روشی هایی به منظور امنیت بیشتر در بانکداری اینترنتی

تاثیر کامپیوتر ، اینترنت و شبکه های ارتباطی بر هر جنبه از زندگی ما انسان ها امروزه به وضوح دیده میشود . هر جا که نگاه کنیم ، ردپایی از اینترنت و شبکه های ارتباطی را میبینیم . تقریبا میتوان گفت که ۹۰ درصد از چیزهای اطراف ما توسط کامپیوتر کنترل میشوند . سیستم های آب رسانی ، برق ، گاز ، تلفن . سازمان های دولتی ، خصوصی ، نظامی و بانک ها هم که جای خود دارند . در واقع با آمدن اینترنت تمامی معادلات قبلی بر هم خورد . اینترنت امکانی را برای ما فراهم میکند تا ساعت ها در صف های طولانی بانک منتظر نمانیم . دیگر مثل قبل لازم نیست برای پرداخت چند قبض درگیر ترافیک و شلوغی صف بانک شوید . کافیست در حالی که روی صندلی خود نشستید ، کار را به اینترنت و انگشتان دست خود بسپارید . تمامی قبض هایتان پرداخت میشود . میتوانید آنلاین بخرید و بفروشید . پولی از حسابی به حساب دیگری انتقال دهید .
اما در این میان که چند حلقه ارتباطی این قابلیت ها را در اختیار ما قرار میدهند ، شاید مهمترین حلقه ، حلقه ی امنیت باشد . مطمئنم که اگر به شما بگویند حتی یک درصد احتمال بروز مشکلات امنیتی در حساب های بانکی شما وجود دارد ، از انجام هرگونه عملیات بانکی به صورت آنلاین خودداری میکنید . چون هیچکس دوست ندارد پولی را که به وسیله کار و تلاش خود به دست آورده ، از دست بدهد .

اما چگونه باید تمام سعی خود را به کار بگیریم تا امنیت را در بانکداری اینترنتی به بالاترین سطح ممکن برسانیم ؟؟؟ یادتان باشد همیشه گفته ایم که " امنیت ۱۰۰٪ وجود نداشته ، ندارد و نخواهد داشت "
نکته : توجه داشته باشید که این مطلب در سطح معمول گردآوری شده است و تعدادی از راهکارهای متداول که میتوانند امنیت را در زمینه بانکداری اینترنتی افزایش دهند در این مطلب آمده است . همچنین هیچ ترتیبی در موارد گفته شده وجود ندارد .

۱- بروز رسانی مرورگر ، آنتی ویروس و سیستم عامل ، اولین قدم : یک سیستم کامپیوتری که توسط یک کاربر مورد استفاده قرار میگیرد ، میتواند از سه طریق آسیب پذیر باشد . امروزه بیشتر آلودگی ها از طریق وبسایت های اشاعه دهنده ی بدافزار ، کدهای مخرب مثل اسکریپت ها و در کل ، اینترنت بوجود می آید .
اولین برنامه ای که در یک کامپیوتر مسئول برقراری ارتباط با اینترنت میباشد ، مرورگر اینترنتی شماست . البته مرورگر شما میتوانید مثل یک پنجره باشد که در برابر خطرات ، شکنندگی زیادی دارد . برای اینکه ما بتوانیم نقص های امنیتی مرورگر خود را مرتفع کنیم ، بایستی آن را بروز نگه داریم . اگر شما مرورگر خود را بروز کنید (و البته این کار را در فواصل زمانی کوتاهی انجام دهید) میتوانید مطمئن باشید که گام بزرگی را در ارتقای امنیت خود برداشته اید .
پس از مرورگر نوبت به آنتی ویروس میرسد . به نظر شما در هر دقیقه چند ویروس ، کرم ، تروجان و انواع دیگر بدافزارها تولید شده و وارد فضای اینترنت میشوند ؟؟؟ به صورت دقیق نمیتوان به تعداد آنها پی برد ، اما باید گفت که تعداد آن ها هزاران عدد است و هر کدام هم با روش جدید اقدام به نفوذ و آلوده سازی سیستم شما میکنند . شرکت های امنیتی نیز به صورت مستمر و بی وقفه این تغییرات را بررسی کرده و روش های جدید

برای مقابله با آنها خلق میکنند . شما باید آنتی ویروس خود را همیشه در وضعیت آپدیت اتوماتیک قرار دهید . زیرا ممکن است در طی یک روز ، چند آپدیت منتشر شود و شما نیز باید بلافاصله این آپدیت ها را دریافت کنید . این آپدیت ها باعث شناسایی بدافزارهای جدید شده و امنیت شما را تا حد زیادی بالا میبرند .
اما آخرین مورد سیستم عامل است . فرقی نمیکند که از چه سیستم عاملی استفاده میکنید . لینوکس ، مک و ویندوز هیچ تفاوتی در این مورد ندارند . شما باید از هر کدام که استفاده میکنید ، بروز رسانی هایی را که توسط شرکت های سازنده آماده میشوند را در اسرع وقت دریافت کرده و نصب کنید . سیستم عامل ها هم یک برنامه کامپیوتری هستند . البته از دسته برنامه های سیستمی . پس ممکن است که آسیب پذیری هایی داشته باشند و این بروز رسانی ها باعث رفع این سری از مشکلات میشوند .
پس با بروز رسانی این سه مورد و موارد دیگری که امکان بروز کردن شان را دارید ، در حفظ امنیت خود و جلوگیری از ورود بدافزارها ، گام بزرگی را برداشته اید .

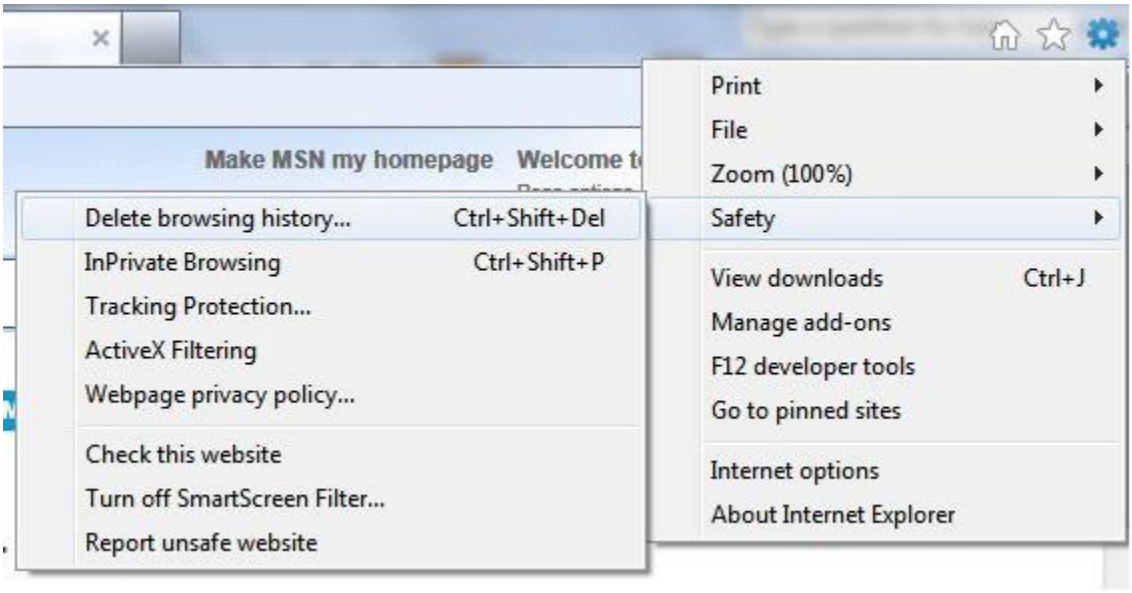
۲- استفاده از مرورگرهای منسوخ شده را کنار بگذارید : در واقع یکی از مشکلاتی که در کشور ما وجود دارد ، استفاده از مرورگر پیشفرض ویندوز است . پرطرفدارترین عضو خانواده ویندوز در کشور ما نیز متاسفانه ویندوز XP میباشد که مرورگر کاملا ناامن اینترنت اکسپلورر ۶ را به همراه دارد . اگر به فکر تامین امنیت خود هستید ، حداقل از نسخه های بالاتر این مرورگر و یا حتی مرورگرهای مدرن و با امنیت بالاتری همچون کروم ، فایرفاکس و اپرا استفاده کنید . البته لازم به ذکر است که استفاده از ویندوزهای جدیدتر مثل ویندوز ۷ نیز کمک شایانی به ارتقای سطح امنیت شما خواهد کرد .

۳- ذخیره کلمه عبور در مرورگر ، یک اشتباه فاجعه آمیز و مرگبار : اگر دوست دارید هر کسی که پشت سیستم شما مینشیند با خیال راحت پول را از حسابتان به حساب خود منتقل کند و یا خریدهایش را انجام بدهد ، لطفا کلمه عبور حساب بانکی خود را در مرورگرتان ذخیره کنید . واقعا نمیتوان پی برد که چرا برخی از افراد با دیدن هر پیغامی در مرورگرشان ، سریعا با آن موافقت میکنند . مرورگر از شما میپرسد که میخواهید کلمه عبور خود را ذخیره کنید و کاربر هم در کمال بی احتیاطی کلمه عبور را ذخیره میکند . اگر شما هم قبلا مرتکب چنین اشتباهی شده اید ، اکنون به شما خواهیم گفت که چگونه این اشتباه خود را جبران کنید .

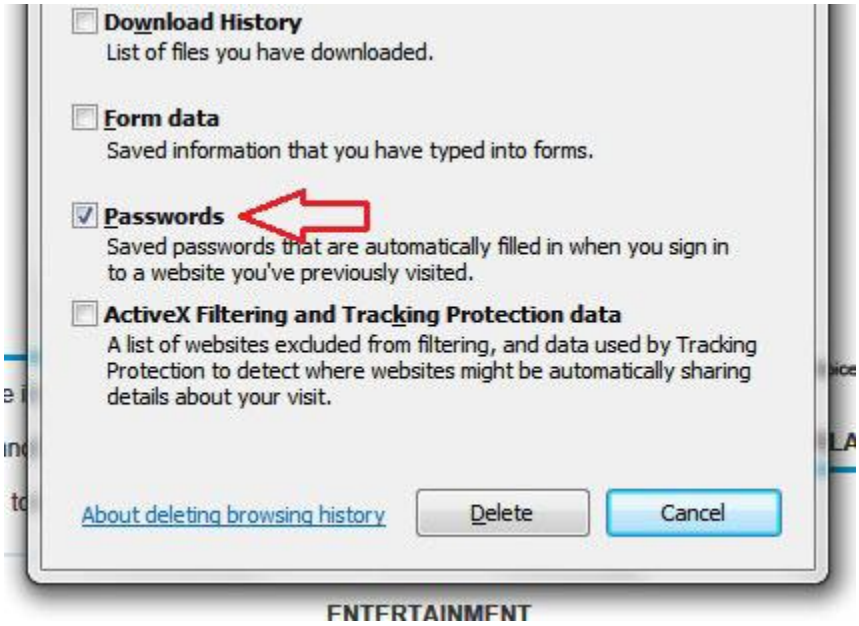
در اینجا ما روش پاکسازی کلمات عبور در ۳ مرورگر اینترنت اکسپلورر ، کروم و فایرفاکس را به شما نشان خواهیم داد .

*** اینترنت اکسپلورر ۹ :**

روی علامت چرخ دنده در قسمت بالا و سمت راست پنجره مرورگر کلیک کرده و منوی Safety را انتخاب کنید . اکنون از بین زیر منوها ، منوی Delete Browsing history را کلیک کنید . میتوانید به صورت ساده کلیدهای Ctrl+Shift+Del را نیز بفشارید .

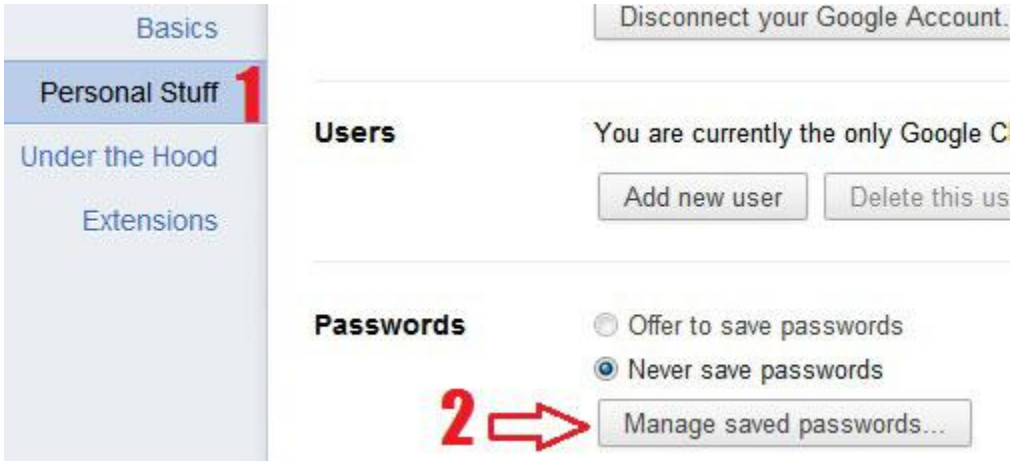


در پنجره باز شده ، گزینه Passwords را فعال کنید . اکنون دکمه Delete را بزنید .



*** کروم :**

از منوی آچار روی گزینه Options کلیک کنید . در صفحه تنظیمات از قسمت سمت چپ ، گزینه Personal Stuff را انتخاب کرده و از سمت راست روی دکمه Managed saved passwords کلیک کنید .



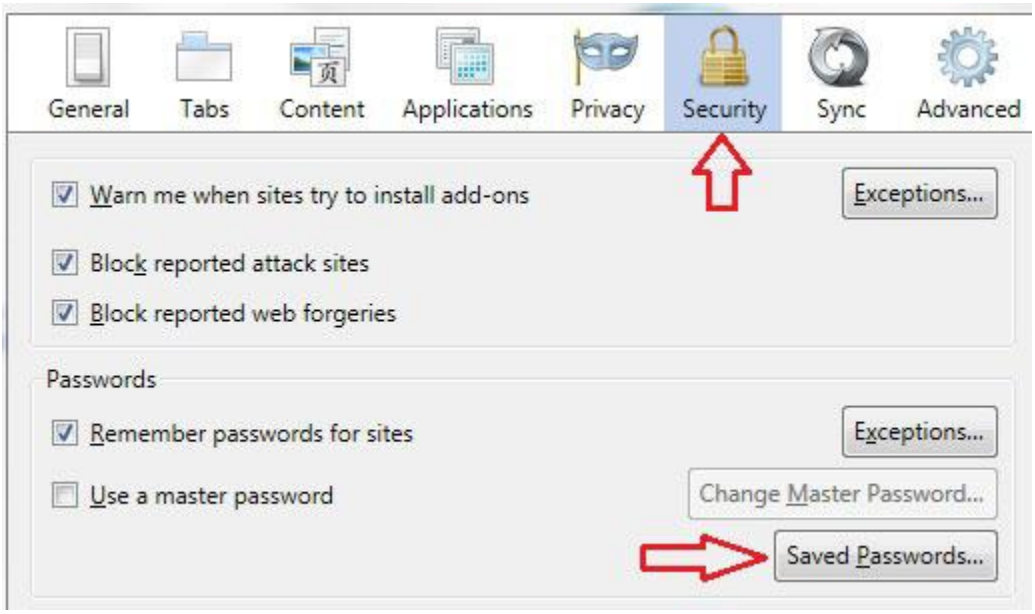
تهران،
خیابان کریم خان، خیابان ایران شهر، خیابان بهشهر، پلاک ۷، واحد ۶
کد پستی: ۱۵۸۳۷۶۷۱۱۱
تلفن گویا: +۹۸ ۲۱ ۸۸۴۹۱۶۱۲
نمابر: +۹۸ ۲۱ ۸۸۴۹۱۶۱۳
سامانه پیام کوتاه: ۱۰۰۰-۲۱-۸۸۴۹۱۶۱۲
وب سایت: www.pardakht.ir
ایمیل: Info@pardakht.ir

اصفهان،
خیابان امام خمینی، ضلع شمالی مخابرات امام خمینی، کوچه جهان فولاد، ساختمان ایران گیت
کد پستی: ۸۱۸۹۸۹۷۸۹۳
صندوق پستی: ۹۴۴ - ۸۱۴۶۵
تلفن گویا: +۹۸ ۳۱۱ ۳۳۲۷۷۷۰
نمابر: +۹۸ ۳۱۱ ۳۳۲۱۲۴۱
وب سایت: www.pardakht.ir
ایمیل: Info@pardakht.ir

اکنون لیستی از سایت هایی که پسوردهای خود را درون آنها ذخیره کرده اید ، باز خواهد شد . در لیست جستجو کرده و نام سایت بانک مورد نظر را پیدا کنید . اگر موس را روی همین آیتم ببرید ، یک علامت ضربدر کوچک در سمت راست آن ظاهر خواهد شد که با کلیک بروی آن ، میتوانید کلمه عبور ذخیره شده را پاک کنید .

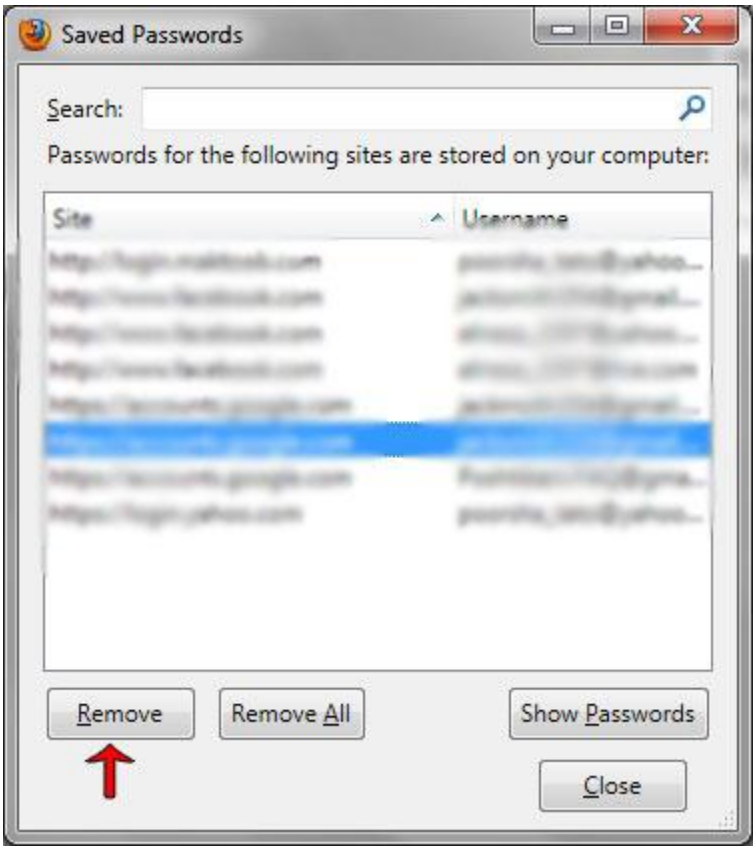
*** فایرفاکس :**

از منوی Tools گزینه Options را انتخاب کنید . البته اگر از ظاهر جدید فایرفاکس (که از نسخه ۴ به بعد استفاده میشود) استفاده میکنید ، نوار منوها را مشاهده نخواهید کرد . میتوانید روی دکمه نارنجی رنگ Firefox کلیک کرده و منوی Options را انتخاب کنید .



در پنجره Options به قسمت Security بروید و در بخش Passwords روی دکمه Saved passwords کلیک کنید .

پنجره جدیدی باز خواهد شد . مانند مرورگر کروم در اینجا نیز باید آدرس سایت بانک مورد نظر خود را پیدا کرده و آن را انتخاب کنید . سپس روی دکمه Remove کلیک کنید .



۴- کلمه عبور خود را دم دست نگذارید : واقعا جای تاسف دارد که برخی از کاربران اینقدر بی خیال هستند . برخی از آنها کلمه عبور خود را روی کاغذ نوشته در کیف ، روی میز و یا هر جای دیگر که دسترسی به آن بسیار راحت است میگذارند . بعضی از آنها خیلی راحت کلمه عبور را در یک فایل تکست نوشته و در دسکتاپ ذخیره میکنند . این افراد واقعا به امنیت مالی خود اهمیتی نمیدهند ؟؟؟

حالا فرض را بر این میگیریم که فرد بسیار حواس پرتی هستید و نمیتوانید کلمه عبور خود را به خاطر بسپارید . حداقل از دو روش بالا برای در اختیار داشتن کلمه عبور خود استفاده نکنید . برنامه های رایگان و قدرتمند و البته معتبر زیادی مثل Keepass هستند که میتوانید کلمات عبور شما را در یک بانک اطلاعاتی قدرتمند و امن ذخیره کنند . نه تنها کلمه عبور حساب بانکی شما ، بلکه هر کلمه عبور دیگری . تنها کافیست یک کلمه عبور را برای

همیشه به خاطر بسپارید . سپس میتوانید با استفاده از آن کلمه عبور که Master Password نام دارد ، به تمام کلمات عبور خود دسترسی پیدا کنید.

۵- کلمات عبور پیچیده و طولانی تر مساویست با امنیت بیشتر : شاید این مورد هزاران بار خوانده باشید . اما باز هم بعضی از کاربران آن را رعایت نمیکنند . افرادی دیده شده اند که کلمات عبور را سال تولد خودشان ، همسر ، فرزند ، شماره تلفن همراه ، اعداد بسیار ساده و قابل حدس مثل ۱۲۳۴۵۶ و مواردی از این دست انتخاب میکنند . خیلی ساده است ، هیچ امنیتی وجود ندارد . با این شاهکارها در انتخاب کلمه عبور باید منتظر بود تا دیر یا زود یک نفر حسابمان را خالی کند . اما برای امنیت بیشتر هم میتوان کارهایی را انجام داد . مثلا کلمات عبور طولانی انتخاب کنید . کلمات عبور طولانی قابلیت حدس زدن را به کمترین حد ممکن کاهش میدهند . بیشتر بانک ها به شما اجازه میدهند تا ۱۵ کراکتر کلمه عبور انتخاب کنید . این کراکترها میتوانند شامل حروف و اعداد باشند . اگر از یک ترکیب عددی و حروفی استفاده کنید خیلی خوب است . در هر قسمت نیز باید دقت کافی را به خرج داد . به عنوان مثال وقتی میخواهید یک کلمه عبور حروفی انتخاب کنید ، سعی کنید که حروف در سطح کیبرد فاصله زیادی با هم داشته باشند و یا در اصطلاح پخش باشند . به عنوان مثال میتوان به اسم Jamshid اشاره کرد . میبینید که حروف اسم Jamshid در سطح کیبرد پخش شده هستند و فاصله زیادی دارند . اما اگر شما کلمه یا اسمی را انتخاب کنید که در حروفش در یک قسمت از کیبرد باشند ، امکان حدس زدن آن بالاتر میرود . مثلا به اسم ASAD توجه کنید . سه کلید A، S و D میتوانند این کلمه را تشکیل دهند و هر سه نیز در کنار هم قرار دارند . حال اگر فردی پشت سر شما باشید و حتی انگشتان شما را نبیند و تنها متوجه شود که دست شما در آن محدوده در حال تایپ کردن است ، ممکن است بتواند حدس های موفقیت آمیزی بزند .
در مورد کلمات عبور عددی نیز همین مسئله صدق میکند . البته در مورد اعداد انعطاف پذیری کمی وجود دارد . چون چند کلیک کنار هم هستند اما باز هم میتوان اعدادی را انتخاب کرد که الگوهای خاصی نداشته باشند . به عنوان مثال بعضی از افراد کلمه عبور عددی با الگوی ضربدری انتخاب میکنند . به عنوان مثال ۱۵۹۷۵۳ . در این وضعیت نیز فرد میتواند بر اساس حرکات دست شما ، یک سری حدس ها بزند و در مواقعی به موفقیت برسد . کلمه عبور عددی ۱۹۴۳۸۲۶۸۲۱ بهتر است و الگوی خاصی ندارد .

۵- تعویض کلمات عبور : تعویض کلمات عبور در فواصل زمانی مختلف هم میتواند راهکار خوبی در جهت حفظ امنیت شما باشد . به عنوان مثال شما میتوانید هر سه ماه یک بار کلمه عبور فعلی خود را عوض کنید . در صورتی که کلمه عبور شما توسط بدافزارها به سرقت رفته باشد ، اما هکر سازنده آن بدافزار هنوز فرصت نکرده باشد که حساب را بررسی کند ، میتوانید شانس خود را برای از بین بردن خطرات احتمالی افزایش دهید .

۶- کانال های ارتباطی امن ، امنیت در دل ناامنی : اگر چند قطعه الماس در اختیار داشته باشید و بخواهید از میان عده ای دزد و خلافکار عبور کنید ، ترجیح میدهید چندین بادی گارد با اسلحه شما را محافظت کنند تا بتوانید با آن الماس ها از بین افراد شرور عبور کنید . در اینجا اطلاعات بانکی شما مثل الماس ، هکرها و

خلافکاران سایبری مانند همان دزدها و کانال های امن ارتباطی هم مثل بادی گاردهای سلاح به دست هستند . اگر شما بخواهید اطلاعاتی به مهمی اطلاعات حساب بانکی خود را در فضای ناامنی مثل اینترنت انتقال دهید ، حتما باید یک محافظت عالی از شما به عمل بیاید . اگر بین کامپیوتر شما و سرور بانک مورد نظر ارتباط امنی برقرار نشود ، هیچ تضمینی وجود نخواهد داشت که اطلاعات به دست هکرها و خرابکاران نیفتد . در اینجاست که کانال های ارتباطی امن به میان می آیند . پروتکل HTTPS که ترکیبی از SSL و HTTP میباشد ، در دل فضای ناامن اینترنت با استفاده از الگوریتم های رمزنگاری بسیار کارآمد ، کانالی امن را بین کامپیوتر شما و سرور مورد نظر (در اینجا منظور سرور بانک است) ایجاد میکنند تا اطلاعات شما بدون کوچیکترین دخالتی توسط هکرها به مقصد خود برسد .

در اینجا ذکر چند نکته در این مورد لازم به نظر میرسد :
* قبل از ورود هرگونه اطلاعات حساب بانکی خود ، به نوار آدرس مرورگر نگاهی بیندازید . مطمئن شوید که از پروتکل HTTPS استفاده میشود . وجود علامت یک قفل در کنار نوار آدرس میتوانید خیال شما را راحت کند . به عنوان مثال تصویر زیر مربوط به سیستم بانکداری اینترنتی بانک تجارت در مرورگر کروم میباشد .

* در صورتی که HTTPS را مشاهده نکردید و یا با حالت همیشگی متفاوت بود و به نظر مشکل دار می آمد ، به هیچ وجه اطلاعات خود را وارد نکرده و با پشتیبانی بانک تماس بگیرید و درخواست راهنمایی کنید .

۷- کافی نت ها ، خطر در کمین شماست : مراکز عمومی اتصال به اینترنت مثل کافی نت ها همیشه یکی از خطرناک ترین مکان ها برای دسترسی به اطلاعات حساس است . مخصوصا اگر آن اطلاعات به مهمی اطلاعات مالی باشند . باید هر لحظه این امکان را بدهید که کلمه عبور حسابتان به سرقت رفته است . تا جایی که امکان دارد ، از این مکان ها برای دسترسی به حساب بانکی خود استفاده نکنید . اما اگر مجبور به استفاده از حساب خود در کافی نت ها شدید ، موارد زیر را رعایت کنید :

* از یک مرورگر مدرن و جدید استفاده کنید . اینترنت اکسپلورر نسخه ۹ ، کروم ، فایرفاکس و اپرا هم نسخه های جدیدشان امنیت خوبی دارند . هر کدام از این چهار مرورگر حالتی دارند که مانع از ذخیره هرگونه اطلاعاتی از مرورهای شما میشود . به عنوان مثال تاریخچه مرورهای شما ، کوکی ها ، کلمات عبور و در واقع هیچ چیز ذخیره نخواهد شد . این حالت در مرورگرهای مختلف با نام های متفاوتی شناخته میشود . روش استفاده از هر کدام نیز ساده است .

این قابلیت در کروم با نام Incognito شناخته میشود . کافیست از منوی آچار گزینه New Incognito Window را کلیک کنید تا پنجره ی جدید با استفاده از این قابلیت برای شما باز شود .

این قابلیت در فایرفاکس با نام Private Browsing شناخته میشود . کافیست از منوی Firefox روی گزینه Start Private Browsing کلیک کنید . در صورتی که از نوار منوی فایرفاکس استفاده میکند ، از منوی Tools زیر منوی Start Private Browsing را انتخاب کنید .

در مرورگر اپرا این قابلیت را میتوانید با عنوان Private Tab پیدا کنید . کافیست روی نوار منوها راست کلیک کرده و گزینه New Private Tab را انتخاب کنید . یک تب جدید با استفاده از این قابلیت برای شما باز خواهد شد .

در مرورگر اینترنت اکسپلورر ۹ این قابلیت با نام InPrivate Browsing شناخته میشود . کافیست از منوی چرخ دنده روی منوی Safety کلیک کرده و زیر منوی InPrivate Browsing را انتخاب کنید .

* از صفحه کلید مجازی استفاده کنید . امروزه در قسمت وارد کردن اطلاعات کاربری بیشتر سایت های بانکی و سایت های فروشگاهی میتوان اینگونه صفحه کلیدها را مشاهده کرد . اگر کمی در زمینه امنیت مطالعه داشته باشید ، تا به حال نام Keylogger را شنیده اید . کار این بدافزارها اینست که کلیدهای فشرده شده کیبرد توسط کاربر را برای سازنده خود ارسال میکنند . بنابراین اگر یک کیلاگر در سیستم شما فعال باشد ، میتوان کلیدهایی را که میفشارید ثبت کرده و برای سازنده خود ارسال کند . اما اگر از یک صفحه کلید مجازی استفاده کنید ، دیگر همه اعداد و حروف ها را میتوانید از طریق محیط مجازی و با موس خود انتخاب کنید . در این صورت هیچ کلیدی فشرده نمیشود و کیلاگر چیزی را ثبت نمیکند . در تصویر زیر دو نوع از صفحه کلید های مجازی را مشاهده میکنید .

تهران،
خیابان کریم خان، خیابان ایران شهر، خیابان بهشهر، پلاک ۷، واحد ۶
کد پستی: ۱۵۸۳۷۶۷۱۱۱
تلفن گویا: +۹۸ ۲۱ ۸۸۴۹۱۶۱۲
نمابر: +۹۸ ۲۱ ۸۸۴۹۱۶۱۳
سامانه پیام کوتاه: ۱۰۰۰-۲۱-۸۸۴۹۱۶۱۲
وب سایت: www.pardakht.ir
ایمیل: Info@pardakht.ir

اصفهان،
خیابان امام خمینی، ضلع شمالی مخابرات امام خمینی، کوچه جهان فولاد، ساختمان ایران گیت
کد پستی: ۸۱۸۹۸۹۷۸۹۳
صندوق پستی: ۹۴۴ - ۸۱۴۶۵
تلفن گویا: +۹۸ ۳۱۱ ۳۳۲۷۷۷۰
نمابر: +۹۸ ۳۱۱ ۳۳۲۱۲۴۱
وب سایت: www.pardakht.ir
ایمیل: Info@pardakht.ir

* مورد شماره ۵ را در سریع ترین زمان ممکن انجام دهید .

۸- فیشینگ ، لطفا کلمه عبور خود را به ما بدهید : سناریوی حملات فیشینگ واقعا دردناک است . مانند این است که یک نفر به شما بگوید لطفا کلمه عبور حساب خود را به من بدهید و شما هم خیلی راحت این کار را انجام دهید . یک طراحی دقیق از سایت بانک مقصد انجام میشود و شما را ترقیب میکند که اطلاعات حساب خود را وارد کنید . به عنوان مثال سناریوی یک خرید اینترنتی کارت شارژ را بررسی میکنیم .

ابتدا به یکی از سایت های خرید کارت شارژ میرویم . سپس کارت شارژ مربوط به اپراتور مورد نظر و همچنین میزان اعتبار آن را مشخص میکنیم . در مرحله آخر از شما پرسیده میشود که کدام بانک را به منظور پرداخت هزینه خرید خود انتحاب میکنید . به عنوان مثال بانک ملت را انتخاب میکنیم . پیغامی ظاهر میشود که شما در حال اتصال به سرور پرداخت بانک ملت هستید . پس از چند لحظه صفحه ای پیش روی شما قرار میگیرد و از شما درخواست میکند که اطلاعات حساب خود مانند شماره حساب ، رمز دوم و کد CVV2 را وارد کنید .

قبل از انجام هر کاری باید چند چیز را بررسی کنید :

* ابتدا مطمئن شوید که فروشگاهی که قصد خرید از آن را دارید ، معتبر بوده و به اندازه کافی شناخته شده باشد .

* هنگامی با صفحه وارد کردن اطلاعات مواجه شدید ، به نوار آدرس نگاه کنید و مطمئن شوید که آدرس سایت بانک درست باشد . البته بعضی از سایت های خرید ، شما را به وبسایت یک بانک دیگر متصل میکنند (مثلا بانک پارسیان) و از شما میخواهند که از طریق این بانک پرداخت خود را انجام دهید . این حالت مشکلی ندارد و شما میتوانید اطلاعات خود را وارد کنید . البته باز هم از درستی آدرس اینترنتی بانک اطمینان حاصل کنید .

سامانه تجارت الکترونیک پرداخت