典型互联网案例：木马分11次“ 驮"走16万 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/485/2021_2022__E5_85_B8_E5_9E_8B_E4_BA_92_E8_c122_485241.htm －－2007上海特大网银盗窃案引发的质疑 网上支付是否安全？数字证书是否安全？出事后倒霉的只能是用户自己吗？ 基本案情 涉及金额16余万元，上海发生过的最大的网络盗窃案----“ 3?10 ”特大盗窃案日前告破。在上海市警方缜密侦查和云南警方的大力协助下，犯罪嫌疑人白某和葛某在云南昆明落网。 蔡先生是上海一家美资软件公司的总经理，在上海工作多年。2005年，建行的客户经理推荐他办理了一张白金理财卡。在IT行业工作的蔡中对网络非常熟悉，早在建行刚开始有网上银行业务的时候就在使用了，后来蔡先生成了签约客户，再后来又办理了数字证书，之后他就经常通过网上银行购物、缴费、转账。 2007年3月10日，蔡先生上网查看自己银证通账户情况。然而，令人意想不到的是，原本16余万元的账户资金只剩下36.62元，蔡先生赶紧登录建行网上银行，但是连续出错，无法查询。通过拨打客服电话查询，卡内钱款果然被人转走了。两个账户共计被转走163204.5元(含转账手续费)。 当天，蔡先生向卢湾分局报案，卢湾警方接报后，迅速成立专案组，展开案件侦查工作。 在分析案情和银行反馈信息并向被害人了解上网情况后，侦查员进行了综合判断，认为被害人的电脑极有可能被黑客侵入，从而导致账号内存款被盗。侦查员通过查询银行转账记录，查出被盗资金全部转入一个开户在云南昆明的建设银行活期账户内，并已被人取走。警方迅速派员赶往云南昆明开展侦查工作，在云南警方的大力协助

下，侦查员查明犯罪嫌疑人的大致身份，以及实施网上盗窃的地点。2007年3月28日晚上，专案组在云南警方的配合下，顺利抓获犯罪嫌疑人白某和葛某，并查获了作案用的电脑和部分赃物。 经查，犯罪嫌疑人在网上利用发照片之际，将携带木马程序的病毒植入被害人的电脑，获取被害人的银行账号、密码和认证信息，随后盗取被害人银行账户里的人民币。 评析 随着互联网技术的飞速发展，网络已经进入千家万户，从网上购物、网上支付、网上证券交易，到交水电费、手机费等这些网上金融活动，有些已经成为了我们日常生活中不可或缺的东西。正是因为我们越来越离不开网络，所以网络安全也就越来越重要。 目前，由于网络盗窃案件时有发生，网络银行的安全性成为人们关注的焦点，一些人利用木马病毒和“ 钓鱼 ”网站，获取了用户的密码和个人资料，从而盗走用户的存款，那么，一旦人们遇到网络盗窃的情况该如何解决？作为运营机构的银行或者网上支付平台将承担怎样的责任？由于涉及到每个消费者的切身利益，一直是媒体和广大用户非常关心的焦点问题。由于本案不仅涉及金额高，影响广泛，而且很重要的是被盗用户还办理了建行提供的数字证书，就必然引发了人们更多的质疑甚至恐慌----网上支付太不安全了！数字证书也不管用了！出事后倒霉的只能是用户自己！ 2006年七八月，国内发生了多起网银账户被盗事件，包括工商银行、农业银行等，还有一些受害者专门成立了“ 工行网银集体受害者联盟 ”，有些媒体的记者还发现网络上到处充斥着办理银行卡、盗取网银的技术，甚至是贩卖制造银行卡设备的帖子。在2007年的“ 两会 ”上，网上银行的安全性也引起了全国人大代表的关注。全国人大代表、中国

工商银行安徽省分行行长赵鹏表示，如果客户操作无误，而是由于黑客攻击等造成账户损失，应该由银行承担责任。全国人大代表杨新人也认为，发生客户网上被盗事件，如果是由客户的不当操作引起的，应该由客户负责，如果是由于银行管理不善造成的则应由银行来负责。 那么，究竟应如何看待网上支付？它到底是否是安全的？用户的权益是否能得到保护？针对这些问题，我们的分析是： 网上支付、电子银行不仅是解决目前我国存在的金融服务资源相对短缺的有效途径，也是金融服务业现代化发展的必然趋势。然而由于网上支付、电子银行增加了更多的技术环节以及自身的虚拟性，就导致了更多的由信息安全问题、身份冒用问题(包括违法犯罪人冒用银行身份和用户身份两种情形)引发的风险。随着网上支付、电子银行的进一步普及，这些风险很可能会随时转变为用户的实际损害，又加之我国目前的电子支付法律体系很不健全，用户在遭遇这样的损害时也往往会遇到相应的维权尴尬。 结合上面这个案例，我们认为，目前我国用户在使用网上支付、电子银行时可能遇到的这种维权中的尴尬主要有： 1、用户在使用网上支付遭受意外损失后，按照一般的民事纠纷举证原则：“ 谁主张、谁举证 ”，由于用户很难证明银行方面的计算机系统存在安全缺陷，导致用户在提起的相关诉讼中难以胜诉； 2、用户在使用网上支付遭受意外损失后，如针对银行方面提起要求赔偿的诉讼，法院往往会等待相关刑事案件破获的结果以判断银行方面是否存在过失，而网络案件存在身份确定难、取证难等难题，一旦相关刑事案件无法取得有效进展，用户的民事权益也就难以得到法院的支持； 3、目前我国乃至全球的计算机信息安全环境都不

是很理想，导致用户面临较高的信息安全风险。在防不胜防的“网络钓鱼”面前，虽然用户“中招”被认定为用户自己的过失，但在相应的事件中银行方面应承担什么样的义务与责任却是我国法律规定目前的不足之处。尤其是一旦发生了这样的群体事件，银行应采取什么样的措施和态度予以应对，是否需要在第一时间以什么方式告知受害人账户的变化、是否应及时通知其他人风险的存在、是否应对网站采取防伪手段、是否应及时侦测是否存在自己网站的冒牌货并采取措施，等等。而根据目前的法律规定，《电子支付指引(第一号)》的第45条，银行只是有“帮助查找原因、尽量挽回损失”的义务；4、“支付宝”等第三方支付服务平台快速发展，在网上支付中起着越来越重要的作用，但作为新生事物，这些第三方支付平台的法律地位还没有得到明确，法律地位的不明确也同时导致相关法律责任的不清晰，不利于纠纷的解决；5、用户在申请使用网上支付时往往需要与银行通过网络签订电子的格式合同，这些格式合同可能存在一些“霸王条款”，如：“凡是凭客户证书和密码进行操作皆视为客户本人所为，银行不承担任何责任”等规定，片面强调了客户的义务而未明确银行方面相应的审核义务，违背了公平原则，值得进一步商榷。但用户签了这样合同以后，一旦发生损害，则处于比较不利的地位；6、目前网络案件存在证据确定困难的问题，电子证据在传统证据认定规则中存在许多认定上的难点，这一点也是解决网上支付纠纷的难点之一；7、使用包括数字签名在内的电子签名等是保障网络安全的有效方式之一，我国《电子签名法》于2005年4月1日实施，确认了电子签名的法律有效性，是我国的第一部电子商务法。

但即便使用数字签名也会面临两个问题，一是是否使用了合法的电子签名，即根据《电子签名法》、《电子认证服务管理办法》的规定由我国信息产业部的电子认证服务管理办公室认可的机构颁发的电子签名，非合法的电子签名无法得到法律的有效保护。而据我所知，目前我们的一些大银行使用的还不是合法的电子签名。另一方面，还需要正确使用、严格保管电子签名，一旦被他人盗用，损害还是会发生；而如果用户正确使用了合法的数字签名，根据我国的《电子签名法》，将由认证机构承担证明自己没有过错的义务，用户将处于一种更为有利的地位。 总之，网上支付、电子银行的安全性和法制化依然任重道远。国家层面需要完善立法，出台电子支付法等法律，明确银行和第三方服务机构在各种情况下的义务与法律责任，考虑用户的弱势地位，采取包括将举证责任向银行方面倾斜等措施，给予其更多更有效的保护。对于个人，可以采取的措施主要有：妥善保管密码、及时修改密码、不在公用机器上用网银、及时杀毒避免中毒、使用合法的电子签名、不随意接收不明邮件、不随意登陆不明网站，等等。 还有，网络银行安全事件借助网络很容易扩散，杀伤力非常广泛且成本低廉，同时负面效应传播得快，使消费者易产生对整个行业的不信任。任何个体的事件都会发展成为全行业的灾难，面对自己的财产安全，用户极易产生“宁可错杀一千，不可放过一个”的心理，值得网络银行全行业重视；另一方面，网上支付作为更高级别的支付方式，其安全保障的有效建立需要整体环境的提高，如法律法规、行业规范与制度、标准、技术保障措施的发展和推广、第三方机构的发展(信用卡机构、保险、认证机构、第三方支付平台

等)、用户的风险防范意识和能力的提高，在整体环境未有效建立前，难免会存在一些较明显的缺陷，但一旦环境得以整体建立，将是比传统支付方式安全得多的。我们还是坚定地看好网上支付的。