه در حین رانندگی آگاه هستند ولی باین‌وجود این کار مخاطره‌آمیز را کنار نگذاشته‌اند، رو به افزایش است.

نرم‌افزاری که هکرها را به حساب بانکی‌تان هدایت می‌کند!

گروه فناوری //

کارشناسان امنیتی به تازگی دریافته و اعلام کرده‌اند که نرم افزار معروف ویرایش محتوای چندرسانه‌ای VSDC به هکرها اجازه ورود و نفوذ به اطلاعات حساب‌های بانکی کاربران را می‌داده است.

با توجه به افزایش روزافزون اهمیت امنیت سایبری و حفاظت از حریم خصوصی کاربران در فضای مجازی، بسیاری از کارشناسان و پژوهشگرانی که در حوزه امنیت سایبری فعالیت و تحقیق می‌کنند، به بررسی آسیب‌پذیری و حفره‌های امنیتی موجود در نرم‌افزار و سرویس‌های مختلف اقدام می‌کنند تا کاربران در فضای مجازی از احتمال نفوذ هکرها و مجرمان سایبری به اطلاعات شخصی آنها مطلع شده و هم زمان شرکت‌های توسعه‌دهنده نرم افزارهای مذکور نیز به برطرف کردن مشکل امنیتی مربوطه بپردازند و یک نسخه به‌روزرسانی جدید از آن راهپه و منتشر کنند. به گزارش ایتنا از ایسنا، در سال‌های اخیر اخبار و گزارش‌های متعددی از سوی رسانه‌های مختلف در سراسر جهان منتشر می‌شود که همواره نشان می‌دهد هکرها و مجرمان سایبری با استفاده از انتشار بدافزار، جاسوس افزار و تروجان‌های پیشرفته به حساب‌های کاربری و اطلاعات شخصی کاربران نفوذ پیدا کرده و از آنها برای اهداف و انگیزه‌های شوم خود سو استفاده کنند.

تازه‌ترین اخبار و گزارش‌های منتشر شده در وب سایت هکرنیوز حاکی از آن است که نرم افزار معروفی که تاکنون برای ویرایش محتوای چندرسانه‌ای توسط خیل عظیمی از کاربران مورد استفاده قرار می‌گرفته است، حالا با انتشار یک تروجان خطرناک به هکرها و مجرمان سایبری این امکان را می‌داده تا با نفوذ به حساب‌های بانکی کاربران به اطلاعات شخصی موردنظر آنها دسترسی پیدا کنند.

نرم‌افزارهای از پیش نصب شده روی دستگاه‌های اندرویدی و خطر امنیتی بزرگ

گروه فناوری //

نرم‌افزارهای اندرویدی از پیش نصب شده گاهی بسیار کاربردی و گاهی فقط دست‌وپا گیر هستند اما محققان به تازگی کشف کرده‌اند که این نرم‌افزارها ممکن است حریم خصوصی دستگاه شما را به خطر بیندازند.

نرم‌افزارهای اندرویدی از پیش نصب شده گاهی بسیار کاربردی و گاهی فقط دست‌وپا گیر هستند اما محققان به تازگی کشف کرده‌اند که این نرم‌افزارها ممکن است حریم خصوصی دستگاه شما را به خطر بیندازند. به گزارش ایتنا از شماران سیستم به نقل از وب‌سایت خبری تحلیلی theinquirer، در پژوهشی که به‌تازگی توسط محققان انجام شده است، برخی از فروشندگان تلفن‌های همراه، دستگاه‌های برند خود را با نرم‌افزارهایی پرمی‌کنند که اطلاعات خصوصی کاربران را می‌دزدند.

این محققان ۱۷۰۰ دستگاه از ۲۰۰ تولیدکننده را مطالعه کردند که در مجموع دارای ۸۲ هزار نرم‌افزار از پیش نصب شده بودند. آنها در بررسی‌های خود به این نتیجه رسیدند که بسیاری از تلفن‌های همراه هوشمند با نرم‌افزارهای از پیش نصب شده غیر از گوگل بدون اطلاع کاربر دسترسی افراد سوم شخص به اطلاعات آنها را ممکن می‌سازند. به این ترتیب داندلود کردن یک نرم‌افزار سوم شخص و اجازه به دسترسی به بخش‌های مختلف تلفن همراه توسط کاربر تا حدودی قابل توجیه است، اما دزدی اطلاعات از سوی نرم‌افزارهایی که به‌صورت پیش‌فرض روی تلفن‌های همراه هوشمند افراد نصب شده و در اغلب مواقع قابل پاک کردن نیستند به‌هیچ‌عنوان قابل توجیه نیست.

