慎用『免密支付』功能 当心账户资金被盗刷

近年来，“免密支付”功能因其便捷性被广泛应用，它为群众带来便利的同时，也存在账户资金被盗刷的风险。寒亭公安分局相关民警提醒，网络购物过程中谨慎使用手机“免密支付”功能，避免因账户权限过度开放而引发资金损失问题。

□本报记者 王晓萌

“免密支付”有风险

“免密支付”功能易产生盗刷漏洞，主要有以下原因：

“免密支付”即“无需密码确认支付”，是部分支付平台或应用为提升支付便捷性推出的功能，用户开通后，单笔交易金额在一定限额内可直接扣款。然而，这一功能若被不法分子利用，可能带来严重安全隐患。

手机丢失或账号泄露时风险激增。若被他人获取账号或设备，通过“免密支付”功能可直接消费或购买虚拟服务，且无需二次验证。

小额免密累积大额损失。部分平台免密额度虽设单笔上限（如1000元），但短时间内高频次小额盗刷仍会造成较大经济损失。

隐蔽性强，难以及时察觉。盗刷交易通常通过绑定支付平台的虚拟服务（如游戏充值、App订阅）完成，或者在机主察觉不到的时段完成，消费者发现时往往已产生多笔扣款。

警方作出安全提示

为降低盗刷风险，消费者可采取以下措施：

非必要不开启“免密支付”功能

检查是否绑定支付宝、微信或银行卡，并关闭“免密支付”权限。若需保留部分免密服务，建议单独设置。另外定期检查授权应用，关闭不常用或不信任的第三方应用支付授权。

强化账户安全保护

设置高强度密码并注意更换。避免使用生日、连续数字等简单密码，开启双重认证功能，防止账号被他人恶意登录。

关闭非必要支付权限，尤其是iPhone用户如无需通过账户购买应用，可禁用相关功能。

谨慎使用公共WiFi，避免在公共网络环境下进行支付操作，防止网络钓鱼或数据截取。

养成定期对账习惯

及时查看电子账单，关注支付宝、微信或银行发送的扣款短信，发现不明消费立即核查。定期检查订阅服务，取消不再需要的自动续费项目。

对于遭遇盗刷后如何快速应对？民警介绍，若发现账户存在异常交易，首先，立即冻结支付渠道，通过银行客服、支付宝或微信平台紧急冻结关联账户，阻止后续扣款。其次，留存证据并投诉：保留盗刷记录截图、交易时间等信息，向支付平台投诉。若损失金额较大，需及时向公安机关报案，并配合提供相关证据材料。

警方提醒广大消费者，主动管理支付权限，切勿图方便忽视潜在风险。如遇消费纠纷，可拨打热线电话或通过“全国消协智慧315”平台进行维权或向公安机关报案。

安全大讲堂

安全生产莫大意 五大隐患需警惕

□本报记者 王晓萌

春季天气多变，很多不利于安全生产的因素凸显。为此，我市应急管理部门送上安全生产提示。

◆新人入场易出事

风险：大批新员工进入各企业生产一线和施工作业现场，由于不少人缺乏相关作业经验，且安全意识淡薄、安全技能不足，易引发生产安全事故。

提示：做好新员工安全教育培训，让其了解作业场所可能存在的职业危害因素；定期组织开展应急演练，教会新员工应急处置；为新员工提供安全防护用品、安排上岗前健康体检。

◆春困疲乏易大意

风险：春季人们易感到困倦疲乏，也就是常说的春困。

提示：在作业中，企业管理人员和作业负责人要密切注意作业人员的精神状态，尤其是在进行有限空间、高处、临时用电、吊装等作业时，防范事故发生。

◆大风天气易坠落

风险：春季大风天气多，易发生围墙坍塌、广告牌坠落、电力线路被损毁等事故。

提示：密切关注气象变化，遇大风、沙尘暴等恶劣天气，及时停止露天高处作业，做好室外防风措施。登高作业时间不宜过长，可实行轮流登高作业制度。

◆触电事故易发生

风险：春季昼夜温差大，电气设施设备易受潮，加之地面导电性增强，易发生触电事故。

提示：农村打井、春耕、春灌、盖房等临时用电增加，不可私拉乱接电线，要到当地供电所申请。严禁在高压线下方搭设临建、堆放材料和进行施工作业。

◆干燥多风易着火

风险：春季干燥多风，是火灾多发期。

提示：进入山林不吸烟、野炊，不带火源；各类动火作业要严格实行申请许可和现场监护制度；不随意焚烧秸秆、垃圾、纸张等易燃物；生产车间内禁止存放油漆、稀料、木材、塑料、填料等易燃物。

AI不是犯罪工具 合法使用才是正道

□本报记者 王晓萌

AI技术为提升工作效率以及解决许多其他问题提供了便利。然而，有些人因法律意识淡薄，利用AI技术盗取他人信息，陷入了网络犯罪的深渊。对此，潍城公安分局相关民警提醒市民，正确使用AI技术，严守法律红线。

典型案例

近日，公安网安部门侦破一起非法获取计算机信息系统数据案，犯罪嫌疑人胡某非法获取两万余条学生个人信息，后利用AI技术向其中的两千余名学生发送骚扰短信。

犯罪嫌疑人胡某是一名在校大学生，为寻求刺激、炫耀技术，通过之前发现的某小程序存在的技术漏洞，利用AI技术编写程序，将盗取的上千余名学生的手机号码在该小程序上批量注册账户，后将短信验证码篡改为违法内容发送至学生本人，对其进行短信骚扰。

目前，犯罪嫌疑人胡某对非法获取计算机信息系统数据罪供认不讳，案件正在进一步侦办中。

法条链接

《中华人民共和国刑法》第二百八十五条第二款指出，违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

《中华人民共和国网络安全法》第四十四条明确，任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

《中华人民共和国治安管理处罚法》第四十二条指出，多次发送淫秽、侮辱、恐吓或者其他信息，干扰他人正常生活的，处五日以下拘留或者五百元以下罚款；情节较重的，处五日以上十日以下拘留，可以并处五百元以下罚款。

警方提醒

民警表示，AI技术本为造福人类，而非犯罪的“帮凶”。广大市民要提高法律意识，正确使用AI技术，营造和谐清朗的网络空间。同时，要严守法律红线，不利用AI伪造公文、证件，不生成谣言、暴力等违法信息。

自觉抵制AI谣言，遇所谓“爆炸性新闻”做到“三不”：不轻信、不转发、不扩散。通过官方平台验证信息，发现AI谣言立即举报，保存证据协助溯源。