سمانه امینی خواه

ملاحظات پدافندی در بانکداری الکترونیک

بانکـداری الکترونیـک همچنانِ چالش‌های خاص خـود در زمینه امنیت مالـی و حریم خصوصی کاربران را دارد. حسـاب کاربـری میلیون‌هـا نفر، عمدتـا به دلیل بانکـداری الکترونیک در معرض تهدید قرار گرفته‌اسـت. چنانچه قصد اسـتفاده از بانکداری‌الکترونیـک جهـت انجام مبـادلات مالی خـود را دارید، بایـد از خطـرات آن اگاه بوده و اقدامات پیشـگیرانه لازم جهـت کاهـش ایـن خطرات را انجـام دهید. اقدامـات زیر، کـه در ادامه مقاله به آن‌هـا می‌پردازیم، در پیشـگیری از مشـکلات ایمنی همـراه با بانکـداری الکترونیک به شـما کمک می‌کنند:

- تمامی اطلاعات حریم خصوصی و خط مشی را مرور کنید.
- از اطلاعـات ورود بـه حسـاب کاربـری خـاص که حـدس زدن آن دشـوار باشد اسـتفاده کنید.
- از کامپیوتر خود محافظت کنید.
- گردش حساب خود را بطور منظم بررسی کنید.
- پرداخت‌ها را با استفاده از کارت‌های اعتباری انجام دهید.
- از مکان‌های عمومی برای ورود به حساب کاربری خود اسـتفاده نکنید.
- ایمیل تطبیق ارسال شده از طرف بانک را تأیید کنید.
- چنانچه حسـاب شـما در معرض خطر اسـت، اقدامات انتقال لازم را انجام دهید.

حملات با هدف بانکداری الکترونیک

چندین نـوع کلاه‌برداری الکترونیک به‌طور خاص بانکداری الکترونیکی را هـدف قـرار می‌دهنـد. برخی از معروف‌تریـن آن‌هـا را در زیر توضیح می‌دهیم:

حملات فیشینگ

حمـلات فیشـینگ بـا اسـتفاده از پیام‌هـای ایمیلـی تقلبـی از یـک سـازمان یـا افـراد خـود را به عنوان بانک یا مؤسسـه مالی شـما معرفی می‌کننـد. ایـن ایمیل از شـما درخواسـت می‌کند تا اطلاعات حسـاس (نـام، گذرواژه، شـماره حسـاب و ...) خـود را در اختیار آن‌ها قـرار داده و لینـک سـایتی جعلی مشـابه بـا آن بانک یا مؤسسـه را در اختیار شـما قـرار می‌دهـد. چنانچـه بـه لینـک داده شـده وارد شـوید و اطلاعـات خواسـته شـده را وارد نماییـد، سـارقین بـه اطلاعـات فردی و سـرمایه شـما دسترسـی پیـدا می‌کننـد (بـرای اطلاعـات بیشـتر بـه قسـمت شناسـایی و خـودداری از ایمیل‌هـای کلاه‌بـرداری مراجعـه کنیـد). در برخـی موارد، پنجره‌هـای pop-up در پیش یک وبسـایت اصلی بانک ظاهـر می‌شـوند. آدرسِ وبسـایت واقعـی نمایـش داده می‌شـود اما هر اطلاعاتی که مسـتقیما داخل pop-up وارد می‌کنید به دسـت کاربران غیررسـمی رسـد (بـرای مشـاهده بحـث فنی ایـن موضوع به قسـمت "Technical Trends in Phishing Attacks" در وبسـایت .http://www us-cert.gov/reading_room/phishing_trends0511.pdf مراجعه کنید). (با شـکل یکسـان، در (فیشـینگ) فردی با شـما تماس گرفته و ادعـا می‌کنـد کـه نماینده بانک اسـت و باید اطلاعات حسـاب شـما را تأییـد کند.)

بدافزار

بدافـزار اصطلاح اسـتفاده شـده بـرای کـد نرم‌افزارهای مخرب نوشـته

شده به‌کار می‌رود. برنامه‌های کامپیوتری خاصی وجود دارد که به سارقین این امکان را می‌دهد که شما را فریب داده و باور کنید که امنیت مرسوم موجود از شما حین تبادلات بانکی الکترونیکی محافظت می‌نماید. حملات شامل بدافزار عامل مهمی در جرم مالی الکترونیکی هستند (برای اطلاعات بیشتر به "Technical Trends in Phishing Attacks" مراجعه کنید). در واقع امکان انجام چنین اقداماتی با استفاده از این نرم‌افزار مخرب وجود دارد:

- سرقت اطلاعات حساب- بدافزار می‌تواند فشرده شدن کلیدها جهت وارد کردن اطلاعات ورود به حساب کاربری را بدست آورد. همچنین بدافزار می‌تواند سایر اطلاعاتی که شما جهت تأیید هویت خود وارد می‌کنید (مانند تصاویر مخصوص انتخاب شده یا واژگان جادویی انتخاب شده) را رصد و به سرقت برد.
- جایگزینی وبسایت تقلبی- بدافزار قادر به ایجاد صفحات وب به ظاهر حقیقی است. آن‌ها صفحه اصلی بانک را با یک صفحه کاملاً یکسان، بجز در آدرس که در برخی موارد اختلاف دارد، جایگزین کنند. این سایت منحرف کننده کاربر از سایت اصلی به سارقین امکان سرقت اطلاعات کاربر را می‌دهد. سارقین زمینه‌های اضافی به نسخه کپی صفحه وب باز شده در جستجوگر شما اضافه می‌کنند. هنگامی که شما اطلاعات خود را وارد می‌کنید، بدون اینکه خودتان متوجه شوید این اطلاعات هم به بانک و هم سارق ارسال می‌شود.
- سرقت حساب کاربری- بدافزار قادر است بدون اطلاع شما جستجوگرتان را سرقت کرده و منابع مالی‌تان را منتقل کند. هنگامی که تلاش می‌کنید در وب‌سایت بانک وارد شوید، این نرم‌افزار یک پنجره جستجوگر مخفی در کامپیوتر شما باز کرده، وارد حساب شما شده، گردش حساب شما را خوانده، و مخفیانه به حساب سارق وجه منتقل می‌کند.

فارمینگ

حملات فارمینگ شامل نصب کد مخرب روی کامپیوتر شما می‌شود؛ با این حال، این موضوع می‌تواند بدون هرگونه اقدامی از طرف شما صورت پذیرد. در یک نمونه از حمله فارمینگ، شما یک ایمیل را بازکرده، یا ضمیمه یک ایمیل را، و آن بر روی کامپیوتر شما کد مخرب را نصب می‌کند. پس از آن شما به وبسایت تقلبی که بسیار شبیه به نسخه بانک یا مؤسسه مالی شما است وارد می‌شوید. هر اطلاعاتی که در زمان مشاهده این سایت تقلبی وارد کنید در اختیار سارقین قرار می‌گیرد.

در تمامی انواع حمله اشاره شده در بالا یک ویژگی مشترک است؛ آن‌ها با استفاده از تکنولوژی بوجود آمده اند اما برای اجرای نیت شوم خود نیازمند اطلاعاتی هستند که شما در اختیار آن‌ها قرار می‌دهید:

- در حملات فیشینگ، باید یا اطلاعات خود را وارد کنید یا به لینک ارسال شده وارد شوید.
- در ارتباط با بدافزارها، لازم است که شما را وادار به انجام کارهایی کنند که معمولاً آن‌ها را انجام نخواهید داد. باید بدافزار را با اجرای یک برنامه، مثلاً ضمیمه یک ایمیل، یا بازدید از یک وبسایت ارسال شده در ایمیل یا لینک یک پیام روی کامپیوتر خود نصب کنید. پس از آن باید اطلاعات ورود به حساب بانکی خود را وارد نمایید. اطلاعات مالی شما تنها پس از انجام این مراحل در خطر قرار می‌گیرد.
- در حملات فارمینگ، باید ایمیل یا ضمیمه ایمیلی را باز کنید تا مستعد حملات گردید. پس از آن شما با مشاهده یک وبسایت تقلبی، بدون اینکه متوجه باشید، اطلاعات خود را در اختیار آن‌ها قرار داده و هویت مالی خود را در معرض خطر می‌گذارید.

ملاحظاتی جهت بانکداری الکترونیکی امن

هنگامی که صحبت از بانکداری الکترونیک به میان می‌آید، هیچ‌گونه نمی‌توان ایمنی کامل آن را تضمین کرد. با این وجود اقدامات و ملاحظاتی وجود دارد که می‌توانند حساب‌های الکترونیکی و تراکنش‌های شما را امن‌تر نمایند. برخی از این ملاحظات عبارتند از:

- اطلاعات بانک خود را در مورد خط مشی حریم خصوصی و اقدامات آن‌ها بررسی کنید.

طبق قانون، بانک‌ها موظف به ارسال سالانه کپی خط مشی حریم خصوصی و اقدامات خود به شما هستند؛ همچنین می‌توانید یک نسخه از این اطلاعات را درخواست دهید (جهت اطلاعات بیشتر به Electronic Code of Federal Regulations, Title 16: Commercial practices, Part 313.9-Delivering Privacy and Opt Out Notices

مراجعه کنید). روی وبسایت بانک نیز باید موجود باشد. ضمن مطالعه این اطلاعات، توجه ویژه‌ای به هرگونه اطلاعات راجع به روش‌های استفاده شده برای کدگذاری تبادلات و تأیید اطلاعات کاربر داشته باشید. همچنین اطلاعات امنیتی اضافی مورد نیاز قبل از تأیید انجام پرداخت به مراکز یا افرادی که پیش از این پرداختی به آن‌ها انجام نشده است را بررسی کنید.

• پیش از تنظیم هرگونه پرداخت رسید الکترونیکی، خط مشی حریم خصوصی شرکت یا خدماتی که قصد واریز وجه به آن را دارید بررسی کنید. شما حق محدود کردن اطلاعاتی که بانک با سازمان‌های مادر خود یا هر مؤسسه مالی دیگری به‌اشتراک می‌گذارد هستید (برای اطلاعات بیشتر به قسمت "Protect-ing Your Privacy" و "How Ananymous Are You?" مراجعه کنید). مطلع باشید که ممکن است برخی از بانک‌های الکترونیک روندهای متفاوتی برای هرکدام از این درخواست‌ها داشته باشند. همچنین ممکن است بخواهید از خدماتی مانند Better Business Bureau جهت مشاهده هرگونه سابقه شکایت مشتریان خاص در مورد تخطی از خط مشی استفاده کنید. از نظر مسائل امنیتی، از یک عدد شناسایی شخصی (PIN) خاص که حدس زدن آن دشوار است استفاده کنید.

• عدد شناسایی شخصی خود را بصورت دوره‌ای تغییر دهید. از انتخاب‌های شامل اطلاعات شخصی خود، مانند تاریخ تولد یا شماره امنیت اجتماعی پرهیز کنید؛ ممکن است فرد سارق قادر به حدس آن باشد.

فارق از موارد استثناء، هرگز عدد شناسایی شخصی خود را در اختیار کسی قرار ندهید (برای اطلاعات بیشتر به قسمت "Choos-ing and Protecting Passwords مراجعه کنید).

• برنامه‌های ضدویروس، دیوارآتشین، و ضد ابزارجاسوسی بر روی کامپیوتر خود نصب کرده و آن‌ها را همواره به‌روزرسانی کنید. نصب و به‌روزرسانی این نرم‌افزار از کامپیوتر و محتوای آن در برابر دسترسی تأیید نشده محافظت می‌نماید. بهتر است به‌روزرسانی خودکار این برنامه‌ها را فعال کنید یا در صورت درخواست تأیید، همیشه با آن موافقت کنید تا به‌روزرسانی سیستم را در اسرع وقت دانلود کند (برای اطلاعات بیشتر به قسمت "Understanding An-ti-Virus Software"، "Understanding Firewall" و "Recogniz-ing and Avoiding Spyware" مراجعه نمایید).

• به‌طور منظم گردش حساب الکترونیکی خود را به‌منظور شناسایی فعالیت‌های تأیید نشده بررسی کنید.

زمان عاملی مهم در عکس‌العمل نسبت به تبادلات مالی الکترونیکی تأیید نشده است. چنانچه کاغذ گردش حساب دریافت می‌کنید، حتماً آن را با گردش مالی الکترونیکی خود مطابقت دهید.

از کارت اعتباری برای پرداخت وسایل و خدمات الکترونیک خود استفاده کنید.

• کارت‌های اعتباری معمولاً نسبت به کارت‌های دبیت کارت حفاظت قوی‌تری در برابر ادعاهای مسئولیت شخصی در انتقال وجه‌های تأیید نشده تا سقف ۵۰ دلار دارند. مسئولیت شخصی در دبیت کارت می‌تواند بیشتر باشد.

طبق قانون حفاظت فدرال، E چنانچه شما ظرف یکی دو روز مشکلی در انتقال وجه الکترونیکی شامل دبیت کارت را به یک بانک یا مؤسسه مالی گزارش دهید، تنها مسئولیت ۵۰ دلاری متوجه شماست. ارائه چنین گزارشی ظرف ۳ تا ۶۰ روز مسئولیت شما را به ۵۰۰ دلار افزایش داده و پس از ۶۰ روز هیچ گونه محدودیتی در مورد مسئولیت شما اعمال نمی‌شود (برای اطلاعات بیشتر به

Electronic Code of Federal Regulations, Title 12: Banks and Banking, Part 205 – Electronic Fund Transfers (Regulation E) مراجعه کنید).

• از شرایطی که ممکن است اطلاعات شخصی شما توسط افراد غیرمجاز قطع، بازیابی، یا مشاهده شود پرهیز کنید.

شما باید تبادلات بانکی الکترونیکی خود را در مکان‌هایی که در معرض دید عموم نباشید انجام دهید. هنگاکه اطلاعات ورود به حساب خود را وارد می‌کنید، از شبکه‌های عمومی یا ناایمن (مانند کافی‌شاپ یا کتابخانه) استفاده نکنید. به عنوان یک قاعده کلی، استفاده از هر کامپیوتری که افراد دیگر به‌راحتی به آن دسترسی دارند ممنوع است؛ چرا که نهایتاً منجر به دسترسی غیرمجاز به اطلاعات مالی شما خواهد شد. به یاد داشته باشید که احتمال ذخیره موقت اطلاعات حساب شما در حافظه جستجوگر وب وجود دارد (برای اطلاعات بیشتر به "Guidelines for Publishing Information Online" مراجعه کنید).

• چنانچه ایمیل در ارتباط با حساب مالی خود دریافت کردید، با تماس گرفتن با بانک یا مؤسسه مالی خود از اعتبار آن اطمینان کسب کنید. نباید به هر ایمیل خواستار اطلاعات امنیتی، هشدار در مورد تعلیق حساب، فرصت کسب آسان پول، درخواست‌های خارج از کشور خود جهت کمک‌های مالی، و غیره پاسخ دهید. همچنین نباید وارد لینک‌های موجود در این ایمیل‌های مشکوک شوید. یک نسخه از ایمیل مشکوک را به کمیسیون تجارت فدرال به آدرس uce@ftc.com ارسال و ایمیل را از جعبه ایمیل خود حذف کنید.

چنانچه اطلاعات مالی خود را در اختیار یک وبسایت نامعتبر قرار داده اید، به سازمان‌های زیر گزارش دهید:

- بانک خود
- پلیس محلی
- کمیسیون تجارت فدرال http://www.ftc.gov
- مرکز شکایات اینترنتی http://www.ic3.gov
- سه سازمان اعتباری اصلی Experian، Equifax و TransUnion (برای اطلاعات بیشتر به "Preventing and Responding to Iden-tity Theft" مراجعه کنید).

نتیجه‌گیری

بانکداری الکترونیک دارای ریسک‌های معینی است. لازم است در مورد این خطرها، نحوه امکان دسترسی غیرمجاز به اطلاعات مالی شما، و مراحلی که باید برای محافظت از اطلاعات مالی خود طی کنید اطلاعات کافی کسب کنید. آشنایی با حقوق خود و مسئولیت‌های متوجه شما به عنوان یک مشتری بانکداری الکترونیک نیز با تغییر جمله معروف قدیمی ذخیره یک پنی مانند کسب درآمد یک پنی است می‌تواند در توانایی مالی شما تفاوت ایجاد کند.