



در طی سال‌های اخیر اکثر بانک‌ها اقدام به تولید و عرضه نرم افزارهای بانکداری مخصوص تلفن‌های همراه و سایر دستگاه‌های کامپیوتری قابل حمل کرده‌اند؛ اما اگر تلفن شما به سرقت برود، چه اتفاقی خواهد افتاد؟ آیا سارق می‌تواند از تلفن همراه شما برای خالی کردن حساب بانکی شما استفاده کند؟

با توجه به این‌که تمایل به استفاده از نرم افزارهای بانکداری رشد بسیار سریع در بخش مالی داشته است، رعایت نکات امنیتی و اقدامات احتیاطی جهت پیشگیری از کلاهبرداری از حساب‌های بانکی، لازم و ضروری است از جمله اقدامات نصب نرم افزارهای ضد ویروس است که برای تضمین امنیت انتقال پول الکترونیکی شما مفید خواهد بود، استفاده کنندگان از این نرم افزارها، باید همان اقداماتی را انجام دهند که در هنگام استفاده از یک کامپیوتر شخصی برای انجام عملیات بانکی خود انجام می‌دهند.

را فراهم کرده‌اند، به گونه‌ای که افراد پر مشغله، نرم افزارهای بانکداری قابل نصب روی تلفن‌های همراه امکانات زیادی برای انجام امور بانکی خود از این نرم افزارها استفاده می‌کنند؛ اما استفاده کنندگان از این نرم افزارها باید نکات امنیتی را رعایت کرده و از گذرواژه‌های قوی استفاده کنند تا اگر تلفن آن‌ها به سرقت رفت، بتوانند، امنیت پول خود را تضمین کنند. اگر کاربران اقدامات احتیاطی لازم را انجام ندهند، امکان کلاهبرداری از بسیاری از کاربران وجود دارد. به استفاده کنندگان از این نرم افزارها پیشنهاد می‌کنیم، نکات زیر را رعایت کنند:

نرم افزارهای ضد ویروس را بر روی تلفن همراه خود نصب کنید تا اگر برنامه یا محتوایی را دانلود می‌کنید، از دستگاه 1. خود در برابر ویروس‌ها و نرم افزارهای مخرب محافظت کنید؛

گذرواژه‌ها، اطلاعات شخصی و شماره حساب‌های بانکی خود را محرمانه نگه دارید. این اطلاعات را در اختیار هیچ 2. شخصی قرار ندهید؛ مگر آن‌که خود شما اقدام به برقرار ارتباط کرده باشید و مطمئن باشید که با بانک یا نرم افزار ارائه شده از طرف بانک کار می‌کنید؛

، و پاسخ‌های مربوط به سوالات محرمانه نرم افزار یا شماره حساب‌های (PIN) گذرواژه‌ها، شماره رمز عبور شخصی 3. بانکی‌تان را در دستگاه خود ذخیره نکنید. اطمینان حاصل کنید که از گذر واژه‌های قوی که شامل ارقام، علائم و حروف است، استفاده می‌کنید؛

تلفن همراه یا دستگاه خود را به گونه‌ای تنظیم کنید تا وقتی که دستگاه روشن می‌شود از کاربر گذر واژه بخواهد. هیچ گاه 4. دستگاه خود را به گونه‌ای تنظیم نکنید که به صورت خودکار با حساب بانکی ارتباط برقرار کند.

به پیام‌های متنی که از شما شماره حساب بانکی‌تان را می‌خواهند، پاسخ ندهید. تصور کنید که هر پیام ناخواسته و ناآشنا 5. به قصد کلاهبرداری از شما ارسال شده است. بانک شما هرگز با ارسال پیام متنی با شما ارتباط برقرار نخواهد کرد؛

اگر تلفن همراه شما گم شد یا به سرقت رفت، مراتب را فوراً به شرکت ارائه دهنده خدمات تلفن همراه و بانک عاملی که 6. خدمات مربوطه را پشتیبانی می‌کند، اطلاع دهید.