简要内容：据专家介绍，钓鱼网站诈骗，就是作案者做一个冒充购物网或者银行的网站，通过各种途径诱使用户进入这个网站。由于钓鱼网站的作案者无需攻击任何现有的系统，作案工具可以反复利用等因素，使得钓鱼网站的投放成本变得极其低廉。

网银安全电子商务蓝天的支柱

2010年11月11日，购物网站淘宝启动了光棍节狂欢购物折扣活动。淘宝网仅在这一天中就创造了9.36亿元交易额，这一数字超过了购物天堂香港1天的零售额（约8.5亿元），部分商户这一天的网上交易额达到了2009年全年的数倍，更传闻有商家的打印机因为连续打印订单最终竟发生自燃。淘宝在这一天创造的成绩已经成为了中国电子商务繁荣发展的一个缩影。而在这背后，支撑起电子商务这片蓝天的支柱网络银行却面临着严峻的安全考验。

2010年12月9日，浙江绍兴突发6起网络银行盗窃案件，累计案值上百万元。受害者在当天收到手机短信提示称其使用的网络银行密码即将到期，请马上更改。用户按照指引登陆到短信中的网址进行修改密码操作。几分钟后，这几位用户银行中的资金便不翼而飞。

类似的案件每天都在发生着。据不完全统计，2010年12月以来，仅浙江省已发同类案件40余起，涉案金额上千万元。另据了解，江苏、广东、北京等地也有很多类似案件发生，涉案总额巨大。据国家计算机网络应急中心估算，网络钓鱼给电子商务用户带来的损失目前已达76亿元，平均每位网购用户被钓走的金额为86元。

如何看好自己的电子钱包，已经成为影响大部分网民上网时最关心的问题。

钓鱼网站：遍地鱼饵，等你上钩

据互联网安全厂商瑞星前不久发布的《2010互联网安全报告》显示，2010年，钓鱼网站已经成为最为泛滥的破坏网络安全的方式。2010年，新增钓鱼网站175万个，比去年增长1186%。在欺骗人数最多的十个钓鱼网站，超过一半是仿冒购物网站和银行网站的，作案目标直接指向网银账号。

据专家介绍，钓鱼网站诈骗，就是作案者做一个冒充购物网或者银行的网站，通过各种途径诱使用户进入这个网站。诱使用户进入的方法极其丰富，如上文提示用户网银升级，或是提示用户有折扣很低的促销活动，或是提示用户中奖请用户领取奖品等。途径也多种多样，几乎所有常用通讯工具，包括手机短信、电子邮件、即时

通讯工具、游戏、社交网站都可以被钓鱼网站所利用。

还有一种最为细腻的钓鱼诱骗手法：许多用户的浏览器首页使用的是网址站导航页，作案者将首页地址更改，指向仿冒的导航页，这些导航页面上的银行网站、购物网站却是真正的钓鱼网站。钓鱼从打开浏览器的一刻就已经开始了，真可称之为计中计。这类手法对普通用户迷惑性极强。

一旦用户不能识别出这是假网站而做出了网上银行操作，那么用户的银行账号、密码就会被记录下来，盗窃者即可得手。上文提及的案例就是一起典型的利用钓鱼网站进行盗窃的案子。

由于钓鱼网站的作案者无需攻击任何现有的系统，作案工具可以反复利用等因素，使得钓鱼网站的投放成本变得极其低廉。据公开媒体报道，当前投放一个钓鱼网站，成本最低不到100元，而大部分抓获的从业者，文化程度不超过初中水平。

看好钱包，暂时只能靠用户自己

目前，尽管社会各界都已经逐步关注到了网银面临的安全问题和其深远影响。但是互联网业界技术进步太快，行政管理难以跟得上其步伐。目前，对钓鱼网站，公安局只能在消费者受害后以诈骗和盗窃案件进行侦破，而对在互联网上制作、传播和投放钓鱼网站几乎没有任何监管。

360安全软件董事长周鸿祎介绍：目前有一个中国反钓鱼网站联盟，是由国内的一些金融机构、电子商务网站、域名管理机构组成的行业协调组织，能够认定部分钓鱼网站并进行查封。但是该组织对于网站投放木马病毒、以及域名不属于CN域名的钓鱼网站无能为力。这就是目前唯一具有半官方性质的机构，该机构也只能在接收到举报后才能进行处理，也不能对犯罪者进行追查和处罚。因此其防止用户损失发生和威吓犯罪者的功能极小。除此之外，能帮助用户防患于未然的就只有商业安全软件了。

周鸿祎说：可以预见在最近的未来，不会有官方主导的针对这个问题的整治行动，也不会出现能够覆盖行业全范围的联合应对。所以，用户暂时只能依靠自己来保护自己的钱包。