امنیت در فضای مجازی

با توجه به شرایط کنونی کشور و افزایش استفاده از سامانه های آموزش مجازی و جلسات آنلاین، ضروری است معلمان عزیز به منظور حفاظت از اطلاعات شخصی خود تمهیداتی را بیندیشند. در این مقاله به نکات و راهکارهایی اشاره می‌شود که در این زمینه می‌تواند به معلمان عزیز کمک نماید.

سعید چگینی

فضای مجازی در کنار آثـــار و برکات فراوان در زندگی انسان‌ها، دارای مخاطراتی نیز هست که می‌تواند موجب ضرر و تلخ‌کامی کاربران شـــود. حتماً بسیار شـــنیده‌اید که سرقت اطلاعات ســـپرده‌های بانکی باعث از دســـت رفتن ســـرمایه بسیاری شـــده و یا اینکه هکرها توانســـته‌اند با ورود به تلفن همراه، اطلاعات و تصاویر شـــخصی را پاک کنند و یا در فضای مجازی منتشـــر کنند. در هر صورت، فضای مجازی با زندگی ما عجین شـــده و گریزی از آن نیست؛ پس باید آداب استفاده صحیح از آن و اقدامات لازم برای حفاظت از اطلاعات شخصی را درنظر داشته باشیم.

در این مطلب، با برخی از این نکات آشنا خواهید شد.

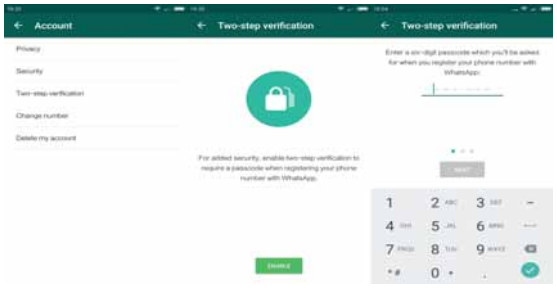
از اتصال به وای‌فای عمومی پرهیز کنید

تقریبا همه کاربران از خطرات اســـتفاده از شـــبکه‌های بی‌سیم عمومی و باز (Wi-Fi) مطلع هستند. وای‌فای عمومی رایگان که در برخی مراکز خرید، کافه‌ها، رستوران‌ها، فرودگاه‌ها و سایر اماکن عمومی ارائه می‌شـــود بهترین فرصت برای سوءاستفاده هکرها اســـت. ســـعی کنید حتی‌الامکان از اینترنت خط خود اســـتفاده کنید و هروقت در مکان‌های عمومی هستید وای‌فای گوشـــی را خاموش کنید. علاوه بر ایـــن، در مکان‌های عمومی بلوتوث گوشـــی را هم خاموش کنید، مگر اینکه ابزار و ســـاعت هوشمند داشته باشید که برای ارتباط نیاز به بلوتوث دارد.

گوشی و نرم‌افزارهای حساس خود را قفل کنید

همیشه برای باز کردن گوشی از کد عبور چهار یا شش رقمی، اثر انگشت یا حسگر تشخیص چهره استفاده کنید. شاید اینکه همیشه برای کار با گوشی نیاز به وارد کردن کد عبور داشته باشید چندان خوشـــایند نباشد، اما به‌یاد داشته باشید که اگر روزی بر حسب اتفاق گوشی شما گم شود، هر کسی می‌تواند از اطلاعات شخصی شما مانند ایمیل‌ها، مخاطبان، تصاویر و اطلاعات بانکی خبردار شود. این قفل را می‌توانید برای اپلیکیشن‌های بانکی و شبکه‌های اجتماعی نیز فعال کنید.

از احراز هویت دو مرحله‌ای استفاده کنید



احراز هویت دو مرحله‌ای هم از آن دســـته روش‌هایی است که معمولا مورد بی‌توجهی قرار می‌گیـــرد. چراکه باید یک مرحله بیشتر برای ورود به گوشی را پشت سر بگذارید. اما با استفاده از آن، یک لایه امنیتی بیشـــتر به گوشـــی اندرویدی خود اضافه می‌کنید. برای اتصال به شبکه‌های اجتماعی مانند WhatsApp، Instagram می‌توانید این قابلیت را فعال کنید.

از کلمات عبور قوی استفاده کنید

کلمه عبوری که برای ورود بـــه تلفن همراه، ایمیل و بانکداری اینترنتـــی و کاربری‌های مختلف انتخاب می‌کنید بهتر اســـت حداقل ۸ کاراکتر و شامل حروف کوچک و بزرگ انگلیسی، اعداد و علایم باشـــد. نفوذگران اینترنتی قادر هســـتند تا در خیلی از موارد کلمات عبور قوی را هم بشکنند. اما ساده کردن کار هکرها با به‌کارگیری اطلاعات فـــردی مانند کد ملی، تاریخ تولد یا هر چیزی شبیه به این موارد به‌عنوان کلمه عبور ایده بسیار هولناکی است.

دقت داشـــته باشید که بهتر است هر شش ماه یک بار کلمات عبور خود را عوض کنید یا اگر اخباری در خصوص هک شـــدن یک برنامه خاص شنیدید خیلی سریع کلمه عبور خود را تغییر دهید.

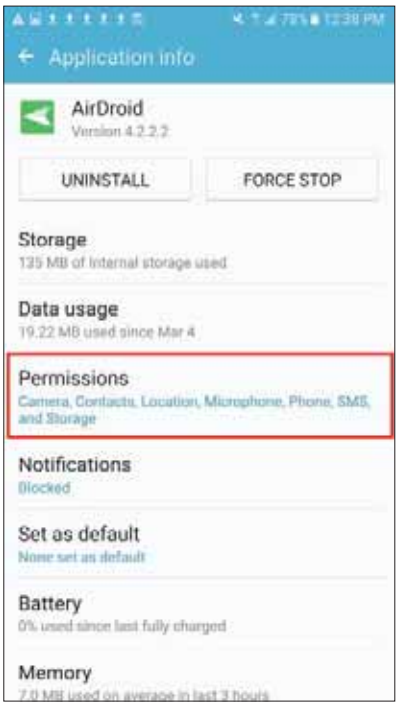
مراقب ایمیل‌های اسپم و فیشینگ باشید

یکی از راه‌های ســـاده برای هکرها نفوذ به گوشـــی از طریق صنـــدوق پســـت الکترونیک اســـت. ایمیل‌های فیشـــینگ به‌گونه‌ای طراحی می‌شوند که با فریب شما امکان دسترسی به پنل کاربری را فراهم می‌کنند. از کلیک بر روی ایمیل‌های تبلیغاتـــی، بـــاز کردن پیوســـت‌های مشـــکوک یـــا اجرای به‌روزرســـانی‌هایی کـــه از راه‌های مختلف همچـــون ایمیل، پیامک و شـــبکه‌های اجتماعی ارســـال می‌شـــوند خودداری کنید.

از آنتی‌ویروس استفاده کنید

برای تلفن همراه و رایانه شـــخصی حتماً از آنتی‌ویروس اصل استفاده کنید. آنتی ویروس‌ها یا فایروال‌ها می‌توانند از ورود و فعالیـــت ویروس و کدهـــای مخرب جلوگیـــری کنند. مزیت آنتی‌ویروس‌های اصلی یا اورجینال نیز به قابلیت به روزرسانی آن‌هاســـت. با همین بـــه روزرســـانی‌ها می‌تواننـــد اطلاعات ویروس‌های جدید را نیز به بانک اطلاعاتی خود اضافه کنند.

مجوز اپلیکیشن‌ها را مدیریت کنید



مجوزهای اپلیکیشن‌ها را بررسی کنید. می‌توانید دسترسی به دوربین، میکروفون، لیســـت مخاطبان یا لوکیشن توسط اپ‌ها را متوقف کنید. مجوزهای داده شـــده به اپ‌را زیرنظر داشـــته باشید و مواردی که مورد نیاز نیستند را حذف کنید. می‌توانید برای مشـــاهده و تغییر در مجوز دسترسی، گزینه Privacy در تنظیمات آیفـــون و Permission manager و App permissions را در تنظیمات سیستم عامل اندروید ببینید.

تهیه نسخه پشتیبان

همیشه باید آماده بدترین حالت‌ها باشید. پس از تمام فایل‌ها و تصاویر مهم خود نسخه پشـــتیبان در ذخیره‌سازهایی مانند هارددیسک‌های خارجی داشته باشید.

همچنین اکیداً پیشنهاد می‌کنم تصاویر شخصی و خانوادگی خود را در تلفن همراه نگهداری نکنید.

اپلیکیشن‌های مناسب برای امنیت در فضای مجازی

AppLock

همه ما تصاویر و ویدیوهایی در گوشی‌هایمان داریم که دوست نداریم جز خودمان چشـــم کس دیگری به آن‌ها بیفتد. بهترین راه برای محافظت از این تصاویر استفاده از اپلیکیشن‌هایی است که با رمزگذاری، این فایل‌ها را پنهان و از دسترس افراد سودجو دور می‌کنند.

اپلیکیشن AppLock به دلیل عملکرد آفلاین، یکی از امن‌ترین این اپلیکیشن‌هاست که به جز پنهان‌سازی تصاویر می‌تواند همین کار را برای اپلیکیشن‌های نصب شده روی گوشی (مثل اپلیکیشن پیامک و تقویم و یادداشت‌برداری و ...) هم انجام بدهد.

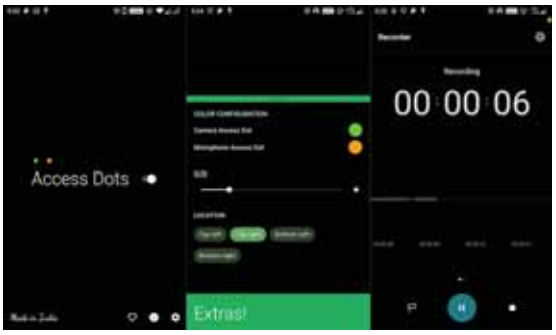
Google Authenticator

این اپلیکیشـــن وظیفه احراز هویت شـــما را هنـــگام ورود به سایت‌ها عهده‌دار هستند. بدین صورت که پس از وارد کردن رمز عبور، کد احراز هویت را هم وارد کرده و به وبسایت مد نظرتان وارد خواهید شد.

استفاده از این اپلیکیشن‌ها تقریبا تضمین می‌کند که یک هکر، قادر به استفاده از حساب کاربری شما و ورود به آن نخواهد بود چرا که باید به جز پسورد، رمز احراز هویت را هم بدست بیاورد که تقریبا غیر ممکن به نظر می‌رسد.

بـــرای آشـــنایی با ایـــن اپلیکیشـــن، قابلیـــت two-Step Verification را روی Gmail فعال کنید.

Access Dots



این اپلیکیشـــن دسترســـی غیرمجاز برنامه‌ها بـــه دوربین یا میکروفون را «در لحظه» به شـــما اعلام می‌کند، فقط و فقط با یک چراغ چشمک زن.

فرض کنید مشـــغول اســـتفاده از اپی هســـتید که نباید به دوربین‌تان دسترسی داشته باشد، اما دارد و شما اطلاع ندارید. خوشـــبختانه Access Dots می‌توانـــد این موضوع را با یک چراغ چشـــمک زن به اطلاع‌تان برســـاند که هر چه ســـریع‌تر اپلیکیشن مشکوک را از گوشی‌تان پاک کنید.

Lookout Security & Antivirus

این اپلیکیشن یکی از قدرتمندترین نرم افزارهای امنیتی و آنتی ویروس برای سیستم عامل اندروید است.

بـــا داشـــتن Lookout Security & Antivirus برروی گوشـــی خود می‌توانید علاوه بر افزایـــش امنیت آن از امکاناتی نظیر تهیه نسخه پشـــتیبانی از فایل‌ها و تماس‌ها و حتی پیدا کردن گوشی گم شده استفاده کنید.

با نصب بودن این اپلیکیشـــن برروی تلفـــن همراه از لو رفتن حریم خصوصی شـــما نگران نباشـــید چرا که این نرم افزار وب ســـایت‌های مخرب را شناسایی و بطور خودکار بلوکه می‌کند و اجازه دسترسی به این وب سایت‌ها را به شما نمی دهد.

با این برنامه قادر خواهید بود فایل‌های گوشـــی خود را اسکن کنید و در صورت موجود بودن ویروس، تروجان و یا کرم‌ها آن‌ها را از بین ببرید و بر سرعت آن بیفزایید.