

با وجود تدابیر شدید امنیتی و راهکارهای حفاظتی اتخاذ شده از سوی بانک‌ها، کلاهبرداری اینترنتی از حساب‌های بانکی آنلاین در برخی از کشورها رواج دارد. خساراتی را متوجه بانک‌ها می‌سازد. از آنجا که توسعه بانکداری الکترونیکی در دنیای امروز امری اجتناب‌ناپذیر است، بانکداران به طور جدی در صدد مقابله با دزدی‌های اینترنتی برآمده و برنامه‌های مختلفی را در این زمینه به اجرا گذاشته‌اند. براساس اظهارات مدیر ارشد یک بانک انگلیسی این اقدامات در سال ۲۰۰۶ منجر به کاهش چشمگیر کلاهبرداری اینترنتی شده است.

«رخا منون» از حيله هکرها برای دزدی از حساب کاربران آنلاین بانک‌ها و موفقیت آنها گزارش می‌دهد. بزرگترین نمونه کلاهبرداری آنلاین در دنیا سال گذشته رخ داد که حدود یک میلیون یورو از حساب مشتریان برجسته سوئدی بانک «نوردی» اسکاندیناوی ربوده شد. هکرها به شکلی باور نکردنی و متقلبانه جزئیات مربوط به ورود مشتریان به سیستم را همانند تراشه تراشه کردند.



اقدامات بانک‌های بزرگ جهان:

مقابله با

کلاهبرداری الکترونیکی

منبع: The Banker
ترجمه: پوپک محبعلی

به گفته دیویس، با پیشرفت فناوری و امور بانکداری و بهبود سرمایه گذاری در سیستم های امنیتی، مجرمان تمام تلاش خود را نه برای حمله به سیستم های بانکی، بلکه برای دفاع حداقل صرف کرده اند و بر این اساس به سادگی از مشتریان بانکی خواسته می شود جزئیات مربوط به حساب های بانکی خود را فاش کنند.

افزایش سطح سیستم های امنیتی بستگی دارد که امروزه از سوی بانک ها گسترش یافته است. به گفته دیویس، با پیشرفت فناوری و امور بانکداری و بهبود سرمایه گذاری در سیستم های امنیتی، مجرمان تمام تلاش خود را نه برای حمله به سیستم های بانکی، بلکه برای دفاع حداقل صرف کرده اند و بر این اساس به سادگی از مشتریان بانکی خواسته می شود جزئیات مربوط به حساب های بانکی خود را فاش کنند.

اعمال مجرمانه به سرعت رو به گسترش است به طوری که تا دو سال پیش دزدی آنلاین بانکی چندان شناخته شده نبود، اما امروزه تهدید بزرگی محسوب می شود. «کاری اوکسانن»، رئیس مدیریت ریسک و بانکداری الکترونیک «نوردی» می گوید: ما باید آمادگی مقابله با این تهدید را داشته باشیم. برنامه امنیتی نوردی به علت زیان های فراوانی که از طریق دزدی اینترنتی متحمل شده، شامل تدابیر شدیدی برای افزایش امنیت خدمات بانکداری الکترونیک خود است. اوکسانن در ادامه خاطر نشان می سازد: ما در گذشته هم برنامه هایی برای بهبود امنیت سیستم بانکداری الکترونیک خود داشتیم، اما با مشکلاتی که در سوئد پیش آمده، پیشبرد برنامه خود را تسریع کرده ایم.

به عنوان گام اول، بانک، فناوری تصدیق مشخصات کاربران از طریق ارائه کارت را در اختیار ۷۸ میلیون مشتری آنلاین سوئدی خود قرار داد که مورد دزدی آنلاین واقع شده اند. بانک پنج میلیون مشتری آنلاین دارد و در صد گسترش برنامه های خود و افزایش تدابیر شدید امنیتی برای مشتریان خود از سایر کشورهای شمالی است.

حفاظت دو جانبه

تصدیق دو عاملی، رایج ترین فناوری است که امروزه بانک های سراسر جهان برای افزایش امنیت خدمات بانکداری خود از آن استفاده می کنند و ضریب امنیت بانکداری الکترونیکی را تا حد قابل ملاحظه ای بالا می برد. مشتریان علاوه بر وارد کردن رمز عبور، با استفاده از یک

برنامه ای است که در ظاهر بی خطر به نظر می رسد، اما نرم افزار مخربی را نصب می کند. کلاهبرداران از نسخه های جعلی وب سایت های بانک برای اغوای مشتریان سود می جستند تا از این طریق مشتریان جزئیات حساب بانکی خود را فاش کنند. مشتریان نوردی ایمیل هایی دریافت می کردند که به نظر می رسید از جانب بانک است و از آنها خواسته می شد به یک ابزار anti-spam را روی رایانه خود دانلود کنند. رایانه افرادی که این ابزار بر روی آن نصب می شد به ویروس haxdoor.ki تروا آلوده و فعالیت های آنلاین آنها کنترل می گردید و هنگامی که کاربران سعی داشتند به حساب بانکی آنلاین خود وارد شوند این ویروس وارد عمل می شد. برنامه تروا جزئیات ورود کاربران به سیستم را ذخیره می کرد و سپس یک پیغام خطا نشان می داد و از کاربران می خواست اطلاعات ورود به سیستم را دوباره وارد کنند. و سپس هکرها از این طریق حساب بانکی مشتریان را خالی می کردند. پایگاه اصلی هکرها در روسیه بود.

خسارات ناشی از نصب نرم افزارهای ویروسی

بدون شک جرایم آنلاین یکی از بزرگ ترین چالش هایی است که امروزه بانک های سراسر جهان با آن مواجهند. براساس گزارش اخیر شرکت Aite Group، ۳۸ درصد از بانک های برتر آمریکایی ۱۲ ماه گذشته با افزایش روزافزون زیان های ناشی از کلاهبرداری های آنلاین بانکی روبرو بوده اند. طبق برآورد انجمن پرداخت های بریتانیا (APACS)، زیان های ناشی از دزدی های اینترنتی بانک ها در سال گذشته میلادی به ۳۳/۵ میلیون پوند (۴۹ میلیون یورو) رسید که نسبت به سال قبل از آن ۴۴ درصد افزایش داشت. براساس تحقیقات APACS دزدی آنلاین در ۱۸ ماه گذشته با افزایش چشمگیری روبرو بوده و از ۱۷۱۳ مورد در سال ۲۰۰۵ به ۱۴ هزار و ۱۵۲ مورد در سال ۲۰۰۶ رسیده است. «بارنابی دیویس»، رئیس بانکداری الکترونیک بانک «بارکلی» در این باره گفت: این گونه کلاهبرداری ها، تهدید مسلمی برای بانکداری آنلاین است. علاوه بر برنامه تروا، ویروس ها و تکنیک های پیچیده دیگری نیز وجود دارد که به این امر دامن می زند. وی افزود: افزایش کلاهبرداری اینترنتی مستقیماً به

تروا، یک برنامه رایانه ای به ظاهر بی خطر اما در واقع مخربی است که جزئیات ورود کاربران به حساب بانکی را ذخیره و سپس هکرها موجودی آن حساب را خالی می کنند

می‌شود تا کسانی که از بانکداری الکترونیک بهره می‌برند، با واریز مبالغ پرداختی خود به حساب شخص ثالث، فرمان‌های ثابتی ایجاد کرده و یا رمز عبور خود را تغییر دهند. بارکلی نیز اخیراً کارت خوان‌هایی را بین ۵۰۰ هزار نفر از دو میلیون مشتری فعال خود توزیع کرده و تصمیم دارد تا پایان سال باقیمانده مشتریان خود را از این مزایا بهره‌مند سازد. «دیویس» از بانک بارکلی می‌گوید: برنامه تصدیق دو عاملی در مبارزه با دزدی آنلاین بسیار موثر خواهد بود و قطعاً کاهش اعمال متقلبانه را به همراه خواهد داشت.

یک راهکار متفاوت

بانک HSBC برخلاف رقبای خود هنوز از برنامه تصدیق دو عاملی استفاده نکرده و برای آینده نزدیک نیز راهکاری ندارد. «نیک استیب»، مدیر ارشد بانکداری الکترونیکی شخصی بانک HSBC می‌گوید: ما فناوری تصدیق دو عاملی را تنها در اختیار مشتریان عمده خود قرار داده‌ایم و به نظر نمی‌رسد این سیستم برای مشتریان خرده پا ضروری باشد.

طبق اظهارات استیب، درحالی‌که بانک HSBC بیش از ۲۰ درصد سهام بازار بانکداری الکترونیک بریتانیا را در اختیار دارد، زبان‌های ناشی از دزدی آنلاین تنها ۳ درصد از این سهام را دربر می‌گیرد. او در ادامه می‌گوید: با اجرای این سیستم امنیتی، بانک HSBC هیچ ضرورتی نمی‌بیند از فناوری تصدیق دو عاملی استفاده کند. علاوه بر این استیب معتقد است تصدیق دو عاملی برنامه مناسبی برای مشتریان بانک‌ها نیست. چالش اساسی امنیت آنلاین، برقراری توازن بین اقدامات امنیتی مناسب با تقاضای مشتری و سهولت استفاده از آن است. ما احساس می‌کنیم مشتریان تکنیک‌های تصدیق دو عاملی را تایید نکرده و آنها را طاقت فرسا تلقی می‌کنند.

ابزار فیزیکی مثل کارت خوان و علائمی که رمزهای یک رویه را در حین ورود به سیستم ایجاد می‌کند، می‌توانند هویت خود را تأیید کنند. در آمریکا که قوانین مربوط به کاربرد بهینه اقدامات امنیتی برای حصول اطمینان از بانکداری الکترونیک بدون خطر برای مشتریان تدوین شده است، بسیاری از بانک‌های بزرگ از تصدیق دو عاملی بهره می‌جویند. این سیستم در بریتانیا نیز مورد استفاده قرار می‌گیرد. بانک لوید TSB طرح مقدماتی دو عاملی خود را در اکتبر ۲۰۰۵ با ۲۳ هزار و ۵۰۰ مشتری و با استفاده از یک دستگاه رمز آغاز کرد و بانک Alliance Leicester در می ۲۰۰۶ طرح خود را به مرحله اجرا درآورد.

بر خلاف اکثر بانک‌ها، Alliance Leicester از ابزار فیزیکی جداگانه‌ای استفاده نکرده است. دارندگان حساب هنگام ثبت نام اینترنتی تصویری را انتخاب می‌کنند که در هر بار ورود به سیستم الکترونیک بانک این تصویر به نمایش در می‌آید تا افراد مطمئن شوند وب سایت اصلی بانک را باز کرده‌اند.

به‌رغم رویکردهای مختلف، بانک‌های فوق به نتایج مثبتی دست یافته‌اند. کارکنان بانک Alliance Leicester معتقدند این فناوری در مبارزه با دزدی آنلاین بسیار موثر بوده است و کارکنان بانک لوید TSB نیز می‌گویند هیچ‌یک از مشتریانی که در طرح مقدماتی مشارکت کردند در ۱۸ ماه گذشته با مشکل دزدی اینترنتی مواجه نشده‌اند.

سایر بانک‌های بزرگ بریتانیا از قبیل RBS و بارکلی نیز در راستای مبارزه با کلاهبرداری‌های آنلاین طرح‌های استفاده از کارت و تصدیق دو عاملی را به مشتریان خود ارائه داده‌اند.

یکی از سخنگویان RBS که طرح خود را در سال جاری آغاز می‌کند، می‌گوید: راه حل افزایش امنیت خدمات بانکداری الکترونیک طی مراحل طی مشتریان عرضه

تصدیق دو عاملی، رایج‌ترین فناوری است که امروزه بانک‌های سراسر جهان برای افزایش امنیت خدمات بانکداری خود از آن استفاده می‌کنند

پرتال جامع علوم انسانی





بانک‌هایی که فناوری تصدیق دو عاملی را بکار برده‌اند، بگونه‌ای دیگر می‌اندیشند. بانک‌های Alliance Leicester و لوید TSB ادعا می‌کنند مشتریان آنها از امنیتی را که در نتیجه این تکنیک حاصل شده، خرسند هستند.

سایر اقدامات متقابل

با این وجود، تکنیک دو عاملی تنها بخشی از راه‌های تامین امنیت آنلاین است. بسیاری از بانک‌ها از اقدامات متقابل برای مبارزه با تهدیدهای حاصل از دزدی اینترنتی استفاده می‌کنند. این اقدام متقابل در بانک بارکلی بهره‌گیری از نرم افزار رایگان آنتی ویروس برای مشتریانی است که از خدمات بانکداری الکترونیک استفاده می‌کنند خدمات اختصار این نرم افزار از طریق SMS ارسال می‌شود هنگامی که شخص ثالثی از حساب آنها برداشت می‌کند، نرم افزار فوق مشتریان را مطلع می‌سازد. بهترین نمونه برنامه امنیتی آنلاین بارکلی به گفته دیویس، ارتباط معمول آن با مشتریان خود و مطلع ساختن آنها از تهدیدهای امنیتی است. استیب معتقد است آموزش مشتریان برای جلوگیری از دزدی آنلاین ضروری است. وی می‌گوید: عدم آگاهی مشتریان ضربه بزرگی به بانک وارد می‌کند و افزایش آگاهی آنها خواسته مهم بانک HSBC است. این بانک یکی از اسپانسرهای سایت getsafeonline.org است و ابتکاری برای افزایش آگاهی عمومی از دزدی آنلاین در بریتانیا محسوب می‌شود.

استیب بر این باور است که صنعت بانکداری در خدمت مشتریان است تا آنها را از کلاهبرداری‌های اینترنتی و سایر تهدیدها آگاه سازد. برآوردهای تحلیلیگر بانک HSBC نشان می‌دهد که سطح دزدی اینترنتی در بریتانیا در ماه فوریه سال گذشته میلادی ۴۰ درصد کمتر از ماه‌های گذشته بوده است. فوریه دورانی بود که سیستم بانکداری بریتانیا برای ماه‌های متوالی کاهش دزدی آنلاین را تجربه می‌کرد و این کمترین میزان کلاهبرداری از سال ۲۰۰۵ تا آن زمان بود.

استیب خاطر نشان می‌سازد: ما باید رشد کلاهبرداری اینترنتی را کمی واقع‌بینانه‌تر بررسی کنیم. تحلیل و بررسی دقیق‌تر نشان می‌دهد که بانک‌ها در مبارزه با دزدی اینترنتی چندان بد عمل نکرده‌اند.

دیویس نیز با اشاره به آمار APACS که نشان می‌دهد زیان‌های ناشی از دزدی کارت‌های اعتباری در بریتانیا در سال گذشته میلادی ۴۲۸ میلیون پوند و در مقایسه با دزدی‌های اینترنتی که تنها ۳۳۷۵ میلیون پوند بوده بسیار زیاد است، می‌گوید: ما فقط باید به جدول خسارات توجه کنیم.

علیرغم ترس از تهدیدهایی که گریبانگیر امنیت آنلاین است و رشد بی حد کلاهبرداری اینترنتی، بانک‌ها به رشد سریع استفاده از خدمات بانکداری الکترونیک خود ادامه

می‌دهند. برای مثال در بریتانیا تعداد کاربران خدمات بانکداری آنلاین در چهار سال گذشته تقریباً دوبرابر شده و به ۱۶/۹ میلیون کاربر رسیده است.

استیب می‌افزاید: تسهیلات بانکداری الکترونیک به حدی زیاد است که حتی کلاهبرداری‌های اینترنتی موجب کاهش استفاده از این خدمات نمی‌شود.

گارانتی‌های ارائه شده به مشتریان از سوی بانک‌ها برای مقابله با دزدی آنلاین نقش مهمی در اطمینان دادن به آنها ایفا می‌کند. برای نمونه نوردی به ۲۵۰ مشتری خود که سال گذشته از دزدی اینترنتی ضرر کرده بودند، خسارت پرداخت کرد.

دیویس می‌گوید: اعطای گارانتی به مشتریان در حالی که بانک‌ها بیشترین خسارات ناشی از دزدی‌های آنلاین را متحمل می‌شوند، اقدام بسیار خوبی است. وی در پایان خاطر نشان می‌سازد: این بانک است که ضرر می‌کند و نه مشتریان.

علیرغم ترس از تهدیدهایی که گریبانگیر امنیت آنلاین است و رشد بی حد کلاهبرداری اینترنتی، بانک‌ها به رشد سریع استفاده از خدمات بانکداری الکترونیک خود ادامه می‌دهند