سه شنبه 03 فروردین 1395 - 07:04

امنیت کجای شبکه‌های اجتماعی است؟

حتما تا به حال خبرهای زیادی درباره حوادث در شبکه‌های اجتماعی شنیده‌اید؛ از انتشار تصاویر خصوصی و باج‌گیری گرفته تا سرقت و کلاهبرداری و حتی قتل که منشأ اولیه همه‌شان در تلگرام، وایبر، لاین، تانگو و... بوده است.

محمد جعفری:حتما تا به حال خبرهای زیادی درباره حوادث در شبکه‌های اجتماعی شنیده‌اید؛ از انتشار تصاویر خصوصی و باج‌گیری گرفته تا سرقت و کلاهبرداری و حتی قتل که منشأ اولیه همه‌شان در تلگرام، وایبر، لاین، تانگو و... بوده است.

با اینکه پلیس فتا حواسش به همه جا هست اما روح‌الله مومن نسب، کارشناس فضاي مجازي معتقد است: «اگر اطلاعات شما در فضاي مجازي منتشر شود و شما شكايت كنيد ممكن است فرد خاطي دستگير و مجازات شود اما هميشه به ياد داشته باشيد آبرويي كه از شما رفته ممكن است به سختي برگردد. پس بهتر است امنيت در شبكه‌هاي اجتماعي را جدي بگيريد». او در گفت‌وگو با همشهري راهكارهايي ارائه داد كه با استفاده از آنها مي‌توانيم با امنيت نسبي از شبكه‌هاي اجتماعي استفاده كنيم.

خيلي‌ها شبكه‌هاي اجتماعي را ابزار مناسبي مي‌دانند كه موجب تسهيل در ارتباطات مي‌شود اما برخي ديگر نسبت به آن بدبين هستند. ارزيابي شما از پديده اين روزهاي عصر ارتباطات چيست ؟

به‌نظر من بايد به شبكه‌هاي اجتماعي نگاه همه جانبه‌اي داشت و آن را در ابعاد مختلف بررسي كرد. مثلا به لحاظ ساختار، ابعاد مختلفي دارند. وايبر، تلگرام، اينستاگرام و... كه بازارشان اين روزها داغ شده رسانه‌هاى تعاملي هستند كه از پروژه شهروند-خبرنگار نشأت گرفتند. ماهيت اين شبكه‌ها خبري است.وقتي از اين نرم‌افزارها استفاده مي‌كنيد بيشتر خبرنگار هستيد تا كاربر. در مجموع اگر بتوانيم اين شبكه‌ها را در اختيار بگيريم كاركردشان مثبت است اما اگر از سوي آنها به‌كار گرفته شويم كاركردشان منفي است. ماهيت اين شبكه‌ها خوب است و خوبي‌هايش از بدي‌هايش بيشتر است.

استفاده از فضاي مجازي در كنار همه محاسني كه دارد قطعا با معايبي نيز روبه‌روست. چند نمونه از آسيب‌هاي امنيتي آن را بازگو كنيد.

نرم‌افزارهاي تعاملي ويژگي فني خاصي دارند كه مخابره رمز انجام مي‌دهند. براساس قانون، مخابره رمز جرم است. يعني مي‌توانند هر مطلبي را از گوشي شما بر دارند، به شكل كد دربياورند و بدون اينكه متوجه شويد به محل ديگري ارسال كنند. دسترسي‌هايي كه اين نرم‌افزارها به اطلاعات شما دارند خيلي زياد است. مثلا مي‌توانند گوشي شما را روشن و خاموش كنند، تصوير برداري كنند و به همه اطلاعات شخصي شما دسترسي پيدا كنند. اين اختيار را شما با عضويت در اين نرم‌افزارها به گردانندگان آنها مي‌دهيد. در حقيقت جسم گوشي در اختيار شماست اما روح آن در اختيار مديران شبكه، كه اين مهم‌ترين چالش امنيتي شبكه‌هاي اجتماعي است.

آيا مي‌توانيم بفهميم از چه بخش از اطلاعات ما استفاده مي‌شود يا نه؟

اگر نرم‌افزاري مثل «پكت كپچر» را نصب كنيد مي‌توانيد بفهميد چه داده‌هايي از گوشي‌تان خارج شده و به كجا منتقل مي‌شود. البته فقط مي‌توانيد ببينيد ولي قطعا غافلگير خواهيد شد چراكه مي‌بينيد مثلا عكسي كه در گالري گوشي‌تان بود به شش كشور فرستاده مي‌شود. مورد امنيتي ديگر اينكه ممكن است پورت گوشي شما باز شود. مثل اين مي‌ماند كه افرادي قفل در خانه شما را باز كنند اما در را باز بگذارند تا ديگران هم وارد شوند. با پورت باز شده، امنيت گوشي شما پايين مي‌آيد. آن موقع است كه هكرها به سادگي مي‌توانند وارد حريم شما شوند. وقتي گوشي شما هك شود پليس فتا به اين سادگي نمي‌تواند هكر را پيدا كند. چون سرور نرم‌افزار داخل كشور نيست. اما اگر اين اتفاق در يك نرم‌افزار ايراني اتفاق بيفتد مي‌شود آن را پيگيري كرد. بيشتر تخلفات انجام شده در فضاي مجازي مربوط است به شبكه‌هاي اجتماعي مثل تلگرام.

با اين فضايي كه شما از فضاي مجازي و شبكه‌هاي اجتماعي ترسيم كرديد آيا اساسا مي‌شود در اين فضا، امنيتي متصور بود؟

به‌طور كلي نمي‌شود در اين فضا امنيت را ايجاد كرد چراكه هيچ شركتي وجود ندارد كه بتواند امنيت يك گوشي تلفن همراه را بيمه كند. چون شدني نيست. چون بيمه‌گزار بايد بفهمد كه گوشي از چه ناحيه‌اي ريسك دارد. گوشي تلفن همراه ريسك‌هاي

زيادي دارد و نمي‌شود گفت كه صددرصد امن است. امنيت نسبي در اينجا موضوعيت پيدا مي‌كند كه براي آن بايد تدبير كرد. مثلا اگر گوشي شما ايراني باشد و از نرم‌افزارهاي ايراني هم استفاده كنيد مي‌شود گفت كه اگر كسي به گوشي شما دستبرد بزند آن وقت مراجع رسمي مي‌توانند پاسخگو باشند. مثلا شبكه ملي اطلاعات يكي از اصلي‌ترين زيرساخت‌هاي ايجاد امنيت در فضاي مجازي است. چون در اين شبكه ارسال و دريافت اطلاعات ما مشخص مي‌شود و قابل پيگيري است.

تبهكاران هر روز از ترفندهاي تازه‌اي براي فريب و سوءاستفاده درشبكه‌هاي مجازي استفاده مي‌كنند. از تازه‌ترين ترفندها بگوييد.

«فيشينگ» يا شبيه‌سازي صفحه‌ها زياد است. سوءاستفاده از اطلاعات عادي مردم هم زياد اتفاق مي‌افتد كه افراد شياد از طريق آن باج‌گيري مي‌كنند. از سوي ديگر دسترسي به حساب‌هاي بانكي نيز زياد شده كه براي مقابله با آن توصيه مي‌شود در گوشي‌هايي كه نرم‌افزارهاي تعاملي نصب شده از نرم‌افزار موبايل بانك استفاده نكنيد چون مي‌توانند اطلاعاتتان را كپي كنند. بيشترين دزدي‌ها از طريق همين شبكه‌هاست. وقتي نرم‌افزارها را روي گوشي‌تان نصب مي‌كنيد افراد ناشناس مي‌توانند به حساب‌هاي شما دسترسي داشته باشند و حساب بانكي‌تان را خالي كند. يا اينكه مي‌توانند عكس خصوصي شما را بردارند و باج‌گيري كنند.

براي مقابله با اين تهديدها از چه شيوه‌هاي پيشگيرانه‌اي مي‌شود استفاده كرد؟

گوشي تماستان و گوشي‌اي كه از آن براي شبكه‌هاي اجتماعي استفاده مي‌كنيد متفاوت باشد. مارك زاكربرگ مدير فيس‌بوك مي‌گويد وقتي شما از گوشي‌هاي اسمارت استفاده مي‌كنيد بدانيد در اتاق شيشه‌اي زندگي مي‌كنيد. در نتيجه چيزي را كه از ديده شدنش خجالت مي‌كشيد در گوشي‌تان نگهداري نكنيد. چون اطلاعاتي كه از آن استفاده مي‌كنيد ممكن است روزي در زندگي‌تان آشكار شود. پس هر اطلاعاتي را نبايد از طريق اين نرم‌افزارها منتشر كرد. راه ديگر اينكه روي دوربين گوشي‌تان برچسب بزنيد. اين كار ضمن اينكه عمر لنز دوربين‌تان را افزايش مي‌دهد باعث مي‌شود هكرها و بدافزارها نتوانند از دوربين شما استفاده كنند.

همان‌طور كه گفتيد هك كردن يكي از شايع‌ترين جرائم در شبكه‌هاي اجتماعي است. هكرها از چه راه‌هايي براي نفوذ به گوشي طعمه‌هايشان استفاده مي‌كنند؟

بيشتر از ناآگاهي افراد سوءاستفاده مي‌كنند. آنها دنبال فرصتي هستند كه در گوشي نفوذ كنند. اما هميشه اين فرصت را خود ما به آنها مي‌دهيم. شايع‌ترين راهي كه در اختيار هكرها است همين شبكه‌هاي تعاملي است. مثلا گاهي پيامي ناشناس براي شما مي‌آيد و از همان طريق ويروسي وارد گوشي‌تان مي‌شود. يا نرم‌افزاري را نصب مي‌كنيد كه كنار خودش يك بدافزار هم نصب مي‌كند و متوجه نمي‌شويد. اگر نرم‌افزار را هم حذف كنيد بدافزار كار خودش را ادامه مي‌دهد و كنترل گوشي‌تان را به دست مي‌گيرد.

براي پيشگيري از هك شدن چه راه‌هايي وجود دارد؟

بايد روي دروازه‌هاي ورودي گوشي‌مان بيشتر دقت كرده و از گوشي مجزا استفاده كنيم. روي لينك‌هاي مشكوك كليك نكنيم و هنگام دانلود كردن مراقب باشيم اسير ويروس‌ها نشويم. از نرم‌افزارهاي ايراني استفاده كنيم. چون اطلاعات از كشور خارج نمي‌شود و اگر هك شديم مي‌شود هكر را پيدا كرد.

نرم‌افزارهاي داخلي شبكه‌هاي اجتماعي تا چه حد امن هستند و آيا به لحاظ كاركرد مي‌شود آنها را با نرم‌افزارهاي خارجي مقايسه كرد؟

نرم‌افزارهايي كه در داخل طراحي شده‌اند حدود 80درصد از نرم‌افزارهاي خارجي امن‌تر هستند. مثلا در نرم‌افزارهاي خارجي وقتي عكسي را ارسال مي‌كنيد آن عكس در 16نقطه كپي مي‌شود اما در نرم‌افزارهاي ايراني حداكثر در 3نقطه شامل: شركتي كه از آن اينترنت خريده‌ايد، شركتي كه عمده فروش اينترنت است و شركت زيرساخت كپي مي‌شود. اما در خارجي‌ها به جز اين 3نقطه، عكس شما در 13نقطه ديگر هم كپي مي‌شود. اگر اطلاعات شما در اين فضا منتشر شود و شما شكايت كنيد ممكن است فرد خاطي دستگير و مجازات شود اما هميشه به ياد داشته باشيد آبرويي كه از شما رفته ممكن است به سختي برگردد. پس بهتر است امنيت در شبكه‌هاي اجتماعي را جدي بگيريد.

چطور مي‌شود از آلوده بودن يك لينك مطلع شد؟

تنها راه اين است كه بدانيد چه‌كسي لينك را براي شما فرستاده و لينك‌هاي ناشناس را باز نكنيد.از سوي ديگر بايد مطمئن شويد لينكي را كه دريافت كرده‌ايد واقعا از طرف دوست‌تان فرستاده شده است. در غيراين صورت لينك‌هاي ناشناس را باز نكنيد.

در مجموع چطور مي‌توانيم با خيال راحت از شبكه‌هاي اجتماعي استفاده كنيم؟

وقتي مي‌خواهيم از نرم‌افزاري استفاده كنيم اول تحقيق كنيم كه از كجا آمده و چه فرد يا شركتي آن را ساخته است. اگر به‌نظر مي‌رسد كه مي‌تواند براي ما مشكل ايجاد كند بهتر است از آن استفاده نكنيم. در اين زمينه بايد تدبير بيشتري به خرج دهيم و از طرفي دانش‌مان را درباره اين شبكه‌ها بالا ببريم تا اسير آنها نشويم.