سازمان بورس و اوراق بهادار
Securities & Exchange Organization

بولتن آگاهی رسانی امنیت سایبری، شماره ۹

چگونه از اطلاعات خود در سامانه های اینترنتی محافظت کنیم؟

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

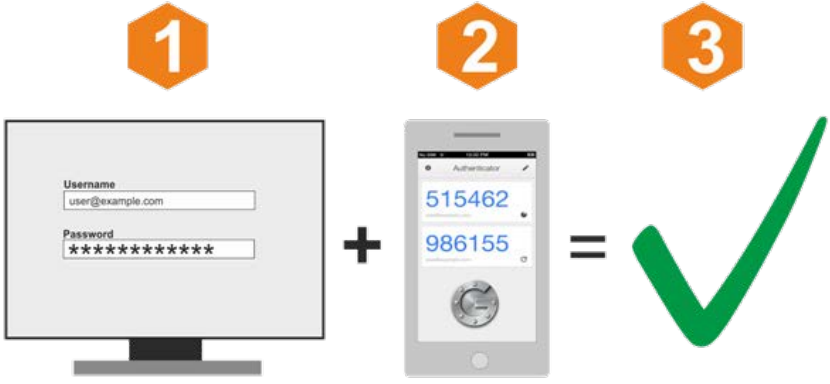
چگونه از اطلاعات خود در سامانه‌های اینترنتی محافظت کنیم؟

آیا تاکنون به عواقب لو رفتن رمز عبورتان در وب سایت‌ها و سامانه‌های اینترنتی فکر کرده‌اید؟ در صورتی که رمز عبور ایمیل‌های شخصی و سازمانی، اطلاعات حساب اینترنت بانک، اطلاعات حساب کاربری سامانه‌های معاملات برخط بورسی و هر سامانه مهم اینترنتی دیگر افشا شود، چه خساراتی خواهید دید؟ آیا با مکانیزم‌هایی همچون «احراز هویت دو یا چند عاملی»، «کپچا»، «صفحه کلید مجازی» و «ورود/خروج امن به/از سامانه» آشنایی دارید؟ در این بولتن سعی بر این است که برخی از مکانیزم‌های حفاظت از اطلاعات در سامانه‌های اینترنتی ارائه شود تا با به‌کارگیری از آن‌ها بتوانید با اطمینان بیشتری در وب‌سایت‌ها و سامانه‌های اینترنتی فعالیت نمائید.

احراز هویت دو یا چند عاملی

مکانیزم ورود به بسیاری از سامانه‌ها و وب‌سایت‌های اینترنتی، وارد کردن نام کاربری و رمز عبور در صفحه ورود کاربران است. در این مکانیزم تنها یک عامل (رمز عبور) محافظتی از حساب کاربری شما وجود دارد و می‌بایست تلاش کنید رمز عبور طولانی، پیچیده و غیر قابل حدس برای حساب کاربری خود در نظر بگیرید. در صورتی که به هر دلیلی رمز عبور پیچیده شما لو برود، هکر به راحتی می‌تواند وارد حساب کاربری شما شده و اتفاقات ناخوشایندی را رقم بزند. برای جلوگیری از این اتفاقات ناخوشایند چه باید کرد؟ آیا می توان راهکاری اتخاذ کرد که حتی در صورت لو رفتن رمز عبور، هکر نتواند به راحتی وارد حساب کاربری شود؟

راهکاری که پیشنهاد می‌شود استفاده از قابلیت احراز هویت دو یا چند عاملی است. در برخی از وب سایت های مهم و کلیدی این قابلیت وجود دارد که می توانید ورود به حساب کاربری خود را منوط به دو یا چند عامل کنید. عامل اول رمز عبور است. عامل دوم می‌تواند کد پیامکی باشد که از وب سایت مدنظر به شماره موبایل شما ارسال می‌شود و از شما خواسته می‌شود کد پیامک را در وب سایت وارد کنید. با توجه به این که این کد فقط به شماره موبایل اختصاصی شما ارسال می شود و در اختیار هیچ کسی قرار ندارد، می توانید به عنوان عامل دوم ورود به وب سایت به این کد اطمینان کنید. در صورتی که هکر بتواند عامل اول (رمز عبور) شما را به دست بیاورد، نمی‌تواند به کد پیامک شده به شماره موبایلتان دسترسی داشته باشد و عملا امکان ورود به سامانه با هویت شما را نخواهد داشت. بنابراین راهکار احراز هویت دو عاملی نقش بسیار موثری را در جلوگیری از افشای اطلاعات ثبت شده شما در وب سایت ها و سامانه های اینترنتی ایفا خواهد نمود.



در برخی از وب‌سایت‌ها ممکن است عامل دوم (کد ارسال شده) صرفا از طریق پیامک ارسال نشود و از اپلیکیشن‌های جانبی برای ارسال کد به گوشی هوشمند شما استفاده کنند. به عنوان مثال می‌توان به اپلیکیشن Google Authenticator اشاره نمود که در بسیاری از وب‌سایت‌های مهم اینترنتی مورد استفاده قرار گرفته است. اپلیکیشن‌های متعدد رمز دوم بانکی در ایران نیز از نمونه‌های دیگر این اپلیکیشن‌ها است. در خصوص سامانه‌های معاملات برخط بورسی نیز قابلیت احراز هویت دو عاملی وجود دارد.

از جمله عامل‌های بعدی احراز هویت می‌توان به توکن(Token)های سخت افزاری اشاره کرد. این توکن‌ها به صورت‌های مختلف متصل شونده و غیر اتصالی وجود دارند. توکن‌های متصل شونده از طریق پورت USB قابلیت اتصال به رایانه را دارد. به ازای هر کاربر، اطلاعات منحصر به فردی بر روی هر توکن متصل شونده ذخیره می‌شود و پس از اتصال به رایانه، در هنگام ورود به وب‌سایت، این اطلاعات با سرور وب سایت رد و بدل می‌شود و به عنوان یکی از عوامل احراز هویت شما برای وب سایت در نظر گرفته می‌شود. توکن‌های سخت افزاری غیر اتصالی دارای نمایشگری هستند که در فواصل زمانی منظم کدی را نشان می‌دهد و این کد به عنوان یکی از عوامل احراز هویت در حین ورود به وب سایت استفاده می‌شود.

کپچا (Captha)

در صفحات ورود به بسیاری از وب‌سایت‌ها از شما خواسته می‌شود که حروفی را که در تصویر می‌بینید در کادر مشخصی وارد کنید. در برخی از وب سایت ها ممکن است حاصل یک عمل ریاضی در تصویر را در کادری مشخص وارد کنید. برخی نیز ممکن است چند تصویر به شما نشان دهند و از شما بخواهند که تصاویری را که حاوی شیئی مشخص است، انتخاب کنید. این مکانیزم که در آن طی یک فرایند تعاملی

از شما خواسته می‌شود ثابت کنید ربات نیستید و انسان هستید، کپچا (Captcha) نامیده می‌شود. چه نیازی به اثبات ربات نبودن وجود دارد؟ چرا باید به همراه اطلاعاتی همچون نام کاربری و رمز عبور، عبارت کپچا را به درستی وارد کنید؟

برای درک بهتر ضرورت وجود کپچا، یکی از حملات اینترنتی را که توسط هکرها صورت می‌پذیرد، بررسی می‌کنیم. وقتی هکر با صفحه ورود یک وب سایت مواجه می شود و نام کاربری و رمز عبور هیچ کدام یک از کاربران آن وب سایت را نمی داند، سعی می کند با تکنیک هایی نام کاربری و رمز عبور آنها را به دست آورد. یکی از این تکنیک‌ها، امتحان کردن نام کاربری‌ها و رمزهای عبور متعدد است. به طور مثال به جای نام کاربری، عبارت Morteza و به جای رمز عبور عدد ۱ را وارد می کند و با پیغام اشتباه بودن اطلاعات مواجه می شود. در مرحله بعدی نام کاربری Morteza را با رمز عبور ۲ امتحان می کند و صحت آن را چک می کند. این فرایند را با تست کردن رمز عبورهای مختلف ادامه می دهد تا به رمز عبور صحیح دست پیدا کند. هکرهای این فرایند را به صورت دستی انجام نمی دهند بلکه ابزارهایی دارند که در یک ثانیه هزاران عبارت مختلف را که ترکیبی از حرف و عدد و کلیدهای دیگر است، بر روی نام های کاربری مختلف تست می کنند و در بسیاری از موارد با موفقیت به رمزهای عبور دست می یابند.

نکته مهم این است که ابزارهای هکرها نام کاربری و رمز عبورهای متعدد را وارد می کنند و نتیجه را مشاهده می کنند و در صورت عدم صحت رمز عبور بعدی را چک می‌کنند و این فرایند بسیار سریع انجام

می شود و این سرعت عمل است که هکر را علاقه‌مند به انجام این عمل می‌کند. تنها راهکاری که می‌تواند برای این ابزارها مزاحمت اساسی ایجاد کند و مانع از موفقیت آن‌ها شود، کپچا است. ابزارهای معمولی هکرها نمی‌تواند کپچا را بخواند و در کادر مربوطه وارد کند. بنابراین با اولین نام کاربری و رمزعبوری که ابزار امتحان می کند، می بایست کپچای صحیح را نیز وارد کند که در این عمل ناتوان است و عملا نمی تواند از صحت یا عدم صحت رمز عبور وارده اطمینان حاصل کند و در نهایت موفق به کشف رمز عبور به این روش نخواهد شد.

شاید وارد کردن کپچا عملی طاقت فرسا به نظر برسد اما با توجه به نقش موثر آن در حفاظت از اطلاعات حساب کاربری، این سختی قابل چشم پوشی است.

استفاده از صفحه کلید مجازی

در صفحات ورود کاربران برخی از سامانه ها و وب سایت های اینترنتی، قابلیت ورود نام کاربری و رمز عبور از طریق صفحه کلید مجازی وجود دارد. برای نمونه می توانید به صفحه ورود سامانه های معاملات برخط بورسی دقت کنید. در کنار کادر ورود رمز عبور آن ها این قابلیت وجود دارد.

با کلیک کردن بر روی آیکن صفحه کلید، صفحه کلیدی مجازی نمایان می شود که می توانید رمز عبور خود را از طریق این صفحه کلید وارد نمائید. کاربرد این صفحه کلید چیست؟ چرا بهتر است به جای ورود رمز عبور از طریق صفحه کلید سخت افزاری خود، از این صفحه کلید مجازی استفاده کنید؟

ابزارهای نرم افزاری و سخت افزاری متعددی به نام «کی‌لاگر (Key Logger)» یا «ثبت‌کننده کلید»، وجود دارند که ممکن است هکرها این ابزارها را به هر روشی بر روی سیستمی که شما از آن استفاده می کنید، نصب کرده باشند. این ابزارها کلیه عباراتی را که شما از طریق صفحه کلید سخت افزاری خود تایپ می کنید، ثبت نموده و برای هکر ارسال می نمایند. بدین روش، هکر به راحتی می تواند نام کاربری و رمز عبوری را که شما برای ورود به هر سامانه ای وارد می کنید، به دست می آورند. در صورتی که شما به جای صفحه

کلید سخت افزاری، از صفحه کلید مجازی استفاده کنید، ابزار کی‌لاگر امکان ثبت آن را نخواهد داشت و رمز عبور شما از این خطر در امان خواهد بود. بنابراین، پیشنهاد می شود در هنگام ورود رمز عبور خود، حتما از صفحه کلید مجازی استفاده کنید.

ورود امن به سامانه‌های بورسی و خروج امن از آن‌ها

نکاتی که تا اینجا اشاره شد، کمک موثری در راستای ورود امن به سامانه‌ها و وب‌سایت‌های اینترنتی می نمایند. بنابراین در صورت وجود قابلیت احراز هویت دو یا چند عاملی حتما از آن استفاده کنید، صفحه کلید مجازی را برای ورود امن رمز عبور خود به کار بگیرید و در هنگام ورود کپچا از ضرورت وجودی آن مطلع باشید. نکات مهم دیگری که در هنگام ورود به سامانه های بورسی و خروج از آن ها بهتر است رعایت گردد، موارد ذیل هستند:

- حتما به آدرس URL وب سایت در مرورگر اینترنتی دقت کنید و اطمینان حاصل کنید که آدرس وب سایت اصلی در آن درج شده است.
- کلیه سامانه های معاملات برخط بورسی به گواهی SSL تجهیز شده اند و می بایست شروع آدرس سامانه آن ها Https معتبر باشد. در غیر اینصورت از آن سامانه استفاده نکنید. (برای آشنایی بیشتر با http و https به بولتن آگاهی رسانی شماره ٤ مرکز نظارت بر امنیت اطلاعات بازار سرمایه مراجعه کنید)
- پس از وارد کردن نام کاربری و رمز عبور خود در سامانه ها، ممکن است مرورگر از شما بخواهد، این اطلاعات را ذخیره کنید. هرگز این ذخیره سازی را انجام ندهید. بولتن آگاهی رسانی شماره ۲ مرکز نظارت بر امنیت اطلاعات بازار سرمایه توضیحات کاملی در این خصوص ارائه می دهد.
- پس از اتمام فعالیت در سامانه ها، حتما با استفاده از دکمه خروج از سامانه خارج شوید. هرگز برای خروج از سامانه، مرورگر خود را نبندید، زیرا این کار موجب خروج از سامانه نخواهد شد. عدم خروج صحیح از سامانه می تواند بستر مناسبی برای سوء استفاده هکرها از اطلاعات حساب شما ایجاد کند.
- در صورت وجود هر گونه فعالیت مشکوک در سامانه های بورسی مراتب را از طریق آدرس ایمیل makna@seo.ir و شماره تماس ۸٤۰۸۳۵۳٤ با مرکز نظارت بر امنیت اطلاعات بازار سرمایه در میان بگذارید.

توصیه های امنیتی ما را جدی بگیرید!

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

تهران، میدان ونک، ابتدای ملاصدرا، شماره ۱۳، سازمان بورس و اوراق بهادار
صندوق پستی: ۶۳۶۶-۱۹۹۳۵
تلفن: ۸۴۰۸۳۵۳۵-۰۲۱
makna@seo.ir

www.seo.ir