① 在探究系统中出现漏洞

我们都知道，移动支付依托于终端技术，而智能手机的核心就是操作系统，移动支付的风险就可以简单体现在操作系统中，这会给用户带来安全性

的问题。

当今，智能手机的操作系统主流的有两大类，分别是Android和IOS，操作系统通过连接互联网的方式，在操作中暴露漏洞，例如网络漏洞、黑客入

侵等探究性的问题，这因此会造成对移动支付行业内的影响，除此之外，还有体现在一些用户信息泄露，密码被盗用等情况。曾经我在使用移动支付时

也面临过密码被盗用的情况，现今也有很多的用户曝出支付密码被解锁，用户名被盗，信息泄露等情况，这种风险经常发生。此外由于在操作系统中出

现漏洞，这将会给不法分子带来好处，给我们带来风险

②诈骗信息

现如今，互联网的发展，给我们生活中带来了很多的便利和好处，与此同时，在人们不经意时也会给我们造成一些网络风险，智能手机能接收人们

的短信，不法分子会使用一些带有木马病毒的链接、网址、网站作为伪基站，和作为普通用户发送的一些诈骗信息，这都是属于安全风险中的一种。

我经常会收到一些不明身份人的发送信息，这些诈骗信息可能是一些不法分子冒充政府机关、运营商、淘宝客服或者一些金融机构的身份进行发送

还经常出现的就是以xxx邀请你参加xxx的活动抽奖，然后xxx中奖了xxx现金，请到xxx网站领取，这时候会让你填写一些用户的个人信息，导致个人信

息的泄露。这一方面体现了在网络安全方面的法律体系暂不健全的问题，也体现了网络监管力度与行动相互欠缺的情况。

无规矩不成方圆，任何行业都要有相关的法律体系，才能使其走得更长远和进步，而在移动支付行业，其所存在得问题之一就是法律体系不全面。

目前我国移动支付得发展得到阻拦，其主要体现在目前对于移动支付来说，其监管所依据得法律主要是为部门规章和一些政策文件，这种文件属于规范

性得文件，是不具备约束力的，对于移动支付行业来说无法进行较强的约束，所以对移动支付的消费者来说，其利益是无法得到保障的。移动支付的发

展需要很多法律法规的指导和牵引，但我国在法律法规中任然处于不完善的阶段，在监督方面也很模糊

③金融下风险分析

1. 技术风险

行业的发展需要有技术，无技术无发展宏图。所谓的技术风险，即指因在技术中存在的某些缺陷而导致的风险，包括在系统中出现漏洞而导致安全问题、交易时中断异常或信息被泄露等问题。其次，在操作系统中存在的漏洞也会在密码破解、病毒入侵中带来风险，给消费者在经济上造成一定的损失。最后，也有很多移动支付的使用者常常忽略一些安全问题，对安全防范措施置之不理，甚至对于个人信息保密的情况都不重视，容易听信他人，也易被一些不明的钓鱼网站诱惑，从而对移动账户造称损伤。

1. 用户风险

近几年来，都出现很多诱骗团队，被诈骗的事件也纷纷在各大网络电视看见，且诈骗形式也千奇百怪，让很多消费者容易上当受骗。现如今很多大学生，在淘宝刷单中屡次被骗，也很多用户是通过连接一些不安全的网络接口，还有一些移动支付的用户将自己移动支付的app于银行卡绑定了。所以这些问题的存在都会给移动支付用户带来一定的风险，这不利于行业的发展，消费者和用户也得不到保障，所以必须要采取一些措施来解决和预防这些问题。

1. 防范措施

目前，移动支付勇起发展，给很多行业都起到一定的带头作用，移动支付行业也要有一定的企业战略，才得以在这个市场环境中生存下去

1. 政策监管不断加强

移动支付的业务从法律层面上来说，很多相关机构，例如法律、金融、政府等都指定了相关的文件去规范移动支付的业务。从2005年开始，我国就已经从移动支付的法律法规入手，随后我国又发布了很多相关的规范性文件和管理办法。到2010年，颁布了《非金融支付服务管理办法》，随后不久，又颁布了《中国金融移动支付条例技术标准》，到2013年6月又颁布了《支付机构备付金存管办法》，到2017年1月，发布了在支付机构客户备付金存管有关事项的通知，这个通知是由中国人民银行办公厅实施的，主要是针对与备付金资金的利息缴存的资金比例问题进行展开。它规定了在支付机构中客户存在的备付金的比例是按照上个季度备付金日均余额与机构所适用的交存比例来计算，并且在每个季度都要进行调整。

目前，在于监管方面，目前的防范现状是对金融行业进行监管和实行管制。用相关的监管部门如央行、证监会、保监会。但对于现在来说，行业相关监管部门都知道自己所要管理和监督的范围对于第三方支付，其与金融行业都有一定的区别，第三方支付和移动支付有相应的联系，其第三方支付在交易中所涉及的主体，都有相应的部门监管做出相对应的规定。结合其支付的现状、现有业务及特点而制定相适应的法律条文和监管标准。第三方支付主要是由央行来监督管制，而与其在业务开展上有相似之处的金融机构是银监会来监督管制。但在监管的同时，在移动支付上对其业务进行区分监管上是有一定的局限性。但为了促进相关监管部门之间的密切合作，金融监管机构在《关于促进互联网金融健康发展的指导意见》中，其意见文件在移动支付管制

相关的监管部门要协助央行的做法来对移动支付进行管理

3、风险管理不断完善

移动支付不管在技术、操作还是用户上都存在着安全风险，这些风险是一直存在并随着移动支付的需求和变化而变化发展。目前，移动支付的发展在中国、美国、日韩等多个国家的发展都是突飞猛进的，但有很多存在不足的是在安全技术方面存在不足。在互联网公司和商业银行的结合下，本公司在移动支付技术上得到很大支持，以及为本公司的技术人才得到培养和接纳，同时在一些技术上得到更新。我们可以以金融机构来举例。根据调整显示，我国的很多金融机构一开始都比较注重业务，在开始新业务的时候，对其业务的各个流程都是

比较完善的，并在管理层面上都加大控制措施，给员工进行个饭概念的技术培训，特别是在技术更新后，给员工普及新技术，学习其技术的核心，并且除此之外，在教育方面的工作也比较注重，在移动支付的快速发展下，风险也是随之改变而改变，我们加强在移动支付风险的宣传工作，在2013年，中国银行和第三方支付机构的联合推动下，对移动支付的用户加强了在支付风险方面的宣传工作，能够让他们更好的了解风险，能提前做好防御准备。

移动支付风险在操作系统中出现漏洞，有很多的非法分子都通过不良的行为进行诈骗，使用户的信息泄露，造成一堆的损害，其次还有在技术上，用户还存在一些风险，人么的防御措施不全面和防御知识不健全，而导致各种各样的损失。按照目前的形式来讲，我国大部分的支付平台的安全管理系统是没有完善的，存在很多的缺陷，特别是系统中国易出现故障，而鼓掌报告不及时和不全面，以及操作系统中的监控管理方面欠缺。因此，在当今经济发展的形式下，为了防止客户的经济损失，也为了在移动支付的发展能够更长远和安全快速，安全问题是我们首要考虑的问题。

移动支付防范对策

1. 操作系统优化

手机的核心技术就是操作系统，移动支付在操作系统中出现漏洞，导致这种风险的主要是由系统中的涉及不足导致的，在操作中对于病毒的侵害没有比较强的拦截，在支付交易时要对敏感信息进行加密处理，以微信转账为例，给对方转账在超过多少钱必须提供收款方的姓或者名，进行身份认证，从根本上防范移动支付安全风险，首先要改善的时加密技术。如今的加密模式主要由人脸识别、指纹验证，，密码输入。对于一些密码进行破解，因此，在移动支付过程中，还需要通过身份认证来确保交易的安全。但目前如果只是单一的身份认证是无法满足移动支付的安全性，必须采用两种或两种以上的安全因素进行身份验证。两种以上的因素则是指出了密码输入时，还应联合时间、地点和设备三个安全因子进行认证，只有这三个安全因子都同时满足了才可以进行下一步的交易，否则交易中断。

1. 加强法律监管

我国的移动支付行业，在法律体系下不全面，监管模糊。况且在移动支付中，其业务所涉及的范围比较少，如果法律体系不全面，监管力度不加强，难以进行防范，容易引发更多风险带来的损害。目前，我国蹄冻支付不断健全，颁布了一系列相关法律法规《支付机构客户备付金存管方法》、《中国金融移动支付系列技术标准》等，其次，在政策监管上不断加强，颁布的相关规范性文件在一定程度上对移动支付的安全风险问题的以降低。移动支付业务的发展，需要政府及其更多的金融监管机构出台更多有规范性、安全性，更具有可行性的政策。首先，相关监制的部门要有一定的行业标准，并且还是统一性的，有这种统一的行业标准，在实施起来更加方便，况且起到一个很好的指导作用。

1. 建立完善用户信息保护

移动支付的发展下，常常有很多的用户是被诈骗，经常收到诈骗信息，存在一定的用户风险，不明的分子通过各种各样的诈骗手段对用户下手，常见的有淘宝傻蛋被骗，不良网站的弹出，还有一些关于抽奖、中奖的链接，然后就会出现中毒的问题，很多用户的钱被骗走或者账号被盗甚至还

会泄露用户的个人信息，因此，移动支付企业要对用户信息保护更加重视起来，要应用先进的技术对用户信息进行保护，加强网络技术的建设，再结合先进的网络技术，对于黑客入侵，病毒的统计进行防范，并且还要不断地对网络安全进行检验，对一切得安全系统进行升级更新，移动支付企业还应该对员工进行调整，再进行招聘时应该与员工签好保密协议，培养员工的安全以是，其次，还应该加大对员工安全意识得培训，并且不定期进行考核。其次，还应该对用户信息进行有规范性得管理，要严格按照国家得相关法律法规进行管理，避免用户得信息混乱，泄露丢失等。除此之外，还应该普及网络安全方面的知识，并且加大力度对用户宣传，通过广告、互联网、网站等方式传达给更多的消费者。同时，应建立风险监控，在遇到这种风险的时候应采取紧急的措施，对监控系统进行远程或近程控制，一旦出现风险会出现警报和数据报告，从根源上减少了风险产生和降低了风险指数，为此，降低了风险所带来的恶劣影响。

最后，要谨慎的保管好自己的手机，防止被盗或遗失。也不要把一些敏感信息存在手机备忘录上或者其他软件上，这会对消费者本身造成伤害，其次，也不要去连接那些不安全的Wi-Fi，特别是不需要密码或其他手机号验证的Wi-Fi。如果真的需要，建议使用熟悉人的热点或者将手机的模式设置为便捷式热点。然后使用 WPA/WPA2加密，防止无线网络的开放，而且还要设置等级较为中等或者高级的密码，不轻易被破解的密码。并且不轻易打开那些来历不明的短信文件、链接、网站等等。