راه‌های جاسوسی از تلفن همراه هوشمند که احتمالا نمی‌دانید

استفاده از تلفن همراه هوشمند در صورت عدم آگاهی، ممکن است ناخواسته به سرویس‌های امنیتی - جاسوسی کمک قابل توجهی کند. استفاده بسیار گسترده و البته ناآگاهانه از فضای مجازی و گوشی‌های هوشمند با توجه به تهدیدات جدی و بسیار زیادی که در این حوزه به خصوص برای مسئولین کشور وجود دارد

ایران هشدار- شبکه‌های مجازی دنیایی از فرصت و تهدید را در کنار خود تولید کرده‌اند، اما استفاده بسیار گسترده و البته ناآگاهانه از فضای مجازی و گوشی‌های هوشمند با توجه به تهدیدات جدی و بسیار زیادی که در این حوزه به خصوص برای مسئولین کشور وجود دارد، این فضا را به مکانی مطلوب برای استفاده از آن به عنوان یک بستر مناسب جهت جاسوسی اطلاعات تبدیل کرده است.

در همین رابطه سردار غلامرضا جلالی رئیس سازمان پدافند غیرعامل کشور چندی پیش از ابلاغ ضوابط استفاده از گوشی‌های هوشمند توسط مسئولین و همچنین تولید گوشی‌های هوشمند بومی توسط وزاتخانه‌های دفاع و صنعت خبر داده بود.

باتوجه به اینکه امروزه فضای مجازی بستری مناسب برای جاسوسی اطلاعات به خصوص از مسئولین کشور فراهم آورده‌است، رئیس سازمان پدافند غیر عامل کشور اخیراً در نشست «بررسی آسیب های شبکه اجتماعی»، به بررسی آسیب‌ها و تهدیدهای حوزه فضای مجازی و گوشی‌های هوشمند پرداخت. با بررسی این سخنان، مشخص شد که ۱۱ تهدید اصلی در فضای مجازی و تلفن همراه وجود دارد.

نکته قابل توجه این است که باید این تهدیدات را مسئولان کشوری و لشکری را بیش از دیگران جدی بگیرند.

** شبکه های اجتماعی و جاسوسی

۱- اگر بر اساس قوانین بخواهیم شبکه‌های اجتماعی را تحلیل کنیم، شبکه‌های اجتماعی می‌توانند یک شبکه کاملا جاسوسی باشند، یعنی می‌تواند ارتباط خارج از کنترل دولتی و حکومتی را با گروه‌های اجتماعی و غیراجتماعی خارج از کشور برقرار کرده و نسبت به جمع آوری و تبادل اطلاعات اقدام کند. بنابراین بستر اقدام جاسوسی فراهم است.

** فضای مجازی؛ هویت مجازی

۲- هر کسی که وارد فضای مجازی می‌شود باید بداند یکی از ویژگی‌های این فضا گمنامی است و چهره‌ها و عکس‌هایی که برای پروفایل گذاشت می‌شود، مجازی است لذا در این فضا هویت‌ها مجازی هستند، اگر جوانان با نگاه ساده‌دلی با هویت واقعی خود وارد این فضا شوند و فکر کنند فردی که آن سوی ماجرا قرار دارد هم هویت واقعی خود را ارائه می‌دهد، باید بدانند با تهدیدات بسیاری روبرو خواهند بود.

** به چه کسی اطلاعات می‌دهیم؟

۳- از آنجایی که در فضای مجازی، هویت واقعی افراد مشخص نیست، شبکه‌های اجتماعی می‌توانند بستری مناسب برای جاسوسی باشند. از این رو نمی‌توانیم عضو هر شبکه‌ای شویم. لذا باید پیش از عضویت در هرکدام از شبکه‌های اجتماعی باید توجه داشت به چه کسی اطلاعات می‌دهیم و مرجع درخواست این اطلاعات کجاست، گرچه دانستن این موضعات سخت و گاهی غیرممکن می‌نماید، مگر آنکه این اطلاعات به مراجع رسمی شناخته شده ارائه شود. بنابراین اگر می‌خواهید از شبکه‌های اجتماعی استفاده کنید باید این مسائل را رعایت کنید.

** تاثیرگذاری با اطلاعات فضای مجازی

۴- فضای مجازی دنیای دیگری است که همه چیز در آن ضبط و ثبت می شود و هیچ راه فراری در آن وجود ندارد، سرورهای فضای مجازی در خارج از کشور است و رفت و برگشت داده‌ها از آنجا شکل گرفته و همه چیز در آن ثبت و ضبط شده است، ممکن است که روی یک موضوع تمرکز کنند، شبکه‌های اجتماعی بر مبنای داده‌های حجیم (BIG DATA) می‌تواند در رفتار یک کشور تاثیر گذاشته موجب تغییرات اساسی شود.

** ۱۱ راه جاسوسی از تلفن همراه

۵- یک بررسی ساده نشان می‌دهد حدود ۱۸ تهدید جدی در حوزه گوشی‌های هوشمند وجود دارد که هشت تهدید در حوزه اجتماعی است و ۱۰ تهدید دیگر در حوزه‌های فردی است.

در حوزه تهدیدات فردی می‌توان به ثبت اثرانگشت، عکس قرنیه چشم، شماره‌های پسورد، شنود صوتی، تصویربرداری مخفی، سرویس مکان‌یاب، دسترسی به باکس شماره تلفن‌های مخاطب، باکس پیام‌ها، باکس عکس‌های و باکس تقویم و برنامه‌ها اشاره کرد.

** برنامه‌ریزی گوشی شما از طریق بروزرسانی سیستم عامل

۶- کسانی که سرورهای فضای مجازی در دست آنها قرار دارد، می‌توانند از طریق بروز رسانی (UPDATE) سیستم عامل (OS)، گوشی فرد مود نظر را طوری برنامه ریزی کنند که این گوشی همه فرامین آنها را انجام دهد.

گوشی‌های دارای سیستم عامل، قابلیت دوباره برنامه‌ریزی و پیکربندی را دارند و وقتی از شما می‌پرسند که بروز رسانی کنند یا خیر، کشف آن خیلی ساده است و هر نرم افزاری (APPLICATION) که شما نصب می‌کنید گوشی شما قابلیت برنامه‌ریزی پیدا می‌کند و می‌تواند و به شما بگوید که کدام قسمت فعال شود، مثلا میکروفن پنهان یا دوربین پنهان یا مکان نمای شما آشکار شود یا نه، اثر انگشت شما ذخیره شود یا نشود که اینها همه قابل برنامه‌ریزی و ساده است.

** مجوز ذخیره‌سازی اطلاعات در سرور خارجی

۷- ممکن است بگوئید مگر من چه اطلاعاتی دارم، تنها اسم خودم و خانواده‌ام اینجا هست، اما مفهومی به نام دیتای حجیم (BIG DATA) وجود دارد؛ وقتی می‌خواهید تلفن خود را عوض کنید، پیامی برای شما مخابره می‌شود که آیا می‌خواهید در فضای ابری خود پشتیبان (BACKUP) تشکیل دهید، معمولا جواب مثبت است تا اگر زمانی اطلاعات از دست رفته داشته باشید، هر چیزی که در فضای ابری تشکیل داده‌اید در سرور (SERVER) ذخیره شود.

** هیچ چیز از چشم‌شان پنهان نمی‌ماند

۸- تکنولوژی‌ای وجود دارد به نام داده‌کاوی (Data Analysis) که به شکل نرم افزار و خودکار از داده‌ها و اطلاعات تک تک افراد در قالب آجرهای یک ساختمان، آنها را طوری کنار هم می‌چیند که یک ساختمان و بنای کلی از آن دریافت شود.

یعنی اطلاعات شماره تلفن شما را گرفته و براساس آن مشخص می‌کند شما چه کسی هستید و به شکل نرم افزاری، شبکه ارتباطی شما را بیرون می‌کشد. باید متوجه باشید داده کاوی اطلاعات بی ارزش شما روی هم چه ساختمان با ارزش اطلاعاتی از آن تولید می‌کند. یعنی دیگر هیچ چیز نیست که راجع به شخص ندانند.

** فضای مجازی و روز قیامت

۹- در روز قیامت، خداوند پرونده شما را جلوی شما می‌آورد و می‌گوید فلان لحظه چه کردی واقعا نمود عینی آن همین فناوری اطلاعات است، همه چیز ثبت می‌شود؛ وقتی شما اطلاعات آشکار خود را به سیستم می‌دهید، سیستم داده‌کاوی خارج از کنترل ما داده‌های پنهان ما را نیز برمی‌دارد که این کار را بر اساس دیتای آشکار تعقیب کرده است.
باید بدانید وقتی وارد فضای مجازی شدید یک دنیای دیگر است که همه چیز در آن ضبط و ثبت می‌شود و هیچ راه فراری وجود ندارد.

** فضای مجازی و انتخابات

۱۰- شبکه اجتماعی بر مبنای داده‌های حجیم (BIG DATA) می‌تواند رفتار یک جامعه را پیش بینی کند؛ برای مثال سه انتخابات اخیری که در آمریکا اتفاق افتاد. در این کشور با استفاده از نرم افزارهای جدیدی که در فرآیند انتخاباتی آمریکا مورد استفاده قرار گرفت، توانستند رای ۴۸ ایالت از ۵۱ ایالت آن را بالای ۹۰ درصد درست پیش بینی‌کنند که چه کسی رای می‌آورد و چه کسی رای نمی‌آورد.

در استرالیا انتخاباتی اتفاق افتاده که صددرصد برآورد کردند که چه کس رای می‌آورد. استراتژی اینترنتی دارد به این سمت می‌رود که IDها ثابت باشد و هر کسی هر جایی می‌خواهد وارد شود یک کد داشته باشد و یک نسخه از پرونده او ذخیره شده و معلوم باشد.

** رعایت مسائل شرعی در فضای مجازی

۱۱- هر پیام، عکس، و یا شماره‌ای که در فضای سایبری نوشته شده، قابل پاک کردن نیست. کسی که عکس فرزندش را در گوشی موبایلش خارج از عرف نگه می‌دارد، باید بداند که در فضای مجازی اصلا فضای محرمی وجود ندارد و هر مطلبی که در آن بگذارد در اختیار دیگران خواهد بود. ممکن است با رمز گذاری بشود از آنها حفاظت کرد، ولی بدانید که راه حل‌هایی وجود دارد که کسی بتواند ورود کند و عکس‌های شما را بردارد و باج خواهی کند که روش‌های آن بسیار است، بنابراین اگر می‌خواهید در فضای سایبری زندگی و از ابزار آن استفاده کنید، پس واجب است مسائل شرعی آن را بدانیم.

منبع: خبرگزاری تسنیم

اداره حراست آموزشکده شهید یزدانپناه سنندج