TOP通信 | 热点

I LOVE SHOPPING 网络购物 把安全放首位

智能手机被内置了吸费软件,用手机时无端被广告骚扰;在咖啡馆上WiFi后居然自己的密码被盗;扫个二维码发现中了木马,住个酒店银行卡就被盗刷了……随着网络骗局的日益猖獗,手机安全问题引起了各方的广泛关注。为此,我们特别总结了几个容易上当的网络骗局,给网友们提个醒,希望网友们养成良好的使用手机和保护个人隐私的习惯。 郑州晚报记者 李冬生

无密码的公用WiFi 不要用

利用免费WiFi盗取用户信息,是不法分子常用的一个伎俩,他们在公共场所提供一个免费WiFi,持卡人使用后,就很容易被植入木马病毒,一旦持卡人利用这个WiFi登录了银行卡,就会导致卡片信息泄露。

目前,在商场、酒店、咖啡店、书吧等地,商家都准备有一些公用WiFi,正因如此,会让一些不法分子混入其中。因此,在连接公用免费WiFi前,最好与相关工作人员确定,看哪个才是真正的WiFi。

此外,目前国内运营商提供的免费WiFi热点安全性相对较高,可通过电话或短信获取免费WiFi账号、密码。同时,最好不要在连接公用WiFi时使用一些重要账号,包括银行卡信息、网银账号、支付宝账号、微信账号等,以保证自身的账户安全。

网购时的短信验证码 不透露

如今,无论是电脑购物,还是手机购物,其支付宝、网银等往往会绑定自己的手机号码,在购物、付款时会收到验证码的短信,输入之后才能完成交易。现在,有不法分子利用短信验证码进入用户账户进行消费、转账等。因此,在网购时,消费者需多多关注此类现象,不要向陌生人透露短信验证码。

我们了解到,不法分子通过非法渠道获取了消费者网购信息,以“退款”或“退货”为由,电话联系消费者,要求消费者加聊天工具,并点击其提供的“钓鱼网站”链接。而实际上,在退货及退款环节不需要校验动态码或交易密码。

专家提醒,在淘宝办理业务时尽量利用淘宝旺旺进行沟通,因为淘宝终端可以监控到旺旺。记住淘宝退货时,店家可自行进行,无需再输入卡号等信息。在收到动态验证码时,请仔细核对短信中的业务类型、交易商户和金额是否正确。同时,记住短信验证码只能用于自己输入信息使用,切记不要告诉其他人。

绑定银行卡快捷支付 小心用

随着互联网的日益强大,无论是家电、手机,还是纸巾、餐具,大部分消费者都会选择从网上搞定。为了方便网购,有消费者会将银行卡绑定快捷支付,这样在支付的时候既不受数额限制,又无需每次输入卡号。

各大公司均拥有安全技术团队维护,支付宝、微信的支付环节理论上比较安全,但是快捷支付将消费者的信用卡绑定后,只需要通过一个输入密码环节就可以完成整个支付过程。如果消费者的淘宝账号一旦被盗,就很容易被盗刷,导致个人财产损失。

因此,专家建议市民取消快捷支付的绑定方式,并将支付环节绑定到手机,每次消费时都需要输入手机动态密码,或者使用U盾进行支付,这样都会比较安全。如果真想利用快捷支付的便捷,建议只将快捷支付绑定一张小额的信用卡或是存款不多的银行卡,这样即使遭到盗刷,也不会造成太大的损失。

低价优惠的链接 要警惕

在日常生活中,我们有时会收到中奖、优惠之类的短信,诸如中了优惠话费套餐,让其根据链接下载客户端进行登记来享受优惠等。白领王甜就曾收到这样的短信,见号码是某通信运营商发来的信息,就没有去细究它的真伪,点击进去后发现业务并不是常用的页面,就起了疑心,通过回拨电话核实了信息,这才发现是假的。

现在,有些打着“低价”、“优惠”等旗号的“钓鱼网站”链接,经常通过互联网、短信、聊天工具、社交媒体等渠道被传播,持卡人一旦输入个人信息就会被不法分子窃取盗用。

特别需要提醒的是,许多不法分子利用伪基站冒充通信运营商向其用户发送短信链接并要求其下载客户端。而这些链接其实是“钓鱼网站”,所下载的客户端实际上是木马病毒。不法分子利用木马病毒窃取卡片信息并进行网络购物,同时将发送到用户手机上的短信验证码转移到自己的手机上,从而完成支付。

因此,用户在网站进行客户信息的注册时要多留份心,即使收到通信运营商的中奖信息,建议加拨电话进行确认。同时,银行卡均要开通短信通知服务,账户发生异常变化后,及时联系银行,封锁账户或挂失卡片。

来源不明的二维码 不要扫

近段时间,由于微店的兴起,淘宝店家纷纷开始了微店的宣传,会经常打出扫二维码加微信送红包的宣传。这也让不法分子找到了空子,他们利用二维码来植入病毒,以此盗取账户信息,一旦进入链接,持卡人的信息就会悄无声息地被盗取。

针对这类情况,业内人士表示,平日上网时,对于不明来源且不确定的二维码,最好慎扫。

在购物时,应尽量选择信誉度比较高的正规商户,不要轻信商户发送的链接、压缩包、图片和二维码等。同时,谨防“山寨”应用软件,在扫码前一定要确认该二维码是否出自正规网站,一些发布在来路不明网站上的二维码最好不要扫描,更不要点开链接或下载安装。最好在移动终端安装杀毒软件等相应的防护程序,一旦出现有害信息,可以及时提醒和删除。

网购骗局的5个特点

■特别提醒

根据网购骗局,相关专家总结了其特点,归纳出以下几个方面,提醒您注意:

■不要相信对方发送的任何文件,双击打开是最大的错误。尽量不要在公共场合使用公用的电脑进行购物、支付等操作。

■如果收到所谓客服人员来电,问清对方客服工号,查找商城真实客服电话,反拨打回去,咨询真实的客服人员,核实来电所述内容的真伪性。

■如发现网站发布不良、违法信息,涉嫌诈骗或已经掉进网络诈骗陷阱的,应及时致电银行,保护银行卡的安全。

■不要在网银或支付宝里存太多钱,设置密码时级别要高,简单的几位数自己虽然容易记住,也很容易被不法分子盗取。

■网购一定要选择正规大型的网站,像淘宝、天猫、京东等商城就有相对高的安全性。同时,仔细甄别网络卖家留下的信息。

■消费者可利用网上搜索引擎,查询供货信息里的联系电话、联系人、公司名称、银行账号等关键信息是否一致。一些以“.pl”、“.tk”、“.ms”、“in”结尾的域名要留意。