黑客盯上物流行业 相关网站频遭“ 挂马 ”物流师考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/597/2021_2022__E9_BB_91_E5_AE_A2_E7_9B_AF_E4_c31_597491.htm 5月20日消息：国内知名物流公司申通快递网站首页“ 挂马 ”被清除。360安全中心提醒广大电脑用户，当前许多购物网站、物流网站普遍存在挂马网页、钓鱼网页等安全威胁。用户电脑中如果存在软件漏洞，就会被植入恶意代码，面临个人信息被盗的威胁。据360安全专家石晓虹博士介绍，黑客此次在申通快递官网所挂的恶意代码，主要是利用了IE7的XML漏洞、百度插件、FLASH、暴风影音、REALPLAY、SYMANTEC WINFAX PRO等流行软件的漏洞，用户电脑中只要存在这些漏洞，在访问申通首页时，就会被自动下载并运行数十个木马、病毒程序，该用户的网游、QQ、网银等账号密码信息就会面临被盗的风险。 据了解，作为淘宝网的核心物流服务提供商，申通快递在全国拥有1000多家网点，年销售额每年都在数十亿元的规模。每天访问这家快递公司网站的独立用户数超过8万人次，日均浏览量超过30万次。如此高人气的网站，难免被黑客、木马从业者盯上。根据360安全中心的监控数据，申通快递的网站今年以来已至少3次被黑客“ 挂马 ”。 360安全中心监测数据显示，当前许多购物网站、购物导航网站、物流网站等网购相关服务性网站，普遍存在挂马网页、钓鱼网页等安全威胁。石晓虹博士建议，经常使用网购服务的用户应尽快安装使用反木马软件以防范“ 挂马 ”攻击。同时，专家提醒广大网民，随着网络购物的日益普及，用户在包括支付、物流在内的各个环节，都要时刻保持警惕。尤其是在需要

提交个人身份、账号密码、联系方式等隐私信息时，更要慎之又慎。 把物流师站点加入收藏夹 欢迎进入：2009年物流师课程免费试听 更多信息请访问：百考试题物流师论坛 欢迎免费体验：百考试题物流师在线考试中心 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