بانک پاسارگاد

راهنمای امنیتی استفاده از خدمات بانکداری الکترونیک

www.bpi.ir
تهران، خیابان میرداماد، شماره ۴۳۰
مرکز اطلاع رسانی ۸۲۸۹۰

آنچه توانستیم لطف خدا بوده است

بانک پاسارگاد
بانک سرآمدان

مشتری ذات بانک است

فهرست مطالب

راهنمای امنیتی جهت افزایش امنیت در استفاده از خدمات بانکداری الکترونیک

با توجه به رشد روز افزون استفاده از خدمات بانکداری الکترونیکی در کشور و همچنین اهمیت رعایت مسائل امنیتی در استفاده از این خدمات بر آن شدیم تا با مرور نکاتی ساده، شاهد تخلفات کمتری در این زمینه باشیم:

۱ استفاده از دستگاه‌های شخصی به منظور انجام عملیات بانکداری الکترونیکی

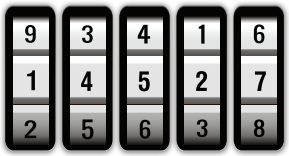
با توجه به اهمیت حساب‌های بانکی و با توجه به وجود خطرات مختلف از جمله وجود برنامه‌های ثبت کننده فعالیت‌های کیبورد و ماوس در حافظه دستگاه (کی لاگر) و استفاده از آن توسط شخص مجرم در مواقع موردنیاز، پیشنهاد می‌گردد به هیچ وجه از دستگاه‌های رایانه، تلفن‌های همراه و سایر دستگاه‌های الکترونیکی دیگران به منظور دسترسی به حساب خود از طریق درگاه‌های الکترونیکی استفاده نکنید.

۲ استفاده از ضد بدافزارهای معتبر و به روز رسانی آنها

با توجه به وجود ویروس‌ها، تروجان‌ها، بدافزارها و... که با هدف سرقت اطلاعات کاربران تهیه و منتشر می‌گردند، اهمیت نصب و به‌روز رسانی ضد بدافزارهای معتبر برروی دستگاه‌های مختلف الکترونیکی هر روز بیشتر از قبل احساس می‌گردد. لذا به کاربران استفاده کننده از درگاه‌های الکترونیکی بانک‌ها پیشنهاد می‌گردد از نصب و به روز بودن نسخه ضد بدافزار بر روی سیستم خود اطمینان حاصل نمایند.

۳ اهمیت رمزها در عملیات بانکداری الکترونیک

- توصیه می گردد در هنگام استفاده از درگاه بانکداری مجازی، حتی المقدور از رمز دو عاملی استفاده نمایید.
- از کلمه‌های عبور ترکیبی برای افزایش امنیت استفاده کنید و کلمه عبور خود را به هیچ وجه به نمایش نگذارید.



- به هیچ وجه از شماره‌های کد ملی، شناسنامه، تاریخ تولد، تلفن ثابت، تلفن همراه و یا هرگونه مشخصات که حدس زدن رمز توسط شخص مجرم را آسان‌تر می‌نماید استفاده نکنید.
- اطلاعات کارت‌های بانکی و اعتباری خود را در مرورگر وب ذخیره نکنید! درست است که پر کردن اطلاعات کارت‌های اعتباری وقت گیر است، اما مطمئن باشید پیگیری‌های مربوط به سوءاستفاده از حساب بانکی شما بیشتر وقت و انرژی شما را می‌گیرد. به ویژه از ذخیره‌سازی اطلاعات خود در وب سایت‌های بانکداری و وب سایت‌های خرید آنلاین بپرهیزید.

۴ دقت درنام وب‌سایت باز شده

استفاده از تکنولوژی SSL به منظور بالا بردن ضریب امنیت در ارتباط بانک و مشتری یکی از راه‌کارهای افزایش امنیت در بستر بانکداری الکترونیکی می‌باشد، در این زمینه استفاده‌کنندگان درگاه‌های الکترونیکی بانک‌ها می‌بایست به نام وب‌سایت باز شده به عنوان درگاه بانک مورد نظر و همچنین به عبارت https:// در ابتدای نام سایت دقت کافی مبذول نمایند، زیرا بسیار مشاهده شده است که متخلفین با ایجاد وب‌سایتی مشابه با نام و محتوای وب‌سایت اصلی بانک، نسبت به کلاهبرداری از مشتریان اقدام نموده اند.(فیشینگ)

آدرس های صحیح اینترنت بانک پاسارگاد عبارتند از:

https://ib.bpi.ir

https://iben.bpi.ir

۵ مسائل امنیتی در استفاده از درگاه‌های بانکداری الکترونیکی

متاسفانه همه روزه شاهد سوء استفاده افراد سودجو از بعضی مشتریان و کلاهبرداری از حساب آنها به خاطر عدم توجه به مسائل ساده امنیتی در این زمینه می‌باشیم که با کمی دقت، امکان کلاهبرداری در این زمینه را به حداقل میزان ممکن می‌توان کاهش داد، تعدادی از این نکات امنیتی به شرح ذیل می‌باشند:

- هرگز از سیستم‌های موجود در مکان‌های عمومی همچون کافی نت‌ها به‌منظور انجام تراکنش‌های مالی استفاده نکنید.
- به هیچ وجه در زمان انجام تراکنش‌های مالی از VPN ها استفاده نکنید.
- به منظور بالا بردن سطح امنیتی سیستم خود از بازدید سایت‌های غیر معتبر و مشکوک و همچنین باز نمودن ایمیل‌های ناشناس خودداری نمایید.
- از تایپ نمودن و نگهداری رمزهای خود بر روی هر وسیله‌ای اجتناب کنید.
- در صورت استفاده از موبایل بانک جهت انجام عملیات بانکداری الکترونیکی تنها از نرم افزار ارائه شده بر روی وب سایت بانک استفاده نموده و به هیچ عنوان نرم‌افزار مربوطه را از شخص و یا مکان دیگری دریافت نکنید.
- در صورتی که تصمیم دارید رایانه شخصی خود را امانت دهید، قبل از امانت دادن حتماً تمامی اطلاعات ذخیره شده بر روی مرورگرهای اینترنتی سیستم را پاک نموده و هرگونه متنی مبنی بر اطلاعات حساب را حذف نمایید.
- در صورتی که رایانه شخصی خود را امانت داده‌اید، بعد از دریافت سیستم حتماً از عدم نصب نرم‌افزارهای مشکوک از جمله ثبت کنندگان

فعالیت‌هـای کیبـورد و مـاوس بـر روی سیسـتم (Keylogger) اطمینـان حاصـل نماییـد.

- در صورتی کـه قصـد فـروش رایانـه شـخصی و یـا تلفـن همـراه خـود را داریـد، حتمـاً سیسـتم‌ها را بـه صـورت کامـل پاک‌سـازی نماییـد. (تـا جایـی کـه ممکـن اسـت هـارد سیسـتم‌تان را نفروشـید)
- از ذخیـره اطلاعـات حسـاب‌های بانکـی بـه هـر نوعـی، در رایانـه شـخصی و یـا تلفن‌هـای همـراه جـداً خـودداری نماییـد.
- بـه منظـور افزایـش سـطح امنیـت در عملیـات بانکـداری الکترونیکـی از مرورگرهـای اینترنتـی بـه‌روز شـده اسـتفاده نماییـد.
- اگـر در هنـگام بازدیـد از یک وب سـایت، از شـما خواسـته شـد چیـزی را نصب کنیـد، از انجـام ایـن کار بپرهیزید.

۶ موارد امنیتی در انجام یک خرید امن آنلاین

همـه مـا گاهـی بـرای خریدهـای شـخصی از خریـد اینترنتـی یـا خریـد آنلایـن اسـتفاده می‌کنیـم و حیـن خریـد بـا صفحاتـی تحـت عنـوان ارزانتریـن، قیمت‌هـای اسـتثنایی، تخفیـف باورنکردنـی، نصـف قیمـت و... مواجـه می‌شـویم بـرای خریـد مطمئـن از ایـن وب‌سـایت‌ها، بایـد مـوارد زیـر را رعایـت کنیـم:

- فروشـگاه‌های معتبـر مشـخصات واقعـی را بـه طور دقیق در وب سـایت خـود درج می‌کنند.
- از سایت‌هایی خرید نمایید که حتماً نماد اعتماد الکترونیکی را داشـته باشـند. ایـن نمـاد توسـط مرکـز توسـعه تجـارت الکترونیکـی صـادر می‌شـود، در حـال حاضـر سـایت‌های دارای نماد را می‌توان از طریق سـایت Enamad.ir جسـتجو کـرد. اغلـب سـایت‌های کلاهبـرداری با عناوینـی نظیر خرید شـارژهای ارزان قیمت ، خرید انواع تلفن همـراه، خرید لوازم بهداشـتی و... در فعالیت هسـتند، پس با کلیک بر روی نماد اعتمـاد از اعتبـار آن ها مطمئن شـوید.

www.eNAMAD.ir

- فروشـگاه‌های معتبـر معمـولا نحـوه دریافـت و پرداخـت وجـه مختلفی دارنـد مانند پرداخت آنلاین، از طریق پسـت و ...کـه خریـد از آن‌هـا بایـد به شـکل مطمئن انجام شـود.
- در پرداخت‌هـای آنلایـن از طریـق درگاه‌هـای بانکـی بایـد بـه دسـتورالعمل‌های امنیتـی آن توجـه شـود.
- یکی از موارد موجود در این گونه سایت‌ها وجود صفحات جعلی فیشینگ می‌باشد، پس مراقب این سایت‌های جعلی باشید و به آدرس سایت در هنگام خریدهای اینترنتی دقت کنید.

نکات ضروری در زمان انجام تراکنش بر روی پایانه های فروشگاهی و درگاه‌های اینترنتی

- دارنده کارت بایستی خود نسبت به کشیدن کارت برروی پایانه فروشگاهی در زمان استفاده اقدام نماید و کارت خود را در اختیار فروشنده قرار ندهد.
- دارنده کارت باید قبل از انجام تراکنش برروی پایانه فروشگاهی اطمینان حاصل نماید که دستگاه دیگری برروی پایانه فروشگاهی نصب نشده باشد. (منظور، دستگاه‌های کپی کننده کارت است که به قسمت شیار کارتخوان POS متصل می شوند.)
- دارنده کارت باید شخصا نسبت به وارد نمودن رمز خود برروی پایانه فروشگاهی اقدام نماید و از ارائه رمز خود به فروشنده و یا افشای آن خودداری نماید.
- دارنده کارت نباید رمزهای قابل حدس مانند اعداد متوالی یکسان و اعداد معنی دار مانند تاریخ تولد را

به عنوان رمزهای اول و دوم کارت خود استفاده نماید.

- دارنده کارت نباید کارت و رمز خود را در کنار هم نگهداری نماید و یا رمز خود را برروی کارت درج نماید.
- توصیه می شود دارندگان کارت حتی المقدور نسبت به قراردادن سقف مبلغی روزانه تراکنش برروی کارت خود اقدام نمایند تا در صورت سواستفاده احتمالی از کارت، کل موجودی سپرده به خطر نیافتد.
- دارنده کارت در صورت استفاده از کارت برروی پایانه‌های مشکوک و یا درگاه‌های اینترنتی مشکوک، باید فورا نسبت به تغییر رمزهای کارت خود از طریق درگاه‌های بانک اقدام نماید.

نکات ضروری در زمان انجام تراکنش برروی دستگاه های خودپرداز

- رمز ورودی کارت می بایست به نحوی وارد شود که به مشتریان در صف نمایش داده نشود.
- در زمان انتقال وجه ترجیحا از منوی انگلیسی استفاده نشود.
- فاصله بین استفاده کننده از خودپرداز و سایرین در صف حفظ گردد.
- مشتریان محترم در هنگام عملیات بانکی نظیر برداشت وجه باید تا انتهای عملیات بانکی و مشاهده آلارم‌های خودپرداز منتظر بمانند.
- تغییرات غیرمعمول بدنه و کارتخوان دستگاه را حتما به بانک گزارش فرمایند.

شناسایی صفحات فیشینگ

- به آدرس سایت موردنظر (درگاه پرداخت)جهت انجام تراکنش های مالی آنلاین توجه کنید.

نمونه ای از آدرس‌های جعلی:

www.bannk.com

www.banck.com

آدرس اصلی سایت باید از پروتکل‌های امنیتی استفاده نماید. مانند:

https://www.bank.com

- به تغییرات نامحسوس در صفحاتی که مراجعه می کنید دقت کنید یعنی شخص فیشر ممکن است سایتی شبیه به سایت اصلی را طراحی کند و دراختیار کاربر قرار دهد.
- این سایت‌های فیشینگ ممکن است با عناوین شارژ ارزان قیمت، تخفیف‌های باورنکردنی و... در دسترس عموم قرار گیرند.

باید به نکات زیر توجه کنیم:

- دقت به آدرس صفحه پرداخت و وارد کردن سایت مورد نظر به‌صورت دستی.

توجه کنید آدرس درگاه مورد نظر باید حاوی پروتکل HTTPS باشد و در صورتی که تنها از HTTP استفاده می نمود به آن مشکوک شوید.

- از کیبورد مجازی خود سایت یا رایانه برای درج اعداد شامل(شماره کارت، رمز اینترنتی، CVV2، تاریخ انقضاء) استفاده نمایید.

- دقت کنید کد امنیتی (Captcha) که قرار است وارد کنید عکس نباشد که برای درک این موضوع کلید Refresh را یک مرتبه فشار دهید تا تغییرات حروف برای شما مشهود گردد. در صورتی که تغییر نکرد سایت مورد نظر جعلی است.
- از سایت Enamad.ir اعتبار فروشگاه اینترنتی را استعلام نمایید.
- تا جایی که امکان دارد فروشگاه اینترنتی دارای نماد اعتماد الکترونیکی را برای خرید انتخاب کنید.

روش‌های متداول مجرمان جهت سرقت رمز کاربران

در ادامه چند روش معمول مجرمان جهت سرقت رمز کاربران را به همراه راه کارهای مقابله با آنها بیان می‌کنیم:

۱ ایمیل جعلی

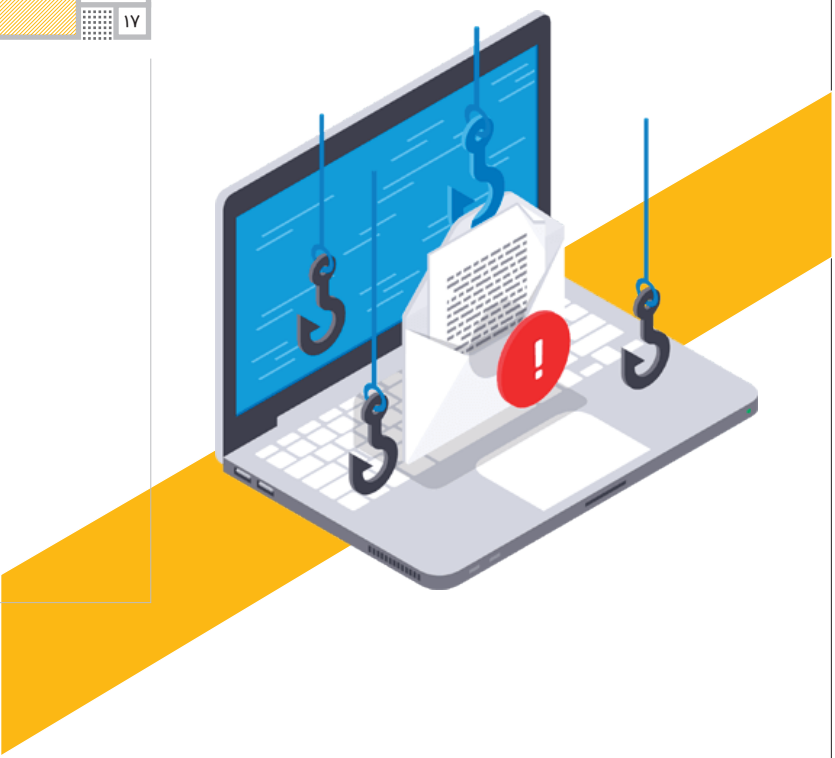
ایمیل جعلی روشی است که به منظور سوءاستفاده از افراد به کار می رود به طوری که فرد کلاهبردار ایمیلی به قربانی ارسال می‌کند که به ظاهر دارای آدرسی معتبر و مهم است. بسیاری از ایمیل‌های ارسالی هرزنامه هستند و هنگامی که فرد ایمیل خود را باز می‌کند با تعدادی هرزنامه مواجه می‌شود. بهترین روش برای مقابله با هرزنامه‌های اینترنتی باز نکردن آنها است و کاربران به هیچ وجه نباید بر روی لینک‌های موجود در این هرزنامه‌ها کلیک کنند.

- هیچ گاه اطلاعات کاربری خود را از طریق یک درخواست یا فرمی که با ایمیل دریافت کرده‌اید، وارد نکنید.
- هیچ گاه در یک ایمیل مشکوک به فیشینگ یا هر ایمیل ناشناخته دیگری، فایل‌های ضمیمه را باز نکنید.
- به طور مرتب فعالیت‌هایی را که در حساب کاربری شما انجام می‌شود، زیر نظر داشته باشید.
- حتما به قسمت From دقت نمایید که مشخصات حساب کاربری ایمیل با ارسال کننده ایمیل مطابقت داشته باشد، به طوری که حتی یک حرف هم جابجا نشده باشد.

مثال یک ایمیل جعلی:

اصلی	Alirezamohammadi@yahoo.com
جعلی	Alirrezamohammadi@yahoo.com

- به طور مرتب مرورگر خود را به‌روز کرده و همه وصله‌های امنیتی آن را نصب و فعال نمایید.
- رایانه خود را با نصب یک ضد بدافزار و ضد جاسوس افزار و یک دیوار آتش مناسب محافظت کنید.
- قبل از واریز کردن وجه معامله ازطریق ایمیل، از دیگر کانال‌های ارتباطی تأییدیه و صحت شماره حساب را استعلام نمایید.
- اکثر ایمیل‌های ویروسی به پوشه اسپم فرستاده می‌شوند. از باز نمودن اسپم‌ها خودداری نمایید.
- آدرس‌های مطمئن و تایید شده افراد مرتبط و طرف‌های معامله را ذخیره نمایید. به جای Reply نمودن، آدرس مورد نظر را از فهرست مخاطبین انتخاب نمایید.
- از رمزهای عبور یکسان استفاده نکنید؛ تا در صورت افشای رمز عبور یکی از حساب‌های کاربری امکان دسترسی به دیگر حساب‌ها وجود نداشته باشد.
- بر روی هر لینکی کلیک نکنید؛ لینک‌های ناشناس یا ضمیمه ایمیل‌های مشکوک را باز نکنید مگر اینکه فرستنده ایمیل را کاملاً بشناسید و بدانید که آن لینک و یا ضمیمه ایمیل چیست. توجه نمایید که در صورت کلیک بر روی لینک‌های ناشناس و نامطمئن امکان نصب نرم‌افزارهای مخرب بر روی سیستم شما وجود خواهد داشت.
- رمز عبور خود را افشا نکنید؛ و در صورت دریافت ایمیلی مبنی بر درخواست اطلاعاتی مانند کلمه عبور حساب کاربری اینترنت بانک، هرگز کلمه عبور را ارائه ندهید.
- بر روی لینک‌های ارسالی که به صورت پیامک یا پیام‌های فریبنده در شبکه های اجتماعی از سوی افراد ناشناس ارسال می‌شود، کلیک نکنید. این لینک‌ها ممکن است حاوی بدافزارهایی باشند که بر روی گوشی همراه شما نصب شده و اطلاعات حساب کاربری موبایل بانک و سایر اطلاعات شخصی شما را سرقت می‌نمایند.

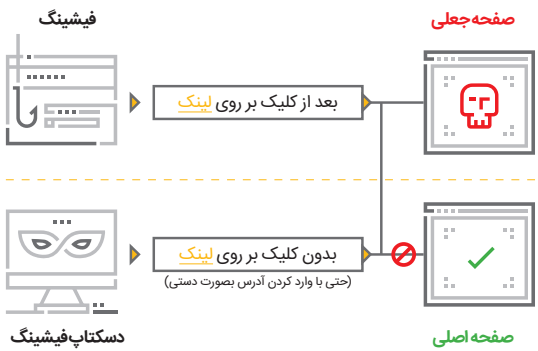


۲ فیشینگ

امروزه یکی از رایج‌ترین حملات در فضای مجازی، حملات «فیشینگ» است. در معمول‌ترین شکل آن، مهاجم با ساخت یک وب‌سایت جعلی شبیه به وب‌سایت اصلی بانک از کاربران شماره مشتری و رمز عبورشان را درخواست می‌نماید، در این هنگام مشتریان با وارد نمودن شماره مشتری و رمز عبور خود در وب سایت جعلی، اطلاعات ورود به اینترنت بانک خود را در اختیار مهاجم قرار می‌دهند.

نوع جدیدتر حملات فیشینگ، «دسکتاپ فیشینگ» نام دارد که در آن مهاجم ابتدا با ارسال یک بدافزار به سیستم فرد قربانی و دستکاری سیستم وی، آدرس جعلی خود را در سیستم قربانی قرار می‌دهد و در این روش حتی با وجود اینکه قربانی، آدرس صحیح را در مرورگر خود وارد نموده است، به وب سایت جعلی مهاجم هدایت می شود.

این شیوه نیازمند آلوده سازی سیستم قربانی به بدافزارهای ویژه این نوع حملات است. همچنین ممکن است حتی مهاجم با استفاده از روش‌های هوشمندانه اقدام به فریب قربانی برای کلیک بر روی لینک‌های حاوی بدافزارهای مخرب نماید.

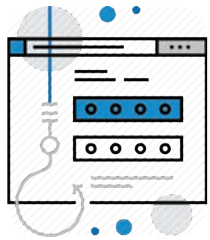


توصیه‌های لازم جهت مقابله با انواع جدیدتر فیشینگ:

- از نسخه‌های قدیمی سیستم عامل ویندوز استفاده نکرده و همواره نسبت به به‌روز کردن آن اقدام نمایید.
- از یک ضدبدافزار مناسب و معتبر استفاده نموده و همواره آن را به‌روز رسانی کنید.
- از مرورگرهایی با قابلیت آنتی فیشینگ استفاده نموده و آن‌ها را همواره به‌روز کنید.
- از دانلود و اجرای فایل‌های پیوست ایمیل‌های مشکوک و ناشناس جداً خودداری نموده و نرم‌افزارهای مورد نیاز خود را از سایت‌های معتبر خریداری و دانلود نمایید.
- به نرم افزارهای رایگان و کرک شده که در اینترنت قرار داده می‌شود اعتماد نکنید.

۳ کی‌لاگرها

کی‌لاگر به‌صورت‌های سخت‌افزاری و نرم‌افزاری تولید می‌شود. کی لاگر های نرم افزاری برنامه‌های رایانه‌ای خطرناکی هستند که برای دزدی هویت اشخاص و پی بردن به اطلاعات خصوصی آن‌ها به کار می‌روند. کی‌لاگرها تمام کلیدهایی را که یک کاربر بر روی کیبورد و یا با استفاده از ماوس فشار می‌دهد، ضبط می‌کنند و در فرصت مناسب از اطلاعات به دست آمده سوءاستفاده می‌نمایند.



راه‌های نفوذ کی‌لاگرها:

- از طریق ابزارهای جانبی مثل فلش مموری‌های آلوده، لوح‌های فشرده آلوده و ...
- ورود به عنوان ضمیمه برنامه‌های کاربردی که از منابع نامطمئن دانلود می‌شوند.
- از طریق ضمیمه شدن به ایمیل (هرزنامه ها)
- نصب مستقیم توسط برنامه نویس آن بر روی سیستم‌های هدف (مانند سیستم‌های موجود در کافی نت ها)
- اتصال کی‌لاگرهای سخت افزاری به درگاه‌های کیبورد و ماوس رایانه‌ها

توصیه‌ها و روش‌های پیشگیری از سرقت توسط کی لاگرها:

- برای وارد کردن اطلاعات مهم و حساس خود از کامپیوترهای مستقر در مکان‌های عمومی استفاده نکنید. امکان سرقت اطلاعات شما به وسیله کی لاگرها وجود دارد.
- در هنگام پرداخت‌اینترنتی حتما از کیبوردهای مجازی تعبیه شده در صفحات پرداخت (درگاه بانک‌ها) یا کیبورد مجازی ویندوز استفاده کنید.
- فایل‌های مورد نیاز خود را از منابع مطمئن و شناخته شده دریافت نمایید. این کار از ورود بدافزار کی لاگر به سیستم شما جلوگیری می‌نماید.
- سعی کنید همیشه ضد بدافزار مناسب و به‌روز داشته باشید. این عمل می‌تواند ویروس‌های مخرب و کی‌لاگرها را شناسایی نموده و اجازه نصب برروی سیستم را ندهد.
- برخی از کی‌لاگرها مخصوص سرقت رمزهای عبور بانکی هستند. این قطعات برای دستگاه‌های خودپرداز طراحی شده‌اند که بر روی صفحه کلید دستگاه نصب می‌شوند. مراقب هر گونه تغییر مشکوک و قطعه اضافی در این دستگاه ها باشید.
- ترافیک ارسال و دریافت اطلاعات سیستم خود را به طور مرتب کنترل کنید. در حالت معمول میزان دریافت اطلاعات باید بالاتر از ارسال اطلاعات باشد. در غیر این صورت باید دلیل موجهی برای ارسال اطلاعات بیابید.

در پایـان لازم اسـت بدانیـم امـکان پیـاده سـازی امنیـت بـه صـورت ۱۰۰٪ هیـچ گاه امکان‌پذیـر نخواهـد بـود ولـی رعایـت نـکات سـاده امنیتـی تـا حـد زیـادی ایـن امـکان را بـرای کاربـران بانکـداری الکترونیکـی مهیـا می‌سـازد تـا بـا اضطـراب کمتـری بـه انجـام عملیـات بانکـی خـود بپردازنـد و متخلفـان امـکان سوءاسـتفاده نداشـته باشـند.

منبع: سایت پلیس فتا www.cyberpolice.ir

بانک پاسارگاد
بانک هزارو سوم
تهران، بلوار میرداماد ، شماره ۴۳۰
۸۲۸۹۰ - ۰۲۱
www.bpi.ir
info@bpi.ir
@bankpasargadtelegram
@bankpasargad

بانک پاسارگاد
بانک بزرگ مردم

آنچه توانستیم لطف خدا بوده است

همراه بانک پاسارگاد

امنیت ورود به همراه بانک پاسارگاد با اثر انگشت

مرکز مشاوره و اطلاع رسانی: ۸۲۸۹۰-۰۲۱ www.bpi.ir