بانک سینا

معاونت فناوری اطلاعات و شبکه ارتباطات

مدیریت امنیت و توسعه سیستم‌ها

اداره امنیت فناوری اطلاعات

دفترچه راهنمای امنیتی کاربران

نسخه ۳

تیرماه ۹۳

فهرست

عنوان **صفحه**

۱- مقدمه

در دنیای فناوری اطلاعات، امنیت یکی از اساسی‌ترین شاخص‌های کاری است بطوریکه می توان گفت امنیت، مهم‌ترین اصل نظام اطلاعاتی می‌باشد. امروزه گسترش خدمات بانکی در اینترنت و استفاده مشتریان از این خدمات به سرعت رو به افزایش است که اگر این پیشرفت در سایه امنیت نباشد بی‌شک کاربران را با مشکلات زیادی مواجه خواهد کرد.

با توجه به اینکه استراتژی بانک سینا در راستای ارائه خدمات گسترده بانکداری الکترونیک و همچنین تمرکز بر افزایش کیفیت و امنیت این خدمات می باشد لذا این بانک علاوه بر ایجاد بسترهای امنیتی مناسب در زیر ساخت سرویس‌های بانکداری نوین، مستند پیش رو را جهت افزایش سطح آگاهی امنیتی کاربران تدوین نموده است.

۲- چند توصیه قبل از شروع

۱- آیا می‌دانید بخش اعظم برداشت‌های غیرمجاز از حساب‌های مشتریان بانک‌ها ناشی از عدم محافظت مشتری از رمز کارت یا حساب اینترنتی خود است؟

۲- آیا می‌دانید با فعال نمودن پیامک حساب اینترنتی یا خودپرداز، از هر گونه ورود به حساب یا جابجایی پول از حسابتان بلافاصله با پیامک مطلع می‌شوید؟

۳- در صورتی که احتمال می دهید شناسه یا رمز عبور شما افشا شده یا به سرقت رفته است سریعاً با شماره ۰۲۱-۴۸۰۵۲۰۰۰ (مرکز تماس مشتریان بانک) پاسخگوی ۲۴ ساعته بانک تماس بگیرید.

۴- هیچ بانکی نیاز به رمز عبور حساب اینترنتی یا خودپرداز شما ندارد، پس هرگز به ایمیل‌ها یا پیامک‌هایی که این موارد را از شما طلب می‌کنند پاسخ ندهید.

۵- از ذخیره نمودن شماره حساب و رمز اینترنتی یا کارت خود در گوشی تلفن همراه جدا پرهیز نمایید.

۶- امن ترین محل برای حفظ رمز عبور، حافظه انسان است، حتی الامکان از یادداشت کردن رمز یا ذخیره آن در کامپیوتر و تلفن همراه خودداری نمایید.

۷- هرگز رمز عبور خود را از طریق تلفن، ایمیل یا پیامک به شخص دیگری بازگو نکنید.

۸- هرگز رمز اول و دوم کارت خودپرداز را در پشت کارت ننوشته و نیز در کیف کارت نگهداری نکنید.

۹- هنگام خرید رمز خود را شخصا وارد نمایید و از بیان آن با صدای بلند خودداری نمایید.

۱۰- آیا می‌دانید برنامه‌هایی وجود دارند که به صورت پنهانی رمز عبور حساب شما را شنود و سرقت می‌کنند؟ برای پیشگیری از این امر:

- از ورود به حساب بانکی از طریق کامپیوترهای عمومی و ناشناس پرهیز کنید. ممکن است در رایانه های این گونه مراکز نرم افزارهای جاسوسی برای سرقت نام کاربری و رمز عبور شما نصب شده باشد. در صورت استفاده از مراکز حتی الامکان از صفحه کلید مجازی استفاده کنید.
- همواره از نرم افزار آنتی‌ویروس معتبر و بروز استفاده نمایید.

- ایمیل‌های ناشناس را باز نکنید، به خصوص اگر دارای فایل ضمیمه هستند.
- از دانلود و نصب نرم افزارهای ناشناخته اجتناب نمایید.

۱۱- بسیاری از ایمیل های تبلیغاتی حاوی بد افزار یا لینک به سایت های آلوده هستند. تا حد امکان ایمیل های تبلیغاتی را باز نکنید.

۱۲- آیا می‌دانید ممکن است تنها با کلیک کردن روی یک لینک، کامپیوتر شما آلوده به نرم افزارهای جاسوسی شود؟ هرگز لینک‌ها و عکس‌هایی که در ایمیل‌ها یا پیام‌های ناشناس و مشکوک وجود دارند را باز نکنید.

۱۳- از دانلود کردن فایل از وب سایت‌های اشتراک گذاری فایل بپرهیزید.

۱۴- برخی از وب سایت‌ها با تشویق کاربران به دانلود آنتی‌ویروس یا انجام اسکن رایگان، سعی در فریب کاربر دارند، هرگز پیشنهادهای این سایت ها را دنبال نکنید.

۱۵-هرگز درخواست افراد ناشناس برای انتقال وجه از کارت یا حساب شما در ازای دریافت پول یا چک را نپذیرید.

۱۶-در صورت بروز اشکال در عملیات بانکی، از توسل به افراد غریبه به شدت خودداری کنید.

۱۷-از بانک درخواست کنید تا سقف جابجایی پول از حساب‌های مختلف شما، از طریق اینترنت بانک، تلفن‌بانک،همبانک و سایر خدمات بانکداری نوین را محدود نماید.

۱۸-موجودی حساب‌های بانکی مخصوصا حساب‌های عابر بانک خود را در فاصله زمانی مناسب چک کنید.

۱۹-در صورت مفقود شدن و یا به سرقت رفتن کارت خود جهت مسدود نمودن آن از طریق سرویس های نوین (اینترنت بانک، تلفن بانک و ..) اقدام نمایید و یا به یکی از شعب بانک مراجعه فرمایید.

۲۰-جهت آگاهی از آخرین اطلاعات مربوط به جرائم رایانه‌ای و تهدیدات امنیتی به سایت پلیس فتا مراجعه نمایید.

۳- نکات امنیتی رمزعبور

۱. همیشه به خاطر داشته باشید که نام کاربری و رمز عبور در دنیای مجازی، همانند آدرس دقیق و کلیدورودی به دارائی‌های شما در دنیای واقعی است، برای انتخاب رمز عبور از مشخصات شخصی مانند سال تولد، نام فرزند، شماره شناسنامه، شماره موبایل، تلفن منزل استفاده نکنید.

۲. رمز عبور خود را در فواصل زمانی مشخص(مثلاً هر ۹۰ روز) تغییر دهید.

۳. توصیه می شود رمز عبور در اولین ورود تغییر یابد.

۴. هیچ‌گاه اطلاعات حساب و کارت بانکی خود را از طریق پیامک برای دیگران ارسال ننمایید. درصورتیکه شماره‌حساب یا شماره‌کارت شما به همراه هریک از اطلاعات ذیل در اختیار افراد غیرمجاز قرار گیرد، امنیت حساب شما در معرض خطر قرار می‌گیرد :

- رمزهای اول و دوم
- شماره CVV2
- تاریخ انقضای کارت

۳- ۱ پیشنهاداتی برای انتخاب رمز عبور امن

پیشنهادات زیر می تواند در انتخاب رمز عبور امن شما را راهنمایی نماید:

۱- حداقل ۸ کاراکتر برای رمز عبور اینترنتی خود استفاده کنید.

۲- در رمز عبور خود از ترکیب حروف بزرگ، کوچک یا اعداد و کاراکترهای ویژه استفاده نمایید.

۳- از حروفی که بر روی صفحه کلید در کنار هم قرار گرفته اند استفاده نکنید. استفاده از رمز های عبوری مانند "qwert" یا "asdf" و"12345678" که از در کنار هم قرار گرفتن حروف یا اعداد ایجاد شده اند دستیابی هکرها به رمز عبور شما را راحت تر خواهد کرد.

۴- برای ایجاد رمز عبور، از حروف بزرگ و کوچک به صورت یک در میان استفاده کنید. مثال: cOmPuTeR

۵- حروف اول کلمات یک جمله را به عنوان رمز عبور خود انتخاب کنید. برای مثال در جمله

"If Sentence Is Longer Password Would Be Safer" رمز عبور آن به ایـن صـورت تبـدیل مـی شـود: "ISILPWBS"

۶- لغتی را در نظر بگیرید و سپس حروف سمت راست آن را که بر روی صفحه کلید قرار دارد، بنویسـید: بـرای مثال Software تبدیل می شود به : dpgyestr

۷- عباراتی که به عنوان رمز در نظر دارید را بـه شـکل خـاص وارد نماییـد. بـرای مثـال بعـد از وارد نمـودن ۲ کاراکتر اول رمز، با موس به ابتدای ۲ کاراکتر بروید و ۲ کاراکتر بعدی را وارد کنید، ایـن عمـل را تـا پایـان انجام دهید. به طورمثال اگر رمز شما عبارت Hard9432 مـی باشـد بـه شـکل مقابـل تبـدیل خواهـد شـد: 3294rdha توجه فرمایید که هدف از این روش نوع وارد نمودن اطلاعات است.

۸- جمله ای را در نظر بگیرید و آنرا بعنوان رمز وارد نمایید. بعضی از جملات یا شـعرها همیشـه در ذهـن فـرد باقی می‌ماند که از آنها می‌توان بعنوان رمز عبور استفاده نمود. بدین ترتیب هم از عبـارت طـولانی اسـتفاده می‌کنید هم در ذهنتان باقی می‌ماند.

۹- لغت یا ترکیبی را در نظر بگیرید و بعد آن را بهم بزنید به این صورت که حرف اول را بـا حـرف دوم، حـرف سوم را با چهارم و به همین ترتیب تا انتها ادامه دهید.

۱۰- لغات یک جمله را به اختصار بنویسید این اختصارات را خود شما تعیین می کنید و از قاعده خاصی پیـروی نمی کنند.

۱۱- در استفاده از خدمات نوین بانک از رمزهـایی متفـاوت و غیرتکـراری بـا سـایر رمزهایتـان در سـایت هـا و برنامه‌های دیگر استفاده کنید.

- ✓ به خاطر سپردن تمام رمزها هم، شاید بسیار سخت باشد لذا می توانید از نرم افزارهـای مـدیریت رمـز[۱] جهت عدم فراموشی رمزها استفاده نمایید.

۱۲-استفاده از رمز های یکبار مصرف (دستگاه رمزساز) به جای رمزهـای ایسـتا (ایـن خـدمت در آینـده ارائـه خواهد شد)

[۱] این نرم افزارها از رمزهای عبور و سایر اطلاعات مهم شما محافظت می کنند. جهت دسترسـی بـه رمـز هـای نگـه داری شـده در ایـن نرم‌افزارها یک رمز اصلی (شاه کلید) نیاز دارید و کافی است همان یک رمز را به خاطر داشته باشید.

۳-۲ دستگاه رمزساز[۲] (خدمات آتی بانک)

رمزهایی که تاکنون درباره نحوه ایجاد و حفاظت از آن توضیحاتی داده شد به رمزهای ایستا موسومند. اما دسته‌ای دیگر از رمزها تحت عنوان رمزهای یکبار مصرف نیز وجود دارند که با ضریب امنیت بالاتری مورد استفاده قرار می‌گیرند. رمزهای یکبار مصرف از طریق دستگاه کوچک رمزساز و یا تلفن همراه در دسترس کاربر قرار خواهد گرفت. جهت هر مرتبه نیاز به وارد نمودن رمز، با استفاده از این دستگاه، رمز جدیدی در اختیار شما قرار می‌گیرد که فقط برای یک بار ورود قابل استفاده خواهد بود و دیگر نیازی به بخاطر سپردن رمز و یا تغییر رمز بصورت دوره‌ای نخواهد بود.

از دستگاه رمزساز خود به خوبی مراقبت کنید و آنها را هرگز به فرد دیگری ندهید. این ابزارها مشابه امضای شما هستند و در صورت استفاده دیگران از این ابزارها، شما مسئول عواقب حقوقی و قانونی ناشی از استفاده نادرست این ابزارها خواهید بود.

۴- نکات امنیتی دستگاه‌های خودپرداز و پایانه های فروشگاهی

۱- آیا می‌دانید سارقان ممکن است هنگام خرید از پایانه‌های فروشگاه‌ها، رمز کارت شما را شنیده و در فرصت مناسب کارت شما را سرقت نمایند؟ همواره رمز کارت را شخصاً وارد نمایید.

۲- مراقب باشید هنگام واردنمودن اطلاعات شناسه کاربری و رمز عبور، شخص دیگری صفحه کلید شما را مشاهده نکند.

۳- رسید خودپرداز را در محل‌هایی که به منظور جمع آوری رسیدهای مورد نظر تعبیه گردیده قرار دهید و از رها نمودن آنها در اطراف دستگاه‌های خودپرداز خودداری نمایید.

۴-اجباری به استفاده از منوی انگلیسی در خود پرداز وجود ندارد این منو جهت بهره برداری اتباع خارجی می باشد.

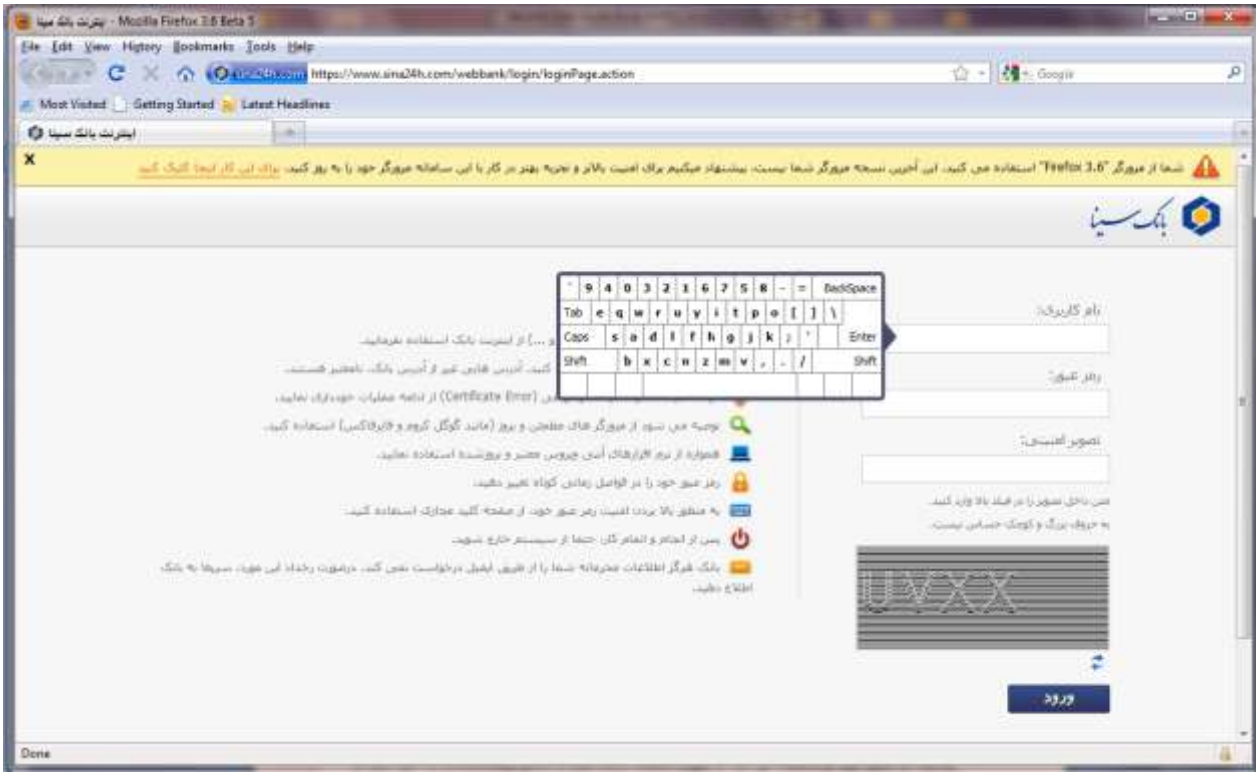
[۲] OTP Token

۵-بهتر است قبل از خرید از موجودی کارت خود آگاه باشید تا در صورت بروز مشکل نسبت بـه کـم شـدن یـا تغییر نکردن موجودی اطمینان داشته باشید.

۶-بعد از انجام تراکنش خرید از پایانه های فروشگاهی رسید دریافتی را بررسی نموده و در صـورت مغـایرت در مبلغ وجه فروشنده را مطلع نمایید.

۵- نکات امنیتی اینترنت بانک و خرید اینترنتی

۱- جهت امنیت بیشتر، از بروز بودن مرورگر خود اطمینان حاصل کنید. چنانچه در تصـویر زیـر نیـز مشـاهده می‌کنید در صورت استفاده از یک مرورگر قدیمی پیغام متناسب با نوع مرورگر و نسخه آن ظاهر می‌شود.



شکل ۱- بروز رسانی مرورگر

با کلیک بر روی پیغام فوق به صفحه بروز رسانی منتقل گردیده و می بایست متناسب با نوع مرورگر مورد استفاده، نسبت به بروزرسانی آن اقدام نمایید.(شکل۲) برای مثال اگر مرورگر شـما Internet Explorer مـی باشـد در پنجـره بروزرسانی بر روی این مرورگر کلیک نمایید همچنین می‌توانیـد نسـخه جدیـد مرورگـر خـود را مسـتقیما از سـایت اینترنتی دریافت نمایید.

شکل۲ - بروزرسانی مرورگر

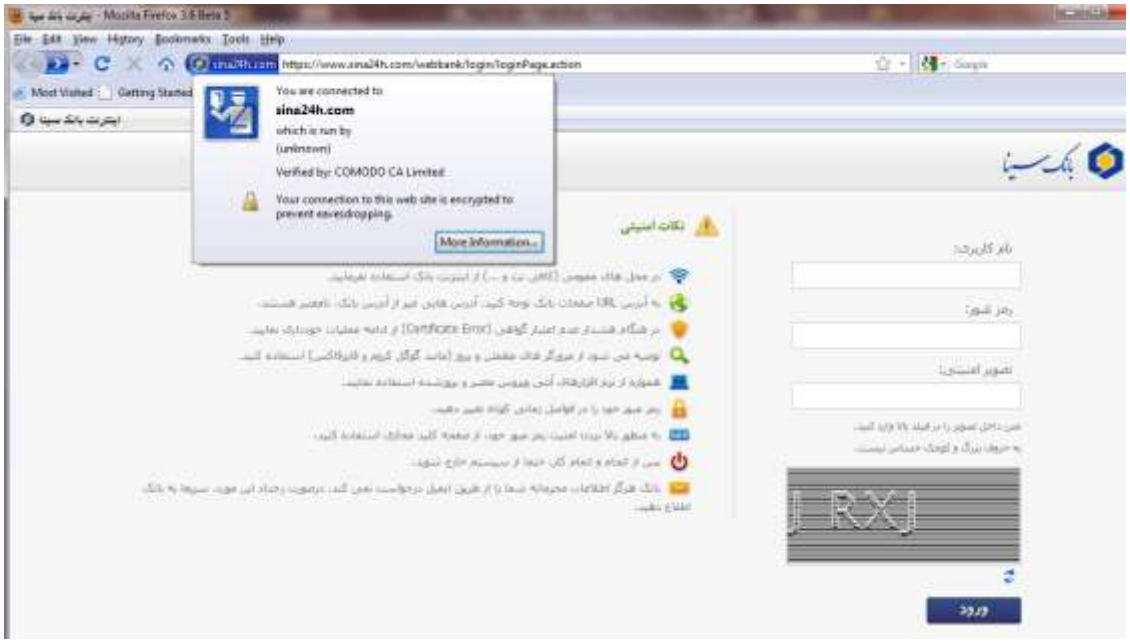
بروز بودن برنامه مرورگر اینترنت باعث بالا رفتن ضریب امنیت می‌شود. در صورت به سرقت رفتن گـواهی امنیتـی مرتبط با سایت‌های مرورگر مثل گوگل، یاهو، موزیلا، مایکروسافت و ..... سارق می‌تواند سرورهـای خـود را جـایگزین سایت‌های نامبرده نموده و به نام کاربری و رمزهای عبور کاربران دسترسی پیدا کنند. بنـابراین اگـر مرورگـر خـود را همیشه بروز نگهدارید و رمز عبور خود را در فواصل زمانی کوتاه مدت تغییر دهید باعث بالا رفـتن امنیـت اطلاعـات خود درهنگام استفاده از برنامه‌های تحت وب می‌شوید.

۲- به علامت قفل طلایی رنگی که در کنار آدرس سایت یـا در پـایین صـفحه مرورگر قرار دارد و از HTTPS بودن ابتدای آدرس اطمینان حاصـل کنیـد، در غیر اینصورت رمز عبورخود را وارد نکنید.

۳- منحصراً از صفحه اصلی بانک به آدرس http://www.sinabank.ir برای ورود به سرویس‌ها و حساب‌هـای الکترونیکی بانک سینا استفاده نمایید و هرگز به لینک‌های موجود در سایت‌های دیگر اعتماد نکنید.

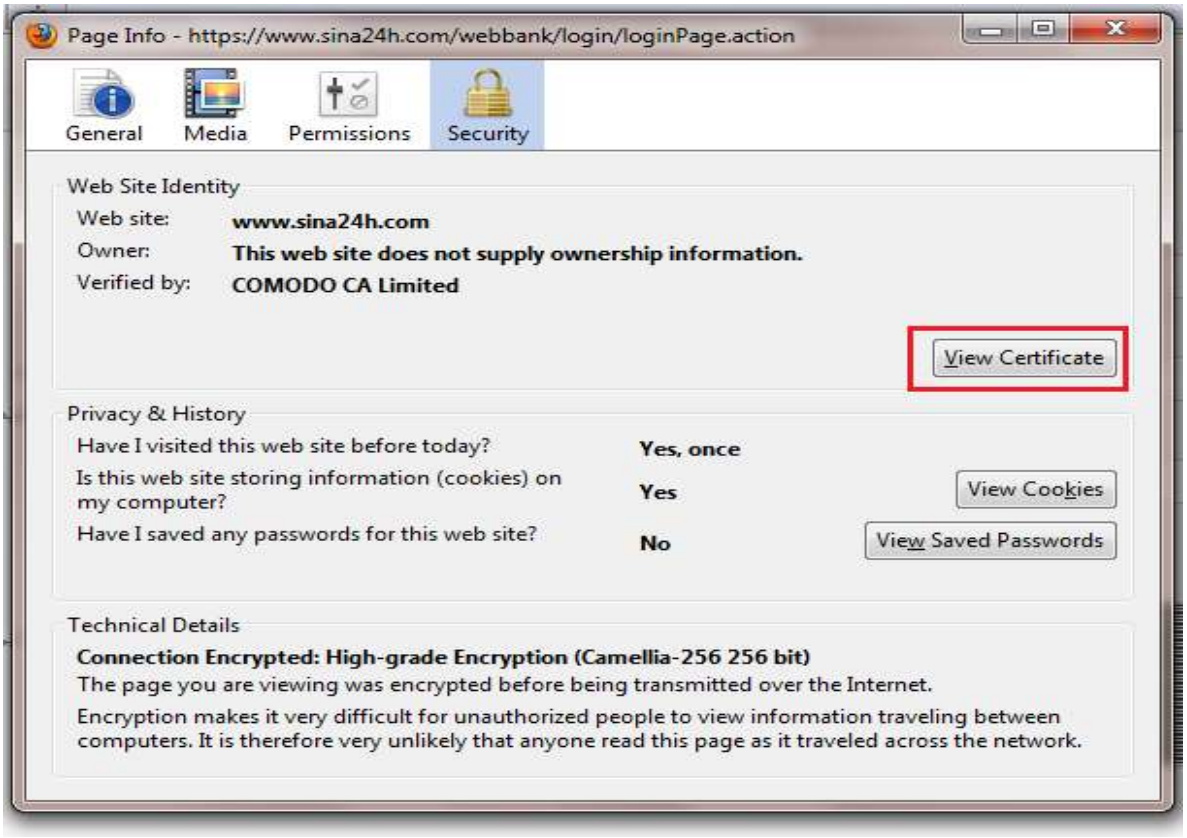
۴- پیش از ورود به حساب اینترنتی بانک خود، از درست بودن آدرس صفحه اطمینـان حاصـل کنیـد. یکـی از روش‌های اطمینان از معتبر بودن سایت بررسی گواهینامه امنیتی سایت بانک می‌باشد بـرای بـازبینی ایـن گواهی در Firefox مراحل ذیل را دنبال نمایید:

- بر روی قفل موجود در ابتدای کادر آدرس کلیک نمایید سپس جهت مشاهده مشخصات گواهی گزینه More Information را انتخاب نمایید:



شکل۳- بازبینی گواهی سایت

- در منوی بعدی بر روی گزینه View Certificate کلیک نمایید تا به صفحه اطلاعات گواهینامه وارد شوید:



شکل ۴- انتخاب گزینه View Certificate

- چنان که در شکل ۵ نیز مشاهده می کنید آدرس سایت بانک به همراه تاریخ شروع و پایان گواهی در این صفحه ثبت شده است.

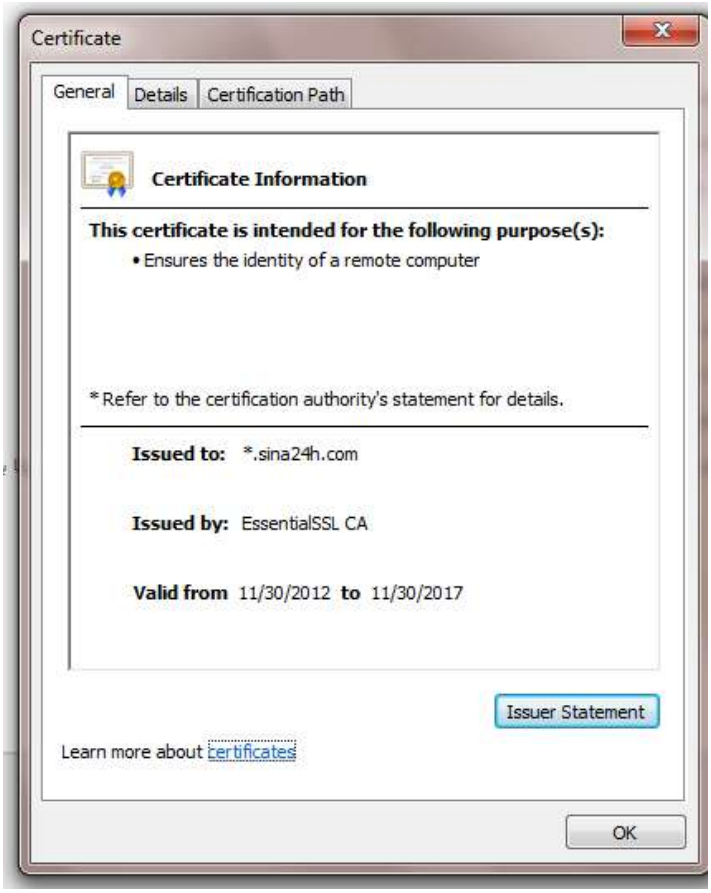
شکل۵- مشخصات گواهینامه امنیتی

همچنین جهت مشاهده گواهی در مرورگر Ineternet Explorer به صورت زیر عمل نماید:

- بر روی قفل کلیک نماید سپس بر روی گزینه View Certificate کلیک نماید تا به صفحه اطلاعات گواهینامه وارد شوید:

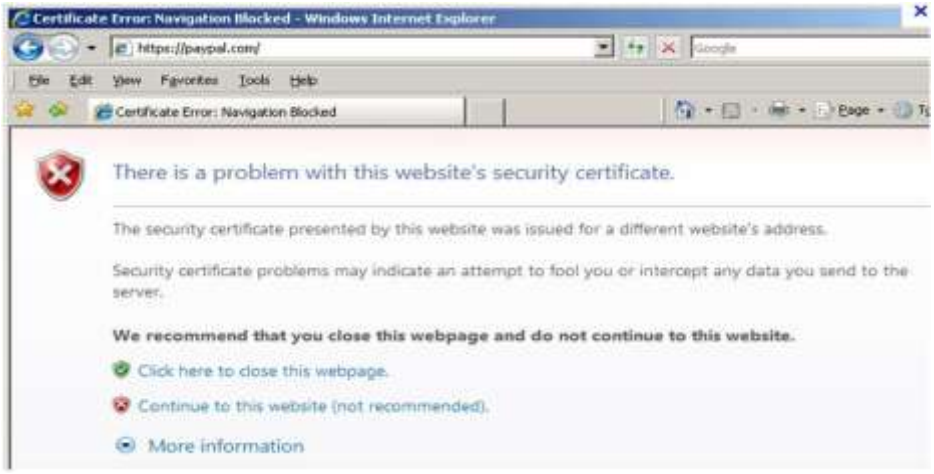
شکل ۶- بازبینی گواهی سایت

- چنان که در شکل ۷ نیز مشاهده می کنید آدرس سایت بانک به همراه تاریخ شروع و پایان گواهی در این صفحه ثبت شده است.



شکل ۷- مشخصات گواهینامه امنیتی

۵- به پیام ها و هشدارهای امنیتی مربوط به نامعتبر بودن گواهی الکترونیکی سایت توجه کنید. به محض مشاهده این پیام ها از ادامه کار چشم پوشی کنید. معمولا در این گونه مواقع امکانی وجود خواهد داشت که در صورتی که خواهان ادامه کارباشید بتوانید نسبت به هشدار صادر شده چشم پوشی نمایید، اما با توجه به خطراتی که در انتظار شماست هرگز این کار را انجام ندهید.

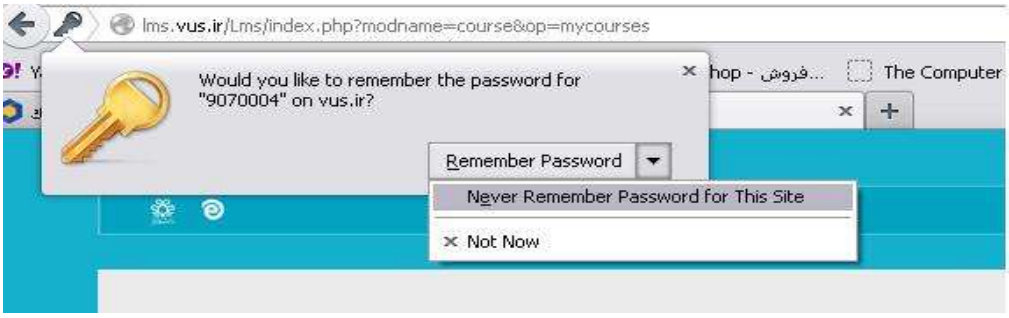


شکل۸- پیام ها و هشدارهای امنیتی نسبت به نامعتبر بودن سایت

۶- برای حفاظت از حساب بانکی خود بهتر است از صفحه کلید مجازی استفاده نمایید.

شکل۹- استفاده از صفحه کلید مجازی

۷- نام کاربری و رمز عبور خود را در مرورگر ذخیره نکنید. کامپیوتر قادر است رمز عبور شما را ذخیره کند تا مجبور نباشید هر بار آن راوارد کنید. در صورت مواجه شدن با پیامی مبنی بر ذخیره نمودن اطلاعات، گزینه ای در جهت ذخیره نکردن انتخاب کنید.



شکل ۱۰- انتخاب گزینه عدم ذخیره سازی اطلاعات

۸- مادامی که از سامانه اینترنت بانک خود خارج نشده‌اید، کامپیوتر خود را ترک نکنید. بعد از اتمام کار خود حتما از سامانه خارج شوید (Logout کنید).

۹- روزانه کلاهبرداری‌های عظیمی در دنیا از طریق سایت‌های به ظاهر قانونی با سرقت شماره حساب و رمز عبور اینترنتی مشتریان انجام می‌شود. بنابراین:

- هرگز از وب‌سایت‌های ناشناس و نامعتبر خرید آنلاین نکنید. فروشگاه‌های معتبر دارای نماد اعتماد الکترونیکی می‌باشند. جهت اطمینان از صحت این گواهی روی آن کلیک نمایید. طبق این نماد فروشگاه ها ملزم به رعایت موارد ذیل می باشند:

طبقه	ردیف	شرح معیار
اطلاعات فروشگاه (صفحه تماس با ما)	۱	نشانی پستی واحد اقتصادی عرضه کننده کالا یا خدمت
	۲	تلفن و نمابر واحد اقتصادی عرضه کننده کالا یا خدمت
	۳	نشانی پست الکترونیکی واحد اقتصادی عرضه کننده کالا یا خدمت
	۴	نام و نام خانوادگی مسئول واحد اقتصادی عرضه کننده کالا یا خدمت (صاحب امتیاز دامنه)
	۵	نام و نام خانوادگی مدیر عامل یا نماینده قانونی یا مسئول وب سایت
	۶	ارتباط با بخش های مختلف (فروش، پشتیبانی، خدمات پس از فروش و ...) از طریق شماره تلفن های گویا، شماره نمابر، نشانی پستی، پست الکترونیکی و ...
	۷	تعریف موضوع فعالیت واحد اقتصادی

	۸	نام دامنه باید با هویت و مشخصات حقوقی وب سایت مربوطه ثبت شود .
شناسنامه کالا یا خدمت	۹	هویت تامین‌کننده (شامل کشور سازنده)
	۱۰	نمایش نام تجاری که تحت آن نام به فعالیت مشغول می باشد (برند)
	۱۱	قیمت کالا یا خدمات
	۱۲	مشخصات فنی و ویژگی های کاربردی
مشخصات سفارشات	۱۳	اعلام میزان مالیات بر ارزش افزوده (VAT) به خریدار (در صورتیکه کالا یا خدمت مشمول مالیات نمی باشد در سایت مربوطه توضیح داده شود و یا در فاکتور صفر ریال در نظر گرفته شود)
	۱۴	اعلام هزینه‌های که برای خرید کالا یا خدمت برعهده‌ی مشتری خواهد بود (قیمت کالا یا خدمت ، هزینه تماس، هزینه حمل، هزینه بسته‌بندی و...)
	۱۵	واضح بودن روند برگرداندن کالا و یا انصراف از دریافت خدمت و روشهای بازپرداخت وجه
	۱۶	تولید پیش فاکتور با امکان نمایش چاپ و یا ارسال به آدرس پست الکترونیکی
	۱۷	مدت زمان اعتبار قیمت ارائه شده برای فروش کالا و خدمات
	۱۸	دادن اطلاعات کامل و تفصیلی در مورد خدمات پس از فروش به مشتری
	۱۹	اعلام تأیید دریافت سفارش از مشتری
	۲۰	ردیابی وضعیت ارسال کالاهای سفارش داده شده امکانپذیر باشد
ویژگی های وب سایت	۲۱	زبان اصلی وب سایتها زبان فارسی باشد. صفحه خانه و صفحه ورودی اصلی باید به زبان فارسی بارگذاری شود. در صورت استفاده از عبارات زبان انگلیسی باید معادل فارسی آن نیز درج شود.
	۲۲	در وب سایت هایی که به صورت چند زبانه می باشند باید امکان تغییر زبان برای کاربران در تمام صفحات فراهم شود
	۲۳	صفحات وب سایت باید مطابق با استاندارد ISO/iec 10646 و با استفاده ار کاراکتر ست یونیکد (UTF-8) طراحی و قابل نمایش باشند
	۲۴	در صورت هدایت بازدیدکنندگان به وب‌سایت های دیگر، صفحه‌ی مربوطه در پنجره‌ی جدید نمایش داده شود.
	۲۵	عدم استفاده از pop up
	۲۶	گواهینامه دیجیتالی SSL داشتن گواهینامه دیجیتالی توسط فروشنده جهت اطمینان از امنیت تراکنش های اینترنتی

جدول ۱- الزامات فروشگاه‌های دارای طرح نماد اعتماد الکترونیکی

- به ایمیل‌ها و پیام‌های ناشناس و مشکوک مبنی بر ورود به حساب اینترنتی خود توجه نکنید.

- زمانی که در خرید اینترنتی برای پرداخت اقدام می‌کنید باید از سایت فروشگاه به سایت بانک منتقل شوید. اما ممکن است افراد سودجو، شما را به سایت بانک منتقل نکرده و از شما درخواست کنند که تمام اطلاعات کارت را در همان صفحه فروشگاه وارد نمایید و یا شما را به سایتی شبیه به سایت بانک منتقل می کنند و با جلب اعتماد شما از طریق نشان دادن آرم بانک و ....، شما را ترغیب به وارد نمودن اطلاعات کارت نمایند. اما به‌خاطر داشته باشید که آدرس صفحه پرداخت بانک با Https:// شروع می شود و در این صفحات تصویر یک قفل در صفحه مشاهده می‌شود. اگر وارد قسمت پرداخت شدید و این قفل رنگی را مشاهده نکردید، شماره کارت و رمز خود را وارد نکنید.

۵- ۱ نکات امنیتی در محیط اینترنت

مشتری گرامی؛ هنگامی که قصد انجام خرید اینترنتی یا امور بانکی یا ورود به هر سایت دیگری دارید، اگر فردی (هکر) در مسیر انتقال داده‌های شما و سایت مورد نظرتان قرار گیرد می‌تواند از اطلاعات مورد تبادل آگاهی پیدا کند. در صورتی که این اطلاعات برای شما ارزشمند باشد (مانند نام کاربری، رمز عبور، شماره سپرده، موجودی و هر پیام با ارزش دیگر)، باید از سایت‌هایی استفاده کنید که مجهز به SSL باشد.

مجهز بودن سایتی که وارد آن شدید به SSL، که نشان آن وجود آدرس Https:// است باعث اطمینان از هویت فروشنده و امنیت اطلاعات مبادله شده بین شما و فروشگاه است. در این سایت‌ها اطلاعات مبادله شده بین شما و سایت مقصد به صورت بهم ریخته مبادله می‌شود تا اگر در راه مبادله با مقصد، هکر به آن دست یافت، برای آن فرد قابل فهم نباشد. این کد، در مقصد بازیابی شده و تبدیل به رمز ابتدایی می شود. بنابراین در صورت وجود هکر در این مسیر، این اطلاعات برای او مورد استفاده نخواهد بود.

شکل۱۱ - محیط امن بانک

۵- ۲ نکات امنیتی درباره اطلاعات ماندگار بر روی سیستم

ورود به هر سایتی همراه با ثبت آدرس سایت در سیستم، همچنین بوجود آمدن فایل‌هایی نظیر کوکی‌ها بر روی سیستم می‌شود، که همانند رد پایی باقی می‌ماند اگر فردی پس از شما از همان سیستم استفاده کند با داشتن کمی اطلاعات نرم‌افزاری، می تواند از سایت‌هایی که شما بازدید کرده‌اید، آگاه شود.

در صورت استفاده از کامپیوتر غیر شخصی جهت انجام امور اینترنتی، از امکاناتی که در برنامه‌هایی نظیر Firefox، Internet Explorer یا Google Chrome وجود دارد استفاده کنید تا باعث جلوگیری از نگهداری اطلاعاتی نظیر بازدید از سایت‌ها یا فایل‌های موقت و کوکی‌ها بر روی سیستم شود. برای استفاده از این امکانات در محیط‌های internet Explorer، Firefox و Google Chrome از قابلیت‌هایی که در زیر شرح داده می‌شود استفاده کنید.

الف) محیط Internet Explorer

۱. از منوی Tools گزینه InPrivate browsing را انتخاب کنید، یا کلیدهای Ctrl+ Shift+P را بزنید.

۲. وارد صفحه InPrivate browsing شوید.

✓ این امکان در Internet Explorer 8.0 و بعد از آن وجود دارد. تا زمانی که در حالت InPrivate browsing هستید این نماد InPrivate کنار کادر آدرس خواهد بود و ورود به سایت‌های مختلف یا جستجوهای شما، ثبت نمی‌شود.

شکل ۱۲- استفاده از Inprivate Browsing در محیط Internet Explorer 8.0

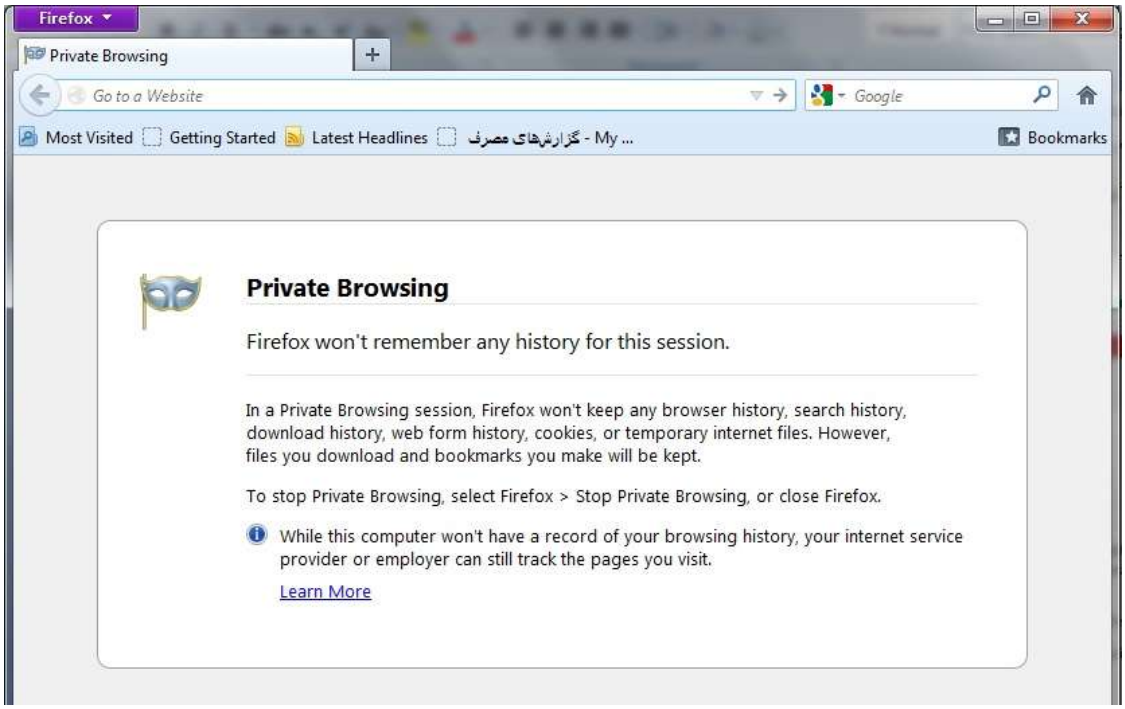
۳. هر زمان که خواستید از این محیط خارج شوید فقط کافی است پنجره Inprivate browsing را ببندید.

ب) محیط Firefox

۱. در محیط FireFox از منوی Tools گزینه Start Private Browsing را انتخاب کنید یا کلید های Ctrl+Shift+P را بزنید.

۲. وارد صفحه Private browsing می شوید.

✓ این امکان در Firefox 3.5 قرار داده شده در نسخه‌های بعدی نیز وجود دارد. تا زمانی که در حالت Private browsing هستید این نماد در بالای کادر آدرس خواهد بود و ورود به سایت‌های مختلف یا جستجوهای شما، در این حالت ثبت نمی شود.



شکل۱۳- استفاده از Private Browsing در محیط Firefox

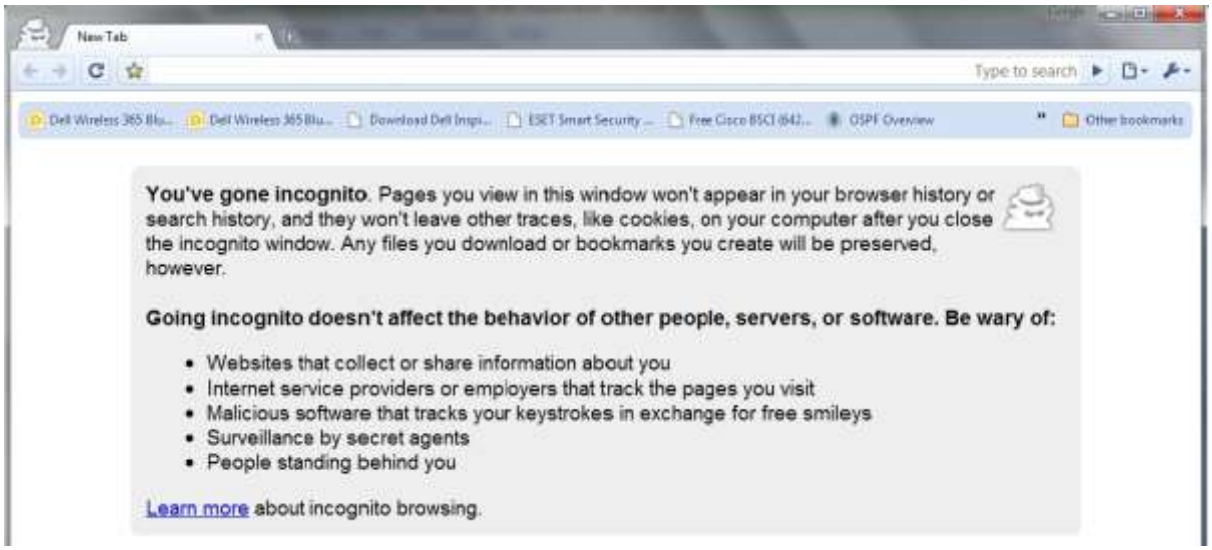
۳. هر زمان که خواستید از این محیط خارج شوید از منوی Tools گزینه Stop Private Browsing را انتخاب کنید، یا کلیدهای Ctrl+Shift+P را بزنید.

ج) محیط Google Chrome

۱. در محیط Google Chrome با کلیک روی ابزار (در سمت راست و بالای صفحه) از منـوی بـاز شـده گزینـه New Incognito Windows را انتخاب کنید، یا کلیدهای Ctrl+Shift+N را بزنید.

۲. وارد صفحه Private browsing می شوید.

✓ تا زمانی که در حالت Incognito Windows هستید ایـن نمـاد  در گوشه بالا سمت چپ خواهـد بود و ورود به سایت های مختلف یا جستجوهای شما، در این حالت ثبت نمی‌شود.



شکل۱۴- استفاده از New Incognito Windowsدر محیط Google Chrome

۳. هر زمان خواستید از این محیط خارج شوید فقط کافی است پنجره را ببندید.

۶- نکات امنیتی همبانک سینا

۱. قفل خودکار صفحه نمایش در صورت عدم استفاده از تلفن همراه را فعال نمایید.

۲. جهت ورود به تلفن همراه از رمز عبور استفاده نمایید.

۳. پس از اتمام کار با سرویس همبانک از منوی خروج استفاده نمایید.

شکل ۱۵- انتخاب منوی خروج در سرویس همبانک مربوط به گوشیiphone

۴. در صورت سرقت کارت، سیم کارت تلفن همراه یا واگذاری سیم کارت، فورا به یکی از شعب بانک اطلاع دهید. سپس حداکثر ظرف ۴۸ ساعت مراتب را مکتوب نمایید.