有一些公司或者个人出于成本的考虑，会选择使用自签名SSL证书，即不受信任的任意机构或个人，使用工具自己签发的SSL证书。这绝对是得不偿失的重大决策失误，自签证书普遍存在严重的安全漏洞，极易受到攻击。一旦使用这种随意签发的、不受监督信任的证书，就很容易被黑客伪造用来攻击或者劫持站点流量。

2. 自签证办理书最非常容易被冒充和仿冒，而被诈骗网址所运用

说白了自签证办理书，就是说自身做的证书，即然你能自身做，那他人能够自身做，能够制成跟你的证书一模一样，就十分便捷地仿冒变成有一样证书的冒充网上银行网址了。

而应用兼容电脑浏览器的SSL证书就不容易有被仿冒的难题，授予给客户的证书是全世界唯一的能够信赖的证书，是不能仿冒的，一旦诈骗网址应用仿冒证书(证书信息内容一样)，因为电脑浏览器有一套靠谱的验证体制，会自动检索出仿冒证书而警示客户此证书不会受到信赖，将会尝试蒙骗您或捕获您向服务器发送的统计数据!

3. 超长有效期，时间越长越容易被破解

自签名SSL证书的有效期特别长，短则几年，长则几十年，想签发多少年就多少年。而由受信任的CA机构签发的SSL证书有效期不会超过 2
年，因为时间越长，就越有可能被黑客破解。所以超长有效期是它的一个弊端。