خبر

قول وزیر برای پیگیری اختلال بازی «کلش آف کلنز»

در پی مسدود شدن دسترسی کاربران ایرانی به بازی موبایلی «کلش آف کلنز»، وزیر ارتباطات و فناوری اطلاعات قول پیگیری این موضوع را داد.

به گزارش «ایران»، وزیر ارتباطات و فناوری اطلاعات در آخرین پست اینستاگرامی خود از پیگیری اختلالات بازی کلش‌آف‌کلنز خبر داد.متن پست واعظی به شرح زیر است: «سلام به دوستان، در چند پست اخیر، اعتراض هایی به اختلال بازی کلش مطرح کرده اید. این مطالب را به اطلاع کمیته تعیین مصادیق مجرمانه خواهم رساند و مطالب مطرح شده را پیگیری خواهم کرد؛ گرچه در بعضی موارد به دلیل استفاده از ادبیات نامناسب مجبور به حذف آنها شدم.» لازم به ذکر است دستور فیلترو اعمال محدودیت برای دسترسی به این بازی موبایلی براساس اجرای بند«ب» ماده ۱۵ قانون جرایم رایانه ای از سوی این کارگروه صادر شده است. به موجب این ماده قانونی، ترویج و آموزش اعمال خشونت آمیز از طریق سامانه ها و شبکه های رایانه ای جرم است و کارگروه تعیین مصادیق محتوای مجرمانه این بازی را خشونت آمیز تشخیص داده است.

بازنگری در مقررات استفاده از امکانات پایه‌ای مخابرات

کمیسیون تنظیم مقررات ارتباطات، با هدف استفاده تمامی اپراتورهای ارتباطی از امکانات شبکه مخابرات کشور، مقررات ارائه و استفاده از این امکانات را اصلاح کرد.

به گزارش مهر، کمیسیون تنظیم مقررات ارتباطات در جلسه شماره ۲۴۷ خود، مصوبه شماره ۲۳۰ خود را در مورد مقررات ارائه و استفاده از امکانات پایه‌ای شرکت مخابرات ایران بازنگری و اصلاح کرد. از آنجایی که مصوبه ۹۷ کمیسیون تنظیم مقررات ارتباطات هیچ گاه به معنای واقعی اجرا نشد و شرکت‌های اینترنتی (PAP) و مخابرات نتوانستند بر سر استفاده از تجهیزات و امکانات شبکه مخابراتی کشور، به توافق برسند، با پایان یافتن پروانه فعالیت شرکت‌های PAP و ورود بازیگران جدید به عرصه ارتباطات کشور (از جمله دارندگان پروانه خدمات ارتباطات ثابت FCP)، کمیسیون تنظیم مقررات ارتباطات، شرایط جدیدی را برای استفاده از امکانات شبکه مخابراتی کشور، وضع و مصوبه ۲۳۰ را جایگزین مصوبه ۹۷ اعلام کرد.هم‌اکنون بار دیگر و با گذشت حدود ۷ ماه از مصوبه قبلی، این کمیسیون مصوبه آیین نامه تعاملی مخابرات و شرکت‌های اینترنتی را اصلاح کرد. برمبنای این مصوبه جدید، شرکت مخابرات ایران موظف شده حداکثر ظرف مدت ۷۲ ساعت از تاریخ درخواست شرکت‌های ارائه‌کننده خدمات اینترنت، نسبت به دایر کردن یا تخلیه خطوط مشترکان (رانژه) اقدام کند. در صورت اجرایی نشدن این الزام، اخذ مبالغ رانژه (مطابق با بند ۴-۱ مصوبه قبلی) مجاز نبوده و شرکت مخابرات ایران موظف به دایر کردن و تخلیه خطوط مشترکان حداکثر ظرف مدت ۷۲ ساعت از تاریخ ابلاغ سازمان تنظیم مقررات ارتباطات خواهد بود.

آغاز احراز هویت کاربران

با اضافه شدن بخش کانال تلگرام و صفحه شخصی در رسانه‌های کاربرمحور مانند صفحات اینستاگرام و پروفایل‌های کلوب به سامانه ساماندهی وزارت ارشاد به آدرس samandehi.ir، احراز هویت فعالان فضای مجازی ممکن شد.

به گزارش فارس، ثبت‌نام برای احراز هویت کانال‌های تلگرامی بیش از ۵هزار عضو پیرو مصوبه شورای عالی فضای مجازی آغاز شده است. هدف این اقدام، ساماندهی فعالان فضای مجازی و تابع قانون شدن فعالیت‌های این عرصه اعلام شده است.سامانه جدید روی سامانه ساماندهی سابق وزارت ارشاد به آدرس samandehi.ir پیاده‌سازی شده و بخش کانال تلگرام و صفحه شخصی در رسانه کاربر محور (مانند صفحات اینستاگرام و پروفایل‌های کلوب) به این سامانه اضافه شده است. دارندگان این شبکه‌ها برای ثبت‌نام و احراز هویت یک ماه فرصت دارند.

فناورانه

شارژ تلفن همراه با حرکت مچ دست

یک استارتاپ امریکایی شارژر موبایلی ساخته که در مشت فرد جا می‌گیرد و با استفاده از گرمای بدن الکتریسیته تولید می‌کند. به گزارش دیجیتال ترند، این شارژر که Hand Energy نام دارد، دستگاهی بسیار کوچک است که قابلیت شارژ وسایل الکترونیکی در هر نقطه و هر زمانی را فراهم می‌کند. نکته جالب آنکه برای تأمین شارژ از انرژی صاحب خود بهره می‌گیرد. کاربر برای استفاده از Hand Energy باید حلقه استارت را تکان دهد. این امر سیگنالی برای فعال کردن روتر ارسال می‌کند، در این زمان کاربر باید مچ خود را بچرخاند تا عمل چرخش روتر نیز ادامه یابد. روتر داخل این دستگاه طی یک دقیقه پنج هزار مرتبه می‌چرخد. به این ترتیب انرژی مکانیکی به جریان الکتریسیته تبدیل می‌شود.

آن سوی خبر

کاربران به دنبال دکمه ویرایش در «توئیتر»

جک دورسی مدیر عامل توئیتر از کاربران پرسیده که این شرکت برای ارتقا و افزایش خلاقیت در سال ۲۰۱۷ چه می‌تواند بکند و ظاهراً پاسخ‌های کاربران وی را به فکر افزودن دکمه ویرایش به توئیتر انداخته است.

به گزارش ری کد، در میان انبوه پاسخ‌هایی که توسط کاربران توئیتر برای جک دورسی مدیر عامل این شرکت ارسال شده این پاسخ بیش از بقیه پاسخ‌ها به چشم می‌خورد: افزودن دکمه ویرایش برای توئیت‌ها. اما کاربران پیشنهادهای دیگری هم داشته‌اند. از جمله این پیشنهادها می‌توان به اضافه کردن دکمه بوکمارک و ارتقای امنیت و تسهیل ارسال گزارش در مورد مزاحمت‌ها اشاره کرد. به دنبال ارسال پیشنهادهای یاد شده دورسی گفته که توئیتر در حال بررسی تمامی پیشنهادهای ارائه شده از جمله پیشنهاد مربوط به ویرایش توئیت‌هاست. دورسی حتی در مورد نحوه اضافه شدن دکمه ویرایش به توئیتر هم پیشنهادهایی داده است. از جمله اینکه برای این کار ۵ دقیقه فرصت در نظر گرفته شود یا کاربران بتوانند هر زمان که تمایل داشتند عمل ویرایش را انجام دهند.

۲۰۱۶، سال بزرگ‌ترین هک‌های تاریخ

میثم لطفی

هنوز هم تیتر اول بسیاری از روزنامه‌های بزرگ جهان به ماجرای فعالیت‌های هکری روسیه در انتخابات ریاست جمهوری امریکا اختصاص دارد و البته کارشناسان امنیتی می‌گویند این تنها اتفاق سایبری بزرگ سال ۲۰۱۶ نیست و دنیای فناوری شاهد جرایم سایبری بزرگتری هم بوده است. در حقیقت می‌توان گفت اتفاقات بزرگی که صورت گرفت، باعث شد تا ۲۰۱۶ به لقب «سال هک» معرفی شود. این عنوان از سوی بسیاری از مراکز امنیتی بزرگ مطرح شد و کارشناسان اعلام کردند بیشترین میزان حملات هکری بزرگ تاریخ در طول سال ۲۰۱۶ صورت گرفت.

■ **حملات سایبری بی سابقه**

برچسب حملات سایبری بزرگ که به سال ۲۰۱۶ اطلاق شد، به نحوه بروز این اتفاقات هم مربوط می‌شد. در تاریخ ۲۱ اکتبر سال جاری یک حمله سایبری از نوع DDoS به شرکت ارائه دهنده خدمات زیرساخت‌های اینترنتی Dyn باعث شد دسترسی به خدمات نتفلیکس، فیس‌بوک، توئیتر و رسانه‌های بزرگی چون گاردین، سی‌ان‌ان، نیویورک تایمز، وال استریت ژورنال و... از کار بیفتد. نوع عملیات هکری که انجام شد به گونه‌ای بود که بسیار مورد توجه قرار گرفت. هکرها در این اتفاق از دستگاه‌های روزمره متصل به اینترنت از جمله وب کم، گوشی هوشمند و سیستم‌های ضبط دیجیتال صدا استفاده کردند تا به سرور مرکزی دسترسی پیدا کنند.

ماه گذشته بانک بزرگی که مدیریت آن را فروشگاه زنجیره ای Tesco بریتانیا برعهده دارد مورد حملات مشابه قرار گرفت و براساس آن ۲.۵ میلیون پوند از حساب کاربری ۹ هزار مشتری به سرقت رفت.

طولی نکشید که خبر هک بزرگ حساب‌های کاربری یاهو به گوش رسید و دامنه این اتفاق به قدری وسیع بود که Verizon صاحب جدید یاهو از خرید خود پشیمان شد و مسأله پس دادن شرکت مذکور و دریافت پول خود را مطرح کرد. البته این عملیات هکری سال ۲۰۱۳ میلادی انجام شده بود، ولی یک ماه قبل در این زمینه افشاگری شد که حساب کاربری بیش از یک میلیارد مشترک پلتفرم یاهو مورد حمله قرار گرفته است و این اتفاق به‌عنوان بزرگترین هک تاریخ معرفی شد. این خبرها در حالی منتشر شد که سپتامبر امسال گفته شده بود در سال ۲۰۱۴ میلادی یک اتفاق ساده به هکرها امکان داد اطلاعات شخصی بیش از ۵۰۰میلیون نفر از کاربران یاهو لو برود.

روسیه تنها کشوری نبود که در عملیات‌های هکری بزرگ سال ۲۰۱۶ دست داشت و در کنار آن دیگر کشورها هم اتفاقات مشابه را دنبال کردند. در چهار ماه نخست سالی که گذشت، کشمکش‌های اپل و دولت امریکا علنی شد و پلیس فدرال ایالات متحده (FBI) اعلام کرد که در جریان ماجرای سَن برناردینو، اپل موظف است قفل آیفون شخصی به نام «سید فاروق» که فعالیت تروریستی انجام داد و کشته شد را باز کند که البته شرکت سازنده گوشی هوشمند مذکور زیر بار نرفت.

■ **ناامنی‌های متوالی**

«ریچارد استینون» نویسنده مشهوری است که بتازگی کتابی را با نام «جنگ سایبری در راه است» منتشر کرده است. او در مصاحبه اخیر خود توضیح داد: «۲۰۱۶ سالی بود که بیشترین تعداد حملات هکری بزرگ تاریخ در آن ثبت شد. ابزارهای جاسوسی سایبری برای هکرها و آژانس‌های اطلاعاتی اهمیت زیادی دارند و دست کم از سال ۲۰۰۴ به بعد بسیار مورد توجه قرار گرفته‌اند. با وجود این هک شدن سیستم کمیته ملی حزب دموکرات امریکا بسیار غیرمنتظره بود و هیچ کارشناسی فکر آن را نمی‌کرد.» او همچنین توضیح داد که آموزه‌های سالی که گذشت برای سال ۲۰۱۷ میلادی بسیار مفید و کاربردی خواهد بود. اگر کارشناسان اندکی دقت کنند بخوبی درمی یابند چه کسانی در یک سال گذشته عملیات هکری انجام داده‌اند و براین اساس می‌توان پیش‌بینی کرد چه اشخاص یا گروه‌هایی در یک سال آینده چنین حملاتی را مدیریت می‌کنند. با این روند بخوبی می‌توان متوجه شد سازمان‌ها به چه میزان تلاش نیاز دارند تا میزان حفاظت از داده‌های خود را ارتقا دهند.

استینون اظهارداشت که سطح حمایت از داده‌های یک سازمان نیازمند آن است که از نقص‌های مشابه و حفره‌های امنیتی یکسان جلوگیری شود. به هر حال اینکه در جریان یک عملیات هکری اسناد محرمانه یا اطلاعات شخصی سرقت می‌شوند اتفاق خوشایندی نیست، ولی تحلیل و بررسی آن می‌تواند جلوی اتفاقات مشابه را بگیرد.

«کرایگ فاگان» مدیر سیاستگذاری «بنیاد جهانی وب» موسوم به WWW ضمن اعلام موافقت خود با این نظریه اظهارداشت: «هر یک از شهروندان این حق را دارند تا بدانند که داده‌های شخصی آنها به صورت کاملاً ایمن در سرورهای شرکت مربوطه ذخیره شده است و زمانی که آنها آنلاین هستند، تمام اطلاعات آنها به صورت شخصی باقی می‌ماند. مرور اتفاقات هکری و سایبری سال ۲۰۱۶ نشان می‌دهد که دولت‌ها و شرکت‌ها باید فعالیت بیشتری در این زمینه انجام دهند تا ایمنی بیشتری برای کاربران برقرار شود و حقوق سایبری کاربران بیشتر رعایت شود. ۲۰۱۷ باید سالی باشد که تغییرات محسوس در این زمینه دیده شود.»

عکس: ZDnet

■ ۲۰۱۶ سالی بود که بیشترین تعداد حملات هکری بزرگ تاریخ در آن ثبت شد. ابزارهای جاسوسی سایبری برای هکرها و آژانس‌های اطلاعاتی اهمیت زیادی دارند و دست کم از سال ۲۰۰۴ به بعد بسیار مورد توجه قرارگرفته‌اند.

■ بنیاد WWW به این نتیجه رسید که در سال ۲۰۱۶ میلادی عملیات‌های هکری بزرگ با پشتیبانی دولت‌ها صورت گرفت وهم اکنون این نگرانی وجود دارد که در سال جدید میلادی عمق این حملات افزایش یابد و کاربران شاهد اتفاقات بزرگتری در این زمینه باشند.

نیم نگاه

■ **گسترش فعالیت‌های هکری**

به نظر می‌رسد میزان حملات سایبری همچنان در حال افزایش است و طی سال ۲۰۱۷ میلادی تهدیدهای بیشتری کاربران را مورد هدف قرار دهد. اداره پلیس مرکزی اتحادیه اروپا (Europol) سپتامبر امسال با انتشار گزارشی تحت عنوان «ارزیابی تهدیدها و جرایم اینترنتی ساماندهی شده در سال ۲۰۱۶» بر این مسأله تأکید کرد که میزان تهدیدهای سایبری همچنان در حال افزایش است.

به گفته «استیون ولیسون» مدیر مرکز جرایم سایبری اروپا در سازمان Europol، در یک سال گذشته دامنه حملات سایبری و میزان اثرگذاری آن روی کاربران شخصی و سازمانی بیش از هر زمان دیگر مشاهده شد و هکرها یاد گرفتند به صورت گسترده‌تر و عمیق‌تر تأثیرات خود را برجا بگذارند.

او در این خصوص گفت: «در یک سال گذشته تهدید باج‌افزارها بیش از هر زمان دیگر مشاهده شد و این قبیل ابزارها براحتی توانستند اثرگذاری خود را نشان دهند. سازمان‌های ارائه دهنده خدمات عمومی از جمله مراکز بهداشتی- درمانی هدف اصلی باج‌افزارها بودند. سازمان Euoropol همچنین دریافت که در یک سال گذشته دستگاه‌های خودپرداز بانک بیش از هر زمان دیگر مورد هدف قرار گرفتند و سرویس‌های پرداخت پول نقد در سراسر جهان چندین بار با حملات سایبری بزرگ مواجه شدند.»

«راب گوئیدری» مدیرعامل شرکت تحلیل شبکه‌های رسانه‌ای SC2 و از مشاوران اسبق فرماندهی مرکزی دولت ایالات متحده اعلام کرد که پول همچنان بزرگترین محرک برای حملات سایبری محسوب می‌شود و بیشتر فعالیت‌های هکری که پول را مورد هدف قرار می‌دهند، از جانب گروه‌های روسی هدایت می‌شود. او توضیح داد: «هکرهای روسی به‌طور ویژه بر عملیات‌هایی نظارت دارند که طی آن داده‌های شخصی با هدف باج‌افزاری و کسب درآمد سرقت شوند. این هکرها به صورت استراتژیک حملات DDoS را مدیریت می‌کنند و در بیشتر مواقع اهداف سیاسی پشت فعالیت آنها مشاهده می‌شود. دولت روسیه طی سال‌های گذشته ارتباط نزدیک با گروه‌های هکری داشته است و به صورت ویژه از آنها استفاده کرده است».

بنیاد WWW به این نتیجه رسید که در سال ۲۰۱۶ میلادی عملیات‌های هکری بزرگ با پشتیبانی دولت‌ها صورت گرفت و این اتفاق در ۱۲ ماه گذشته بیش از هر زمان دیگر مشاهده شد. به هر حال از هم‌اکنون این نگرانی وجود دارد که در سال جدید میلادی عمق این حملات افزایش یابد و کاربران شاهد اتفاقات بزرگتری در این زمینه باشند.

روی وب

تأثیر سرما روی تلفن‌های همراه

برخی افراد از این موضوع که تلفن‌های همراه‌شان هنگام قرار گرفتن در برابر هوای سرد دچار مشکل شود، ابراز نگرانی می‌کنند و البته باید توجه داشت که دما روی عملکرد باتری گوشی‌ها چندان هم بی‌تأثیر نیست.

به گزارش ایسنا، شایعاتی وجود دارد مبنی بر اینکه هوای سرد موجب از کار افتادن باتری‌های تلفن همراه می‌شود، اما هوا باید چقدر سرد باشد که روی این ابزار فناوری تأثیر منفی بگذارد و مشکل ایجاد کند؟ در گزارش وب‌سایت پی‌سی ادوایزر نگاهی به تأثیرات دما روی باتری تلفن‌های هوشمند شده است و اینکه آیا هوای سرد برای تلفن‌های همراه مضر است یا خیر. اغلب دیده می‌شود که باتری‌های ماشین در هوای سرد از کار می‌افتند و به دستگاه‌های دیگری نیاز دارند که دومرتبه به کار بیفتند. آیا این قاعده برای گوشی‌های هوشمند نیز صدق می‌کند و آیا دستگاه شوکی وجود دارد که با استفاده از آن، بتوان گوشی هوشمند را به کار انداخت؟

انواع باتری

اول از همه، باید بدانید که چه نوع باتری در گوشی شما وجود دارد و این را باید با استفاده از مشخصات گوشی خود در سایت یا اطلاعات لازم روی جعبه گوشی پیدا کنید یا اگر بتوانید به باتری دسترسی داشته باشید، این اطلاعات معمولاً روی خود باتری موجود است.

در حال حاضر بسیاری از سازنده‌ها، از باتری‌های لیتیوم- یونی استفاده می‌کنند (که با نام‌های باتری Li-ion یا LIB شناخته می‌شود). این باتری‌ها اندازه‌های متنوعی دارند اما بیشتر باتری‌های گوشی‌های هوشمند در اندازه‌های کوچک و فرم مستطیل هستند و البته در برخی از گوشی‌های هوشمند نیز از باتری‌های لیتیوم-پلیمری استفاده می‌شود.

■ **نحوه فعالیت باتری‌های لیتیوم-یونی**

به طور خلاصه می‌توان گفت باتری‌های لیتیوم-یونی با جابه‌جا کردن یون‌ها بین قطب منفی و مثبت برای شارژ یا تخلیه شارژ کار می‌کنند و هوا یا به طور دقیق‌تر دما، می‌تواند در چگونگی جابه‌جایی یون‌ها بین الکترودها مؤثر باشد. اگر هوا بسیار سرد شود، یون‌ها حرکت نمی‌کنند و باتری کار نخواهد کرد، البته نکته کلیدی در چنین شرایطی این است که هوا باید واقعاً خیلی سرد باشد. فعالیت باتری‌های لیتیوم-یونی در دماهای متفاوت بدین ترتیب است که در دمای کمتر از ۴۰ درجه سانتیگراد زیر صفر فعالیت باتری متوقف و در دمای کمتر از ۲۰ درجه سانتیگراد زیر صفر، درصدی از شارژ باتری‌های لیتیوم-یونی تخلیه می‌شود. همچنین در دمای بیشتر از صفر درجه سانتیگراد، باتری لیتیوم-یونی بدون مشکل شارژ خواهد شد و در دمای بیشتر از ۴۵ درجه سانتیگراد، باید از شارژ کردن باتری‌های لیتیوم-یونی پرهیز کرد. باید دانست که در دمای بیشتر از ۶۰ درجه سانتیگراد نیز باتری لیتیوم-یونی شروع به تخلیه شارژ می‌کند.

■ **راهکار حفظ عملکرد باتری گوشی‌های هوشمند**

دمای مناسب برای شارژ باتری‌های لیتیوم-یونی بین ۱۰ تا ۳۰ درجه سانتیگراد است. در حالی که میزان شارژ مناسب که باید در باتری ذخیره شده باشد، بین ۴۰ تا ۸۰ درصد است. اگر این توصیه‌ها را جدی بگیرید، می‌توانید اطمینان حاصل کنید عمر باتری شما افزایش می‌یابد. لازم به ذکر است که متوسط طول عمر یک باتری، بین ۵۰۰ تا هزار چرخه است و هر چرخه، زمانی است که باتری شما به اتمام رسیده و دومرتبه شارژ شده است.

قاب فناوری

ردیابی سلامت چشم با تلفن همراه

میترا جلیلی

امروزه بیشتر مردم ساعات زیادی از شبانه روز با رایانه یا گوشی هوشمند خود کار می‌کنند در حالی که کمتر به فکر سلامت چشم خود هستند. با اینکه مراجعه سالانه به چشم‌پزشک برای اطلاع از وضعیت چشم‌ها موضوعی ضروری است ولی بسیاری تنبلی می‌کنند و اهمیتی به این چکاپ سالانه نمی‌دهند به همین دلیل فعالان عرصه فناوری دست به کار شده و یک ردیاب بینایی ساده، ارزان و کارآمد به نام EyeQue را ارائه داده‌اند که به تلفن هوشمند متصل می‌شود و کاربر هر زمان که بخواهد می‌تواند از وضعیت بینایی خود مطلع شود. تنها کافی است کاربر این ردیاب را به تلفن هوشمند خود متصل کرده و پس از قرار دادن آن در مقابل چشم، تلاش کند که دو خط سبز رنگ و قرمز را در یک ردیف قرار دهد که به این ترتیب عیوب چشم از طریق یک اپلیکیشن به وی اطلاع داده می‌شود. پیش از این نیز کیت‌هایی همچون SVOne و Peek تولید شده بود ولی از آنجا که گران بودند و کار با آنها چندان راحت نبود مورد استفاده عموم قرار نگرفت در حالی که کاربر با کمک EyeQue حتی می‌تواند از عیوب انکساری چشم خود مانند آستیگماتیسم، دوربینی یا نزدیک بینی مطلع شده و با توجه به میزان ضعیف بودن چشم، همچون پزشک یک نسخه آنلاین بنویسد و از همین طریق نیز عینک طبی سفارش دهد. با وجود دقت این ردیاب سلامت چشم، سازندگان آن معتقدند کاربران حتماً باید در طول سال به پزشک نیز مراجعه کنند. این ردیاب درنمایشگاه CES ۲۰۱۷ ارائه می‌شود و در حالی که مدت زیادی به پایان جمع‌آوری سرمایه در سایت کیک استارتر باقی نمانده موفق به جذب رقم قابل توجهی شده است. سازندگان این ردیاب همچنین ۳ درصد از سرمایه جمع‌آوری شده را به مؤسسه غیرانتفاعی TWOBILLIONEYES که در کشورهای فقیرنشین عینک توزیع می‌کند اهدا خواهند کرد. این ردیاب که قرار است در آوریل ۲۰۱۷ راهی بازار شود اکنون با بهای ۳۰ دلار پیش فروش می‌شود.

عکس: Verge

راهی برای کاهش حجم فایل‌های ویدئویی

تاپ اپ

ماهرخ چنگیز

اگر فایل ویدئویی دارید اما به دلیل حجم بالا امکان ارسال آن به افرادی که می‌خواهید را ندارید، پیشنهاد می‌کنیم از اپلیکیشن Video Compressor کمک بگیرید. با استفاده از این برنامه می‌توانید حجم فایل‌های ویدئویی خود را قبل از اشتراک گذاری کاهش دهید. از قابلیت‌های کاربردی این برنامه حفظ کیفیت ویدئو با وجود کاهش حجم آن است. بعد از نصب برنامه روی گوشی فایل مورد نظر خود را به Video Compressor بدهید. در قدم بعدی این برنامه حجم‌ها و وضوح تصویر مختلفی را برای انتخاب در اختیار شما می‌گذارد که باید براساس حجم خروجی، حالت تبدیل را انتخاب کنید. در نهایت نیز در کمتر از چند دقیقه می‌توانید فایل ویدئویی کم حجم شده را در اختیار داشته باشید. از دیگر قابلیت‌های جالب این اپلیکیشن این است که قبل از گرفتن خروجی نهایی از فشرده‌سازی می‌توانید فایل کم حجم ویدئویی را ببینید تا اگر از کیفیت آن راضی نبودید از دیگر گزینه‌های موجود در برنامه برای کاهش حجم فایل استفاده کنید. برای نمونه می‌توانید ببینید اگر یک فایل FULL HD را ۶۰برابر ابعاد اصلی فایل کم کنید آیا کیفیت آن قابل مقایسه با نسخه اصلی هست یا خیر.

همچنین شما می‌توانید چند فایل ویدئویی مختلف را به برنامه بدهید تا حجم آن را برای شما کم کند. البته بهتر است با توجه به کیفیت و سرعت اینترنت خانگی خود فایل‌های ویدئویی فشرده سازی را یک به یک در اختیار برنامه بگذارید. همه قابلیت‌های Video Compressor به نکات اشاره شده ختم نمی‌شود یکی از امکانات دیگر این اپلیکیشن، برش بخش‌هایی از ویدئو است. یعنی شما می‌توانید قسمتی از فایل ویدئو را انتخاب و حذف کنید یا از یک ویدئو چند دقیقه‌ای تنها بخش‌هایی که برایتان مهم است را انتخاب کنید.

این برنامه یک برنامه رایگان است اما رایگان بودن آن همیشگی نیست و به صورت محدود امکاناتش را به صورت مجانی در اختیار کاربرانش قرار می‌دهد. Video Compressor برای کاربران سیستم‌عامل اندروید و IOS قابل استفاده است.

برای استفاده از امکانات این برنامه روی لپ‌تاپ‌های ویندوزی می‌توانید به سایت video-compressor.en.softonic.com مراجعه کنید.