中国人民银行
宁波市中心支行

宁波市金融业信息安全知识百问百答

中国人民银行宁波市中心支行
宁波市网络与信息安全协调小组办公室
中国银行业监督管理委员会宁波监管局
中国证券监督管理委员会宁波监管局
中国保险监督管理委员会宁波监管局

2014年2月

序

近年来，金融信息化高速发展，金融机构与人们日常生活联系越来越紧密，网络购物、网上银行、手机证券、电子保险、移动电子商务、020 等现代化金融服务产品不断推陈出新，极大地便利了人们的学习、工作和生活，但也面临着病毒传播、黑客攻击、信息泄露等风险，引导人们加强金融信息安全防范的重要性日益突出。

根据国务院关于金融信息安全工作的重要指示精神，人民银行总行认真研究，周密部署，通过全国各级分支机构加强对金融业信息安全的管理与协调。在这一工作开展中，人民银行宁波市中心支行会同宁波市网络与信息安全协调小组办公室、中国银行业监督委员会宁波监管局、中国证券监督委员会宁波监管局、中国保险监督委员会宁波监管局成立了宁波市金融业信息安全协调小组，协调小组致力于发挥宁波市金融业信息安全整体合力，保持金融信息化与城市信息化安全工作的跨部门协调运作，将有效提高宁波市金融业信息安全整体水平，提升辖区金融消费者信息安全保护意识，为广大人民群众提供安全、便捷、高效的金融服务。

宁波市金融业信息安全协调小组编制了这本大众化的金融业信息安全知识普及性读物，本读物由通用信息安全保护知识、银行业信息安全保护知识、证券业信息安全保护知识和保险业信息安全保护知识等四部分组成，通过最贴近现实生活的内容和文字，从金融消费者的角度认识金融业信息安全保护，将引导读者学会并运用于保护自身信息安全。

目 录

一、金融业通用信息安全保护知识

1. 问：什么是信息安全？

答：根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。

绝对的零风险是不存在的，要想实现零风险，也是不现实的，安全是一种动态平衡，一劳永逸绝对的信息安全是不存在的。

2. 问：消费者与金融业相关的敏感信息有哪些？

答：消费者与金融业相关的敏感信息主要有个人身份信息、个人职业信息、个人财产信息、个人通信信息、向金融机构申请办理/变更/注销业务的申请单据及获得的实物载体、与金融机构进行日常交易中取得的交易回单、使用金融机构系统需要的各种用户名和密码等信息。这些敏感信息主要表现为纸质文档、电子文档、其他信息介质。

3. 问：为什么不能把身份证件借给他人？

答：不要将自己的身份证件借给他人，以防被他人用于办理信用卡、银行卡、存折、手机号、证券/期货类等账户进行违法交易，特别是他人有偿借用时更要引起警惕。

4. 问：为什么不能把金融产品介质借给他人？

答：借用自己的银行卡、存折、证券交易账户、保险单、支付宝等第三方支付账户等金融产品实体/虚拟介质给他人，容易被他人用作洗钱、套现、骗保、诈骗等违法获罪活动，因此不能因为借用者有偿借用就将金融产品介质借给他人使用。

5. 问：向金融机构提供身份证件信息时应注意什么？

答：（1）提供身份证件原件时，请勿让身份证件脱离视线，并注意金融机构业务人员复印了几份复印件。

（2）在提供的身份证件复印件上注明用途和日期，如“仅限于申请XX 行信用卡”、“仅限于XX证券公司开户”、“仅限购买XX 保险公司XX 保险产品”等字样。

6. 问：个人通信地址变更后为什么要及时通知金融机构进行变更？

答：当个人通信地址（家庭或办公地址）变更后，应立即通过拨打金融机构客服热线、网上自助交易或柜台办理方式通知金融机构修改信息，以免金融产品对账单、重要通知等寄送给您的资料落入他人之手或未被及时安全销毁引起信息泄露，影响金融产品安全。

7. 问：与金融机构签约的手机号更换需要及时联系金融机构变更吗？

答：金融消费者与金融机构签约的手机号更换后，请及时持有效身份证件和金融产品介质去金融机构营业网点办理变更手续，以确保相关敏感、重要信息发送到您的新手机上，其中部分金融业务是绑定手机号的，如不及时变更手机号您将不能正常使用该服务。

8. 问：为什么不能把身份证件和金融产品介质放在一起？

答：不要将身份证件和已办理的金融机构相关资料放在一起，这些资料包括银行卡（含信用卡）、存单、存折、证券账户股东卡、国债凭证、保险单等，避免资料遗失后被他人持您的身份证件冒用这些金融产品，给您造成损失。

9. 问：金融产品介质丢失该怎么办？

答：当银行卡、存单、存折、证券类账户卡、保险单证等金融产品介质丢失时，应立即拨打金融机构客服热线进行临时挂失，然后到相关金融机构营业网点办理正式挂失和后续补办等业务，保障金融资产安全。

10. 问：不再使用的金融产品介质该怎么处理？

答：当银行卡、存折、证券类账户卡、保险单证等金融产品介质不再使用时，不要随便丢弃，应到金融机构办理注销手续后采用粉碎、焚毁等方式彻底销毁，防止金融产品介质上的相关重要信息泄露。

11. 问：如何设置金融产品密码防止密码被破译？

答：设置银行卡、存折、证券类账户、保险账户等金融产品密码，不要将生日、证件号码、电话号码等与自身有直接关联、较简单的间接关联关系或简单数字设置为密码，如不要把设置为全是1、生日中的某6 位数字、手机号码中连续几位，安全性低，极其容易被猜测破解，密码长度至少6 位；网上自助系统密码长度应不少于8 位，应同时包含数字、大/小写字母、特殊字符，提高密码强度。应定期修改金融相关产品密码，适当缩短密码更换周期，一般建议至少3 个月修

改一次密码，防止密码被破解。

12. 问：如何保管金融产品密码？

答：（1）应记住自己的密码，密码请勿告诉其他任何人。

（2）不要把账号密码直接记录在自己电脑、纸条或手机上，更不能写在金融产品介质正面或背面上。

（3）如果密码太多可以加密方式记录，并使用加密狗等硬件加密方式对密码文件加密，切勿随意向他人透露金融产品相关的用户名、密码或任何个人身份证件信息资料。

13. 问：金融产品密码忘了该怎么办？

答：当您遗忘银行卡、网银登录密码、U 盾/UKEY 密码、证券交易密码/通信密码/资金密码、保险官网登录和交易等密码时，请您凭本人的有效身份证件和金融产品介质，到金融机构网点书面申请密码挂失，挂失期间您的金融产品安全将得到保障。

14. 问：为什么不能使用盗版软件？

答：使用盗版软件存在法律风险；另外盗版导致系统存在漏洞或者后门，无法正常升级使用，致使系统存在重大安全隐患；部分盗版软件自身就植入有病毒，容易导致信息泄露。

15. 问：如何应对金融交易用的电脑中病毒情况？

答：发现电脑中病毒后，杀毒软件会报警并自动查杀，如能正常杀掉病毒，则电脑可正常使用；不能杀掉病毒时，应该做到：

（1）拔掉网线，断开网络，如是通过无线网线上网，应断开无线网络连接。

（2）在另外的电脑上下载该病毒的专杀工具和杀毒软件最新病毒定义码，并使用光盘介质转移到中毒电脑上进行查杀。

（3）仍不能杀掉病毒时，建议将重要文件备份到光盘介质，使用前在其他电脑上进行杀毒，确认安全后使用，全盘格式化后重装操作系统的相关应用软件。

（4）如怀疑密码可能被窃取时，请尽快修改相关密码。

16. 问：如何提高电脑的安全性保障使用金融机构网上服务安全？

答：加强电脑安全性可以从以下几方面着手：

（1）设置复杂的开机登录密码。将操作系统开机密码设置为长度不少于8 位，

包含数字、大写字母、小写字母、特殊符合的组合，如设置成为A2bz!8906，极大提高密码强度，并定期修改密码。

（2）使用Windows 操作系统的用户，停用guest 账户，禁止未授权的访问。

（3）使用Windows 操作系统的用户，删除不使用的账户，防止黑客利用这些账户攻击系统。

（4）请打开Windows 系统自带的防火墙，关闭共享和远程功能，以防止恶意程序入侵电脑。

（5）定期下载安装最新的操作系统和浏览器安全程序补丁，使用正版软件，并养成定期更新杀毒软件病毒定义码并杀毒的习惯。

（6）不打开来路不明的程序、链接、邮件，保持良好的上网习惯，防止不法分子利用软件中的漏洞进入您的电脑窃取资料，特别是网银、证券类账户、保险类账户等金融产品交易用户名和密码信息。

17. 问：如何防范电脑中重要数据丢失？

答：定期对重要文件进行备份；对重要文件备份进行加密存储，加密的密码不要和存储介质存放一起；对电脑系统进行定期杀毒，以免重要文件感染病毒被破坏。

18. 问：如何识别和防范网络钓鱼？

答：“网络钓鱼”是危害性极大、成功率很高的一种窃取个人信息的手段，攻击者利用欺骗性的电子邮件和伪造的金融机构WEB 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料 ，如金融机构系统登录用户名/密码、身份证件信息等内容，进而危及金融资产安全 。

针对电子邮件欺诈，不要轻信和打开；针对假冒金融机构网站要核对网址；针对虚假电子商务交易要识别交易对象；另外要加强自己电脑的安全加固措施。

19. 问：电脑故障维修时如何保护电脑上的敏感信息？

答：电脑硬盘上存放了个人资料，很多包含了私密信息、金融机构产品用户名、使用金融机构交易系统临时缓存等敏感信息，泄露后有较大风险。

电脑维修或外送处理时，应做到电脑不离开视野；如必须离开视野，应将硬盘拆下或将个人资料、金融资料等信息备份后再彻底删除，确保存放在电脑上的敏感信息不外泄。

20. 问：用于金融交易的电脑丢失后该如何补救？

答：（1）尽快向警方报警。

（2）建议尽快修改相关金融机构网上系统密码。

（3）及时关注自己的相关金融资产是否有异常变动情况。

21. 问：网上金融交易中常见的信息安全不良习惯有哪些？

答：金融交易中常见的信息安全不良习惯有：

（1）将用户名、密码写在便签上，贴在电脑监视器旁；或将与金融相关的用户名、密码记录在电子文档中，明文方式存放在电脑上。（2）开着电脑离开，未锁定屏幕。（3）轻易相信来自陌生人的邮件、程序、链接，好奇地打开邮件附件，导致中病毒。（4）使用简单容易猜测的密码，或者根本不设密码。（5）丢失金融交易使用笔记本电脑。（6）个人重要数据、敏感信息没有安全备份。（7）使用过的硬盘、光盘、U 盘等介质报废时未做物理彻底破坏。

22. 问：登录金融机构系统输入的附加码起什么作用？

答：在登录网银、证券交易软件、保险机构网站等业务系统时，附加码机制能起到重要的保护作用。附加码随机生成，每次都不同，配合登录密码输入错误锁定、附加码超时机制，可以有效防止密码被暴力破解，常见的是输入密码连续错误5 次，当天禁止登录交易系统等。

23. 问：金融机构交易系统使用到的手机验证码起什么作用？

答：手机验证码是以短信形式发送到金融消费者手机上的一串字母或与数字组合，一般使用有效期较短，与当前用户提交的金融业务关联，用以再次确定用户真实性，增强金融交易的安全性。

24. 问：使用金融机构网上交易系统时通信有安全保障吗？

答：金融机构提供的网上交易系统（网页或客户端软件形式）时，对用户客户端和金融机构系统之间的网络通信进行了加密处理，在互联网上以密文形式传输，可有效保护网上交易的通信安全。

25. 问：金融机构官方网站地址会经常变更吗？

答：金融机构官方网站地址很少变更，变更前会通过旧网站首页、报纸等主要媒体进行长期的公告和提示，请注意识别。

26. 问：如何避免访问各类网站时填写个人信息导致泄漏个人信息？

答：网络应用多种多样，各类网站需要填写个人信息的地方很多，做到不随便填写自己的家庭地址、手机等信息，特别是不要在不明网站输入金融产品账号、密码等个人资料，以免被钓鱼网站或网络木马等软件窃取。

27. 问：如何识别和处理针对金融机构的电话和短信诈骗？

答：（1）多个心眼识别“李鬼”。万一拨打了虚假信函、电话、短信等中所留电话，可以反问对方是否知道自己的手机号或金融产品信息(如银行卡号尾号、证券账户号、保单号等)，由于虚假短信的发送是随机的，所以一般诈骗分子是无法知道你的金融产品详细信息。

（2）虚假信函、电话、短信等中无论以何种名义编造理由，最重要的一点就是不法分子会留下各种电话，一旦你打电话过去后，对方就会最终指导或要求你到ATM 或网银进行转账操作，并要求你的电话不要断开，不要和别人交谈。因此，切记不要按照不法分子去ATM 或网银进行任何操作，应及时到银行柜台、相关金融机构或权威部门去咨询。

（3）若金融消费者不幸落入诈骗分子的骗局应做到：一是及时致电金融机构客服热线或直接向金融机构营业网点报告欺诈交易；二是对已发生损失或情况严重的，应及时向当地公安机构报案；三是配合公安机关或金融机构做好调查、举证工作。

28. 问：安全使用金融机构电话交易服务应注意什么？

答：使用金融机构提供的电话银行、证券电话委托、电话保险等服务时，应做到以下几个方面：

（1）不要在身边有人关注的情况下进行电话交易服务。

（2）不要在公用、共用电话上进行电话交易。

(3)尽量少使用液晶显示的电话进行交易，如果使用的是这一类电话委托，使用完后按下电话键，再重新拿起来随便拨几个数字，使原来委托时的数字消失。

（4）经常更改交易密码，尤其是在感觉到交易密码泄露时。

29. 问：柜面交易时金融机构服务人员能看到用户输入的密码吗？

答：金融机构提供柜面交易服务时，输入密码时使用的是密码键盘防止密码泄露，且用户输入的密码直接与相关业务系统对接，服务人员无法查看到用户输

入的密码。

30. 问：金融机构电话客服人员能看到用户输入的密码吗？

答：金融机构提供电话银行、证券电话委托等电话服务时，用户输入的密码直接与相关业务系统对接，服务人员无法查看到用户输入的密码。

31. 问：金融机构客服电话回访会询问金融产品密码吗？

答：金融机构客服电话回访时，绝不会询问用户金融产品密码信息，如银行密码、网银密码、证券交易账户密码、网上保险密码等信息。如遇询问金融产品密码信息情况，很可能是诈骗电话，应请对方告知工号、姓名信息，然后挂断电话，再回拨金融机构统一服务热线确认该人员是否存在，能有效防范利用软件将电话号码设置为金融机构统一服务热线的骗局。

32. 问：如何加强手机安全保障金融交易安全？

答：手机病毒主要通过蓝牙、下载、短信和彩信方式传播，主要的危害有话费损失、隐私泄露、功能损坏、导致手机硬件损坏无法使用，近年来，手机病毒呈爆发式增长，也出现了利用二维码进行传播等新方式，防范手机病毒的主要措施有：

（1）购买正规品牌手机，“山寨”手机很容易出现内置恶意程序。

（2）通过正规网站下载手机应用软件。

（3）不要随便打开蓝牙功能或与陌生人进行蓝牙匹配，对于陌生号码和不确定号码发来的短信链接或彩信链接不要贸然点开。

（4）为手机安装具有防火墙功能的手机杀毒软件，以保障手机上网和其他手机应用的安全。

（5）不要通过手机浏览可能存在安全隐患的色情类等网站。

（6）不要把手机随便借给别人。

（7）保管好自己的手机，并设置复杂的登录密码。

（8）二维码仅是信息编码手段，有病毒、木马的链接、网页都可以轻易制作成二维码，因此不要随意扫描二维码，扫描前应尽量先核实来源。

（9）使用完手机网上银行、手机证券、手机保险等金融产品后，安全退出后，再关闭程序。

33. 问：宁波市金融业信息安全推动的组织形式怎样的？

答：2012 年3 月，中国人民银行宁波市中心支行会同宁波市网络与信息安全协调小组办公室、中国银行业监督委员会宁波监管局、中国证券监督委员会宁波监管局、中国保险监督委员会宁波监管局成立了宁波市金融业信息安全协调小组。该协调小组制定发布了《宁波市金融业信息安全协调工作预案》及一系列子预案，有利于发挥宁波市金融业信息安全整体合力，保持金融信息与城市信息化安全工作的协调动作，提高宁波市金融业信息安全整体水平，提升金融消费者信息安全意识和信息安全保护能力。

34. 问：宁波市金融业信息安全侵权事件投诉渠道是怎样的？

答：发生金融信息安全侵权事件后，涉及银行业和保险业时消费者可以拨打宁波市消费者权益保护委员会服务电话0574-87324385，或各金融机构客服电话；涉及证券业时请拨打各证券机构客服电话。

35. 问：宁波市金融业信息安全信息官方发布网址是什么？

答：宁波市金融信息安全信息互联网上官方发布渠道是宁波市政府网公民站的智慧金融栏目，网址是：

http://gtoc.ningbo.gov.cn/col/col16322/index.html。

二、银行业信息安全保护篇

36. 问：为什么金融 IC 卡比传统磁条介质的银行卡更安全？

答：传统磁条卡技术简单，存储空间小，磁条信息极易被复制，伪造磁条卡、复制磁条信息的案件频繁发生，给持卡人、发卡机构造成了巨额损失。金融IC 卡又叫芯片银行卡，技术含量高，使用集成电路芯片取代磁条，存储量巨大，使用了非对称密钥体系，安全保密性高，能有效防止被复制和伪造，能同时处理多种功能，为持卡人提供了一卡多用的便利，确保用卡安全。宁波市民卡就是以金融IC 卡为载体实现了一卡多应用功能。根据中国人民银行统一规划，2015 年后新发行银行卡中金融IC卡将全面取代磁条银行卡。

37. 问：为什么手机和磁条介质银行卡不能放在一起？

答：建议手机和磁条介质银行卡分离放置，因为手机磁场可能会破坏银行卡磁道数据，但不会影响芯片介质银行卡。

38. 问：银行卡发生故障会影响银行账户资金安全吗？

答：银行卡由于物理损坏、磁道信息损坏等原因会导致银行卡不能正常在ATM、柜台等设备上正常使用，用户可以持本人有效身份证件和故障银行卡到发卡银行营业网点办理更换手续，不会影响银行账户中的资金安全，与银行账户相关联的代缴水电费、扣划保费等业务仍可正常处理。

39. 问：为什么不能通过报纸上申办信用卡中介机构办理信用卡？

答：一般来说网上或报纸上自称可以帮助申办金卡或提供信用卡融资服务的所谓中介机构绝大多数都不可信，用户办理信用卡时应注意以下几点：

（1）要通过正规渠道申请信用卡，如果申请人要申请信用卡应直接到银行柜台或有经银行授权的正规营销机构办理，而这类营销机构都不需要交纳任何办卡费用，也不会为你提供信用卡融资或套取现金的服务。

（2）信用卡是银行基于申请人个人良好的资信状况给予的一种循环信用额度，发卡银行会根据持卡人使用信用卡状况和资信情况调整相应的信用额度。因此，不能图一时方便或为取得更高的信用额度而去通过一些非法中介机构办理，更不能主动参与信用卡套现，一旦被银行发现将对个人信用状况造成很大伤害。

（3）持卡人若发现非法中介或套现商户，欢迎积极拨打发卡银行的电话或银联客服热线95516予以举报，共同维护银行卡健康良好的发展环境。

40. 问：申请信用卡时如何保护自身敏感信息？

答：申请信用卡时应注意以下几个方面：

（1）切勿相信非银行金融机构的信用卡代办小广告。

（2）不要将自己的身份信息、个人资料等泄露给陌生人，以防被他人伪冒办卡。

（3）不要通过非银行金融机构等渠道（如中介公司）申办信用卡。

（4）不要被申办信用卡时的小礼品所诱惑，应根据自己用卡需求办理。

（5）不要过度要求高额度，根据自己的消费需求和经济能力，以免透支过度。

（6）申请信用卡时认真阅读信用卡申请表背面的领用协议，牢记自己的权利和义务。

（7）填写申请表时，确保自己填写的个人信息完整有效，以便后续激活卡

片；另外确保自己的卡片邮寄地址准确有效，以免被不法分子冒领盗用。

41. 问：如何处理收到的信用卡密码函？

答：收到信用卡密码函后，应注意以下几项内容：

（1）确认信封封口应完整无损，如有破损请及时联系发卡银行。

（2）在信用卡背面签名。

（3）通过电话或网银方式激活卡片。

（4）尽快通过ATM 更改密码，如暂时无法更换，应记住初始密码并立即销毁密码信函。

（5）牢记并保管好自己的密码。

（6）如果遗忘，可立即拨打客服热线补寄密码函。

42. 问：信用卡使用密码要注意什么？

答：信用卡使用密码时应注意：

（1）不论是否设定“消费验密”，取现交易都须校验密码。

（2）若设定“消费验密”，境内消费或境外通过银联网络的交易都须校验密码。

（3）设置复杂密码并定期更换。

43. 问：银行卡背面是否需要签名？

答：银行卡背面最好签名，以防在刷卡过程中被人调包。如果消费验证方式选择为“签名”，需要使用卡背签名做核对。

44. 问：银行卡使用签名或密码确认交易有什么区别？

答：签名和密码都是持卡人对银行卡消费进行确认的方式之一，是保护持卡人资金安全的重要手段。通常来说，我们大多数人使用的借记卡（即一般在卡片里面预先存有资金、没有透支功能的卡）是通过密码加签名来进行消费确认的，而许多国内银行发行的信用卡（贷记卡、准贷记卡）提供了凭密码或凭签名进行交易确认的功能，可由持卡人自主选择。

45. 问：刷卡时可以直接把银行卡给收银员吗？

答：刷卡时直接把银行卡给收银员很方便，但存在磁条卡被复制、卡被刷多次、卡号被记录等重大风险，影响用户银行卡账户资金安全，因此不要让卡片离开视线范围。

46. 问：刷卡过程需要注意哪些内容？

答：刷卡消费时，应注意以下情况：

（1）先查看清楚消费的金额是否正确，输入密码时，并用身体、手等遮挡操作手势。

（2）刷卡成功后核对签购单上的卡号、金额。

（3）签名应与卡片背面的签名一致。

（4）不要在空白签购单或在未填妥金额的签购单上签名。

（5）交易取消时，应确认签购单已彻底销毁。

（6）签账后确认商店人员交还的卡片确实为自己的卡片。

（7）妥善保存签购单存根联，收到账单后及时核对信息。

（8）如已取消刷卡交易改用现金付款，应要求商户撕毁其保留的刷卡签购单，并妥善保管好现金付款凭据。

47. 问：刷卡不通过时应该了解什么？

答：当消费刷卡不通过，应了解以下内容：

（1）刷卡机使用的线路繁忙或线路发生故障。

（2）刷卡机故障，无法传送交易信息。

（3）卡片可用额度不够，交易无法通过授权。

（4）卡片背面的磁条消磁或卡片损坏。

（5）交易突破了银行对特定商户消费金额或次数的控制。

（6）刷卡不通过时如有任何疑问，可即刻拨打银行客服热线咨询。

（7）应妥善保管交易凭据，如发生卡重复扣款等现象，可凭交易单据及对账单及时与发卡银行联系。

48. 问：为什么不能在网吧等公用场所进行网银操作？

答：网吧里的公共电脑由于使用人员比较复杂，可能有不法分子在电脑上安装木马、屏幕录像或键盘记录等恶意软件，窃取您的账号、密码等，因此请不要在网吧等公共场所使用网银，需要转账等交易服务请去附近的营业网点办理。

49. 问：网银登录密码和对外支付密码可以设置成一样的吗？

答：设置网银登录密码和对外支付密码应做到：

（1）将网银密码和对外支付的密码设置成不同的密码，并定期更新密码，

增强安全级别。

（2）网银登录密码和对外支付密码相当于设置了二道防线，增强了网银对外支付的安全性。

50. 问：网上购物和消费时应注意什么？

答：（1）访问正规的购物网站购物。

（2）不要随意打开网上卖家发来的文件，因为很可能存在木马，威胁您的电脑安全。

（3）不要打开卖家发来的非正常购物网站的链接，如果已打开卖家发来的可疑链接（如链接已跳转到别的网站，或连续自动打开多个网页），请立刻关闭该网页，中止与该卖家的交易，并对电脑进行杀毒。

（4）付款时请确认浏览器地址中的信息为正确的网银网址，确认支付的金额、支付对象、预留信息是否一致。

51. 问：登录网银时输入登录密码连续错误多次导致被锁该么办？

答：登录网银时输入密码连续错误次数超过限制次数会导致网银登录被锁，一般24 小时后会自动解锁，如急需使用网银，请持有效身份证件、银行卡或存折到银行营业网点办理解锁或重置密码。

52. 问：登录网银后显示的预留信息是做什么用的？

答：预留信息为客户输入的私密信息，其他人不会知道，如果客户登录后发现预留信息不符，表明很有可能登录了钓鱼网站，请立即登录正确的网银并修改密码，并银行举报钓鱼网站。

53. 问：网银对外支付的主要安全保障手段有哪些？

答：通过网银进行对外支付的主要技术保障方式有：对外支付密码、U 盾/UKEY、手机动态验证码、动态口令卡。U 盾使用硬件和数字证书技术实现对支付信息的保障，是目前主流的最安全的保障手段；手机动态验证是利用客户手机的唯一性来保障支付信息安全；动态口令卡的原理是动态口令生成的随机性，且该口令在认证过程中只使用一次，用来保障信息安全。

54. 问：网银使用的U 盾能一直接在电脑上吗？

答：如果U 盾/UKEY 一直接在电脑上存在被黑客、木马截取口令并利用的风险，建议在不使用网银交易时拔下U 盾/UKEY。

55. 问：输入口令连续错误多次导致 U 盾被锁该怎么办？

答：网银交易用的U 盾/UKEY 输入口令连续错误次数超过限制次数，会导致U 盾被锁，您可以持有效身份证件、银行卡和U 盾到银行营业网点办理解锁。

56. 问：申领新 U 盾后旧 U 盾还能用吗？

答：网银交易用的U 盾/UKEY 等介质丢失，申请新U 盾/UKEY、密码卡介质时，银行会在系统中停用原来的U 盾/UKEY、密码卡，因此旧的介质不能再用于交易，不会威胁到用户的账户安全。

57. 问：U 盾中的数字证书过期了该怎么办？

答：网银交易用的U 盾中的数字证书一般有效期不超过3 年，在证书过期前银行会通过短信、登录网银时的提前预告等方式提醒用户及时更新证书。用户可以持银行卡、有效身份证件和U 盾到营业网点办理证书更新，数字证书更新后立刻启用。

58. 问：U 盾故障后银行卡还能取现吗？

答：U 盾被锁、U 盾数字证书过期、介质损坏等故障情况，用户将不能正常使用网上银行的相关交易功能，但不影响用户进行柜面、ATM、手机银行等方式进行取现、刷卡消费、转账、缴费等交易功能。

59. 问：如何才算安全地退出网银？

答：安全退出网银应采用如下步骤：

（1）网银的安全退出方式，会清空电脑上的客户缓存信息，更能确保客户信息安全，因此网银签退时一定要选页面上的“退出”，不要直接关闭页面，防止未完全退出网银系统，给不法分子留下空子；

（2）做完交易应立即拔出U 盾/UKEY，平时应保管好网银的U 盾/UKEY，不要将U 盾/UKEY 借给他人。

60. 问：进入银行 ATM 区域需要输入银行卡密码吗？

答：目前，自助银行门禁无需输入密码即可通过，如需输入密码，说明门禁被不法分子改装，请尽快向银行举报或报警。

61. 问：ATM 交易输入的密码会被拍摄到吗？

答：ATM 区域监控摄像头在用户输入口令时无法拍摄到用户输入的密码，但仍建议用户输入密码时用手或身体遮挡，防止被他人偷窥。

62. 问：ATM 旁边的银行张贴的 “紧急通知”是否有效？

答：（1）不要相信ATM 旁边的任何“紧急通知”，不要拨“紧急通知”上的所谓“银行值班电话”。如果有要求客户将钱转到指定安全账户之类的公告，尽快向银行举报或报警。

（2）当取款中发生事故或者ATM 机故障时，应拨银行客服热线请求帮助。如果客服热线无人响应，则可以直接报警或者拨114 查询所在支行的电话号码，然后请求银行工作人员现场帮助。

63. 问：手机银行采用的主要安全措施有哪些？

答：手机银行通常采用了多种安全措施：一是将签约客户信息与手机号码唯一绑定，只有客户开通该服务时的手机号码才能登录账务操作；二是利用签约机制、登录密码限额控制、超时退出等管控手段，为客户安全使用手机银行保驾护航；三是每次退出手机银行后，手机内在中关于用户名、密码等关键信息将会被自动清除，账务信息不在手机中存储，四是在签约手机银行时，客户可一并办理短信通知服务，随时关注账户资金变动。

64. 问：手机遗失会影响手机银行的安全性吗？

答：手机银行有密码保护，此密码存储在银行核心业务系统中，即使他人捡到遗失的手机，在不知道手机银行密码的情况下，也无法使用手机银行业务，不影响手机银行的安全。建议用户在发现手机遗失后立刻使用备用电话拨打银行客户电话挂失，然后尽快到银行营业网点办理正式挂失和补办相关手续。

65. 问：如何识别银行卡诈骗短信？

答：常见的手机诈骗短信有“商场消费请您确认”或“银行卡资料泄露”等内容，由于发送虚假短信的不法分子并不知道持卡人的真正卡号，因此虚假短信中绝对不会包含发生交易的银行卡卡号尾数几位、刷卡地点等信息，而只是简单包含“您在XX 时间消费XX 元”内容，没有详细信息。

银行发给用户正规的消费提醒短消息中一般会明确显示用户银行卡的消费时间、地点、消费金额以及卡号的末尾几位。如有疑问应直接拨打银行客服热线进行查询，不要拨打短信中提到的联系电话。

66. 问：如何识别要求提供银行账户、密码的诈骗电话?

答:电话诈骗的常见方式有冒充警察、法院等车家机关索要银行账户和密码，

冒充国家税务机关提示退税索要银行账户信息等，遇到这类电话时，消费者应了解和做到：

（1）警察、法院等国家机关不会通过电话调查或索取您的银行账户，更不会询问您的银行账户密码。

（2）在任何情况下都不要将您的账号、密码告诉别人，不要相信任何人通过电子邮件、电话等方式索要银行账户和密码的行为；

（3）对于任何与银行有关的存在疑问的事请直接联系银行客户服务热线。

三、证券业信息安全保护篇

67. 问：投资者应该到哪里下载交易软件？

答：投资者应到证券公司的官方网站下载电脑/手机交易软件。一些不正规网站上的炒股软件存在被黑客攻击，植入病毒的风险，使用这些软件可能会影响投资者的证券账户安全。

68. 问：证券交易使用的交易密码、通信密码和资金密码功能是什么？

答：（1）交易密码是投资者证券交易使用的密码，在登录交易软件和登录后软件锁定后的解锁时需要使用此密码。

（2）通信密码是用于保护网络通信的密码，在登录交易软件时会要求输入此密码。

（3）资金密码是投资者的第三方存管银行与证券账户之间进行资金划转用的密码。

69. 问：为什么证券账户的交易密码、通信密码和资金密码不能相同？

答：（1）投资者应将证券交易密码、通信密码和资金密码设置为互不相同，避免泄露一个密码即泄露全部密码，影响证券账户安全。

（2）不同的证券账户不要使用相同的交易密码。

70. 问：如何安全更换证券账户交易密码、通信密码和资金密码？

答：（1）通过证券公司电话交易方式，直接在电话的语音提示下操作。

（2）通过证券公司网上交易软件，在自己电脑或营业部电脑上修改。

（3）到证券营业部柜台持有效身份证件申请更改密码。

71. 问：证券账户无法向银行转账该怎么办？

答：银行账户正常，但证券账户无法和向银行账户转账，出现此情况可能是

投资者开户时登记的有效身份证件已过有效期，证券公司将限制该证券账户的业务办理功能，请投资者持有效身份证件到开户营业网点办理信息更新手续。

72. 问：使用证券交易软件提供的记住账号功能有风险吗？

答：多数证券交易软件提供了记住账号功能，下次登陆时只需要输入密码即可，提供了一定的便利性，但也使得账号信息容易泄露。建议不要在公用电脑或营业部的电脑上使用此功能，尽可能每次都手工输入账号。

73. 问：使用网上证券交易软件要注意什么？

答：（1）尽量不要在网吧、图书馆等公用电脑上使用网上交易。若在公用电脑上使用网上交易，请务必确认所有信息都被清除后再关闭电脑。

（2）应避免让太多人使用您的个人电脑，并设置开机登录密码。请打开 Windows 系统自带的防火墙，关闭共享和远程功能，以防止恶意程序入侵电脑。

（3)定期下载安装最新的操作系统和浏览器安全程序补丁，使用正版软件，并养成定期更新杀毒软件的习惯。防病毒软件必须持续更新，最好安装个人防火墙、保险箱等。

74. 问：寻求证券公司客服中心帮助时是否需要告诉对方证券账户密码？

答：在主动寻求证券公司客服中心帮助时，不管遇到什么情况，都无需告诉对方账户资金的交易密码，如确有需要一定要到营业部现场申请。

75. 问：在证券营业部自助终端上交易如何保证安全？

答：在证券营业部自助终端上交易输入账号密码是要注意周围是否有别人偷窥，在交易时尽量不要让他人看到你的账号信息，离开终端时一定要退出交易软件，以防后来人员直接登录投资者的账号。

76. 问：暂时离开证券交易用的电脑为什么要退出或锁定交易软件？

答：投资者不管是在公司还是在营业部交易室，离开电脑时一定要退出或锁定交易软件，并且电脑屏幕锁屏。避免他人操作，造成交易指令的误发，造成股票和账户资金的损失。

77. 问：不用的交割单、对账单可以随便丢弃吗？

答：交割单、对账单等记录了投资者的账户、交易信息，属于投资者的私人敏感信息，确认无用后将其销毁，不可随意丢弃，以防有心之人利用。

78. 问：证券账户中的资金可能被证券公司挪用吗？

答：目前客户保证金都要签订第三方存管协议，第三方存管指券商将投资者的证券交易保证金委托商业银行单独立户进行存管，存管银行按照法律、法规要求，负责完成投资者的资金存取、保证金账户与银行存款账户之间的封闭式资金划转，所以不存在被证券公司随意挪用和被转移至他人账户的可能性。

79. 问：投资者平时可以不用检查自己账户吗？

答：投资者不经常交易尽，但还是要定期查看证券账户，核对对账单，检查密码是否被人篡改，是否有不是本人操作的交易记录。

80. 问：使用手机炒股软件安全吗？

答：手机上的证券交易软件对手机与证券公司之间的通信也有相关安全处理，和互联网交易软件一样，可以保障交易信息安全。请到证券公司官方网站上下载手机交易软件。

81. 问：如何防范互联网非法证券活动以保护资金安全?

答：（1）在证券业协会官方网站上查询合法机构的名录。国家法律规定，开展证券投资咨询业务（俗称“荐股”）、证券资产管理业务（俗称“委托理财”、“代客理财”）都必须经过中国证监会的批准，没有经过批准的，不得从事这些业务。在中国证券业协会的官方网站首页（http://www.sac.net.cn/）， 有所有合法机构的信息公示，投资者可以查询。但也有一些假冒网站会冒用合法机构的名义，投资者应注意识别。

（2）注意识别汇款账号。从事非法证券投资咨询活动的网站提供的汇款账户一般为私人账户。根据有关财务制度规定，给公司汇款不应进入私人账户。遇到此类情况，投资者应分外警惕。

（3）注意识别网站域名。对于冒名网站，域名往往采用无特殊意义的字母和数字构成，如www.gp58889.com, 或直接以数字构成， 如www.61278.cn，或采取偷梁换柱、画蛇添足等方式在合法机构网站域名基础上变换或增加字母（数字）。投资者应通过google、百度等主流搜索引擎，仔细辨别域名真假。

（4）注意识别宣传手段。从事非法证券投资咨询活动的网站往往以“内幕信息”、“黑马”等煽动性语言信息吸引投资者注意，或者以承诺收益、保证盈利的夸大宣传来诱骗投资者。这明显违反了《证券、期货投资咨询管理暂行办法》。

对于这些虚假宣传、承诺受益的网站，投资者不要轻信。

（5）注意索取合同。通过合法机构从事任何证券活动，都必须签订书面合同。如果不能提供合同，或者只能以传真、电子邮件的方式提供合同副本，不能提供合同书面原件的，投资者一定要谨慎对待。

除了掌握上述方法，更重要的是投资者应当保持理性的投资心态，不轻信道听途说，不指望一夜暴富。如果投资者一直想着天上的馅饼，很有可能落入了网上的陷阱。要知道，根据《非法金融机构和非法金融业务取缔办法》（1998 年国务院令第247号）的规定，“因参与非法金融业务活动受到的损失，由参与者自行承担”，也就是说所有损失最终将由投资者自己买单。请投资者加强警惕，合法投资，自觉远离非法证券活动，保护自己资金安全。

四、保险业信息安全保护篇

82. 问：保险业务开展过程中采用了哪些信息化手段？

答：信息技术的高速发展推动了保险业信息化进程，保险业务开展过程中充分采用了网络平台、3G 技术、流程化的信息系统等手段，并使用密码学、电子签名等多种信息化安全保障措施保障信息安全。

83. 问：信息化手段是如何推动投保便利化？

答:利用信息化手段,投保人在可以足不出户,靠电脑就可以实现电子投保,相比以前传统手工投保一张保单最少需要5天时间，电子投保仅需15-30分钟。

84. 问：信息化手段是如何提升理赔速度的？

答：部分保险公司开发的专业理赔系统，实现了理赔受理、资料上传和材料审核等“一站式”全流程服务，将理赔平均结案时间由原来的10 天左右提升至最快10 分钟。

85. 问：如何通过信息化手段识别保险机构信息真假？

答：当消费者对保险公司真伪有疑问时，可以在中国保监会、各地保监局或保险行业协会的网站上查询以确认真伪，防止被骗。特别是很多所谓的外资保险公司在我国境内不具备保险销售资质,消费者购买这些保险公司的“黑保单”后，相差权益将得不到法律保障。

86. 问：如何通过信息化机制识别保险公司营销人员的身份？

答：当保险公司的营销员推荐保险产品时或协助办理保险相关业务时，首先

应要求对方出具有效的身份证明和展业资格证明，或通过监管机构的网站验证其身份。

87. 问：可以通过营销人员携带的笔记本电脑进行网银转账交纳保费吗？

答：部分保险公司推出了新的信息化服务措施，客户可以通过营销人员携带的笔记本电脑进行网银转账交纳保费。由于不是消费者自己的电脑，不能确保该电脑的安全情况，因此建议不要随便使用营销人员携带的笔记电脑进行网银转账交纳保费。

88. 问：哪些保险交费方式是安全合理的？

答：交纳保费时，可以选择保险公司柜台现金支付、POS 机刷卡、网上银行转账、银行柜台转账等支付方式，建议选择通过银行转账办理或亲自到保险公司柜台办理。

89. 问：电子方式交纳保险费用需要注意什么？

答：投保人如需以汇款、网上银行转账等电子方式交纳保险费用，请务必确定账号的收款人为保险公司的专户。若不是，请第一时间报警并与保险公司客服取得联系。保费是不会交纳到个人账户的，千万不要汇给保险销售人员或其他单位名称的账户以免受骗。

90. 问：办理保险红利分红业务时需要银行卡密码吗？

答：保险机构的红利分配情况一般会通过邮政寄送红利分配通知形式告知客户，保险机构不会要索要投保人的银行卡密码，遇到电话或保险代理人索要银行卡密码时要坚决拒绝。

91. 问：核对交纳保费 POS 清单时需要注意哪些信息？

答：核对交纳保费POS 签单时要注意：一是保费金额是否与保单一致，二是打印出的POS 签单上的收款单位名称是否为投保的保险公司专户名称，如果不是，请立即与保险公司客服取得联系。

92. 问：如何通过电子化方式确认理赔资金已安全收纳？

答：根据规定，保险公司必须直接将赔付资金支付到被保险人银行账户上，保险公司一般会通过短信告知客户理赔进度，被保险人可以通过网上银行、手机银行和电话银行等电子方式进行信息确认，确认时应注意银行账户到账金额和理赔协议金额是否一致。

93. 问：如何保持投保人电子信息的准确性？

答：当投保人和被保险人的地址、联系电话等重要信息变更后，需要及时通过到保险公司柜台或保险公司官方网上自助服务办理电子信息变更，确保投保人电子信息的准确性，以免因为信息的变更导致保险公司无法及时联系到投保人影响服务质量。

94. 问：委托代办保险业务时如何保护个人信息？

答：办理保险业务时，尽量选择本人前往公司服务网点办理，若确实无法自行办理需委托销售人员办理时，请在提供有效身份证件复印件等资料时标明办理某年度办理某业务专用字样，并记住销售人员工号和姓名。不要将身份证原件交给代理人，不要将银行卡及密码等信息告知代理人。

95. 问：为什么保险公司从客户银行账户上扣划保费不需要密码？

答：客户和保险公司在签订保险合同会约定通过银行转账的委托授权书，授权保险公司从银行账户划转指定金额的保费，保险公司只能按照合同约定的保费金额划转，不会多扣钱，也不会影响客户银行账户资金安全。

96. 问：投保人保险账户信息安全吗？

答：为保障投保人的保费安全和个人隐私，保险公司业务人员无法查询投保人保险账户资金余额情况，也不能查询投保人用于交纳保费或接受理赔资金的银行账户余额等信息。

97. 问：网上投保需要注意哪些信息安全事项？

答：现在网上投保可以通过多种渠道实现，如在保险公司官网上直接投保，或是与保险公司有合作的旅游网站投保，或是在第三方的电子商务网站网站购买。为保障客户自身的合法权益，首先要选择安全可靠的保险网上投保平台，各保险公司都建议去保险公司的官网上购买，价格便宜，也不易上当受骗。

98. 问：已开通保险网上自助服务的客户应注意什么？

答：正确访问保险公司的官方网站，为自己设置复杂度高的密码，并定期更换密码，防止密码被盗；定期登录系统，确保账户正常。

99. 问：手机投保时需要注意什么？

答：使用手机投保时要注意一是访问保险公司的官方手机网站，二是从保险公司官方网站下载保险交易应用程序，三是注意核对保险公司发送的投保成功短

信。

100. 问：自助投保时怎样才算投保成功？

答：使用网上投保、手机投保、短信投保等自助渠道投保时，投保成功后保险公司会向投保人指定的手机上发送保单生效短信，请确认短信内容中保单信息与投保内容一致。