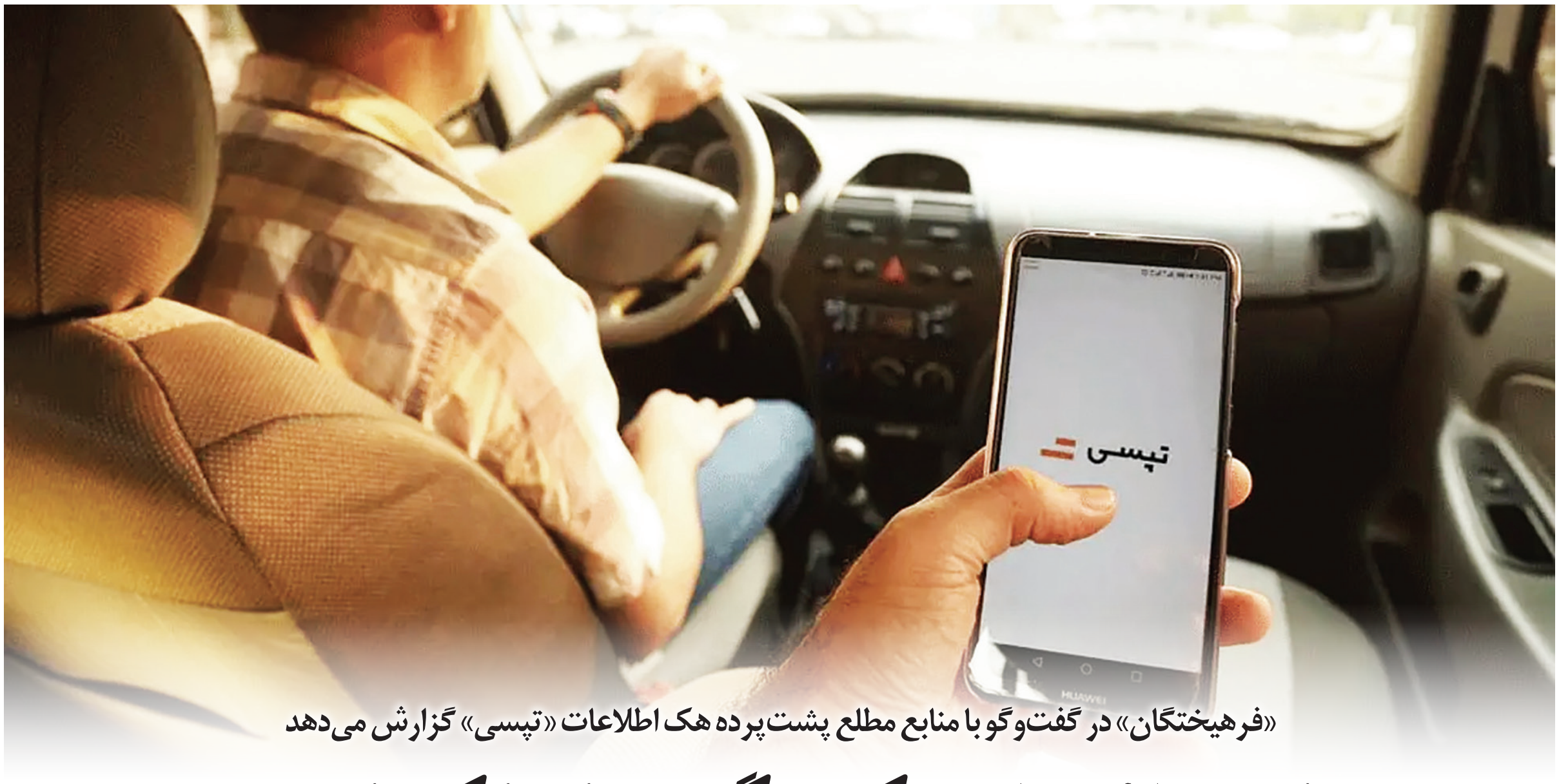
مدیرمسئول: محمدامین ایمانجانی- سردبیر: مسعود فروغی
تلفن و فکس: ۶۲۹۹۹۴۹۵ (۰۲۱) کدپستی: ۱۱۳۵۶۳۳۸۱۶
چاپ: چاپخانه دانشگاه آزاد اسلامی
نشانی: خیابان حافظ، پایین‌تر از جمهوری، روبه‌روی ساختمان بورس، ساختمان فرهیختگان، طبقه سوم



«فرهیختگان» در گفت‌وگو با منابع مطلع پشت‌پرده هک اطلاعات «تپسی» گزارش می‌دهد

پاشنه آشیل هک بیگ دیتاها کجاست

زینب مرزوقی
خبرنگار گروه جامعه

خبر از توییتر بنیان گذار و مدیرعامل تپسی منتشر شد. دقیقا دوروز گذشته، میلاد منشی‌پور، مدیرعامل تپسی در توییتر خود نوشت: «طی روزهای گذشته، متوجه دسترسی غیرمجاز به زیرساخت شرکت تپسی و برداشت بخشی از اطلاعات شدیم. به محض کشف این موضوع، ضمن ثبت شکایت، پلیس را در جریان قرار دادیم و راه دسترسی آنها را بستیم. مطابق ایمیل هایی که از گروه مهاجم دریافت کرده‌ایم، قصد آنها از این کار اخاذی بوده و برای عدم نشر اطلاعات، درخواست پول کرده‌اند. ما تصمیم گرفتیم به این اخاذی تن ندهیم؛ چراکه در مذاکره با آنها متوجه شدیم که نه‌تنها ضمانتی برای عدم نشر اطلاعات و سوءاستفاده‌های آتی وجود ندارد، بلکه تشویقی برای ادامه این اقدام درمورد سایر شرکت‌ها نیز خواهد بود. در ادامه، تلاش ما کمک به پلیس برای شناسایی گروه مهاجم و جلوگیری از فروش اطلاعات است. در انتها، بابت این اتفاق متاسفم، مسئولیت آن را می‌پذیرم و حتما بررسی دقیقی درمورد دلایل وقوع آن انجام خواهم داد. متعاقبا گزارش این بررسی را اعلام خواهم کرد.»

تا اینجای کار و تا لحظه نگارش این گزارش (ساعت ۱۶ و ۲۹ دقیقه روز یکشنبه ۱۲ شهریور ماه) هیچ‌گونه بیانیه‌ای نه در سایت و نه در اپلیکیشن تپسی برای عذرخواهی از کاربران به جز توییت مدیرعامل منتشر نشده است. به دنبال انتشار این خبر نیز «فرهیختگان» برای دستیابی به اطلاعات بیشتر به سراغ مدیران تپسی رفت. نگار عرب، مدیر روابط‌عمومی تپسی برای ارائه توضیح بیشتر در رابطه با هک صورت گرفته توضیح داد: «همان‌طور که در اطلاع‌رسانی مدیرعامل شرکت اشاره شد، ما از یک طرف ثبت شکایت کردیم و پلیس را در جریان قرار دادیم و از طرف دیگر در در تلاش بودیم جلوی سوءاستفاده از اطلاعات را بگیریم اما متوجه شدیم هیچ ضمانتی برای عدم سوءاستفاده‌های آتی وجود ندارد. به همین دلیل تصمیم گرفتیم اطلاع‌رسانی کنیم. هدف هکرها اخاذی بود و در مقابل عدم فروش اطلاعات، درخواست پول کرده بودند اما هیچ ضمانتی هم برای عدم سوءاستفاده‌های بعدی وجود نداشت.»

میلاد نوری، کارشناس امنیت سایبری در گفت‌وگو با «فرهیختگان» در رابطه با ابعاد فنی هک تپسی گفت: «معمولا همه‌جای دنیا اینکه چگونه هک انجام شده و چه کارهایی برای آن انجام شده، از طریق یک بیانیه شفاف از سمت آن شرکت مشخص می‌شود. همه‌جای دنیا چه هک‌های داخلی و چه هک‌های خارجی، اعلام می‌شود که مسئولیت را قبول کرده‌اند. دقیقا در توجیه این امر این مساله را مطرح می‌کنند که همه‌جای دنیا این اتفاق می‌افتد. این درست است ولی تفاوتی که وجود دارد درباره برخورد و عملکرد بعد از هک است. در توییتر و فیسبوک هم این اتفاقات رخ داده و بلا استثنا وقتی بررسی می‌کنیم، می‌بینیم که بیانیه منتشرشده از سوی این شرکت‌ها در سریع‌ترین زمان ممکن منتشر شده است. یعنی هدف تیم‌های روابط‌عمومی این است که همیشه پیش از اینکه خبر و موج به دست دیگران بیفتد، خودمان شفاف‌سازی کنیم. تیم‌های رسانه‌ای این شرکت‌ها کنش انجام می‌دهند اما در ایران، واکنش است. خبر منتشر می‌شود، موج به راه می‌افتد و راست و دروغ خبرها قاطی می‌شود. پس از آن دیگر شرکت چاره‌ای به جز شفاف‌سازی ندارد و حتی در آن موقع هم درست عمل نمی‌کنند. همین الان اینستاگرام، توییتر، وب‌سایت و اپلیکیشن هیچ اطلاعیه‌ای در آنها وجود ندارد. درصورتی که اولین کار این است که بیانیه شفاف صادر شود در راستای اینکه کاربران محق هستند. اینکه توضیحی ارائه دهی، باعث نمی‌شود که همه‌چیز بسته شود. شما در کوتاهی یا هر چیز دیگری که نامش را می‌توان گذاشت، سر این اتفاق به کاربران مدیونید. برای اینکه کاربران خیال‌شان راحت شود و به احساس بهتری دست پیدا کنند این بیانیه را منتشر می‌کنید. وگرنه با بیانیه، چیزی قابل جبران نیست و دکمه بازگشت به عقب ندارد. در خارج از کشور معمولا می‌گویند به این دلیل هک شدیم و بیانیه فنی به جز بیانیه روابط عمومی ارائه می‌دهند و این کار برای این است که کاربر خیالش راحت باشد از اینکه از چه طریقی هک شده و برای این مساله هم این تمهیدات را اندیشیدیم. درصورتی که چندسال پیش هم تپسی هک شده بود اما اطلاعات رانندگان بود. باز هم همان علی بابا وقتی هک شد، اعلام کرد که مسئولیت را پذیرفته‌ایم. خب این تنها یک جمله است. مسئولیت چه چیزی را پذیرفته‌اید؟ اطلاعات فنی و کارهایی که برای جلوگیری از این کار صورت گرفته کجاست؟ خارجی‌ها یکی از کارهایی که برای این کار انجام می‌دهند این است که در سریع‌ترین زمان ممکن، کاربر را آگاه می‌کنند و به کاربر اطلاع می‌دهند که کاربر هک شده. هرکسی در درجه مختلفی حائز اهمیت است. ممکن است کاربری بگوید اطلاعات من به چه دردی می‌خورد؟ یا یکی دیگر بگوید سفرهای من برایم حساس بوده‌اند و از طرف فرد ناشناس در فضای مجازی تهدید می‌شد. افرادی که در دارک وب این اطلاعات را دسته‌بندی و استفاده می‌کنند هم آدم‌های سالمی نیستند یا کلاهبرداری است یا هک‌های اجتماعی یا هر استفاده غیرسالم از کاربر است. تپسی اعلام کرده از یک ماه گذشته در جریان این امر قرار گرفته‌ایم. خب چرا در این یک ماه کاربر را مطلع نکردید؟ یا همین الان چرا از توییتر مدیرعامل شخصی اعلام کردید؟ آیا همه کاربران تپسی توییتر مدیرعامل را می‌خوانند؟ خیر! همین الان ممکن است کاربران زیادی از تپسی حتی این خبر به گوش‌شان هم نرسیده باشد. ممکن است با موج خبری که راه افتاده باخبر شده باشند اما تپسی باید آن را در جای عمومی‌تری مانند وب‌سایت خود تپسی، توییتر، اینستاگرام و اپلیکیشن تپسی اعلام می‌کرد. کاربر از سوی منابع رسمی تپسی از این موضوع آگاه نشده است. متاسفانه بعضی وقت‌ها هکی اتفاق می‌افتد که اسم و شماره تلفن و... معطوف به همان کسب‌وکار است. اما در اطلاعاتی که از تپسی هک شده ظاهرا آیدی تبلیغ گوگل و دیگری دیوایس آیدی است که این دیوایس آیدی روی گوشی‌های اندروید منحصربه‌فرد است و تا اندروید ۸ به بعد برای همه گوشی‌ها مشترک است. یعنی گاهی چند سفر است که حساسیتی روی موضوع نیست اما گاهی کاربری در اپلیکیشنی حضور داشته و به هر دلیلی نمی‌خواسته که هویتش و حضورش فاش شود. این کاربر در اپ دیگری خبری را خوانده و آن اپ شناسه و دیوایس کاربر را ذخیره کرده است. اگر این دو تا دیوایس را کنار هم قرار دهیم مثلا می‌توانیم بفهمیم که فلان شخص با این حجم از سفرهاست. حالا شما این را در همه دیتاباک‌های منتشرشده کنار هم قرار دهید. همه دیتاباک‌های منتشرشده هویت افراد معنی پیدا می‌کرد. مثلا شما لیست سفرتان که درمی‌آمد از دیتاباکس دیگری کدپستی‌تان لو می‌رفت. اما این دیوایس آیدی و شناسه‌هایی که از روی تپسی لو رفته با روش آن ناشناس حتی به‌عنوان خواننده یک خبر هم لو رفته است. این یک قسمت به این بازمی‌گردد که کسب‌وکارها چه بزرگ و چه کوچک کاربر را به مقاصد تبلیغاتی دوباره بازگرداند و سازمان‌ها هم عطش ذخیره چنین اطلاعاتی را دارند. شما خیلی وقت‌ها می‌بینید روی دیتابیس آن اپ برای آنالیز رفتار کاربر حتی ابعاد گوشی فرد را هم ذخیره کرده است. شاید دیتای مهمی هم نباشد اما در دیتای تپسی وقتی نگاه می‌کنیم، چند پلتفرم در این پلتفرم‌های تبلیغاتی می‌بینیم و این دیتایی اضافه است که نگه داشته‌اند و حتی ممکن است اضافه هم باشد. مثلا دیتای لیست سفرها و لزوم نگه داشتنش را اطلاعی ندارم و ممکن است برای پیگیری‌های قضایی ذخیره کنند. البته همین هم راهکاری دارد که ممکن است این سفرهای قدیمی‌تر را در سریال‌های دیگری ذخیره کنند اما اینها بایدها و نبایدهاست.»

پساهک و هکرهای کلاه‌سفید

نوری همچنین درباره بیشتر شدن کاهش بستر سایبری کشور در چند سال اخیر نیز ادامه داد: «بازگشت دوباره اعتماد کاربر کاملا به بیانیه روابط عمومی و فنی بستگی دارد. مثلا توییتر که هک شده بود لحظه به لحظه توییت می‌زدند که ما اکنون تا این لحظه به این اطلاعات رسیده‌ایم و درحال بررسی هستیم. اما درحال حاضر تپسی از هیچ کانال رسمی‌ای اظهارنظر نکرده که به‌دست همه کاربران آن برسد. حتی اکنون با این اظهارنظر در توییتر خیلی‌ها منتقد این هستند که وقتی شما یک ماه از مساله خبر دارید، چرا این همه دیر اطلاع‌رسانی کرده‌اید؟ چرا پس از اینکه هکرها نمونه‌های دیتاها را منتشر کرده‌اند، این عملکرد را داشتید؟ خود این عملکرد اشتباه پی‌آری باعث می‌شود که از این اطمینان بیش از پیش آسیب ببینید. یا مثلا از طرف معاونت اجتماعی پلیس فتا دیدم که گفته شده برای کاربران هیچ جای نگرانی نیست. اتفاقا در چنین مواقعی پلیس فتا باید کاربران را آگاه کنند، چون خیلی از کاربرهایی که آگاهی و دانش‌شان کم است این استرس را دارند که من کاربر باید چه کاری کنم؟ در توییترم نوشتم که یکی از ساده‌ترین کارها این است که جی‌آی‌پی‌تان را در گوگل تغییر دهید. حداقل زنجیره اتصال شما در کنار چند دیتابیس دیگر که ناشناس حضور داشتید، شکسته می‌شود. این آگهی را باید بدانند. تمام اینها به‌عهده کسب‌وکار است. اکنون نیز باید کسب‌وکارها کارهایی را انجام دهند که طبق استاندارد همه‌جای دنیا انجام می‌شود. دلیل اینکه هک‌ها زیاد شده و از سمت مسئولان نیز انکار می‌شود، مهاجرت است. اینکه ما نیروی متخصص به تعداد کافی داشته باشیم یک بحث است و اینکه نیروی متخصص باتجربه داشته باشیم یک بحث دیگر. وقتی افرادی که ۱۰ الی ۱۵ سال در حوزه امنیت و برنامه‌نویسی یا سرور تجربه دارند مهاجرت می‌کنند و افرادی که سابقه کمی دارند در شرکت جایگزین می‌شوند نتیجه‌اش این می‌شود. وقتی آمارها را می‌بینیم، متوجه می‌شویم که تعداد برنامه‌نویسان چند درصد رشد داشته‌اند، ولی این درحالی است که فلان شرکت نیروهای باسابقه‌اش را از دست داده و نیروهایی با سابقه کم جایگزین شده‌اند. مهم‌ترین مشکل ما در هک‌های اخیر بحث مهاجرت نیروهای باتجربه و متخصص است. در شرکت‌های فنی، بدون استثنا همیشه چندنفری هستند که برنامه مهاجرت‌شان را دارند پیش می‌برند. یکی دیگر از دلایلش هم این است که خیلی وقت‌ها ما صورت‌مساله را پاک کرده‌ایم. ببینید اکنون شرکت‌های دولتی یا بانک‌ها دسترسی خارج از ایران را بسته‌اند. به نظرشان اینها امنیت‌شان را حفظ کرده‌اند اما به‌جای اینکه امنیت را بالا ببرند، دسترسی را کلا بسته‌اند تا هکرها و خرابکارها دسترسی نداشته باشند. این درصورتی است که ما در جهان هکرهای کلاه‌سفید داریم که باگ‌ها را تشخیص می‌دهند و درعوض دسترسی به باگ سایت‌ها پول می‌گیرند و گزارش می‌دهند اما سازمان‌های ما وقتی هکرهای کلاه‌سفید باگ را پیدا می‌کنند یا پول‌شان را پرداخت نمی‌کنند یا حتی پیش آمده از آنها شکایت هم کرده و برای خیلی‌ها دردسر ایجاد می‌کنند. مساله دیگر این است که هر چه در این چندسال خبرهای بیشتری از هک‌ها در ایران منتشر می‌شود، هکرهای خارجی نسبت به تست هک در سایت‌های ایرانی کنجکاو شوند و بخواهند هک در ایران را تست کنند.»

شکل سرقت‌ها در عصر تکنولوژی تغییر کرده است

محمد کشوری، کارشناس فضای مجازی نگاه کلان‌تری به موضوع دارد. کشوری معتقد است که طبعا هرقدر بیشتر ابعاد مختلف زندگی‌مان بسته به شبکه و فضای مجازی می‌رود، این امر طبیعی است: «در این فضا مشکلات و معضلات امنیتی نیز بیشتر خودش را نشان می‌دهد. زمانی اگر شخصی از بانک قصد خروج داشت، باید از پولش مراقبت می‌کرد. اکنون اما این شیوه از سرقت دیگر کم شده و دیگر شما خبری از این مساله نمی‌شنوید که افراد جلوی بانک‌ها منتظر این باشند که چه کسی با کیسه پول خارج می‌شود. وقتی که ما زندگی‌مان روی شبکه می‌رود، طبیعتا سرقت‌هایمان هم آنلاین می‌شوند. ما تا چندسال پیش، سرقت اطلاعات تاکسی برایمان بی‌معنی بود اما وقتی حمل‌ونقل شهری‌مان را با تاکسی اینترنتی پیش می‌بریم، طبیعی است که این اطلاعات مثلا هک شود یا از طریق این اطلاعات اخاذی شود. پس به نظرم بخشی از طبیعت این فضا است. همان‌طور که برای قوی‌ترین تیم‌های اینترنتی نشت اطلاعات و سرقت اطلاعات اتفاق افتاد. اینها توجیه نیست ولی بخشی از آن توجیه‌ناپذیر است. طبیعی است که سارقان نیز مدل سرقت‌شان تغییر می‌کند. در مساله دوم اما یک سری سازوکارها به حاکمیت بازمی‌گردد و آن این است که ما قوانین درستی درباره پردازش و جمع‌آوری داده‌ها داشته باشیم. ما در طرح صیانت هم این موارد را می‌گفتیم که به جای اینکه شما چیزهایی بنویسید که عملا امکان تحقق ندارند، برای پلتفرم‌های داخلی چهارچوبی برای جمع‌آوری داده‌ها داشته باشیم. بعضی از پلتفرم‌ها، داده‌هایی را گاهی جمع‌آوری می‌کنند که تنها برای همان زمان ارائه سرویس ضرورت دارد و ضرورتی برای نگهداری ندارند. یعنی بعد از اینکه سرویس تمام شد، داده‌ها باید امحا شوند و از بین بروند. نکته بعدی این است که پس از اینکه داده‌ها را جمع‌آوری می‌کنند، این داده‌ها را باید با مقررات مشخص نگه‌داری کنند. یعنی امنیت سروری که نگهداری می‌کند و الزامات امنیتی را رعایت کنند. مساله بعدی هم این است اگر تمام این موارد را رعایت کردند، از هکرهای کلاه‌سفید کمک بگیرند. مسابقه و فرآیندی را بگذارند که از هکرهای کلاه‌سفید برای شناختن باگ‌های پلتفرم‌شان استفاده کنند.» پوریا استرکی نیز در گفت‌وگو با «فرهیختگان» گفت: «به‌طور کلی اختلالاتی که از پارسال به وجود آمد، عمدی ایجاد شد و به همین دلیل امنیت را به خطر انداخت. یعنی بعضی از پروتکل‌های شبکه را مختل کرد. مثلا پروتکلی که ارتباط بسیار امن را با سرور ایجاد می‌کند؛ اختلالاتی که روی پروتکل‌های امنیتی نیز ایجاد شد و این اختلالات هم امنیت جابه‌جایی داده را مخدوش می‌کند و کاهش می‌دهد. یا اینکه سرعت را کاهش می‌دهد یا به‌طور کل امکان استفاده از پروتکل‌های امنیتی برای افرادی که کارهای امنیتی در حوزه سایبری انجام می‌دهند؛ از بین می‌رود. این اختلالات گاهی شدید و گاهی ضعیف می‌شد. اینها دشواری خاص خود را برای افرادی که کارهای روزمره را با شبکه انجام می‌دادند ایجاد می‌کرد. به جز این، طبعا مهاجرت بچه‌های فنی و باسابقه نیز شدت زیادی گرفت. دلایل این مهاجرت نیز یکی همین ناامنی شبکه و به تبع آن بازار کار در رشته‌های فناوری و کاهش سرمایه‌گذاری در اکوسیستم فناوری است. دلیل دیگر هم سقوط ارزش ریال است. یعنی حقوق‌هایی به افراد از همین کشورهای اطراف به بچه‌های کاربلد و فنی پیشنهاد شد که اصلا شرکت‌های ایرانی امکان پرداخت این حقوق‌ها را ندارند. برای همین یک شرکت فنی در ایران، امکان پرداخت چنین حقوق‌هایی را به بچه‌های فنی ندارد. بنابراین بچه‌های این حوزه یا مهاجرت می‌کنند یا در کشور خودمان از خارج پروژه می‌گیرند.»

متاسفانه این اولین باری نیست که اطلاعات کاربران از یک پلتفرم ایرانی لو می‌رود و به دنبال این لو رفتن، آنچه که ضربه می‌خورد اعتماد کاربر است. مشکل تپسی برای هک چه سخت‌افزاری بوده باشد و چه نرم‌افزاری، باز هم متاسفانه یک ماه این مساله را کتمان کرد و با کاربران خود صادقانه مشکل را پیش نبرد. علاوه‌بر این اطلاع به کاربران از شیوه رسمی صورت نگرفت و توییتر مدیرعامل خبر هک شدن و لو رفتن اطلاعات کاربران را اعلام کرد. این امر نیز به خودی خود به جز عدم شفافیت با کاربران، ضعف محسوب می‌شود؛ چراکه اطلاع‌رسانی سلسله مراتب لازم را برای باخبر شدن کاربر طی نکرده و از این گذشته تنها به چند رشته و بدون توضیح دلایل فنی، بسنده کرده‌اند. این خود به تنهایی نشان از این است که هنوز ابعاد فنی هک برای مسئولان این پلتفرم روشن نشده است. داستان تپسی از قصه لو رفتن تصویر مانیتور کارشناسان بله هم برای کاربران دارک‌تر است و به قول میلاد نوری، این مساله با یک عذرخواهی ساده و پذیرفتن مساله پس از یک ماه شاید از سوی کاربر پذیرفته نشود.