گزارش هفته
تپش
۴ | ویژه‌نامه حوادث | روزنامه جام‌جم
چهارشنبه ۱۱ بهمن ۱۴۰۲ | شماره ۱۰۵۰

گزارش «جام‌جم» از افزایش ف

جولان هکر

مجید غمخوار
تپش

نام‌شان مجرمان پنهان یا سیاه است. همیشه یک قدم از پلیس و مردم جلوتر هستند و با شگردهای جدید، مدت‌ها حساب بانکی افراد را تخلیه و از آنها کلاهبرداری می‌کنند. این روزها هکرها با ارسال لینک‌های آلوده و بدافزار بلای جان کاربران شده، حساب شهروندان را هک کرده یا از طریق گوشی آنها از دیگران کلاهبرداری می‌کنند. افزایش پرونده‌های هک، صدای پلیس را هم درآورده و رئیس پلیس فتای تهران از افزایش پرونده هک خبر داده است. تا چند سال قبل فیشینگ، کلاهبرداری کارت به کارت و اسکیمر روش‌های مورد استفاده کلاهبرداران مجازی بود اما با اطلاع‌رسانی گسترده و راه‌اندازی رمز پویا با همکاری بانک مرکزی و پلیس فتا، درصد زیادی از این کلاهبرداری‌ها کاهش یافت. این روزها براساس اعلام پلیس فتا، هک تلفن همراه و دسترسی غیرمجاز به سیستم‌های الکترونیکی برای کلاهبرداری و اخاذی مجازی افزایش یافته و بیشترین شکایت‌های مجازی را تشکیل می‌دهد.

ارسال لینک آلوده جدیدترین روش کلاهبرداری

کلاهبرداران که همیشه روش جدیدی را برای رسیدن به مقاصد خود طراحی می‌کنند، سراغ روش جدیدی رفته‌اند و با ارسال لینک آلوده، دسترسی غیرمجاز به گوشی یا سیستم فرد پیدا کرده و دست به کلاهبرداری و گاهی اخاذی می‌زنند. مجرمان سایبری برای این‌که بتوانند لینک آلوده را فعال کنند، بیشتر از عناوین جذاب به‌ویژه ثبت‌نام سهام عدالت، دریافت یارانه یا قرعه‌کشی برای اهدای جایزه استفاده می‌کنند. افراد نیز به علت جذاب بودن متن و طمع دریافت جایزه یا سود سهام عدالت، روی لینک کلیک کرده و با دریافت بدافزار، اجازه ورود مجرمان به گوشی خود را می‌دهند. مجرمان سپس اطلاعات شخصی و مهم مالباخته را سرقت و از او اخاذی می‌کنند.

لینک دریافت سهام عدالت گرفتارم کرد

عباس، پسر ۳۶ ساله که گرفتار هکرها شده، به جام جم گفت: پیامی روی گوشی تلفن همراهم آمد که خبر از دریافت هفت میلیون تومان سود سهام عدالت داشت. چون سهام عدالت نداشتم، وارد آن لینک شدم و پس از ثبت اطلاعات، اپ مورد اشاره را نصب کردم. دقایقی بعد یکی از دوستانم تماس گرفت و گفت از تلگرامم برایش پیام آمده و هک شده‌ام. شوکه بودم تا این‌که فهمیدم تلگرامم هک شده و پیامی برای تمام مخاطب‌هایم ارسال و از آنها درخواست پول شده است. سریع وارد تنظیمات گوشی شدم و فهمیدم با دو دستگاه گوشی به تلگرامم دسترسی دارند. آنها نتوانستند از حسابم پول برداشت کنند اما لینک آلوده را برای ۵۰۰ نفر از مخاطبانم ارسال کردند و حالا تمام اطلاعات هویتی من را هم در اختیار دارند.

هک برای قدرت‌نمایی یا کلاهبرداری؟

این روزها با بررسی پرونده‌های پلیس فتا، متوجه افزایش شکایت‌های هک و دسترسی غیرمجاز به تلفن همراه و داده‌های شخصی افراد می‌شویم. در این میان اما موضوع قابل‌توجه انجام هک از سوی مجرمان کم‌سن و سال است. برخی از این مجرمان از روی کنجکاوی یا نشان دادن قدرت خود در تسلط به فضای مجازی و نرم‌افزارها، اقدام به هک کرده و تبدیل به مجرم سایبری می‌شوند. گروهی نیز مجرمان قدیمی این حوزه‌اند که بیشتر به دنبال کلاهبرداری هستند و برای رسیدن به هدف‌های خود، سراغ بدافزارها رفته‌اند. این گروه از مجرمان به حساب قربانیان رحم نکرده و تمام موجودی آن را برداشت می‌کنند. عده‌ای نیز سعی کرده‌اند با معرفی خود به عنوان هکر در این فضا پول مفتی به جیب بزنند. این کلاهبرداران با تیلیغات گسترده ادعا می‌کنند می‌توانند خیانت همسر را فاش کنند و به شبکه‌های اجتماعی و گوشی آنها دسترسی داشته باشند.

کلاهبرداران این حوزه پس از دریافت پیش‌پرداخت ناپدید شده و راه ارتباطی قربانی را مسدود می‌کنند. گاهی نیز شماره همسر را از سفارش‌دهنده گرفته و مسیر دیگری را برای اخاذی در پیش می‌گیرند. آنها با سفارش‌دهنده تماس گرفته و برای این‌که نیت آنها را پیش همسرشان افشا نکنند، اخاذی کلان می‌کنند.

هکرهای کلاه‌سفید چه می‌کنند؟

دسته دیگری از مجرمانی که به صورت حرفه‌ای اقدام به هک می‌کنند، هکرهای کلاه‌سفید هستند. این دسته بیشتر سراغ ارگان‌ها و سازمان‌ها رفته و با هک سیستم‌های آنها به دنبال نشان دادن ضعف‌های ایمنی هستند. این هکرها معمولا بعد از توافق با سازمان برای درز ندادن اطلاعات آنها، مبلغی را دریافت و ایرادات فنی و امنیتی سیستم‌های آنها را در اختیارشان قرار می‌دهند.

هشدار درباره افزایش هک

سرهنگ داوود معظمی‌گودرزی
رئیس پلیس فتا تهران

با توجه به افزایش پرونده‌های پلیس فتا در مورد کلیک روی بدافزارها و کلاهبرداری از کاربران و هک، باید گفت که این روش اگرچه تازه است اما در حال افزایش است و متاسفانه شهروندان زیاد قربانی آن می‌شوند. آنچه مهم است، این‌که تنها با کلیک نکردن روی لینک ناشناس، می‌توان به‌سادگی از وقوع جرم و تبدیل شدن به مالباخته جلوگیری کرد. افراد باید بدانند به هیچ عنوان برنامه‌های ناشناس، ناامن یا زیاد تبلیغ‌شده در فضای مجازی را نصب نکنند. بهترین روش، فعال کردن تایید هویت دو مرحله‌ای است و به هیچ عنوان نباید رمز و اطلاعات شبکه‌های اجتماعی خود را در اختیار دیگری قرار دهند. در صورتی که پیامی در شبکه‌های اجتماعی از سوی دوستان یا آشنایان‌تان مبنی بر درخواست واریز وجه دریافت کردید، حتما از طرق دیگر نظیر برقراری تماس تلفنی صحت محتوای پیام ارسالی را قبل از واریز وجه احراز کنید. یکی از آسان‌ترین روش‌ها برای گرفتار نشدن در دام این مجرمان، فعال کردن احراز هویت دو مرحله‌ای شبکه‌های اجتماعی است که در این صورت کار برای مجرمان سخت و تقریبا محال می‌شود. متاسفانه بسیاری از کسانی که در دام مجرمان گرفتار و تبدیل به مالباخته شدند، رمز ورود دو مرحله‌ای نداشتند. البته مجرمان هک هم باید بدانند که قانون با آنها برخورد می‌کند. براساس ماده ۱ قانون جرایم رایانه‌ای «هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده، دسترسی یابد؛ به حبس از ۹۱ روز تا یک سال یا جزای نقدی از دو تا هشت میلیون تومان یا هر دو مجازات محکوم خواهد شد.»