**鉴别钓鱼、诈骗邮件的常用方法**

1. **观察邮件所属文件夹**

正常邮件一般不会出现在垃圾邮件夹内，如下图。垃圾邮件夹是系统通过反垃圾策略自动识别的，出现在垃圾邮件夹内的邮件，大家就应该引起警惕。



1. **观察发件人实际发送邮箱**

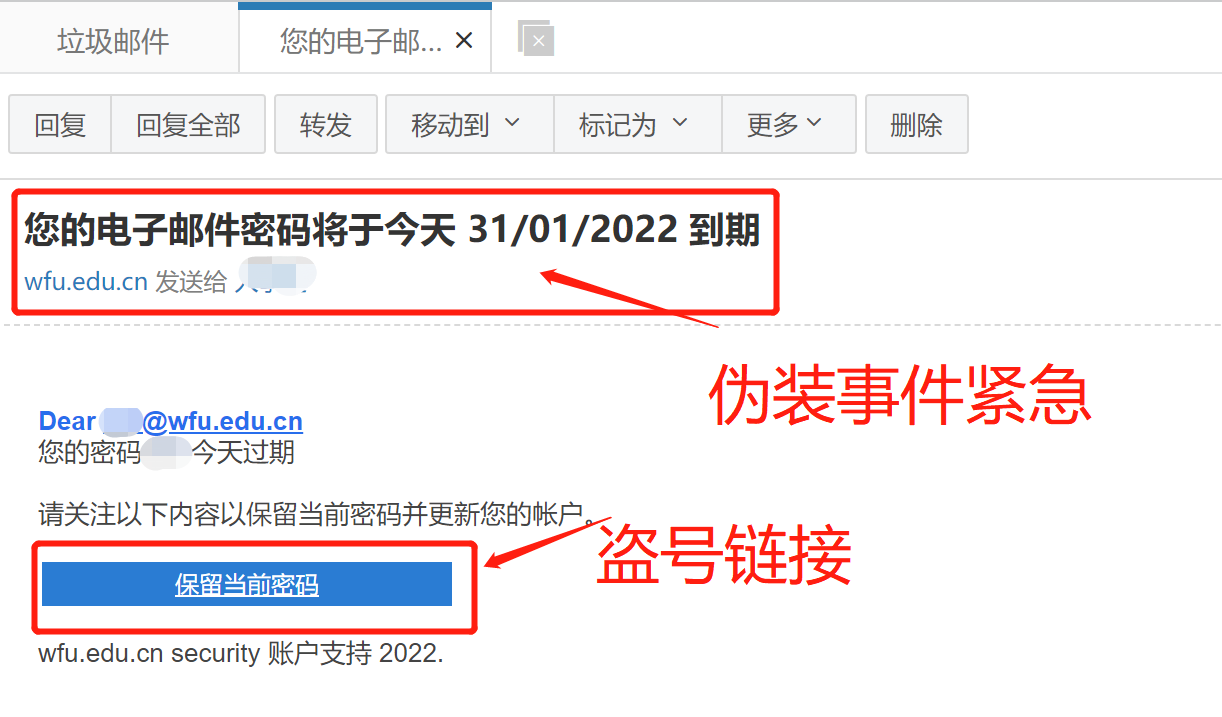
犯罪分子经常将发件人的名字伪装成support、管理员、admin等有特定含义的名称，或者某校长、某处长等领导名称迷惑收件人。这时可通过点击名字来观察实际发送邮箱。我校电子邮件系统统一使用@wfu.edu.cn为域名结尾的邮箱地址。如收到使用迷惑名称标记的奇怪域名结尾邮箱发送的邮件，需格外提高警惕。



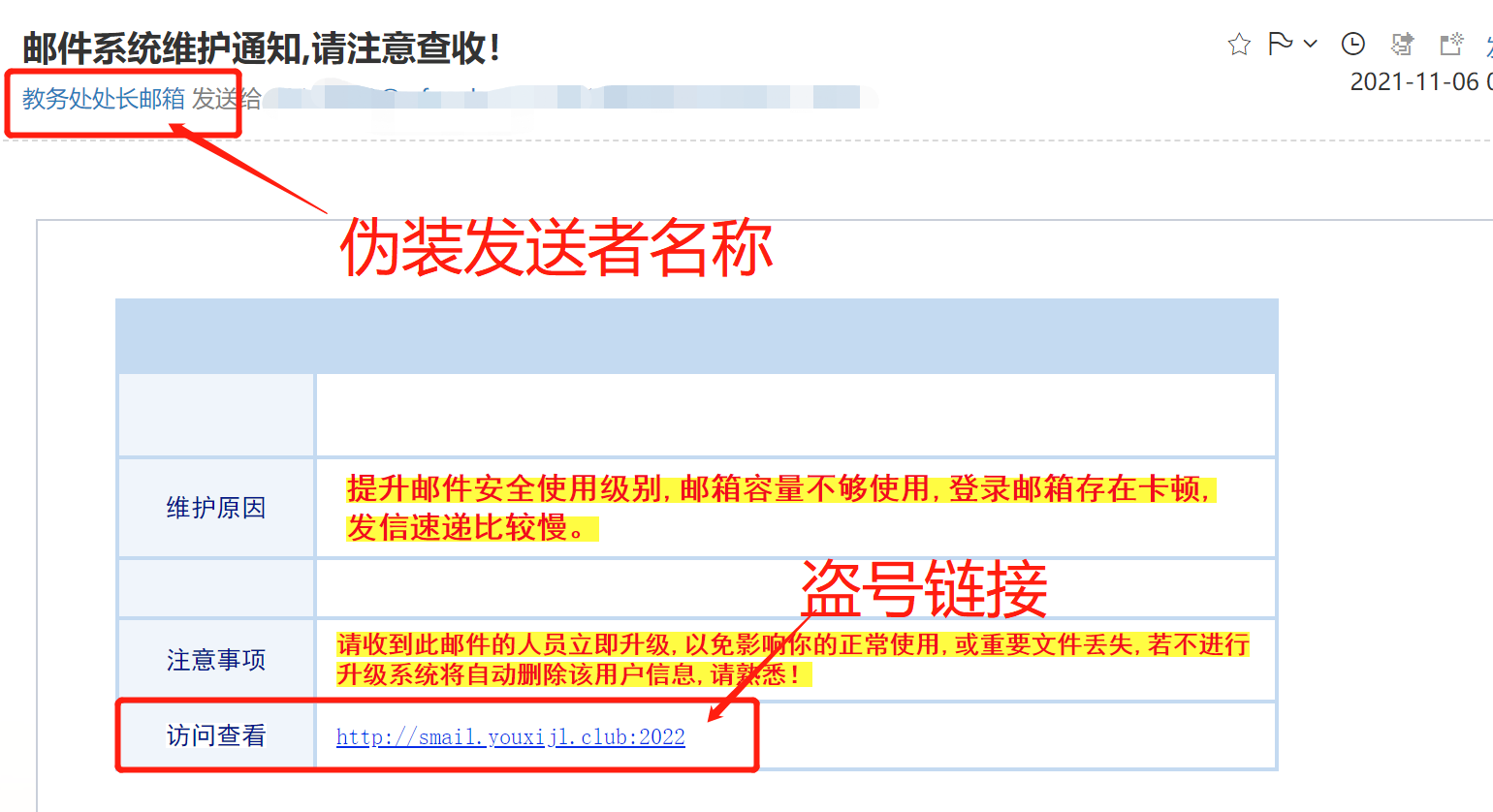


1. **判断邮件内容**

观察如下几封钓鱼邮件可发现，邮件命中了很多危险因素：1、以学校重要部门或系统管理员的名义下发；2、邮件标题内容紧急，内容书写正式；3、以修改密码或获取密码为邮件主要目的；4、存在URL地址；5、强调严重性、重要性和紧迫性，制造紧张氛围。这大概率就是钓鱼邮件了。





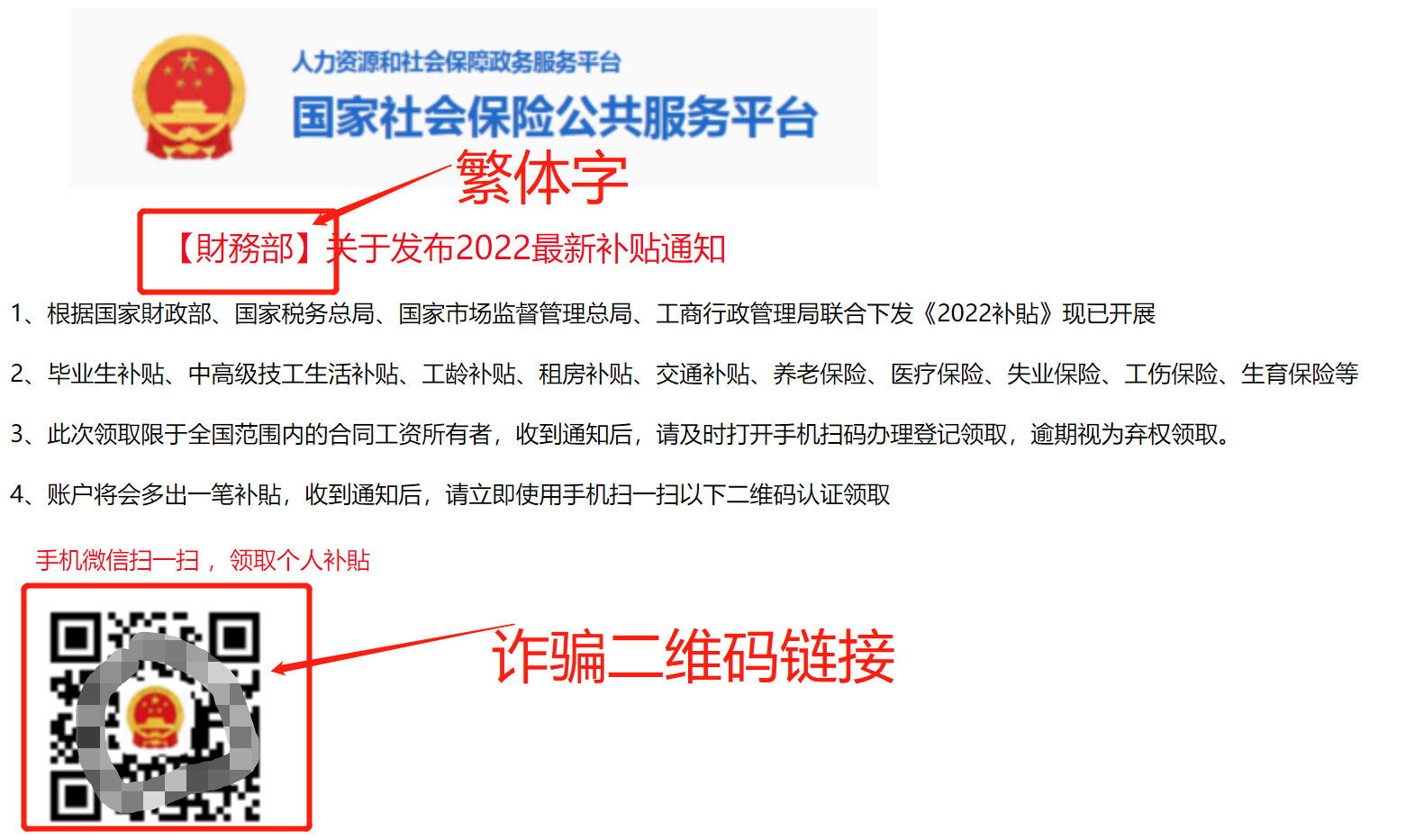


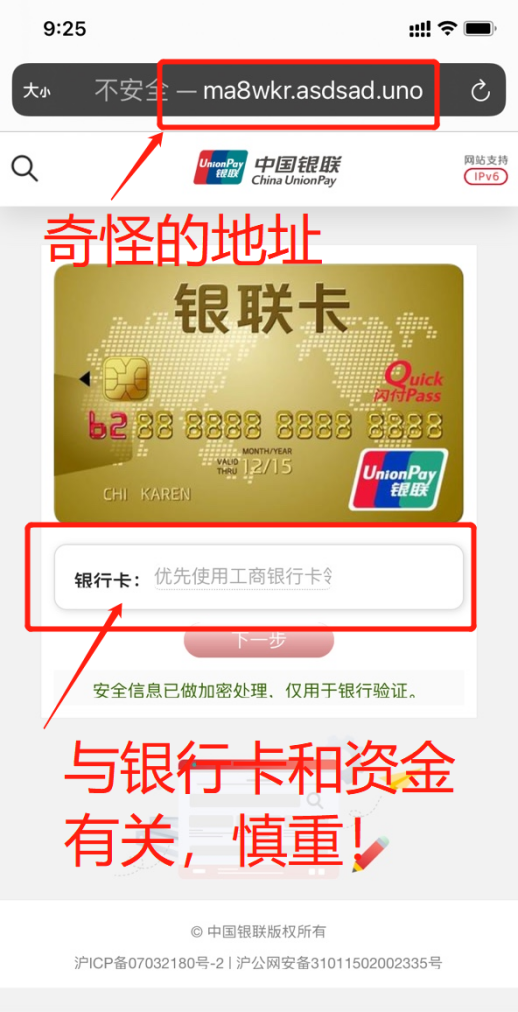
1. **认真核实**

如经以上判断都无法确定的，可直接与内容相关部门或人员电话联系或当面确认邮件内容的真实性。特别是与账号密码、个人信息、银行账号及资金相关内容。

如下图，该邮件为教师账号被盗后，发送的诈骗邮件。因是来自校内邮箱用户，所以邮件未进入垃圾邮件夹。邮件标题内容具有一定诱惑力但有一个繁体字（风险点），邮件内容为空（降低收件人防范意识），附件内容冒充国家部门，付二维码（诈骗链接）。







此类邮件前期隐蔽性较高，如无法确认可与发件人或发件部门联系（切勿使用邮件自带联系方式）。

诈骗方式层出不穷，希望大家认真阅读以上内容，掌握鉴别技巧，提高警惕，切勿上当受骗。如有实在难以分辨的，可电话咨询网络信息中心。

网络信息中心

2022.2.28