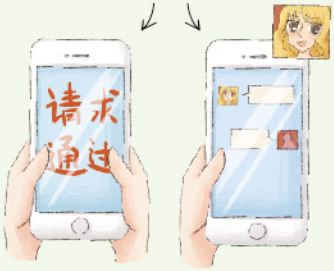
【增强风险识别能力，共享金融网络安全】

生活中我们面临着形形色色的通讯网络安全风险：

场景一：社交陷阱

有些不法分子通过设定场景，利用当事人急于求成的心态，获取当事人个人信息，并通过一些重要信息盗取当事人的资金。



小张，大四学生，面临毕业求职，在招聘网站投递简历。一家招聘公司人事部经理要求其通过微信方式缴纳介绍费、押金。

场景二：木马病毒

特洛伊木马是一种基于远程控制的黑客工具，它通常会伪装成程序包、压缩文件、图片、视频等形式，通过网页、邮件等渠道引诱用户下载安装，如果用户打开了此类木马程序，用户的电脑或手机等电子设备便会被编写木马程序的不法分子所控制，从而造成信息文件被修改或窃取、电子账户资金被盗用等危害。

小李，毕业两年，程序员
平时在家特别喜爱打网页游戏。

如何预防金融网络信息安全风险？

- 不轻信来历不明的电话和短信；
- 不点击短信、网络聊天工具或网站中的可疑链接，不登录非法网站，慎扫不明来历的二维码；
- 慎连免费WiFi，连接免费WiFi时不登录网上银行、手机银行、支付机构APP进行账户查询、支付等操作；
- 不随意透露自己和家人的身份、存款、银行卡等重要个人信息，不向陌生人转账汇款。

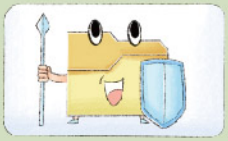
网上银行安全提示

- 使用不同的用户名和密码，不要外泄您的密码；
- 使用数字、字母、符号相结合的密码并经常更改您的密码；
- 保护您的网络服务安全；
- 小心留意欺诈性邮件；
- 避免在公共电脑或网吧进行任何网上银行交易；
- 保护您的个人电脑。

网上支付安全常识

第一招

直接访问我行官网或拨打24小时客服热线，不使用呼入、转接等方式。



第二招

电脑安装银行官方控件，定期更新系统，安装防火墙和杀毒软件，将计算机的“host文件”修改为“只读”。

第三招

不点击陌生链接、可疑邮件，不轻信退款、领优惠、换积分等短信，支付时慎用公共WIFI，有疑问时向官方渠道咨询。

第四招

不要将本人的电脑、手机、电话等，随意借给他人使用。