网银动态密码存两大安全隐患 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/207/2021_2022__E7_BD_91_E9_93_B6_E5_8A_A8_E6_c40_207107.htm 近年来，国内多次发生“ 假冒网站 ”以及客户资金被盗案件，凸显网银安全性问题。 为了提高安全性，一些银行通过“ 动态密码 ”或“ 动态口令 ”验证网银用户的身份，如发给客户一张印有一组数字或字母的卡片，使用时按照一定的规则输入其中一组，下次使用再输入另一组。此外，让客户购买专门传发密码的电子器件，每按一次按钮就可以生成一个密码，或者将一次性密码通过手机短信的方式发给客户等方式，在应用中也比较常见。“ 动态密码 ”使用方便，但它只适用于金额小的交易，对于金额大、使用频繁的用户，其安全性并不理想。目前“ 动态密码 ”隐患主要有两类，一是以病毒等为主的系统安全风险，目前还未形成规模；二是身份风险，目前大多数案件都来源于此。身份风险又分为银行方面的身份风险和用户方面的身份风险，如“ 网上钓鱼 ”案件，是银行的身份被仿制，用盗窃的账户密码进行盗窃，是因为个人的身份被仿制。据有关专家介绍，遭遇病毒和黑客的攻击时，一旦用户输入“ 动态密码 ”并通过网络传送，位于用户与网银服务器通信通道间的黑客便可通过键盘监听、内存读取等方式将其截获，使用户无法完成登录，并造成网络连接断开、连接超时等假象；另一方面黑客利用截获的“ 动态密码 ”假冒用户登录到网银，肆意作案，使用户蒙受损失。 此外，通过“ 动态密码 ”登录的用户没有电子签名，这样也就没有具有法律效力的认证材料，一旦出现纠纷，用户的合法权利将不受保护，

同时也给银行带来一定的风险。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com