



# راهنمای امنیتی استفاده از خدمات بانکداری الکترونیک



www.bpi.ir

تهران، خیابان میرداماد، شماره ۴۳۰  
مرکز اطلاع رسانی ۸۲۸۹۰



آنچه توانسته ایم لطف خدا بوده است

مشتری ذات بانک است

فهرست مطالب

۲ راهنمای امنیتی جهت افزایش امنیت در استفاده از خدمات بانکداری الکترونیک

- ۳ ■ استفاده از دستگاه‌های شخصی به منظور انجام عملیات بانکداری الکترونیکی
- ۴ ■ استفاده از ضد بدافزارهای معتبر و به روز رسانی آنها
- ۵ ■ اهمیت رمزها در عملیات بانکداری الکترونیک
- ۶ ■ دقت در نام وبسایت باز شده
- ۷ ■ مسائل امنیتی در استفاده از درگاه‌های بانکداری الکترونیکی
- ۹ ■ موارد امنیتی در انجام یک خرید امن آنلاین
- ۱۰ ■ نکات ضروری در انجام تراکنش بر روی پایانه‌های فروشگاه‌های اینترنتی
- ۱۱ ■ نکات ضروری در زمان انجام تراکنش بر روی دستگاه‌های خودپرداز

۱۲ شناسایی صفحات فیشینگ

۱۴ روش‌های متداول مجرمان جهت سرقت رمز کاربران

- ۱۵ ■ ایمیل جعلی
- ۱۸ ■ فیشینگ
- ۲۰ ■ کی‌لاگرها

## استفاده از دستگاه‌های شخصی به منظور انجام عملیات بانکداری الکترونیکی

۱

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.

## 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:

برای خرید بسته کامل سوالات استخدامی بانکها، اینجا کلیک نمایید.

## اهمیت رمزها در عملیات بانکداری الکترونیک

۳

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



- به هیچ وجه از شماره های کد ملی، شناسنامه، تاریخ تولد، تلفن ثابت، تلفن همراه و یا هرگونه مشخصات که حدس زدن رمز توسط شخص مجرم را آسان تر می نماید استفاده نکنید.
- اطلاعات کارت های بانکی و اعتباری خود را در مرورگر وب ذخیره نکنید! درست است که پر کردن اطلاعات کارت های اعتباری وقت گیر است، اما مطمئن باشید پیگیری های مربوط به سوءاستفاده از حساب بانکی شما بیشتر وقت و انرژی شما را می گیرد. به ویژه از ذخیره سازی اطلاعات خود در وب سایت های بانکداری و وب سایت های خرید آنلاین بپرهیزید.

## استفاده از ضد بدافزارهای معتبر و به روز رسانی آنها

۲

با توجه به وجود ویروس ها، تروجان ها، بدافزارها و... که با هدف سرقت اطلاعات کاربران تهیه و منتشر می گردند، اهمیت نصب و به روز رسانی ضد بدافزارهای معتبر بر روی دستگاه های مختلف الکترونیکی هر روز بیشتر از قبل احساس می گردد. لذا به کاربران استفاده کننده از درگاه های الکترونیکی بانک ها پیشنهاد می گردد از نصب و به روز بودن نسخه ضد بدافزار بر روی سیستم خود اطمینان حاصل نمایند.



برای خرید بسته کامل سوالات استخدامی بانکها، اینجا کلیک نمایید.

## مسائل امنیتی در استفاده از درگاه‌های بانکداری الکترونیکی

۵

متأسفانه 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 به منظور 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 نرم افزار 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 نرم افزارهای مشکوک از جمله ثبت کنندگان

## دقت در نام وبسایت باز شده

۴

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 نموده‌اند. (فیشینگ)

آدرس‌های صحیح اینترنت بانک پاسارگاد عبارتند از:

<https://ib.bpi.ir>

<https://iben.bpi.ir>



## موارد امنیتی در انجام یک خرید امن آنلاین



همه ما گاهی برای خریدهای شخصی از خرید اینترنتی یا خرید آنلاین استفاده می‌کنیم و حین خرید با صفحاتی تحت عنوان ارزانترین، قیمت‌های استثنایی، تخفیف باورنکردنی، نصف قیمت و... مواجه می‌شویم برای خرید مطمئن از این وب‌سایت‌ها، باید موارد زیر را رعایت کنیم:

- فروشگاه‌های معتبر مشخصات واقعی را به طور دقیق در وب سایت خود درج می‌کنند.
- از سایت‌هایی خرید نمایید که حتماً نماد اعتماد الکترونیکی را داشته باشند. این نماد توسط مرکز توسعه تجارت الکترونیکی صادر می‌شود، در حال حاضر سایت‌های دارای نماد را می‌توان از طریق سایت Enamad.ir جستجو کرد. اغلب سایت‌های کلاهبرداری با عناوینی نظیر خرید شارژهای ارزان قیمت، خرید انواع تلفن همراه، خرید لوازم بهداشتی و... در فعالیت هستند، پس با کلیک بر روی نماد اعتماد از اعتبار آن‌ها مطمئن شوید.



- فروشگاه‌های معتبر معمولاً نحوه دریافت و پرداخت وجه مختلفی دارند مانند پرداخت آنلاین، از طریق پست و... که خرید از آن‌ها باید به شکل مطمئن انجام شود.
- در پرداخت‌های آنلاین از طریق درگاه‌های بانکی باید به دستورالعمل‌های امنیتی آن توجه شود.
- 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.

فعالیت‌های کیبورد و ماوس بر روی سیستم (Keylogger) اطمینان حاصل نمایید.

- در صورتی که قصد فروش رایانه شخصی و یا تلفن همراه خود را دارید، حتماً سیستم‌ها را به صورت کامل پاک‌سازی نمایید. (تا جایی که ممکن است هارد سیستم‌تان را فروشید)
- از ذخیره اطلاعات حساب‌های بانکی به هر نوعی، در رایانه شخصی و یا تلفن‌های همراه جداً خودداری نمایید.
- به منظور افزایش سطح امنیت در عملیات بانکداری الکترونیکی از مرورگرهای اینترنتی به‌روز شده استفاده نمایید.
- اگر در هنگام بازدید از یک وب سایت، از شما خواسته شد چیزی را نصب کنید، از انجام این کار بپرهیزید.





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 بر روی کارت درج نماید.
- توصیه می شود دارندگان کارت حتی المقدور نسبت به قراردادن سقف مبلغی روزانه تراکنش بر روی کارت خود اقدام نمایند تا در صورت سواستفاده احتمالی از کارت، کل موجودی سپرده به خطر نیفتد.
- دارنده کارت در صورت استفاده از کارت بر روی پایانه‌های مشکوک و یا درگاه‌های اینترنتی مشکوک، باید فوراً نسبت به تغییر رمزهای کارت خود از طریق درگاه‌های بانک اقدام نماید.

### نکات ضروری در زمان انجام تراکنش بر روی دستگاه های خودپرداز

- رمز ورودی کارت می بایست به نحوی وارد شود که به مشتریان در صف نمایش داده نشود.
- در زمان انتقال وجه ترجیحاً 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 آلام‌های خودپرداز منتظر بمانند.
- تغییرات غیرمعمول بدنه و کارتخوان دستگاه را حتماً به بانک گزارش فرمایند.

### نکات ضروری در زمان انجام تراکنش بر روی پایانه های فروشگاه های اینترنتی

- دارنده کارت بایستی خود نسبت به کشیدن کارت بر روی پایانه فروشگاه در زمان استفاده اقدام نماید و کارت خود را در اختیار فروشنده قرار ندهد.
- دارنده کارت باید قبل از انجام تراکنش بر روی پایانه فروشگاه اطمینان حاصل نماید که دستگاه دیگری بر روی پایانه فروشگاه نصب نشده باشد. (منظور، دستگاه‌های کپی کننده کارت است که به قسمت شیپار کارتخوان POS متصل می شوند).
- دارنده کارت باید شخصا نسبت به وارد نمودن رمز خود بر روی پایانه فروشگاه 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



- 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.

## شناسایی صفحات فیشینگ

- به آدرس سایت مورد نظر (درگاه پرداخت) جهت انجام تراکنش های مالی آنلاین توجه کنید.  
نمونه ای از آدرس های جعلی:

www.bannk.com

www.banck.com

آدرس اصلی سایت باید از پروتکل های 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 در اختیار کاربر قرار دهد.
- این سایت های فیشینگ ممکن است با عناوین شارژ ارزان قیمت، تخفیف های باور نکردنی و... در دسترس عموم قرار گیرند.

## باید به نکات زیر توجه کنیم:

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





## 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 می کند که به ظاهر دارای آدرسی معتبر و مهم است. بسیاری از ایمیل های ارسالی هرزنامه هستند و هنگامی که فرد ایمیل خود را باز می کند با تعدادی هرزنامه مواجه می شود. بهترین روش برای مقابله با هرزنامه های اینترنتی باز نکردن آنها است و کاربران به هیچ وجه نباید بر روی لینک های موجود در این هرزنامه ها کلیک کنند.



- هیچ گاه اطلاعات کاربری خود را از طریق یک درخواست یا فرمی که با ایمیل دریافت کرده اید، وارد نکنید.
- هیچ گاه در یک ایمیل مشکوک به فیشینگ یا هر ایمیل ناشناخته دیگری، فایل های ضمیمه را باز نکنید.
- به طور مرتب فعالیت هایی را که در حساب کاربری شما انجام می شود، 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:

Alirezamohammadi@yahoo.com اصلی

Alirezamohammadi@yahoo.com جعلی



# روش های 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 می کنیم:

عبور حساب کاربری اینترنت بانک، هرگز کلمه عبور را ارائه ندهید.

■ بر روی لینک‌های ارسالی که به صورت پیامک یا پیام‌های فریبنده در شبکه‌های 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.

■ به طور مرتب مرورگر خود را به روز 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 از طریق 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





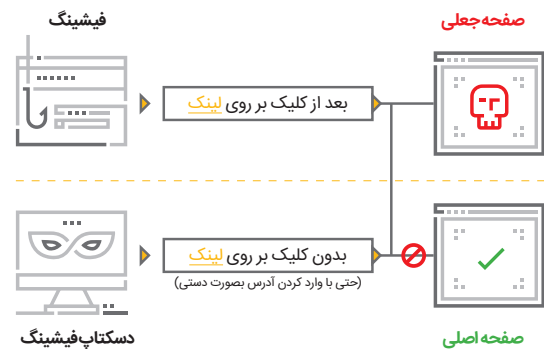
امروزه یکی از رایج ترین حملات در فضای مجازی، حملات «فیشینگ» است. در معمول ترین شکل آن، مهاجم با ساخت یک وب سایت جعلی شبیه به وب سایت اصلی بانک از کاربران شماره مشتری و رمز عبورشان را درخواست می نماید، در این هنگام مشتریان با وارد نمودن شماره مشتری و رمز عبور خود در وب سایت جعلی، اطلاعات ورود به اینترنت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

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 می دهد 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 روش های هوشمندانه اقدام به فریب قربانی برای کلیک بر روی لینک های حاوی بدافزارهای مخرب نماید.

### توصیه های لازم جهت مقابله با انواع جدیدتر فیشینگ:

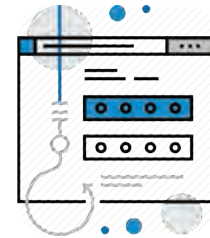
- از نسخه های قدیمی سیستم عامل ویندوز استفاده نکرده و همواره نسبت به به روز کردن آن اقدام نمایید.
- از یک ضد بدافزار مناسب و معتبر استفاده نموده و همواره آن را به روز رسانی کنید.
- از مرورگرهایی با قابلیت آنتی فیشینگ استفاده نموده و آن ها را همواره به روز کنید.
- از دانلود و اجرای فایل های پیوست ایمیل های مشکوک و ناشناس جداً خودداری نموده و نرم افزارهای مورد نیاز خود را از سایت های معتبر خریداری و دانلود نمایید.
- به نرم افزارهای رایگان و کرک شده که در اینترنت قرار داده می شود اعتماد نکنید.



## کی لاگرها



کی لاگر به صورت‌های سخت‌افزاری و نرم‌افزاری تولید می‌شود. کی لاگرهای نرم‌افزاری برنامه‌های رایانه‌ای خطرناکی هستند که برای دزدی هویت اشخاص و پی بردن به اطلاعات خصوصی آن‌ها به کار می‌روند. کی لاگرها 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 کی لاگرها:

- 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 (هرزنامه‌ها)
- نصب مستقیم توسط برنامه نویس آن بر روی سیستم‌های هدف (مانند سیستم‌های موجود در کافی نت‌ها)
- اتصال کی لاگرهای سخت‌افزاری 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 پرداخت اینترنتی حتماً 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 بد افزار کی لاگر به سیستم شما جلوگیری می‌نماید.
- سعی کنید همیشه ضد بد افزار مناسب و به روز داشته باشید. این عمل می‌تواند ویروس‌های مخرب و کی لاگرها را شناسایی نموده و اجازه نصب بر روی سیستم را ندهد.
- برخی از کی لاگرها 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 دستگاه‌ها 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.



برای خرید بسته کامل سوالات استخدامی بانکها، اینجا کلیک نمایید.

# کیپاد

کیف پول همراه پاسارگاد

www.kipaad.ir

## با همراهتان پرداخت کنید



در پایان لازم است بدانیم امکان پیاده سازی امنیت به صورت ۱۰۰٪ هیچ گاه امکان پذیر نخواهد بود ولی رعایت نکات ساده امنیتی تا حد زیادی این امکان را برای کاربران بانکداری الکترونیکی مهیا می‌سازد تا با اضطراب کمتری به انجام عملیات بانکی خود بپردازند و متخلفان امکان سوءاستفاده نداشته باشند.



راه‌های  
امنیتی  
استفاده  
از خدمات  
بانکداری  
الکترونیک

۲۲



تهران، بلوار میرداماد، شماره ۴۳۰		
۰۲۱ - ۸۲۸۹۰		
www.bpi.ir		<b>بانک پاسارگاد</b> بانک هزاره سوم
info@bpi.ir		
@bankpasargadtelegram		
@bankpasargad		

برای خرید بسته کامل سوالات استخدامی بانکها، اینجا کلیک نمایید.