

۱۰ راهکار امنیتی برای جلوگیری از هک تلفن همراه



در این گزارش سعی کرده ایم ساده ترین روش های محافظت از اطلاعات در برابر هکرها را به شما آموزش دهیم. نکته ای که کاربران گوشی های هوشمند باید به آن توجه ویژه ای داشته باشند امنیت اطلاعات ذخیره شده و جلوگیری از دسترسی افراد سودجو به آنها است.

ایران هشدار- گوشی های هوشمند تبدیل به بخش جدایی ناپذیری از زندگی

روزمره ما شده اند. بیشتر افراد از تلفن هوشمند شان برای انجام کارهای مختلفی مانند: خرید های روزانه، سفارش غذا، رزرو بلیط سینما، انواع پرداخت های آنلاین و استفاده می کنند. همچنین این دستگاه هوشمند برای بسیاری از افراد تبدیل به محلی برای نگه داری از اطلاعات محرمانه مانند: کلمات عبور، اطلاعات کارت های اعتباری و.... شده است.

نکته ای که کاربران گوشی های هوشمند باید به آن توجه ویژه ای داشته باشند امنیت اطلاعات ذخیره شده و جلوگیری از دسترسی افراد سودجو به آنها است. در ادامه این گزارش ۱۰ راهکار امنیتی ساده که باید کاربران گوشی های هوشمند اندرویدی برای حفظ اطلاعاتشان در مقابل هکرها و افراد سودجو رعایت کنند را برای شما بازگو میکنیم:

استفاده از یک PIN (رمز عبور) برای صفحه قفل

همیشه از یک PIN یا رمز عبور برای حفاظت از اطلاعات گوشی هوشمند خود استفاده کنید. اضافه کردن این لایه های امنیتی به گوشی های هوشمند می تواند بسیار موثر باشد. اما اگر از آن دسته افرادی هستید که رمزهای عبور را به سرعت فراموش می کنید و به سختی به یاد می آورید می توانید از یک الگو برای قفل کردن گوشی خود کمک بگیرید.

بر روی برنامه هایتان قفل بگذارید

گاهی اوقات استفاده از یک کلمه عبور کافی نیست. برای اطمینان بیشتر باید برنامه های شخصی خود مانند: کیف پول تلفن همراه و... که حاوی اطلاعات محرمانه هستند را رمزگذاری کنید. برای این کار می توانید از اپلیکیشن های رمزگذاری کمک بگیرید.

برنامه هایتان را از منابع اصلی و قابل اعتماد دانلود کنید

شما می توانید برای اطمینان بیشتر از سالم و امن بودن برنامه های مورد نیازتان، آنها را از سایتها و یا فروشگاه های معتبر دانلود کنید.

نکته: بهتر است قبل از دانلود یک نرم افزار، آن را از نظر کیفیت و رتبه بندی بررسی کنید.

همچنین بررسی نرم افزار از نظر سیاست حفظ حریم خصوصی نیز از دیگر نکاتی است که باید به آن توجه کنید.

مجوزهای دسترسی نرم افزار را قبل از دانلود مطالعه کنید

انجام این کار نیز گام مهم دیگری برای حفظ امنیت اطلاعات شماست. در زمان دانلود نرم افزار از فروشگاه های معتبر از میزان دسترسی آن به داده های تلفن همراهتان مطمئن شوید. به طور مثال دانلود یک برنامه پولی که نیازمند دسترسی به دوربین تلفن همراه شماست ضروری نیست.

از نرم افزارهای مدیریت دستگاه اندرویدی کمک بگیرید

مدیریت دستگاه Android یکی از برنامه های مفید محسوب می شود که یکی از طراحان آن کمپانی گوگل است. اگر به هر دلیلی تلفن همراهتان را گم کردید این برنامه به شما کمک می کند تا تلفن همراه اندرویدی تان را ردیابی و به راحتی پیدا کنید؛ همچنین می توانید برای محافظت از اطلاعاتتان از طریق کنترل از راه دور آن را به تنظیمات کارخانه برگردانید.

از Google Authenticator کمک بگیرید

با استفاده از قابلیت Authenticator Google می توانید یک لایه امنیتی جدید را به حساب کاربری خود اضافه کنید. این نرم افزار یکی از بهترین راهکارها برای اهراز هویت اکانت گوگل محسوب می شود که در صورت فعال سازی در کوتاهترین زمان می توانید آن را از طریق شماره تلفن همراهتان دریافت کرده و با اطمینان خاطر بیشتری وارد حساب کاربری خود شوید. نکته: این برنامه برای برخی خدمات غیر از گوگل نیز قابل استفاده است.

یک آنتی ویروس خوب دانلود کنید

استفاده از یک آنتی ویروس قدرتمند و مفید در عین ضرورت یک گام مهم و اساسی در حفظ اطلاعات محسوب می شود؛ پس هرچه سریعتر برای نصب یک آنتی ویروس قوی اقدام کنید.

از وای فای های عمومی استفاده نکنید

بهتر است تا جایی که می توانید از استفاده از وای فای عمومی اجتناب کنید. شما هیچ گاه نمی توانید مطمئن شوید که این شبکه رایگان ۱۰۰ درصد امن است. همچنین اطمینان حاصل کنید که تلفن همراه شما به صورت خودکار به شبکه های وای فای رایگان متصل نمی شود.

نکته: بهتر است در صورت نیاز نداشتن به وای فای آن را خاموش نگه دارید.

تنظیمات بلوتوث تلفن همراهتان را به درستی پیکربندی کنید

برای این کار به تنظیمات بلوتوث رفته در آنجا عبارت "Non-discoverable" یا غیر قابل کشف را انتخاب کنید. دلیل این کار این است که اگر بلوتوث در همه جا قابل رویت باشد افراد بیشتری برای دستیابی به اطلاعات و اتصال به تلفن همراه شما تمایل پیدا می کنند. در این باره نیز مانند وای فای اگر نیازی به استفاده از بلوتوث ندارید بهتر است آن را خاموش نگه دارید. هرگز گوشی خود را روت نکنید، شاید با روت کردن تلفن همراه دسترسی های بیشتری برای شما باز شود اما اگر عاقلانه فکر کنید این کار به نفع شما نیست. با انجام این کار تلفن همراهتان را آسیب پذیر کرده و راه ورود هکرها به آن را باز می کنید.

منبع: باشگاه خبرنگاران جوان

اداره حراست آموزشکده شهید یزدانپناه سنندج