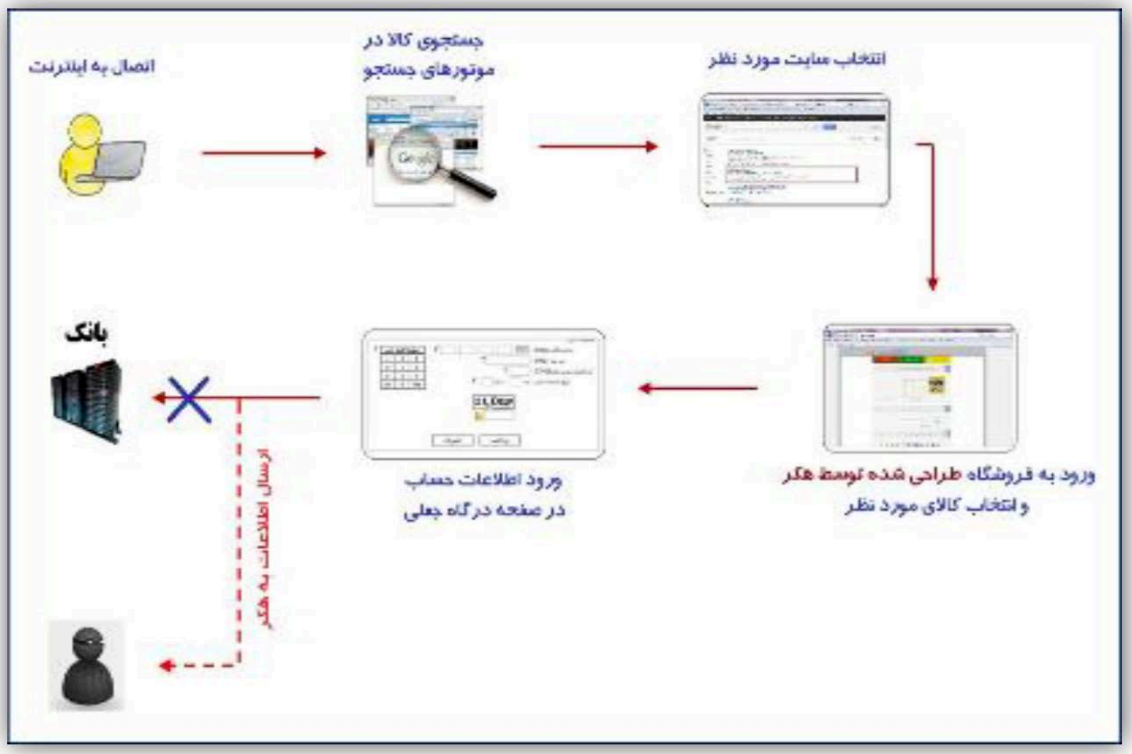
فیشینگ (سایت جعلی)

روشی است که کلاهبرداران با طراحی صفحاتی جعلی اقدام به سرقت اطلاعات مهم کاربران می کنند این صفحات بیشتر در مورد صفحات لاگین، درگاه های بانکی و... می باشد. سارقان نوین یا همان هکرها یک سایت که از نظر ظاهری کاملا مشابه سایت های بانک ویاسایتهای اصلی هست‌را طراحی کرده و ضمن فریب افراد، اطلاعاتشان را سرقت میکنند و حساب فریب خوردگان خالی می شود.

اینفوگرافی حمله فیشینگ



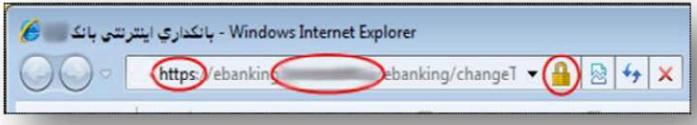
فیشینگ(جعلی)

به دو تصویر زیر دقت کنید که کاملا مشابه می باشد و کمتر کسی می تواند حدس بزند که یکی از آنها توسط سارقان طراحی شده است. تصویر اول متعلق به دروازه پرداخت بانک ملت می باشد و تصویر دوم توسط یک هکر حرفه ای و با هدف سرقت اطلاعات بانکی طراحی شده است.

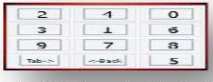
به عنوان مثال:

روش های پیشگیری و شناسایی سایتهای جعلی(بانک ها)

- آدرس اینترنتی را بررسی نمایید و مطمئن شوید که آدرس سایت اصلی باشد.
- در آدرس اینترنتی بانک ها نشان قفل امنیتی وجود دارد
- سایت های اصلی در گاه های بانک از پروتکل **https** استفاده مینماید.



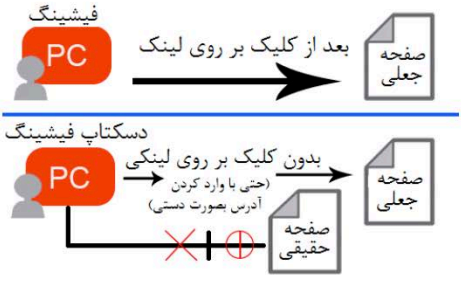
- هنگام وارد کردن اطلاعات خود از صفحه کلید مجازی ویندوز استفاده شود.
- در پایان ثبت اطلاعات بانکی کد امنیتی در صورت اشتباه وارد کردن باید تغییر کند.



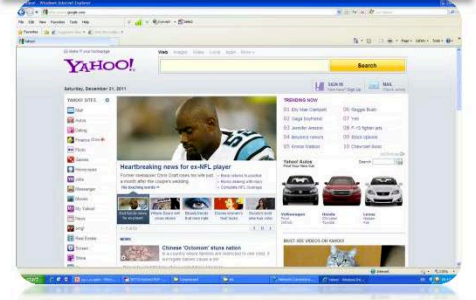
- یکی از روش های ساده برای شناسایی سایت فیشینگ این است که کاربر یکبار تمامی اطلاعات خود را اشتباه وارد نماید در این صورت اگر سایت اصلی باشد خطا خواهد داد ولی اگر سایت جعلی یا فیشینگ باشد هرگونه اطلاعاتی را که شما وارد نمایید ثبت خواهد نمود چرا که سایت جعلی هیچگونه ارتباطی با سرور بانک ندارد.

دسکتاپ فیشینگ

نسخه پیشرفته فیشینگ می باشد با این تفاوت که کلاهبرداران با تغییر ip سعی بر سرقت اطلاعات دارند.



سایت google بعد از دسکتاپ فیشینگ



سایت google قبل از دسکتاپ فیشینگ

دسکتاپ فیشینگ

روش های پیشگیری

- از نسخه های قدیمی سیستم عامل ویندوز مانند ویندوز XP استفاده نکنند و همواره نسبت به بروز کردن آن اقدام نمایند.
- از یک آنتی ویروس مناسب و قوی و نسخه اصلی استفاده و همواره بروز رسانی کنید.
- از مرورگرهای با قابلیت آنتی فیشینگ استفاده و مرورگرها را همواره بروز کنید.
- از دانلود و اجرای فایل‌های پیوست ایمیل‌های مشکوک و ناشناس جدا خودداری شود 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 می شود اعتماد نکنید.

راه های شناسایی دسکتاپ فیشینگ: برای مطمئن شدن از اینکه ما را دسکتاپ فیشینگ نکرده اند باید به آدرس زیر مراجعه و فایلhosts را کنترل نماییم **C:\WINDOWS\system32\drivers\etc\hosts**

- نمونه فیشینگ انجام شده