
汇聚金融力量
共创美好生活
2023年金融消费者权益保护教育宣传月
9月15日-10月15日
国家金融监督管理总局 中国人民银行
中国证券监督管理委员会 国家互联网信息办公室

✓ 【以案说险】张女士与手机银行安全风险

张女士是手机银行的忠实用户，她享受着手机银行带来的便捷和高效。然而，有一天，她在使用手机银行时遭遇了安全风险。

事情是这样的，张女士收到一条来自银行的信息，提示她登录手机银行完成一项重要操作。张女士不假思索地点击了信息中的链接，然而，当她输入用户名和密码后，发现登录的并不是自己的手机银行，而是一个仿冒的网站。

幸运的是，张女士及时发现并立即停止了操作，避免了可能的损失。她及时找到银行，并在银行工作人员的指导下，加强了手机银行的安全设置。

✓ 深入分析：安全使用手机银行的风险与防范

随着智能手机的普及，手机银行已成为我们日常生活中不可或缺的一部分。然而，不法分子利用各种手段试图盗取消费者的资金，造成安全风险。

安全使用手机银行的风险包括但不限于：

1. 钓鱼网站：不法分子通过短信、邮件等方式发送仿冒的银行网站链接，诱导消费者点击并输入用户名和密码，盗取个人信息。

2. 诈骗电话：诈骗者可能会冒充银行工作人员，通过电话诱骗消费者进行资金转账或提供敏感信息。

3. 应用程序漏洞：一些第三方手机银行应用程序可能存在漏洞，容易被黑客利用。

✓ 提供建议：如何防范手机银行安全风险

1. 确认链接真实性：当收到类似银行发来的链接时，消费者应先通过官方渠道验证其真实性，避免点击不明链接。

2. 保护个人信息：不要随意泄露个人敏感信息，如身份证号、银行卡号、密码等。同时，应谨慎对待包含个人信息的邮件、短信等。

3. 安装安全软件：使用手机时，应安装可靠的安全软件，例如杀毒软件、防火墙等，以防范恶意软件和病毒的攻击。

4. 定期更新密码：消费者应定期更新手机银行的密码，避免使用过于简单的密码。同时，不要在其他地方记录或保存手机银行的密码。

5. 注意保护应用程序：消费者应关注手机银行应用程序的更新和修补漏洞情况，确保使用的应用程序是安全的。不要使用不熟悉的银行应用程序或从非官方渠道下载。

6. 与银行保持联系：如果收到可疑的信息或电话，应立即与银行联系并说明情况。同时，如果发现任何异常或损失，应尽快向公安机构报案并提供相关证据。

7. 备份重要数据：为了防止数据丢失或被篡改，消费者可以定期备份手机中的重要数据，包括通讯录、照片等。同时，如果手机丢失或损坏，应及时联系银行并冻结相关账户。

以上信息为模拟案例