

网络诈骗高发！如何做到见招拆招？

在数字化时代，网络诈骗层出不穷，让人防不胜防。你是否也曾接到过冒充客服的 FaceTime 来电，被诱导泄露个人信息或进行转账？今天，让我们通过一则真实案例，深入了解网络诈骗的套路，学习网络安全法如何保障我们的安全，一起提高警惕，共同抵御网络诈骗的侵害！

真实案例警示

2023 年 10 月 11 日，许女士接到一个 FaceTime 视频电话，对方自称是某网购平台的客服，询问她是否购买过某种药品。由于许女士确实在该平台购买过相关产品，她对对方的话深信不疑。随后，对方称许女士在购买时开通了一个名为“百万医疗保险”的项目，现在免费体验期已结束，如果不关闭该功能，每个月将自动扣除 800 元保费。对方还威胁说，如果未按期缴费，将会影响个人征信。

许女士对此感到十分恐慌，于是按照对方的要求登录了一个虚假的客服网站，并输入了所谓的“退保代码”和手机验证码。然而，她并不知道，这些操作实际上是在进行转账和贷款。最终，许女士的 9000 余元钱款被骗子转走，她这才意识到自己被骗了。

案情分析

这起案件是一起典型的“冒充客服”诈骗案。诈骗分子利用 FaceTime 视频电话与普通电话界面相似的特点，骗取受害人的信任。他们以关闭“百万医疗保险”为名，诱导受害人登录虚假网站并输入敏感信息，最终达到诈骗的目的。

法规护身符

《中华人民共和国网络安全法》第四十六条

任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

《中华人民共和国网络安全法》第六十七条

设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

在这起案件中，诈骗分子设立虚假的客服网站，利用网络发布涉及实施诈骗的信息，严重违反了《中华人民共和国网络安全法》的相关规定，应当受到法律的制裁。

提高防范意识 谨防上当受骗

结合网络安全法要求与反诈实战经验，牢记以下应对策略：

- 1、进行官方验证：**前往正规的官方平台或拨打官方客服热线，与工作人员确认信息的真实性。
- 2、保护个人信息：**妥善保管个人身份信息、银行账户信息、验证码以及各类密码，切勿向任何人透露。
- 3、谨慎开启好友申请和视频功能：**若有人要求在社交平台添加好友或进入视频会议共享视频等协助操作，请坚决拒绝。
- 4、不要进行转账或借款操作：**如果有人索要求转账或借款，请立即拒绝，很可能是诈骗行为。
- 5、理性对待征信问题：**个人征信是由中国人民银行统一管理，没有人有权删除或更改，如果对个人征信有疑问，可登录中国人民银行征信中心进行查询。

【特别提醒】

中老年群体为网络诈骗重灾区，需重点防范：

- ① 协助设置手机安全防护
- ② 定期进行反诈知识更新

③ 建立家庭紧急联络机制

全民国家安全教育 走深走实 10 周年