



بانک سینا

معاونت فناوری اطلاعات

اداره امنیت فناوری اطلاعات



دفترچه راهنمای امنیتی کاربران

نسخه ۴

تیرماه ۱۳۹۹

فهرست

عنوان	صفحه
۱- مقدمه.....	۳
۲- چند توصیه قبل از شروع.....	۴
۳- نکات امنیتی رمز عبور.....	۶
۳-۱ پیشنهاداتی برای انتخاب رمز عبور امن.....	۶
۳-۲ رمزهای یکبار مصرف.....	۸
۳-۲-۱ نرم افزار تولید رمز دوم یکبار مصرف (پویا) کارت.....	۸
۳-۲-۲ سرویس رمز یکبار مصرف (بلیط امنیتی) اینترنت بانک.....	۹
۴- نکات امنیتی دستگاه‌های خودپرداز و پایانه های فروشگاهی.....	۹
۵- نکات امنیتی اینترنت بانک و خرید اینترنتی.....	۱۰
۵-۱ نکات امنیتی در محیط اینترنت.....	۱۹
۵-۲ نکات امنیتی درباره اطلاعات ماندگار بر روی سیستم.....	۲۰
۶- نکات امنیتی موبایل بانک.....	۲۳

۱- مقدمه

در دنیای فناوری اطلاعات، امنیت یکی از اساسی‌ترین شاخص‌های کاری است بطوریکه می‌توان 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 می‌باشد 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 بانکی، از هر گونه ورود به حساب یا جابجایی پول از حسابتان

بلافاصله با پیامک مطلع می‌شوید؟

۳- در صورتی که احتمال می‌دهید شناسه کاربری یا رمز عبور شما افشا شده یا به سرقت رفته است، سریعاً با

شماره ۰۲۱-۴۱۷۳۱ (مرکز ارتباط مشتریان) پاسخگوی ۲۴ ساعته بانک سینا تماس بگیرید.

۴- هیچ بانکی نیاز به رمز عبور حساب بانکی 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- امن‌ترین محل برای حفظ رمز عبور، حافظه شما 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 بانکی خود را در پشت کارت ننویسید و یا در کیف کارت نگهداری نکنید.

۹- هنگام خرید، رمز خود را شخصاً وارد نموده 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 رایانه‌های عمومی و ناشناس پرهیز

کنید. ممکن است در رایانه‌های این گونه مراکز، نرم افزارهای

جاسوسی برای سرقت نام کاربری و رمز عبور شما نصب شده باشد. در صورت ضرورت، حتی

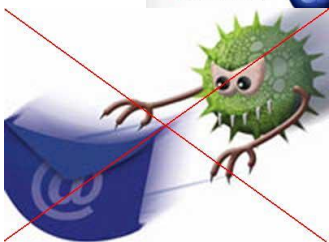
الامکان از صفحه کلید مجازی استفاده کنید.

❖ همواره از نرم افزار آنتی ویروس معتبر و بروز استفاده نمایید.



❖ ایمیل های 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 هدایت به سایت های آلوده هستند. تا حد امکان ایمیل های تبلیغاتی را باز نکنید.

۱۲- آیا می دانید ممکن است تنها با کلیک کردن روی یک لینک، کامپیوتر شما آلوده به نرم افزارهای جاسوسی شود؟ هرگز لینک ها و عکس هایی که در ایمیل ها یا پیام های ناشناس و مشکوک وجود دارند را باز نکنید.

۱۳- از دانلود کردن فایل از وب سایت های اشتراک گذاری فایل بپرهیزید.

۱۴- برخی از وب سایت ها با تشویق کاربران به دانلود آنتی ویروس یا انجام اسکن رایگان، سعی در فریب کاربر دارند، هرگز پیشنهاد های 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 حساب های مختلف شما، از طریق اینترنت بانک، موبایل بانک و سایر خدمات بانکداری نوین را محدود نماید.

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

۱۹- در صورت مفقود شدن و یا به سرقت رفتن کارت بانکی خود، در اسرع وقت جهت مسدود نمودن آن از طریق سرویس های نوین (اینترنت بانک، تلفن بانک و ..) یا تماس با مرکز ارتباط مشتریان بانک (۰۲۱-۴۱۷۳۱) اقدام نموده و یا به یکی از شعب بانک مراجعه فرمایید.

۲۰- جهت آگاهی از آخرین اطلاعات مربوط به جرائم رایانه ای و تهدیدات امنیتی به [سایت پلیس فتا](#) مراجعه نمایید.

۳- نکات امنیتی رمز عبور



۱. همیشه به خاطر داشته باشید که نام کاربری و رمز عبور در دنیای مجازی، همانند آدرس دقیق و کلید ورود 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 و ... استفاده نکنید.
۲. رمز عبور خود را در فواصل زمانی مشخص (حداکثر هر ۹۰ روز) تغییر دهید.
۳. توصیه می‌شود رمز عبور در اولین ورود تغییر یابد.
۴. هیچ‌گاه اطلاعات حساب و کارت بانکی خود را از طریق پیامک برای دیگران ارسال ننمایید. در صورتیکه شماره حساب یا شماره کارت 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

پیشنهادهای زیر می‌تواند 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، حروف کوچک، اعداد و کاراکترهای ویژه استفاده نمایید.



- ۳- در رمز عبور خود از حروفی که بر روی صفحه کلید در کنار هم قرار گرفته‌اند استفاده نکنید. استفاده از رمز های عبوری مانند "qwerty" یا "asdf" و "12345678" که از در کنار هم قرار گرفتن حروف یا اعداد ایجاد شده‌اند 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 این صورت تبدیل می شود:

"ISILPWBS"

۶- لغتی را در نظر بگیرید و سپس حروف سمت راست آن را که بر روی صفحه کلید قرار دارد، بنویسید: برای

مثال Software تبدیل می شود به : dpgyestr

۷- عباراتی که به عنوان رمز در نظر دارید را به شکل خاص وارد نمایید. برای مثال بعد از وارد نمودن ۲ کاراکتر

اول رمز، با موس به ابتدای ۲ کاراکتر بروید و ۲ کاراکتر بعدی را وارد کنید، این عمل را تا پایان انجام دهید.

مثلا اگر رمز شما عبارت Hard9432 می باشد به شکل مقابل تبدیل خواهد شد: 3294rdha

۸- جمله ای را در نظر گرفته و آن را بعنوان رمز وارد نمایید. بعضی از جملات یا شعرها همیشه در ذهن فرد

باقی می ماند که از آنها می توان بعنوان رمز عبور استفاده نمود. بدین ترتیب هم از عبارت طولانی استفاده

می کنید هم در ذهنتان باقی می ماند.

۹- لغت یا ترکیبی را در نظر گرفته و بعد آن را بهم بزنید؛ به این صورت که حرف اول را با حرف دوم، حرف

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 پیروی

نمی کنند.

۱۱- در استفاده از خدمات نوین بانک از رمزهایی متفاوت و غیر تکراری با سایر رمزهایتان در سایت ها و

برنامه های دیگر استفاده کنید.

✓ به خاطر سپردن تمام رمزها هم، شاید بسیار سخت باشد لذا می توانید از نرم افزارهای مدیریت رمز^۱

جهت عدم فراموشی رمزها استفاده نمایید.

۱۲- از رمز های یکبار مصرف به جای رمزهای ایستا استفاده کنید.

^۱ این نرم افزارها از رمزهای عبور و سایر اطلاعات مهم شما محافظت می کنند. جهت دسترسی به رمز های نگه داری شده در این نرم افزارها یک رمز اصلی (شاه کلید) نیاز دارید و کافی است همان یک رمز را به خاطر داشته باشید.

۳-۲ رمزهای یکبار مصرف

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 رمزساز^۲ و یا تلفن همراه در دسترس کاربر قرار خواهد گرفت. با استفاده از این روش، جهت هر مرتبه نیاز به وارد نمودن رمز، 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.

۳-۲-۱ نرم افزار تولید رمز دوم یکبار مصرف (پویا) کارت

کارتهای بانکی همواره یکی از پرکاربردترین سرویس‌هایی بانکی می‌باشد که مشتریان از طریق آن می‌توانند امور بانکی خود از قبیل انواع انتقال وجه، پرداخت قبض، دریافت صورتحساب، خرید شارژ و ... را انجام دهند. با توجه به در دسترس بودن کلیه اطلاعات کارت مشتریان در هنگام خریدهای اینترنتی حفظ امنیت رمز دوم کارت از مهمترین ارکان استفاده از این سرویس می‌باشد.

یکی از راهکارهای افزایش امنیت این سرویس در جهت عدم امکان دسترسی سوء استفاده کنندگان به رمز دوم کارت مشتریان، استفاده از رمز یکبارمصرف می‌باشد. در همین راستا بانک سینا اقدام به ارائه نرم افزار تولید رمز دوم یکبار مصرف کارت برای گوشی‌های دارای سیستم عامل اندروید و iOS نموده است. مشتریان می‌توانند با دانلود این نرم افزار و فعالسازی آن مطابق با راهنمای فعالسازی ارائه شده در [وب سایت بانک](#)، هر بار برای انجام تراکنش خرید اینترنتی اقدام به دریافت رمز دوم یکبار مصرف از نرم افزار مربوطه نمایند.

برای استفاده از امکانات این نرم افزار کافی است نسخه مناسب با گوشی تان را انتخاب کرده و نصب کنید. پیشنهاد می‌گردد پیش از دانلود نرم افزار، راهنمای نصب و کاربری را مطالعه نمایید.

برخی مزایای نرم افزار تولید رمز دوم یکبار مصرف کارت عبارت است از:

- جلوگیری از افشای رمز دوم کارت و سوء استفاده‌های احتمالی

² OTP Token

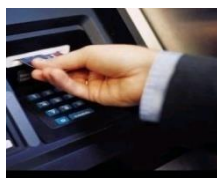
- افزایش امنیت در تراکشنهای مالی و غیرمالی

- عدم نیاز به اینترنت در زمان تولید رمز

۲-۲-۳ سرویس رمز یکبار مصرف (بلیط امنیتی) در اینترنت بانک

این سرویس در تداوم اقدامات و فعالیت هایی است که از سوی بانک برای افزایش ضریب امنیت و استحکام سامانه های اینترنتی و نرم افزارهای بانکی در جهت کاهش کلاهبرداری های اینترنتی صورت می گیرد. نحوه استفاده از این خدمت برای کاربران اینترنت بانک بدین صورت است که در هنگام ورود به سامانه یا انجام عملیات بانکی مختلف شامل انتقال وجه از سپرده (عادی، مستمر، پایا و ساتنا)، خرید شارژ، پرداخت قبوض و پرداخت اقساط تسهیلات، یک کد امنیتی با عنوان بلیط امنیتی به شماره تلفن همراه مشتری که در بانک ثبت شده است، ارسال می گردد که با وارد نمودن این کد در قسمت مربوط به بلیط امنیتی، عملیات مربوطه انجام می پذیرد.

از دستگاه رمز ساز و تلفن همراه 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 دستگاه های خودپرداز و پایانه های فروشگاهی

۱- آیا می دانید سارقان ممکن است هنگام خرید از پایانه های فروشگاهی، 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 وارد نمودن 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 دستگاه های خودپرداز خودداری نمایید.

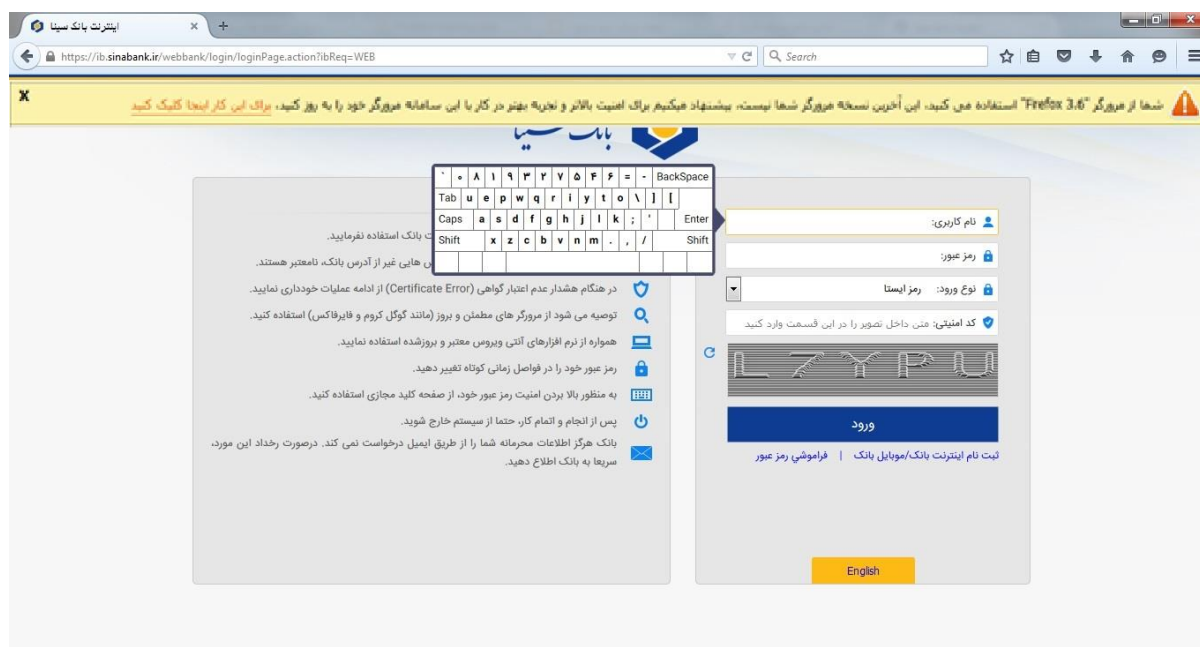
۴- اجباری به استفاده از منوی انگلیسی در خود پرداز وجود ندارد. این منو جهت بهره برداری اتباع خارجی می باشد.

۵- بهتر است قبل از خرید از موجودی کارت خود آگاه باشید تا در صورت بروز مشکل، نسبت به کم شدن یا تغییر نکردن موجودی اطمینان داشته باشید.

۶- بعد از انجام تراکنش خرید از پایانه های فروشگاه های رسید دریافتی را بررسی نموده و در صورت مغایرت 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 تصویر زیر نیز مشاهده می کنید در صورت استفاده از یک مرورگر قدیمی پیغام متناسب با نوع مرورگر و نسخه آن ظاهر می شود.



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 بروز رسانی آن اقدام نمایید. (شکل ۲) برای مثال اگر مرورگر شما Internet Explorer می باشد در پنجره بروز رسانی بر روی این مرورگر کلیک نمایید همچنین می توانید نسخه جدید مرورگر خود را مستقیماً از سایت اینترنتی دریافت نمایید.

بروز رسانی مرورگر

برای بروز رسانی مرورگر خود، بر روی تصویر آن در فهرست زیر کلیک کنید.



شکل ۲ - بروز رسانی مرورگر

بروز بودن برنامه مرورگر اینترنت باعث بالا رفتن ضریب امنیت می شود. در صورت به سرقت رفتن گواهی امنیتی مرتبط با سایت های مرورگر مثل گوگل کروم، موزیلا فایرفاکس و ... سارق می تواند سرورهای خود را جایگزین سایت های نامبرده نموده و به نام کاربری و رمزهای عبور کاربران دسترسی پیدا کنند. بنابراین اگر مرورگر خود را همیشه بروز نگهدارید و رمز عبور خود را در فواصل زمانی کوتاه مدت تغییر دهید، باعث بالا رفتن امنیت اطلاعات خود در هنگام استفاده از برنامه های تحت وب می شوید.



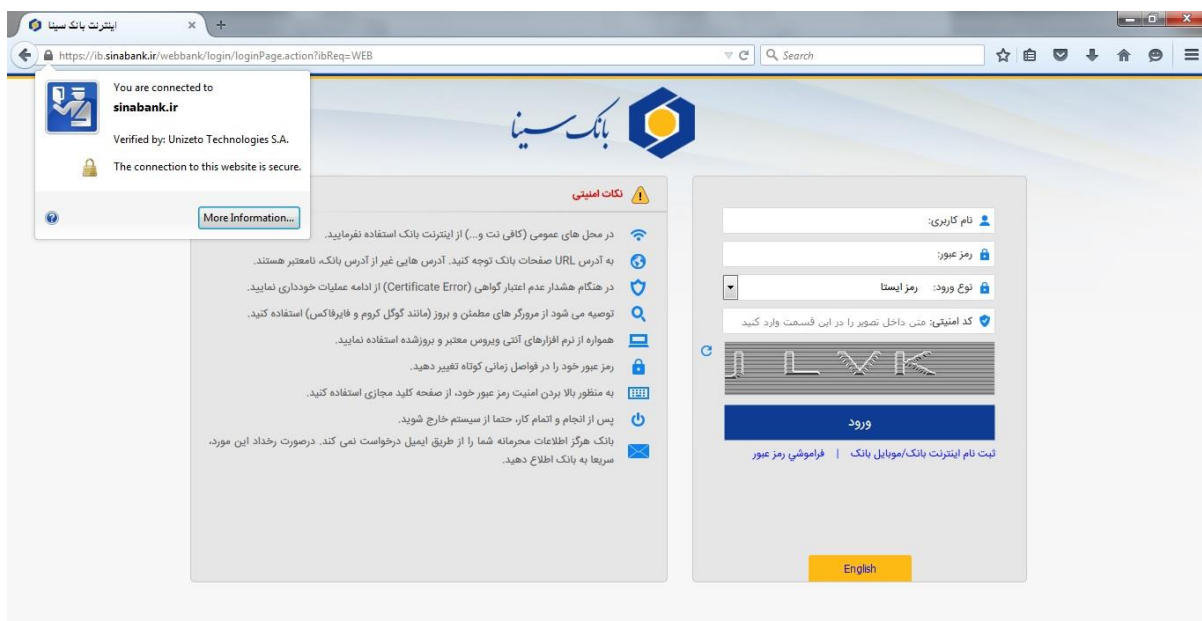
۲- به علامت قفل طلایی رنگی که در کنار آدرس سایت یا در پایین صفحه مرورگر قرار دارد و از HTTPS بودن ابتدای آدرس اطمینان حاصل کنید، در غیر این صورت رمز عبور خود را وارد نکنید.

۳- منحصراً از صفحه اصلی بانک به آدرس <https://www.sinabank.ir> برای ورود به سرویس ها و حساب های الکترونیکی بانک سینا استفاده نمایید و هرگز به لینک های موجود در سایت های دیگر اعتماد نکنید.

۴- پیش از ورود به حساب اینترنتی بانک خود، از درست بودن آدرس صفحه اطمینان حاصل کنید. یکی از روش های اطمینان از معتبر بودن سایت، بررسی گواهینامه امنیتی سایت بانک می باشد. برای بازبینی این گواهی در مرورگر Firefox مراحل ذیل را دنبال نمایید:

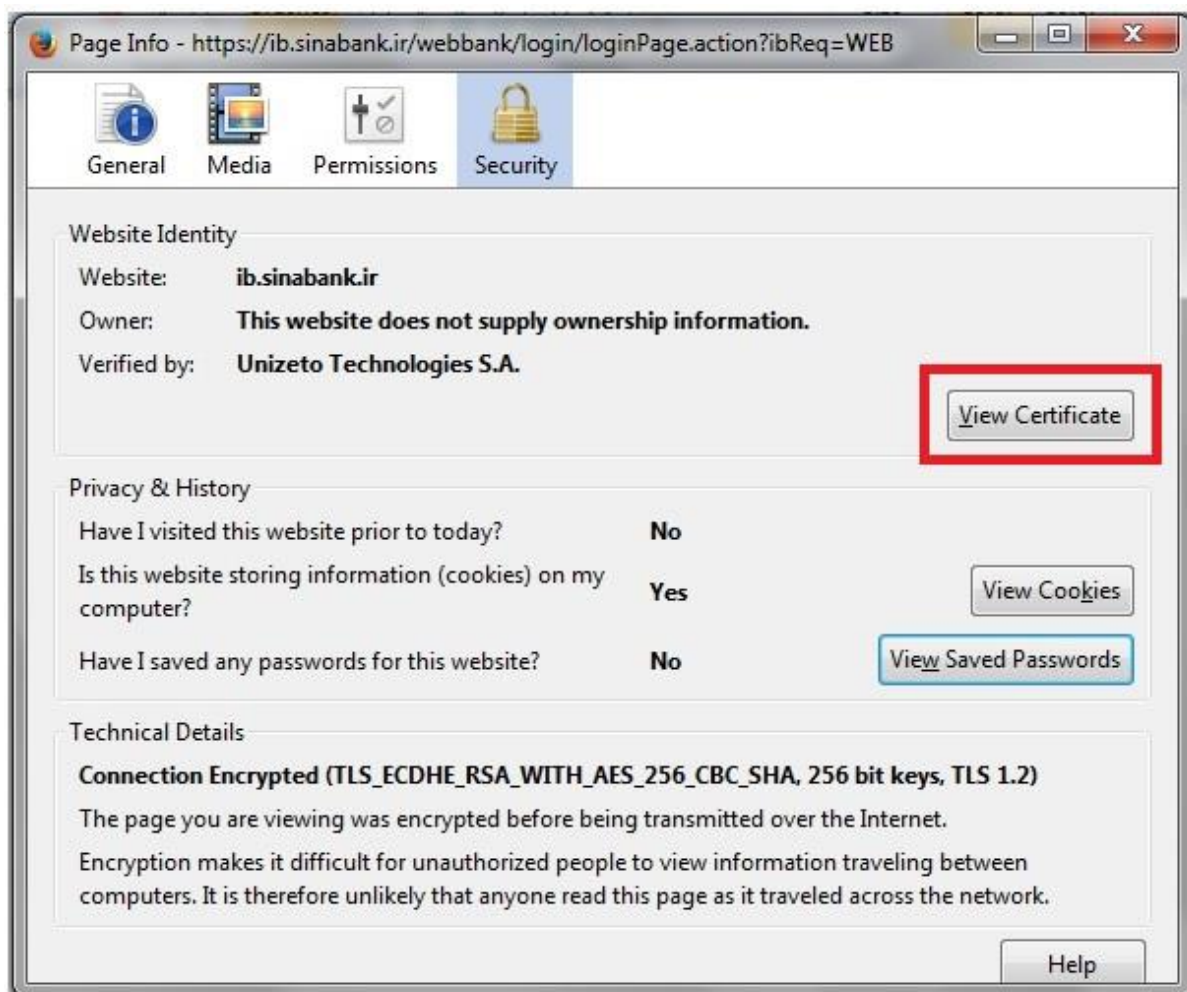
- بر روی قفل موجود در ابتدای کادر آدرس کلیک نمایید. سپس جهت مشاهده مشخصات گواهی،

گزینه More Information را انتخاب نمایید:



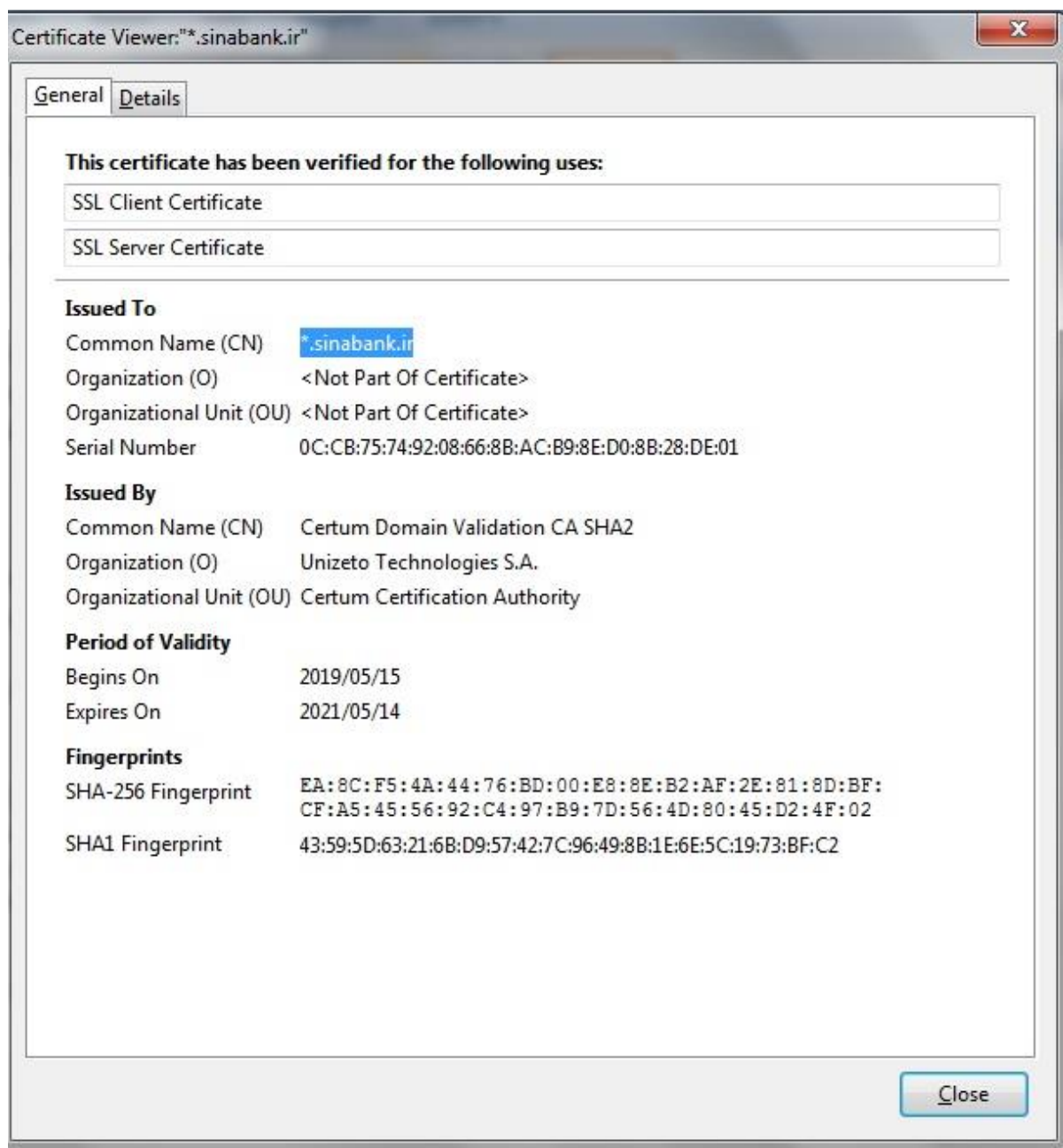
شکل ۳- بازیابی گواهی سایت

- 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.



شکل ۵- مشخصات گواهینامه امنیتی

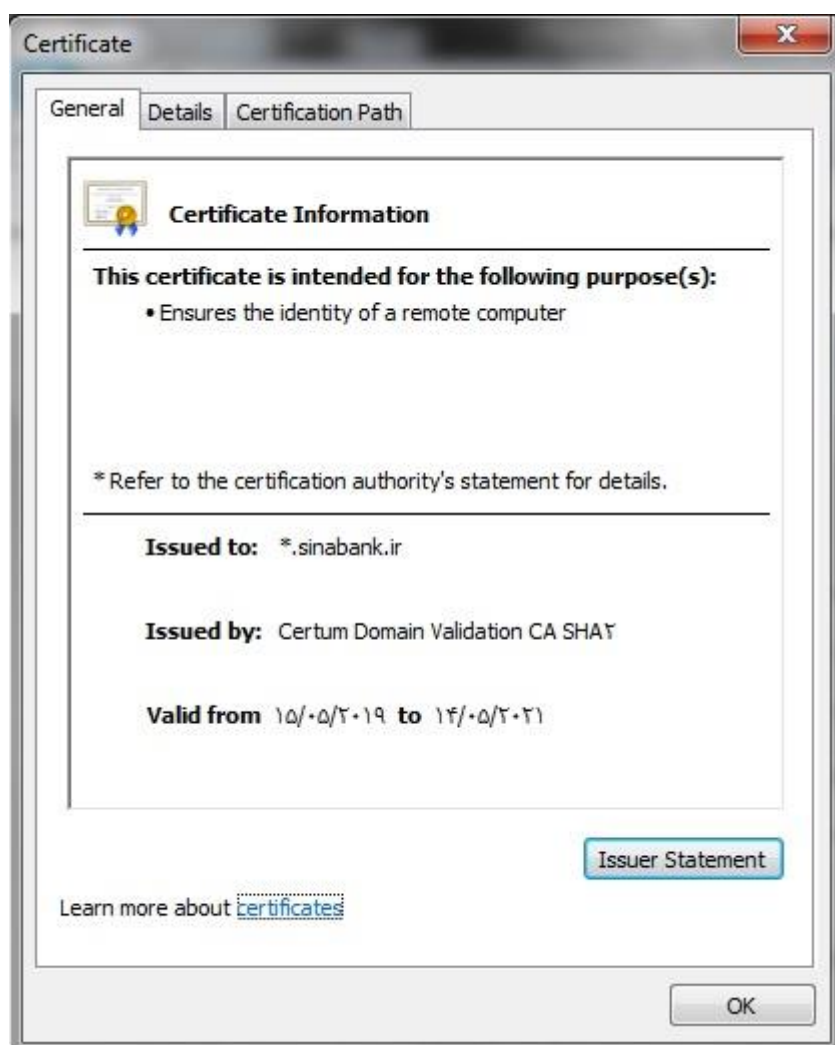
همچنین جهت مشاهده گواهی در مرورگر Internet Explorer به صورت زیر عمل نماید:

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



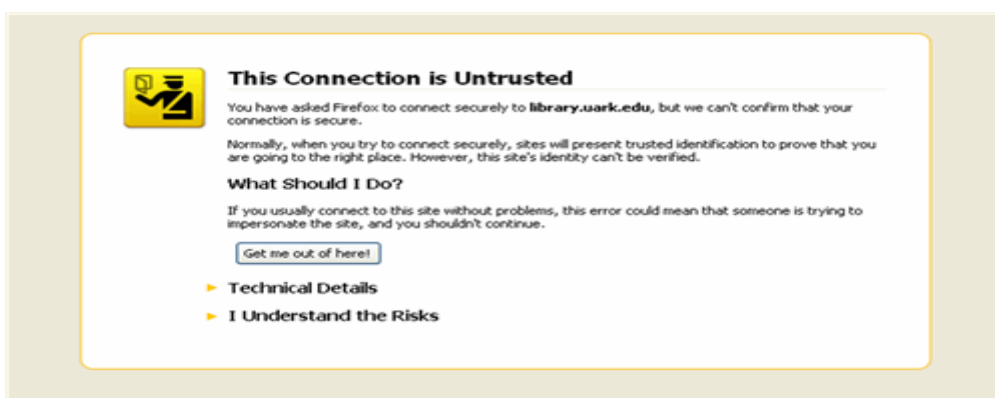
شکل ۶- بازبینی گواهی سایت

- 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. معمولاً در این گونه مواقع امکانی وجود خواهد داشت که در صورتی که مایل به ادامه کار باشید، بتوانید نسبت به هشدار صادر شده چشم پوشی نمایید. اما با توجه به خطراتی که در انتظار شماست، هرگز این کار را انجام ندهید.



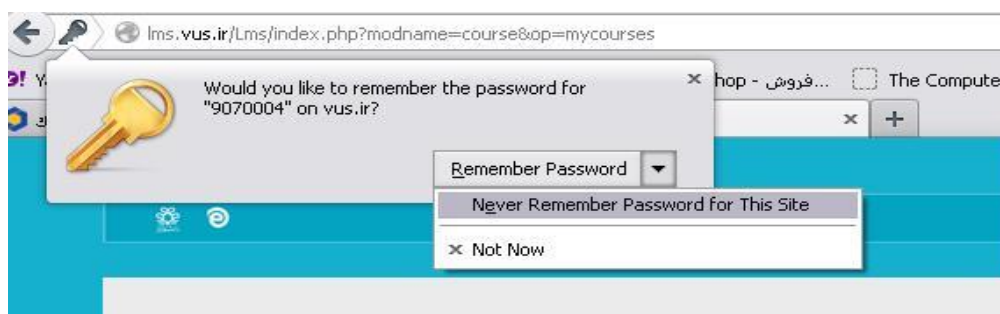
شکل ۸- پیام ها و هشدارهای امنیتی نسبت به نامعتبر بودن سایت

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



شکل ۹- 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 را وارد 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، حتماً 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، فروشگاه‌ها ملزم به

رعایت موارد ذیل می‌باشند:

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 بخش‌های مختلف (فروش، پشتیبانی، خدمات پس از فروش و ...) از طریق شماره تلفن‌های 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 می‌باشد (برند)
	۱۱	قیمت کالا یا خدمات
	۱۲	مشخصات فنی و ویژگی‌های کاربردی
مشخصات سفارشات	۱۳	اعلام میزان مالیات بر ارزش افزوده (VAT) به خریدار (در صورتیکه کالا یا خدمت مشمول مالیات نمی‌باشد 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	
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.	ویژگی های وب سایت
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 از 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

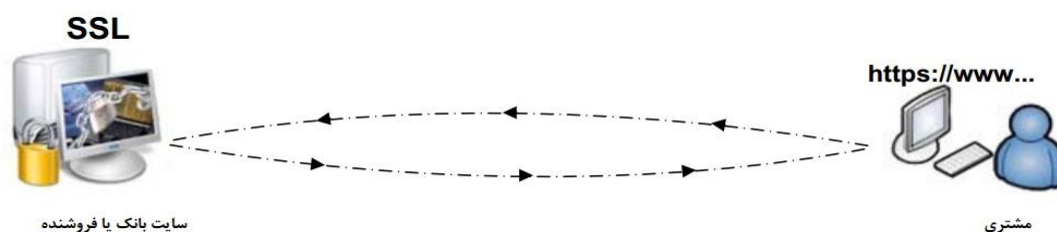
- ❖ به ایمیل‌ها و پیام‌های ناشناس و مشکوک مبنی بر ورود به حساب اینترنتی خود توجه نکنید.
- ❖ زمانی که در خرید اینترنتی برای پرداخت اقدام می‌کنید باید از سایت فروشگاه به سایت بانک منتقل شوید. اما ممکن است افراد سودجو، شما را به سایت بانک منتقل نکرده و از شما درخواست کنند که تمام اطلاعات کارت را در همان صفحه فروشگاه وارد نمایید و یا شما را به سایتی شبیه به سایت بانک منتقل کنند و با جلب اعتماد شما از طریق نشان دادن آرم بانک و شما را ترغیب به وارد نمودن اطلاعات کارت نمایند. اما به‌خاطر داشته‌باشید که آدرس صفحه پرداخت بانک با <https://> شروع می‌شود 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- نکات امنیتی در محیط اینترنت

مشتري 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 حساب، 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 بازبازی شده و تبدیل به رمز ابتدایی می‌شود. بنابراین در صورت وجود هکر در این مسیر، این اطلاعات برای او مورد استفاده نخواهد بود.



شکل ۱۱ - 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 پای باقی می‌ماند اگر فردی پس از شما از همان سیستم استفاده کند با داشتن کمی اطلاعات نرم‌افزاری، می‌تواند 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.

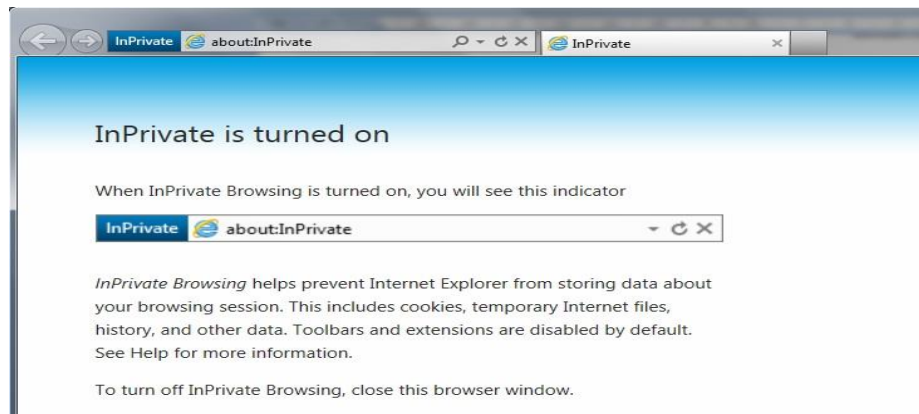
الف) محیط Internet Explorer

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 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.

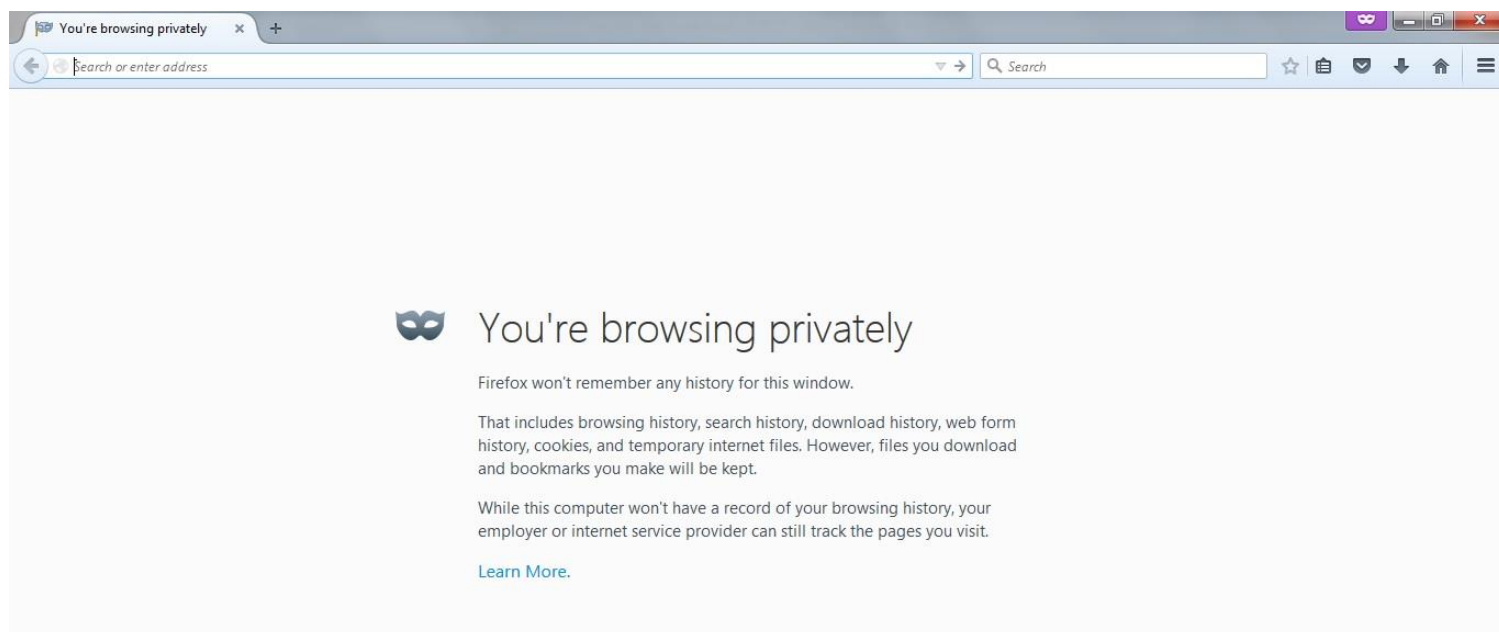
ب) محیط Firefox

۱. در محیط FireFox از منوی Tools گزینه New Private Window 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 نمی‌شود.



شکل ۱۳- استفاده از Private Browsing در محیط Firefox

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

ج) محیط Google Chrome

۱. در محیط Google Chrome با کلیک روی ابزار (در سمت راست و بالای صفحه) از منوی باز شده گزینه

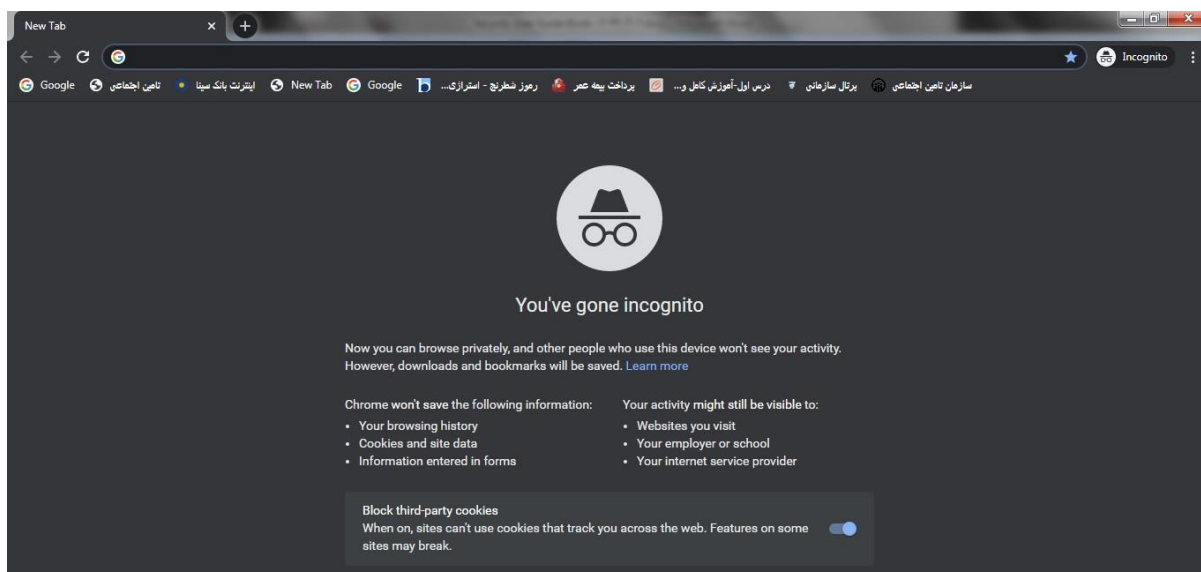
New Incognito Windows را انتخاب کنید، یا کلیدهای Ctrl+Shift+N را بزنید.

۲. وارد صفحه Private browsing می شوید.



✓ تا زمانی که در حالت Incognito Windows هستید، نماد در گوشه بالا سمت راست خواهد بود

و ورود به سایت های مختلف یا جستجوهای شما، در این حالت ثبت نمی شود.



شکل ۱۴- استفاده از New Incognito Windows در محیط Google Chrome

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

۶- نکات امنیتی موبایل بانک

۱- نرم افزار موبایل بانک سینا را فقط از طریق مراجعه مستقیم به وب سایت بانک سینا و از منابع معتبر

معرفی شده در [وب سایت بانک](#) دریافت نمایید.

۲- جهت نصب موبایل بانک هرگز از منابع غیرمعتبر مانند بلوتوث ناشناس، ایمیل، وب سایت ها و فروشگاه

های متفرقه اینترنتی و غیره استفاده ننمایید.

۳- نام کاربری و رمز ورود سامانه موبایل بانک خود را در اختیار دیگران قرار نداده و آن را در فواصل زمانی

منظم تغییر دهید.

۴- هنگام نصب همراه بانک، مجوزهای دسترسی لازم برای نصب و پیغام های خطای احتمالی را بررسی نموده

و در صورت مشاهده مورد مشکوک، آن را به مرکز تماس بانک اطلاع دهید.

۵- گوشی تلفن همراه خود را Root ننموده و از تغییرات و دستکاری هایی که سبب کاهش سطح امنیت می-

شود خودداری نمایید.

۶- از نصب و اجرای برنامه ها و فایل های متفرقه و ناشناس بر روی تلفن همراه خود تا حد امکان خودداری

نمایید.

- ۷- از باز نمودن فایل ها و لینک های ناشناخته در ایمیل های مشکوک و ورود به وب سایت های متفرقه از طریق تلفن همراه خود خودداری نمایید.
- ۸- سیستم عامل، مرورگر وب و سایر نرم افزارهای نصب شده روی تلفن همراه خود را به طور مستمر بروزرسانی نمایید.
- ۹- آنتی ویروس های بروز شده و مطمئن در تلفن همراه خود استفاده نمایید.
- ۱۰- هنگامی که به بلوتوث نیازی ندارید از خاموش بودن آن مطمئن شوید.
- ۱۱- اطلاعات بانکی خود را در تلفن همراهتان ذخیره ننمایید.
- ۱۲- در صورت سرقت یا مفقودی تلفن همراه، در اسرع وقت به یکی از شعب بانک مراجعه نمایید. در صورت عدم دسترسی به شعبه، موضوع را به مرکز تماس بانک اطلاع داده و کارت خود را غیرفعال نمایید.
- ۱۳- پیش از فروش یا واگذاری گوشی تلفن همراه خود، نرم افزار موبایل بانک را از روی آن حذف (Uninstall) نموده و کلیه اطلاعات شخصی و رمزهای حساب بانکی را پاک نمایید.
- ۱۴- تنظیم قفل شدن خودکار تلفن همراه خود را فعال نمایید و جهت ورود به گوشی خود رمز تعریف نمایید.
- ۱۵- از سیستم های عمومی اینترنت نظیر کافی شاپ ها، کافی نت ها، فروشگاه ها و غیره برای انجام عملیات بانکی استفاده نکنید.
- ۱۶- از انتخاب رمز ورود قابل حدس نظیر سال تولد، سال ازدواج، شماره شناسنامه و غیره برای ورود به سامانه همراه بانک، اجتناب کنید.
- ۱۷- در نرم افزار موبایل بانک اندرویدی، حتماً از طریق منوی تنظیمات، یک رمز عبور مناسب برای ورود به نرم افزار تعریف نمایید.