

网络骗子手段高明:钓鱼网站、木马程序等无所不用 三位市民讲述网购受骗经历

随着越来越多的人选择网络的方式购物,一些骗子也开始盯上了网络购物,除了传统的网络诈骗公司外,有不少骗子利用钓鱼网站、木马程序等盗取买家的支付宝或网银的账户和密码。昨天,有三位市民向记者讲述了他们的网购受骗经历。针对这三个典型案例,记者请金山网络安全专家李铁军为大家逐一解读。

□快报记者 王竞 张虎

【案例一】 购物遭遇网络诈骗

近日,市民王先生向快报热线96060反映称,去年年底他为单位购买一桶工业酒精,因为购买量不大,他就通过一家B2B网络找到了一家南京本地企业,名称为南京市麟威石化贸易有限公司。他根据网络上的电话打了过去,对方报价790元后,给了他一个银行账号,让他先将货款打过来,称次日就可到货。由于货款数额不大,王先生没有怀疑,也没有去现场核实,就很快将790元货款打了过去。

但等了一天,王先生没等到货,再打对方电话,对方不接。王先生只好换了个电话打过去,“我直接去你们公司提现吧,你们公司地址在哪里?”“在江宁金盛路金盛大厦。”男子说完就挂了电话。王先生赶到金盛大厦,整栋楼

都找不到这个公司,询问门口的保安,保安称这里根本没有这家公司,王先生这才发现自己上当了。

专家解读:这种属于技术含量比较低的网络诈骗,骗子通过搜索引擎优化(简称SEO),让自己的公司在网络搜索中排名更靠前,以使用户更容易发现,并通过低价策略吸引用户购买。用户联系到网站客服以后,对方会要求用户先付款,然后再送货。然而,在没有任何支付保障的情况下,用户的付款很可能石沉大海。

【案例二】 钓鱼网站窃取用户密码

昨天,在江北一所学校当老师的叶小姐告诉记者,前几天她在淘宝网搜到一款自己喜欢的羽绒服,而且同样的裤子网上要比商场里便宜多了。叶小姐选中了一家卖价为230元的商家后,便开始用淘宝

旺旺联系卖家,但她连发了数遍,都只得到卖家的一个自动回复:很忙,请联系我的业务QQ,号码是××××××。

叶小姐因为急于想买到那条羽绒服,于是便加了QQ。卖家通过QQ发过来一个很长的链接,叶小姐打开一看,是一个和淘宝店铺页面一模一样的网页,上面显示的果然是那条她想要的羽绒服。“你可以直接在上面拍,但今晚支付宝可能有点问题,付不了款,你有网银吗?”卖家问道。“我没有网银,不行的话我明天给你付款吧。”叶小姐说完,输入支付宝账号和密码试了一下,果然跳出来一个提示,显示支付宝系统故障,付款没有成功,她以为是淘宝出了问题,还是没有在意。

次日一早,叶小姐习惯性地打开旺旺,却发现旺旺账号已经被盗。随后,她又试图给前几天拍下的宝贝付款,但支付宝提醒她账户存在风险,已经被冻结。叶小姐联系支付宝得知,她的账户在头天晚上有很多交易,但只成功了一笔,支付了99元出去。

因为叶小姐淘宝账号的登录密码和支付宝是一样的,她很快发现淘宝账号也被盗了。她找淘宝拿回账号后发现,自己的号在当晚被

骗子用来开了一个店铺。受骗后,叶小姐才知道,骗子通过链接发给她的网页就是所谓的“钓鱼网站”,只要在这个页面上输入账号和密码,就会被骗子盗取。

专家解读:这是典型的钓鱼网站陷阱,交易过程中,卖家会给用户发来一条技术处理过的链接要求用户点击,这种链接一般很长。用户打开链接后发现网页内容和原来浏览的网页一模一样,便放松警惕。其实对方已经利用钓鱼网站给用户挖好了陷阱,用户在新的网页上完成交易的同时,钱已经到了对方的账户里。而且,对方还会通过钓鱼网站窃取用户的账号和密码,并且对其充分利用,利用用户的账号在网上开店,继续欺骗其他用户。

【案例三】 木马程序盗取网银存款

昨天,在徐庄软件园工作的吴小姐也向记者反映,前天下午2点,她在淘宝上看中了一件400元的绿色棉衣,于是便通过旺旺联系了卖家,卖家给她发了一个exe格式的文件,说是衣服的细节图。于是她试图点开,但系统显示打开失败,于是她便没有再看。随后,她

用网银直接付款,点了付款后,淘宝却一直显示等待付款,于是她又点了一次,仍然是等待付款的状态。但此时卖家说他已经收到了。吴小姐便以为是她的网络较慢,所以没显示付款。

当晚,吴小姐越想越不对劲,上网看了看,发现有类似受骗的例子,于是她立即与支付宝客服联系,得知与她联系的那个卖家是个骗子,账号也是被盗用的,已经被冻结了。而她的淘宝仍然是等待付款的状态,但她网银中的400元钱已经被转走了。“幸好我的网银中只有400来块钱,不然损失更大。”吴小姐说。

专家解读:这是严重威胁网购安全的新型交易劫持木马,这种攻击手段技术含量较高,它的表现形式为,卖家给用户发来一个据称包含商品细节图的文件,吸引用户点击。用户运行该文件后会弹出一个“打开失败”的报错窗口,这是木马作者事先设计好的,用户误以为传过来的文件出错而放松了警惕。其实,此时木马程序已经开始运行。用户所有的支付操作,收款人都是网络骗子。由于新型交易劫持木马只是篡改容易被用户忽略的收款人信息,所以这种威胁让人防不胜防。

网络购物作为一种消费时尚,逐步成为消费者购物的热门渠道之一。然而,网络购物的火爆和安全意识薄弱的用户群使黑客集团垂涎三尺。日前,国内互联网安全厂商金山网络发布的《2010年中国网络购物安全报告》显示,2010年有超过1亿用户曾遭遇过至少一种针对网络购物的安全威胁,带来直接经济损失突破150亿元,网购用户的人均经济损失也由2009年的80元上升至150元左右。你在网购过程中受过骗吗?

□快报记者 张虎

近四成受访者网购遭遇过骗局

网友最担心账号被盗,安全专家教你如何防范

截至昨晚8点,512位网友参与了本期“你网购时被骗过吗”的主题调查。本期调查同时发布于第三方调查官方微博(<http://t.sina.com.cn/dsfdc>)。由于价格低廉、方便快捷、品种齐全等原因,网购已经成为网友购物的主要渠道之一,调查中,96%的网友有过网购经历。然而,随着网购日益火爆,其安全问题也成为众多网友关注的焦点,调查显示,38%的网友在网购过程中受过骗。尽管如此,网友并没有对网购安全问题一棒子打死,65%的网友认为网购是否安全还要看具体情况。

网购已成时尚

对于经常上网的年轻人来说,没有经历过网购似乎已经OUT了。调查中,96%的网友有过网购经历。

网购甚至已经成为一些网友的主要购物渠道。花满楼论坛网友“快乐飞扬”在帖子里称,每个月都要网购,手机、电子秤、吹风机、零食,最多的是童装,至今没有出现过问题。梦溪论坛网友“借我1块钱”也表示,小到开关插座,大到电器家具,都在网上购买,一直用得很满意。

梦溪论坛网友“爱如少年”有着较长的网购经历,对爱如少年来说网购确实方便。网友们选择网购的原因有哪些呢?调查显示,“价格低廉”是吸引网友的主要原因,选择该项的网友占86%,很多网友网购就是奔着东西便宜去的;84%的网友观点和网友爱如少年一样,那就是网购方便快捷,足不出户选



择商品,而且还送货上门,避免了出门购物的麻烦;网上商品“品种齐全”也吸引了很多网友,66%的网友选择该项;还有7%的网友网购是纯属好奇。

38%的网友上过当

虽然网购日益流行,不过,也有网友对网购并不热情,主要原因是担心网购的安全问题。

“不喜欢网购,主要是怕被骗。”化龙巷网友“treely8848”表示,目前网购中唯一让人感到遗憾的就是诚信问题,所以只能买一些金额不大的东西,即使被骗,损失也不大。

化龙巷网友“兄台”网购时就被骗过,“在淘宝买东西时,旺旺跟卖家交流,差不多的时候他就发了链接过来让你拍吧,打开之后界面跟淘宝一样,是我想买的那件东西,拍完付款后没声音了,仔细一看发现被骗了。”

调查中,38%的网友称在网购



制图 李荣荣

过程中被骗过。

尽管如此,网友们对网购安全并没有完全失去信心。化龙巷网友“踹走山P抱泆泽”在帖子里称,经常网购至今没有被骗过,原因是自己比较谨慎,不会相信网上那些把戏。

调查中,65%的网友认为网购是否安全不能一概而论,要看具体情况;28%的网友认为目前网购很安全;仅有7%的网友认为网购不安全。不难看出,对网购安全性的认识和网友们的切身经历有关。

最担心账号被盗

网络骗子利用钓鱼网站、木马等手段盗取用户账号和密码,窃取用户直接经济利益(如支付宝、网银的真实财产)。这种安全威胁逐渐成为主流,随着网络购物规模的迅速扩大而普遍化,这也成为网友们最担心的一点。而且,网络骗子应用新技术,骗局花样不断翻新,使用户在网购安全问

题方面防不胜防。

调查中,网购中网友最担心的就是号码被盗,其中包括ID号、网银账号、支付宝账号等,选择该项的网友占67%;其次是“网络诈骗交易”,选择该项的网友占66%;个人信息泄露也是网友主要担心的问题之一,选择该项的占61%;接下来是“网购交易被木马劫持”和“遭遇钓鱼网站”,分别占比50%和49%。

面对各种各样的安全威胁,苏州19楼论坛网友“贼子蒙”在帖子里建议喜欢网购的朋友,在购物的时候尽量选一些信誉比较好、知名度比较高的网站。贼子蒙的建议也反映了大多数网友的心声。

在问及“你比较信任哪类购物网站”时,97%的网友选择了“知名度高的购物网站”;其次是“商家指定的官方购物网站”,39%的网友选择该项;网友们最不信任的是“电视广告上的购物网站”。

四招防范网络骗术

金山网络安全专家李铁军指出,比较常见的网购安全威胁都是可以防范的,用户在网络购物时要注意以下几点:

一、用户要掌握这样一个基本常识,就是当你已经登录购物网站,正在浏览商品或者网络店铺时,不需要再重新登录。

二、在交易过程中,无论如何不要接收对方传来的链接或者文件。如果对方发送的文件是exe、pif、scr等可执行程序的扩展名,基本可以断定为骗子。

三、一旦发现自己上当受骗后,应该立刻停止所有交易,并立刻杀毒,修改ID、支付宝、网银密码。如果发现自己的网银出现问题,应尽快去银行查询。

四、启用专业安全软件,并及时更新。

第三方调查

快报微博 t.dsqq.cn
掌上快报 m.dsqq.cn
化龙巷/
hualongxiang.com
镇江网友之家/
www.my0511.com
苏州19楼论坛/
suzhou.19lou.com
扬州花满楼论坛/
bbs.huamanlou.com

调查统筹 宋学伟
执行 张虎

无限接近真民意