جرایم و امنیت در فضای سایبری

سرگرد مهدی فرازپور*

مقدمه

وضعیت فضای سایبری کشور و جرائم آن، تفاوت‌هایی نسبت به جرائم امسال و سال قبل وجود دارد که با توجه به اولویت جرائم سایبری و عقبه آنها، باید کلیاتی درباره فضای سایبر و حوزه تقسیم بندی جرائم بیان و سپس مصادیق جرائم و اولویت‌های جرائم «سایبری» را تشریح کنیم.

فضای سایبر، بستری است که بخش‌های مختلف زندگی اجتماعی افراد در آن قابل تعریف هستند؛ پرداخت مالی، ارتباط اجتماعی، توانمندسازی، بهره‌مندی از امکانات، خدمات چه در حوزه خصوصی و دولتی، حوزه ازدواج و... . وقتی یک اجتماع انسانی، شکل مجازی در بستر این فضای سایبری بگیرد؛ مسلماً بخشی از همان آسیب‌ها و جرائم به این فضا کشیده خواهد شد.

---

* کارشناس پلیس فتا.

فضای سایبری و انحراف ذهنی

در حوزه جرائم، یک پدیده جرم‌شناسی نشأت گرفته از انحراف ذهنی افراد وجود دارد که می‌گوید: جرائم، سرریزِ عدم کارکردهاست (کارکردهای اجتماعی- فرهنگی)؛ یعنی اگر انحراف ذهنی که در ذهن افراد وجود دارد، با استفاده از قابلیت‌های فضاهای مختلف، از جمله فضای سایبری تسری پیدا کند، بعد از مدتی به آسیب اجتماعی تبدیل می‌شود.

بنابراین عدم کنترل و مهار آسیب اجتماعی و نیز عدم توانمندسازی اقشار آسیب‌پذیر در برابر آنها، به سرریزی در اجتماع منجر می‌شود که همان جرم است؛ یعنی در همه جوانب، فرایند انحرافات ذهنی و کجروی‌ها تا ارتکاب جرم، یک فرایند شناخته شده است. فضای سایبری نیز در انحراف کجروی‌ها یا در تکثر توسعه آسیب‌ها یا مستقیماً در ارتکاب جرم هم تأثیر می‌گذارد.

اقسام جرائم و مصادیق آن

جرائم به دو دسته تقسیم شده‌اند:

الف. جرائم سنتی؛

ب. جرائم نوپدید.

این جرائم به واسطه افزایش سطح کاربری عموم مردم، در فضای سایبری به وجود آمده است. جریان نوپدید در فضای سایبری نیز به دو دسته تقسیم می‌شود:

۱. جرائم سنتی در بستر فضای سایبری که عبارتند از: سرقت، انتشار

تصاویر خصوصی افراد و انواع و اقسام توهین‌ها در فضای سایبری.
۲. جریانی که فضای سایبری به صورت نوپدید با خودش به همراه آورده است.

از سال ۱۳۹۲ به بعد، میزان تأثیر فضای سایبر در ارتکاب جرائم سنتی قابل توجه است. برای مثال آمارهای مختلفی که در مکان‌های متفاوت و اشکال‌های گوناگون جمع‌آوری شده است، بیانگر آن ۶۵٪ علت‌های قتل به عنوان جرم سنتی، تا قبل از سال ۱۳۹۰، نزاع و درگیری بوده است. از سال ۱۳۹۰ به بعد، علت از سمت نزاع و درگیری، به قتل‌های خانوادگی تغییر کرده است. سهم نزاع و درگیری‌ها در بروز قتل کاهش یافته و سهم بحث اختلافات خانوادگی یا قضایای ناموسی افزایش یافته است. آنالیز آمار کلی کشور در حوزه ارتکاب جرم، از سال ۱۳۹۲ به بعد نشان می‌دهد که نقش فضای سایبری به عنوان وسیله یا ابزاری در زمینه‌چینی برای ارتکاب قتل‌های خانوادگی، قابل توجه است.

جرائم سنتی به وسیله ابزار فضای سایبر، از سال ۱۳۹۲ یک جهش پیدا کرده است؛ برای مثال بیشتر عملیات‌های پلیس مبارزه با مواد مخدر برای کشف باند، سنتی است؛ یعنی یا به وسیله فرد نفوذی دارد یا گزارش افراد و یا اجیر کردن یکی از مرتکبین برای کسب اطلاعات. اگر چه پلیس از ابزار فنی نیز استفاده می‌کند، ولی اگر حوزه فضای مجازی پلیس مواد مخدر فعال شود (که شده است)، کشفیات آن کمتر از کشفیات فیزیکی نخواهد بود. فضای سایبر با قابلیت‌هایی که دارد، در حوزه پلیس آگاهی در جریان جنایی، قتل، تجاوز به عنف و سرقت

مسلحانه، نقش گسترده‌ای پیدا کرده است. در حوزه جرائم امنیتی نیز بیش از ۹۰٪ تمام ارتباط‌گیری و شبکه‌سازی‌هایی که علیه جرائم امنیتی در کشور انجام می‌شود، از طریق فضای سایبر شبکه‌سازی شده است. از این روست که از سال ۱۳۹۲ به بعد، تأثیر ابزار فضای سایبر در ارتکاب جرائم و جریان سنتی افزایش یافته است.

جرائم نوپدید

جریان نوپدید، یعنی جایی که به آن جرم محض سایبری می‌گوییم. بیشتر مرتکبین جرائم سنتی، بزه‌دیدگان، قربانیان و دستگیر شده‌های جرائم سنتی در فضای سایبر، متأهل هستند. ۶۳٪ قربانیان جرائم سنتی در بستر فضای سایبر، خانم‌ها هستند. رنج سنی قربانی‌های خانم، کمتر از بیست سال و قربانیان آقا، بالای بیست سال است.

خانم‌ها برای مراجعه و ابراز شکایت به مراجع انتظامی و قضایی، خیلی زود اقدام نمی‌کنند؛ بلکه وقتی مشکل حاد می‌شود، فرد مراجعه کرده و ماجرا و شیوه خدشه‌دار شدن حیثیت زندگی‌اش را بیان می‌کند. این در حالی است که در بستر فضای سایبر، جسارت و انگیزه ارتکاب جرم در خانم‌ها نیز بالاست؛ برای مثال در یک جرم اخلاقی حالت نامشروع، اگر آقایی بخواهد تمهیدات یک ارتباط نامشروعی در فضای سایبر را بچیند و مرتکب چنین جرم یا آسیب و انحرافی شود، با احتیاط بسیار و انجام ملاحظات فنی این کار را انجام می‌دهد تا چیزی در جایی ثبت نشود و رد پایی از خود به جا نگذارد، اما خانم‌ها بدون هیچ احتیاط و ملاحظه‌ای این کار را انجام می‌دهند.

یکی از خصوصیات ابتدایی در فضای سایبر برای مردم، عادی‌سازی محرمانگی و خصوصی‌سازی است. آنچه باعث نقض محرمانگی و خصوصی‌سازی می‌شود، حذف «ناظران اجتماعی» است. به عبارت بهتر مرحله تأثیرگذاری فضای سایبر در زندگی عادی مردم که ناظر اجتماعی در آن تاثیرگذار نباشد، مرحله انحراف و آسیب است. عوامل تأثیرگذار را می‌توان کلمات، گفتگوها و عبارات جدید دانست که شخص در بیست سال قبل زندگی‌اش نشنیده، تصاویرش را ندیده و کلیپ و چالش مخصوصش را هم ندیده است. این مواجهه ناگهانی او را به مرحله انحراف می‌رساند. برای مثال خانمی، مرد دیگری در زندگی‌اش وجود دارد که گاهی با او چت می‌کند. این مرد به او القا می‌کند که بد نیست برای روز مبادا زمانی که آدم دعوایش می‌شود، دوست پسری داشته باشد.

جرائم اقتصادی

بخشی از جرائم مالی و اقتصادی، برداشت‌های غیر مجاز است که برخی به گونه قمار و شرط‌بندی، و بعضی به شیوه کلاهبرداری است. منظور از برداشت‌های غیر مجاز این است که آقا یا خانم هکر اطلاعات حساب بانکی افراد را به دست می‌آورد و از آنها بهره‌برداری می‌کند. به این صورت که اگر حساب فرد قربانی پول داشته باشد، هکر پولش را از طریق خرید کالا یا کارت به کارت یا خرید شارژ به صورت غیر مجاز برداشت می‌کند. نکته جالب توجه آنکه عمده مرتکبین این جرائم مالی، زیر هیجده سال سن دارند.

در حوزه فضای سایبری، بیشتر هکرها در چند استان مشخص از جمله قم، به سبب وجهه مذهبی مردم شهر، از ترفندهای معنوی هم چون برنده شدن فیش عتبات عالیات یا برانگیختن احساس دلسوزی و... استفاده می‌کنند. برای مثال پسر چهارده ساله‌ای شش تا کانال دارد که در دو تای آنها، صد و بیست و پنج هزار عضو و در دیگری سیصد و پنجاه هزار عضو دارد. بدون هیچ محدودیت و رعایت خطوط قرمزی فقط با شعر، هزل، عکس و تمسخر و ... عضو جمع کرده است و در لابلای مطالب ارائه شده، به چند شیوه مختلف نرم‌افزاری، ربات و بدافزار خود را نیز تبلیغ می‌کند و با شگردهایی که دارد، اطلاعات حساب افراد را خالی می‌کند. بر اساس آمار، ۵۷ نوجوان در کشورمان با استفاده از فضای سایبری، توانستند یک تریلیارد و صد میلیارد تومان، یعنی هزار و صد میلیارد تومان از حساب مردم بردارند.

از هر ۱۰۰ نفر، ۷۲ نفر در کشور دسترسی کاربردی به اینترنت دارند و این، یعنی توسعه بستر و پهنای باند! اولین وظیفه هر دولتی برای مردمش، تأمین امنیت در فضای سایبری یا تأمین اینترنت پاک[1] است. می‌گویند با دسترسی مردم به اینترنت، میزان داده و ستانده آنها با هم برابر می‌شود. اما به راستی چه داده‌ای می‌دهید و چه ستانده‌ای می‌گیرید؟ اینترنت برای همه مردم فراهم شده است، ولی در مقابل این داده به مردم، چه چیزی از آنها گرفته شده است؟ برای مثال خانم

۱. مراد از اینترنت پاک، اینترنتی است که در آن خبری از فیس‌بوک، یوتیوپ و بیشتر سایت‌های آپلود عکس و فیلم و تقریبا تمام شبکه‌های اجتماعی مانند گوگل ریدر، بلاگر و وردپرس، فرندفید، توییتر و هر سایت خلاقانه و پر ترافیک دیگر نخواهد بود.

بیست ساله‌ای به واسطه دسترسی به فضای سایبری و خرید کالا از آن، مرحله انحراف ذهنی‌اش با جنس مخالف به گونه‌ای آسیب‌رسان رشد کرده که سبب جدا شدن وی از همسرش می‌شود. بازگشت این خانم بیست ساله با برچسب ارتباط نامشروع و صد ضربه شلاق به خانه پدری، حیثیت سه نسل هیأت امنایی بودن پدرش و نذرهای مادر خیرش را از بین می‌برد. اگر فضای سایبری نبود، شاید مدت زمان این ارتباط‌گیری خیلی بیشتر بود. یکی از دستاوردهای فضای سایبر در حوزه فرهنگی- اجتماعی در کشور ما، حذف این فاصله زمانی است، یعنی اگر این خانم به سبب وجود مشکلات خانوادگی، مهارتی، ارتباطی و روانشناسی می‌خواهد باعث از بین رفتن خانواده خود شود و برای این کار سه ماه یا هشت ماه زمان می‌خواهد، با بستر فضای مجازی این زمان به سه روز تبدیل می‌شود.

مهم‌ترین علت به دام افتادن و قربانی شدن بخش عظیمی از مرتبطین با فضای سایبر در کشور اعم از زن و مرد را می‌توان انحراف ذهنی دانست. انحراف ذهنی، علتی است که به عنوان زمینه‌ای در همه افراد وجود دارد و باید با آموزش مهارت‌های خود کنترل‌گری و سواد رسانه ای، فرهنگ سازی شده و توسط ناظران اجتماعی مهار شود.

سواد رسانه‌ای یا مهارت‌های سایبری

مهارت سایبری، استانداردهای دارد که برخی استانداردهای سازمان ملل و برخی دیگر استانداردهایی است توسط افراد متخصص در کشور به آن اضافه شده است. مردم برای ورود در فضای سایبری، باید

این حداقل استانداردها را رعایت کنند. بنا بر تحقیقات، بیشترین تقاضا و نیاز مردم در بحث آموزش، بحث فضای سایبری است؛ بنابراین عدم وجود مهارت ارتباطی و مهارت‌های سایبری برای ارتباط‌گیری، مهم رین مشکل مردم ماست. مروری بر پرونده‌های جرائم سایبری، گویای آن است که استفاده‌کنندگان از اینترنت فاقد این مهارت هستند. برای مثال نمی‌دانند قربانی شدن یعنی چه و نمی‌دانند منتشر کردن تصویر خصوصی چه عواقبی دارد. در حوزه مسائل مالی، شرایط اسفناک‌تر است. بیشتر مشکلات قربانیان در فضای مجازی، ناشی از نا آگاهی و ساده‌انگاری است.

بزه‌دیده‌ها و بزهکارها

درصد بزه‌دیدگان نا آگاه در کشور، بیش از ۶۰٪ است؛ یعنی بزهدیده آگاه خیلی کم است؛ زیرا مهارت سایبری در افراد وجود ندارد. این در حالی است که بزهکارهای فضای سایبر، عمدتاً آگاهند و از خلأ نا آگاهی بزه‌دیده‌ها استفاده می‌کنند.

بیشترین جرائم در کشور، مربوط به جرائم مالی و ۸۲٪ از پرونده‌ها، مربوط به این حوزه است که به دلیل برداشت غیر مجاز و کلاهبرداری ایجاد شده‌اند. پلیس فتا در هر نیم ساعت، حداقل دوازده تا سیزده پرونده برداشت غیر مجاز تشکیل می‌دهد. اگرچه بیشترین جرائم سایبری در کشور مالی است، اما در واقع رقم خاکستری جرائم اخلاقی بیشتر است.

برداشت‌های غیر مجاز از حساب‌های بانکی

برداشت‌های غیر مجاز در اثر لو رفتن اطلاعات حساب بانکی افـراد و به دو روش رخ می‌دهد: روش‌هـای مهندسـی اجتمـاعی و اسـتفاده از قابلیت‌های ابزارهای فنـی در فضـای سـایبری. بـرای نمونـه در روش مهندسی اجتماعی، فردی با شما تماس می‌گیرد و به شما اعلام می‌کند که برنده سفر عتبات عالیات شده و اکنون روی آنتن زنـده در حضـور وزیر با شما صحبت می‌کند. سپس برای پرداخت هزینه سفر شما را به سوی عابربانک می‌کشاند؛ در حالی که از شما می‌خواهد تماس با او را قطع نکنید و پای خودپرداز هر آنچه او می‌گوید انجام دهید.

خانم وکیلی تماس گرفته بـود و می‌گفـت هفتـاد میلیـون از حسـابش برداشته‌اند. وقتی پرسیدیم چرا شـکایت نکـرده اسـت؟ گفـت دو روز است که به سبب این اتفاق بیمار شده است. به او گفتیم شما که وکیـل هستید چرا گول این افراد را خورده‌اید؟ گفت: به اندازه‌ای با اعتماد بـه نفس صحبت می‌کرد که مرا نیز اغفال نمود.

متأسفانه در برخی ادارات، وقتی حقوق واریز می‌شود، عده‌ای از افـراد با آگاهی از مشخصات پرسنل به بهانه واریز شدن اشتباهی حقوق مـثلاً رئیس اداره به حساب آنها، قصد کلاهبرداری از طریق فضای سـایبری دارند. بنابراین در حوزه برداشت‌های غیر مجاز، اطلاعات مالی افراد به وسیله ابزار فنی یا به وسیله مهندسی اجتماعی از دست می‌رود.

اطلاعات حساب بانکی چیست؟ شماره کارت، رمز دوم، تاریخ انقضـا و پی سی وی که روی کارت نوشته شده است که بیشتر در خریدهای

اینترنتی لو می‌رود. اگر چه این حرف باعث نگرانی خیلی از افراد می شود، اما اگر فرد از یک درگاه امن خرید کند، به مشکل بر نمی‌خورد. اگر فردی در خرید به مشکل خورد، معلوم است که درگاه جای نا امنی است. چه زمانی این مشکل به وجود می‌آید؟ زمانی که انحراف ذهنی در ذهن هکر وجود داشته باشد، آن انحراف ذهنی به کمک هکر می‌آید و به وسیله ربات‌ها و ... دست به کلاهبرداری می‌زند.

آیا اپلیکیشن‌های پرداخت اینترنتی معتبرند؟

فقط چند شرکت وجود دارد که زیر نظر بانک مرکزی و بانک‌های دولتی هستند که دارای «درگاه واسط»[1] می‌باشند؛ این شرکت‌ها معتبرند. هفت شرکت واسط در کشور که درگاه واسط ارائه می‌دهند، تحت نظارت پلیس یعنی دیتایبس و تحت نظارت بانک مرکزی است؛ به طوری که نمی‌توانند یک ریال را هم جابه‌جا کنند. هر فردی که حتی یک ریال از پولش جابه‌جا می‌شود، قابل استیفاست. این هفت شرکت عبارتند از: آسان پرداخت، ایوا، روبیکا، بله (تراکنش مالی دارد) و هفت هشتاد.

راهکار پرداخت‌های امن اینترنتی کدامند؟

درگاه‌های پرداخت یک آدرس یونیک دارد که آن را در نوار آدرس تایپ می‌کنند. در مورد تقلبی آن، وقتی فرد وارد درگاه می‌شود، ظاهر سایت را مانند درگاه پرداخت می‌بیند. اما اگر در آدرس دقت کند،

---

۱. درگاه واسط، یعنی اگر فردی کسب و کار اینترنتی راه بیاندازد، لازم است پرداخت و دریافت پول و تراکنش مالی انجام دهد، از شرکت واسط یک درگاه می‌گیرد.

می‌تواند متوجه تفاوت آدرس درگاه تقلبی با آدرس درگاه واقعی شود. آدرس درگاه واقعی http://pardakht.ir است، اما آدرس درگاه تقلبی، این است: http://pardäkht.ir این آدرس فرد را به صفحه پرداخت هکر منتقل می‌کند.[۱] آما از آنجایی که بسیار شبیه درگاه‌های پرداختی واقعی است، فرد تفاوت کوچک ä در آدرس را متوجه نمی‌شود. این یکی از انواع هک، به نام فیشینگ است. بنابراین از ورود به درگاه پرداخت فروشگاه‌های نا امن باید به شدت پرهیز شود؛ زیرا فروشگاه‌های نا امن، نماد اعتماد الکترونیکی کسب و کارهای اینترنتی را ندارند.

به اپلیکیشن‌ها و ربات‌های ناشناس اعتماد نکنید

برای امنیت بیشتر بهتر است هر از پنج یا شش کارت بانکی که دارید، تنها رمز دوم یک کارت را فعال کنید و کارت را هم همیشه خالی نگه دارید. هر زمانی که نیاز به خرید اینترنتی پیدا می‌کنید، به میزان خرید، کارت به کارت کرده و از آن کارتی که رمز دوم دارد، خرید اینترنتی انجام دهید.

برای وارد کردن رمز عبور و نام کاربری، همیشه از وب‌سایت‌های ایمن که با https شروع می‌شوند، استفاده کنید.

گاهی این سؤال مطرح می‌شود که مبلغی از حساب فرد کم شده است، آیا قابل برگشت است یا خیر؟

وقتی فردی متوجه می‌شود که از حسابش پول کسر شده است، باید در اسرع وقت با پلیس فتا تماس بگیرد تا پیگیری کنند؛ زیرا وقتی پول از

---

۱. برای مطالعه بیشتر.

حساب فرد خارج شده و به حساب دیگری وارد شده باشد، می‌توان آن حساب را مسدود کرد. اگر پول در حساب‌ها در چرخش باشد، می‌توان به سرعت شناسایی و حساب مربوطه را مسدود کرد.

انحراف ذهنی دختران و پسران

میزان انحرافات ذهنی دختران، بیشتر از پسرها می‌باشد؛ به‌ویژه میزان انحرافات دختران پایه دهم تا دوازدهم. انحراف ذهنی، یعنی کمبود بلوغ عاطفی. فرایند بلوغ عاطفی در دختری که توسط پدر و مادر درک نمی‌شود، پدر او را با خود به اجتماع و فضاهای مورد علاقه‌اش نمی‌برد و ارتباطش با مادرش نیز خوب نیست، ناقص است. از این رو می‌کوشد خود را به هم‌سالانی که با آنها در ارتباط است، شبیه کند. اگر آنها دوستی از جنس مخالف دارند، او هم می‌کوشد تا دوستی از جنس مخالف برای خود داشته باشد.

حمایت‌های قانونی

قانون قضایی می‌تواند از حقوق دختران و بانوان بدون شکایت شخصی و توسط مدعی‌العموم دفاع کند. برای مثال اگر کسی را می شناسید که حقوقش تضییع شده است، می‌توانید او را به مراجع قضایی راهنمایی کنید. مانند ماجراهای تجاوزگرانه که خود فرد هم شاید به نوعی مقصر باشد؛ چرا که نا آگاهانه ارتباط دوستانه برقرار کرده است و اکنون به دلیل ترس از آبرو یا خانواده اقدامی نمی‌کند. وقتی برای مقام قضایی محرز شود که تضییع حقوق فرد صورت گرفته است، بدون اینکه این مسئله در جایی آشکار شود (حتی برای دخترهای زیر سن قانونی)، مدعی‌العموم به پرونده رسیدگی می‌کند.

معضل تن‌فروشی

اکنون تن‌فروشی به معضل بزرگ جامعه تبدیل شده است. همیشه یک عده تن‌فروش خیابانی وجود داشت، اما اکنون تن‌فروش‌های مجازی به وجود آمده‌اند. تن‌فروشی در فضای سایبری روش دیگری برای کلاه‌بردار است. برای مثال در شبکه اجتماعی کره‌ای، افرادی زیادی هستند و چون نام و مشخصات فرد به چینی نوشته شده، به ذهن خطور نمی‌کند در میان این افراد ایرانی هم باشد، اما با یک جستجو بر اساس لوکیشن، مسافت و پروفایل، تن‌فروش ارائه می‌دهد.

تن‌فروش به بهانه شروع آشنایی، ویدئو زنده چندثانیه‌ای، آدرس خیابان، آدرس کوچه و پلاک بارها از مشتری خود از طریق اینترنت پول دریافت می‌کند. وقتی فرد به آدرس می‌رود، متوجه می‌شود اشتباه است. فرد برای شکایت به پلیس مراجعه می‌کند و بدون خجالت می گوید: برای صیغه‌یابی پول دادم، لطفاً شکایت من را رسیدگی کنید. پول من را خورده است.

نظارت در فضای سایبری

در فضای سایبر وقتی بحث فضای محرمانگی و خصوصی افراد به وجود می‌آید، ناظر اجتماعی خود به خود حذف می‌شود؛ ولی بحث نظارت در فضای سایبری فرق می‌کند. در همه دنیا سی آی ای یا مرکز امنیت ملی آمریکا، در حوزه خدمات سایبری در کشور فعالیت می‌کند؛ یعنی دامنه می‌فروشد، میزبانی داده می‌کند، امور فنی و طراحی امنیتی شبکه را انجام می‌دهد و در کشور تراکنش مالی انجام می‌دهد؛ یعنی

در اساس در فضای سایبری! از این رو باید مانند همه جای دنیا، دیتایی که توسط هر سایتی و هر درگاهی از مردم گرفته می‌شود، نگهداری شود تا هر گاه حقی از فردی ضایع شد، قابل استفاده شود. این مسئله به معنای نقض حریم نیست؛ بلکه با مجوزهای قضایی صورت می‌گیرد و هنگام گرفتاری و مشکلات مردم می‌تواند بسیاری از مشکلات را حل کند. شنود مکالمات نیز بر همین اساس است.

شاید این سؤال مطرح شود که پیامک و صوت در دیتاها ثبت می‌شود و می‌ماند؟ اگر می‌ماند، ماندگاری آن چقدر است؟

در پاسخ باید گفت: بله، توسط بسیاری از سرورهای شبکه‌های پیام رسانی که خارج از کشور است، نگهداری می‌شود. این سرورها طبق قانون موظفند یک سال داده‌های مردم، مانند صوت، فیلم و... را نگه دارند تا در صورت تضییع حق، مردم بتوانند شکایت کنند. بیش از یک سال هم شکایت مسموع نیست، چون مشمول مورد زمان است.

توصیه به خانواده‌ها

۱. سیستم عامل اندروید که فعلاً نود و دو درصد بازار سیستم موبایل را در کشور در اختیار دارد، یک سیستم عالم «متن باز»[۱] و بسیار نا امن است.شرکت گوگل قول داده است در سال ۲۰۱۹ این سیستم عامل را از برنامه‌های خود خارج خواهد کرد. نکته قابل توجه اینکه نسخه

۱. متن باز یعنی سیستم عامل مشخصات مدل گوشی شما را تشخیص می‌دهد و شماره سریال و باینری آن را بر می‌دارد، مشابه آن را پیدا کرده و دو خط کد به آن اضافه می‌کند و روی گوشی شما می‌گذارد. بدین وسیله دیگر گوشی برای شما نیست!

شش اندروید به قبل، یعنی هک کامل! اگر امنیت برایتان مهم است، بهتر است در صورت پشتیبانی سخت‌افزاری گوشی، اندرویدتان نسخه هفت به بعد باشد. در غیر این صورت، اندروید ۶ به پایین را حتماً به روزرسانی کنید. هر چند شش به بعد هم باگ[۱] دارد.

۲. اپلیکیشنی که نمی‌دانید کجا ساخته شده است، نصب نکنید. هم چنین اپلیکیشن‌هایی که هنگام نصب دسترسی‌های بسیاری چون لیست تماس، گالری و ... را از شما می‌گیرند. برای مثال اپلیکیشن روبیکا که گویا فردی دیگری آمده و در خانه شما نشسته است.

۱. باگ، یعنی خطاهایی که در برنامه به وجود می‌آید و ممکن است در اجرا و نیز از نظر امنیتی نرم‌افزار را دچار خطر کند. برای مثال برخی از باگ‌ها به هکر اجازه می‌دهد تا از طریق فرستادن فایلی که در آن کدهای مخرب جاسازی شده است، کنترل دستگاه قربانی را به دست بگیرد.