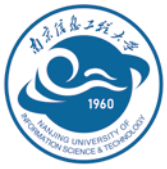


南京信息工程大学

Nanjing University of Information Science & Technology

防诈工作指南

保卫处

二〇二四年八月

序　言

近年来，随着电信网络技术的高速发展，网络购物、电子支付给人们生活带来巨大便利，同时也给电信网络诈骗犯罪带来可乘之机，电信网络诈骗案件呈多发高发态势。据国家权威部门统计，电信网络诈骗案件以每年20%到30%的速度增长，已成为我国当前最主要的侵财类犯罪方式，给高校师生员工造成了巨大的财产损失。2023 年,南京高校发生电信网络诈骗案件 7000 余起,共造成经济损失 4000 余万元，而且仍然呈上升趋势。其中，虚假购物类、游戏交易类、裸聊约炮类、冒充熟人类、兼职刷单类、中奖返利类、冒充客服类、冒充公检法类等 8 类案例是高校高发案件类型，高校师生正成为电诈受害对象增速最快的群体。

自 2023 年 8 月 30 日以来，学校成立防范电信网络诈骗工作专班，持续实行每周例会制度，将防范电信网络诈骗纳入“书记工程”，对被骗师生“一案一复盘”“一案一反查”，通过“暴风骤雨”“和风细雨”式宣

传教育，我校电信网络诈骗案件数量、被骗金额大幅下降。学校防范电信网络诈骗工作专班科学研判，决定从2024年秋季学期开始，学校防范电信网络诈骗工作转入“常态化”防范阶段，即把新生作为防诈工作重点，对教职工和老生采取针对性的提醒教育。

为实现“常态化”阶段我校电信网络诈骗案件稳定在低位运行目标，我们结合近几年防范工作实践，将电信网络诈骗的现状、发案形势、高发案件类型特点、防范方法、各级开展工作的内容和方法编纂成册，为各单位和全校师生常态化防诈工作提供行动指南，为学校常态化防范宣传教育提供有力支撑。

此手册通过诈骗手段剖析、典型案例回顾、心路历程反查、防诈预警提示、受骗人群类型分析等，详细介绍当前高校频发的电信网络诈骗手段，深层次挖掘电信网络诈骗利用的人性弱点，既从根源上进行分析，又从方法上加以指导，以此提升师生员工的防骗意识，为高校开展防范电信网络诈骗工作贡献南信大智慧与方案。

目　录

附件

1．什么是电信网络诈骗？

答：电信网络诈骗是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。

2．电信网络诈骗有哪些危害？

电信网络诈骗通常导致个人财产损失，严重时可能导致倾家荡产；不仅影响受害人的个人信誉，还对社会诚信体系产生负面影响；诈骗行为破坏了人与人之间的信任，使得人们在社交活动中变得谨慎小心，影响社会和谐；诈骗电话满天飞，给人的印象是中国到处都是骗子，国家的形象被电信诈骗的骗子们玷污，电信诈骗正在蚕食国家形象；加剧了社会负面现象的传播，诈骗分子利用人们的爱占小便宜、贪婪、好奇、恐慌等心理进行诈骗，导致受害人在情感上受到伤害，甚至可能诱发其他社会问题，如家庭纠纷、自杀等；电信网络诈骗犯罪往往涉及到多个地区，多为跨国犯罪，给公安机关打击犯罪带来难度。此外，诈骗分子通常采用虚假身份、隐蔽通讯手段等方式进行犯罪，导致法律秩序受到破坏。总之，电信网络诈骗对个人、社会和国家都造成了严重的危害。

3．电信网络诈骗危害如此严重，国家采取了哪些措施应对电信网络诈骗？

答：党中央高度重视打击治理电信网络诈骗工作，习近平总

书记先后多次作出重要批示指示，提出以人民为中心，统筹发展和安全，强化系统观念、法制思维，注重源头治理、综合治理，坚持齐抓共管、群防群治，全面落实打防管控各项措施和金融、通信、互联网等行业监管主体责任，加强法律制度建设，加强社会宣传教育防范，推进国际执法合作，坚决遏制此类犯罪多发高发态势，为建设更高水平的平安中国、法制中国做出更大贡献。

2022 年 9 月 2 日，第十三届全国人民代表大会常务委员会第三十六次会议通过了《反电信网络诈骗法》，为打击电信网络诈骗犯罪提供了有力的法律武器，使得执法机关能够依法对电信网络诈骗犯罪分子进行惩处，从而有效遏制电信网络诈骗犯罪的蔓延势头，铲除危害社会稳定的“毒瘤”，保护广大公民的财产安全。

4．驻宁高校、江北新区电信网络诈骗发案形势如何？

答：尽管各地各部门、学校开展了铺天盖地式的防范电信网络诈骗宣传教育，仍不时有师生被骗。2023 年驻宁 51 所高校发生电信网络诈骗案件 7000 余起，被骗金额达 4000 多万元；2023 年江北新区共发生电信网络诈骗约 3000 余起，被骗金额 2 亿多元。

5．我校近几年电信网络诈骗情况是怎样的？

答：我校 2021 年共发生电信网络诈骗 142 起，累计被骗金额×××万元；2022 年全校共发生电信网络诈骗 100 起，累计被骗

××万元；2023 年全校共发生电信网络诈骗 69 起，累计被骗××万元。师生在接受防诈宣传教育时，总认为电信网络诈骗不会发生在自己身上，不认真听取防诈宣传；自认为自己智商极高，能够轻易识别得了诈骗，可是，电信网络诈骗犯罪分子充分利用了部分大学生轻信、贪婪、大意、恐惧等心理弱点，师生在遭遇电信网络诈骗时，又识别不了诈骗套路，以至于电信网络诈骗案件总会不时发生。

6．被骗钱财都通过银行卡转账，骗子网络使用 IP 地址，为什么被骗钱财难以被追回？

答：（1）身份伪装：在网络黑市，大量丢失、被盗的第二代居民身份证被公然叫卖。黑市，为诈骗分子提供了源源不断的身份信息资源。对普通人来说，实名制是唯一身份认证，但对诈骗分子来说，实名制成为了规避风险的最佳手段之一，因为这些实名的身份信息都是买来的，虽然是真实的，但和诈骗分子没有一点关系。

（2）技术伪装： 在电信网络诈骗案件的侦办过程中，技术层面的伪装是最难突破的。我们经常会收到诈骗短信，最常用的就是伪基站群发器，只需一个笔记本电脑、一个软件、一个发射器，就可以向周边的手机用户发送编辑好的诈骗短信。如果单纯想靠手机定位抓人，非常困难。此外，浮动 IP 和改号平台也是诈骗分子较为常用的两种技术伪装手段。浮动 IP 就是利用网络跳

板不断掩盖真实 IP，利用虚假 IP 实施网络诈骗行为；改号平台是利用技术手段，掩盖真实号码，将电话改成任何号段，甚至是“110、119”等看似“正规”部门的服务电话号码。

（3）地域伪装：随着我国对电信网络诈骗的打击力度不断增强，诈骗犯罪集团都转移到了境外（缅北、柬埔寨、老挝、越南、台湾等地），电信诈骗的金主和其团队基本都在国外，根据我国很多地区反诈民警追踪的信息来看，大部分诈骗团伙的最终落脚点都在东南亚一带，东南亚已经不知不觉成为亚洲的“诈骗基地”，骗子都经过专业培训，熟练掌握反侦察技能，善于利用各种伪装，隐去一切可能会曝光自己身份的痕迹。虽然通过国际合作，跨国抓了一些诈骗团伙，但只是其中的一小部分。

（4）专业化的洗钱团队：诈骗团队之所以能在短时间内转移并洗白赃款，一个重要原因是拥有一支专业化的洗钱团队。他们能够在最短的时间内，将其他诈骗同行骗来的钱取出，并将赃款洗白。将银行卡上的一串串数字变成能装在口袋里的真金白银。集团各个层级的人组织严密、分工合作、随时响应，形成了一张无形却又强大的蜘蛛网，只要一有资金触网，立即就会在这张网络的作用下消失得无影无踪。在诈骗洗钱团队内部，其职责明确，一般分为五个层级。第一层称为“声佬”，专门负责打电话、发信息，让受害人上钩；第二层称为“接数佬”，负责连接“声佬”和下一层；第三层称为“刷机佬”，负责刷 POS 机把钱刷到网上结算中心；第四层称为“卡佬”，负责提供各种银行卡、信用卡、

第三方支付账号等等，用于赃款转移；第五层称为“取款仔”，专门负责取钱，有时也会花钱雇人取钱。五个层级之间分工明确，跨级之间互不认识，每个层级只能跟上一层对接，绝不允许越级与上上层联系。因此，即使“取款仔”一层被抓，一般也很难问出上一级的人是谁，更无法抓到上上一层，这给侦察工作带来了较大困难。

（5）错综复杂的拆分账： 诈骗分子在收到骗款后，会对骗款进行拆分转出，通过银行账户和第三方支付平台进行多次分散转账，最后再通过“取款仔”取现。受害人钱款进入到这一步后，很难证明资金权属和资金来源。有时诈骗分子也会找“水房”处理，“水房”这个词很多人可能第一次听，如它的字面意思一般，就是专门用来洗白赃款的新型犯罪窝点，用这样的方式洗白赃款，更快捷也更安全。一般“水房”都服务于多个诈骗团伙，最终使诈骗款项大多都流向海外账户，难以被追讨。

（6）诈骗团伙受地方保护：诈骗团伙盘踞在缅北、柬埔寨、老挝、迪拜等地，当地政府与诈骗团伙沆瀣一气，导致打击难、追赃难。缅北地方武装割据，山头林立，政府军每次前往征讨，都难以奏效。通过国家间引渡协议等都难以彻底打击电信网络诈骗犯罪。

7．学校内外有哪些防诈工作队伍？

答：学校内部

（1）学校层面：学校成立防范电信网络诈骗工作专班，由保

卫处、学生工作处、研究生工作部、国际教育学院、党委教师工作部、机关党委、总务处、校团委等部门负责人组成。

学校还成立了由 30 个安全网格长和 185 名社团成员组成的平安信大社团学生志愿者队伍，开展校级防诈宣传活动，重点落实防诈例会工作要求。

（2）二级单位层面：防范电信网络诈骗工作作为书记工程，各学院明确了专门负责人员。

（3）班级层面：每班设立 1 名安全网格员，全校共计 1016 名安全网格员。

（4）宿舍层面：宿舍长是本宿舍防诈工作责任人，有责任和义务及时发现并制止同宿舍同学被骗。

学校外部设有盘城派出所反诈预警专班（8 人）及学校与学生家长的家校联动机制。

8．盘城派出所反诈预警专班工作内容有哪些？

答：盘城派出所成立了由 1 名治安副所长牵头、8 名民警组成的反诈预警专班，专门从事资金预警工作。对于已经下载涉诈 APP 或者开始向诈骗账户转账的潜在受害人，公安部反诈预警平台下发核查指令至属地公安机关，反诈预警专班第一时间联系潜在受害人，核查遭遇电信网络诈骗情况，并对其开展专门反诈劝防，如组织观看反诈影视内容，宣防高校频发的 8 类电信网络诈骗类型，教育引导师生，避免继续上当受骗，达到及时止损的效果。

9．我校采取了哪些措施，帮助师生们守牢“钱袋子”？

答：我校成立防范电信网络诈骗工作专班（详见附件 1），实行每周例会制度，把防诈工作纳入“书记工程”，建立“网格化”管理体系，在全校设立 30 名（每个学院 1 名）安全网格长、1016 名安全网格员（不含教职工安全网格员），建立宿舍长防诈工作责任制，建立“一对一”结对子帮扶机制，打通防范电信网络诈骗宣传教育“最后一公里”，体现了“最温暖大学”的责任担当，帮助每名师生守好自己的“钱袋子”，践行“以生为本”“以人民为中心”服务理念。

我们结合大量工作实践发现，师生在遭遇电信网络诈骗时，并不是一蹴而就的，而是经历了类似于“钓鱼”过程，发布引流信息、勾引受害人、诱导受害人转账，被骗经历少则几十分钟多则几天甚至几个月。我校探索实施“按钮式”防诈工作法，建立防诈预警“按钮”体系，希望通过“按钮”体系主动施助、接受求助，将电信网络诈骗扼杀在萌芽状态。

10．每周例会制度是如何开展的？

答：每周一下午分管保卫副校长准时召开防范电信网络诈骗工作例会，上周被骗师生所在学院党委书记列席会议并报告相关工作情况，内保专班、保卫处、学生工作处、研究生工作部、国际教育学院、党委教师工作部、机关党委、总务处、校团委等

相关部门负责人参加会议。内保专班通报全市、全区高校电信网络诈骗案件发案形势，保卫处通报复盘反查情况，梳理工作中存在的问题，与会人员提出堵塞漏洞的对策，各职能部门从本条线落实相关亡羊补牢、防微杜渐工作方案。若上一周未发生诈骗警情，则本周不召开防诈例会。

11．什么是“按钮式”防诈工作法？

答：所谓“按钮”是设立在师生中间，便于向师生施助、接受师生求助的相关人员及其联系方式。一旦师生遭遇电信网络诈骗，“按钮”能够发挥作用，及时避免师生被骗，挽回损失。

12．“钮”有哪些？

答：（1）“一对一”结对子，双方互为钮；（2）宿舍：宿舍长；（3）班级：安全网格员、学生干部；（4）学院：辅导员、安全网格长；（5）校园：宿舍管理员、快递点工作人员以及关系密切的其他人；（6）学校：校园报警中心 58736110，保卫处防骗宣传教育老师徐蒙田 18651680803；（7）警方：盘城派出所 58732981，盘城派出所驻校民警孙跃 18913865881，江北新区公安分局驻校工作专班李警官 17721596268。

13．如何增强师生“按”意识？

通过经常性的防诈宣传活动，增强师生防诈意识，从而让师生在遇事时，主动求助。

一是说，学样职能部门及二级单位通过组织反诈讲座等多种形式向师生们宣讲防诈形势、注意防范的重点，辅导员、安全网格员利用课前、课后 3 分钟，主题班会、安全教育大会等契机，向师生们进行防诈宣传。

二是抄，全校师生全部亲自抄写《防范电信网络诈骗知晓书》（详见附件 2），诈骗发生的关键环节和被骗以后如何做，被列入必抄内容。

三是传，学校建立了 5 个安全网格员工作微信群，及时将防诈安排、防诈重点、重要提醒等最新动态信息，通过工作微信群推送给全校师生。

14．网格化管理体系是如何运作的？

答：学校在每个学院设立 1 名安全网格长，全校共计 30 名安全网格长：在安全网格长的基础上，每个学院设立了 1 名教师安全网格员，每个班级设立 1 名学生安全网格员，全校共设立了 1016 名学生安全网格员、76 名教职工安全网格员。为了便于工作，我们建立了 5 个安全网格员工作微信群，其中本科生安全网格员工作群 3 个（东苑、中苑、西苑），研究生安全网格员工作群 1 个，教职工安全网格员工作群 1 个。群内成员除了安全网格员外，还有分管校领导、保卫处防骗宣传教育老师、学工处（研工部）业务主管老师。对于发布到群内的防诈提示，各安全网格员及时转发，对于工作不积极的群，学工处（研工部）老师会及时提醒。

15．安全网格长工作职责有哪些？

答：安全网格长是各学院防诈工作联系人，由学院党委副书记推荐，主要服从学院领导安排，配合学院开展防诈宣传教育工作，业务上由保卫处负责指导。负责将学校防诈工作要求及时传达至本学院所有安全网格员；组织本学院安全网格员业务技能培训；督促安全网格员工作落实。接受本学院师生电信网络诈骗求助，对本学院师生电信网络诈骗预警劝阻，收集本学院师生遭遇的电信网络诈骗风险隐患，及时采取应对措施，防止本学院师生被骗。若本学院频发电信网络诈骗，安全网格长需参加平安信大社团骨干工作例会，报告相关工作开展情况，及时落实学校防诈例会工作要求。

16．安全网格员工作职责有哪些？

答：安全网格员负责及时转发安全网格员工作群内防诈、法制宣传教育提示；组织力量开展行之有效的防诈宣传教育活动；接受本班学生求助、主动向本班学生施助，防止本班学生被骗。对已经被骗的受害人，积极协调开展心理安抚。

17．宿舍长在防诈工作中有哪些职责？

答：宿舍长是推进防诈“最后一公里”落地落细的重要一员，负责本宿舍同学的防诈宣传教育；及时发现本宿舍同学宿舍内被骗行为，主动施助；接受本宿舍同学求助，帮助识别是否正在遭

遇电信网络诈骗。若本宿舍同学在宿舍内被骗，宿舍长有责任、有义务及时发现并止损。

18．什么是“一对一”结对子帮扶机制？

答：“一对一”结对子帮扶机制是打通防诈工作“最后一公里”的重要手段，也是设立在学生身边的防诈按钮。结对子就是以班级为单位，以自愿配对为主、组织配对为辅的原则，在本班两个同学之间建立“一对一”结对子朋辈帮扶机制。配对双方是相互救助、施助的第一对象，有相互求助、相互救助的责任和义务。重在鼓励同学之间互帮互助，防止上当受骗。若两人都识别不了电信网络诈骗，要主动通过有效途径进一步咨询核实。

19．如何发现身边人被骗？

答：当身边人有以下特征时，可能正在遭遇电信网络诈骗：

（1）长时间玩手机，神志投入，神情或焦躁或兴奋或叹息，变化无常；

（2）有意无意，炫耀有能轻松赚钱的门道；

（3）向周围同学借款，声称可以一夜暴富；

（4）一直在接打电话，神态紧张、眼神闪烁、行踪神秘；

（5）远离人群到密闭、安静的地方接打电话，同学联系却电话不接，信息不回。

当身边人有以上特征时，我们应特别关注、主动关心、及时施助。

20．发现可能被骗怎么办？

答：通常情况下，受害者发现自己可能被骗后，大脑思绪混乱、情绪懊恼，甚至不愿接受被骗的事实。此时应该稳住情绪，让自己镇定下来，立即做好以下几件事：

（1）立即停止任何交易，及时止损，切不可幻想对方退钱给你，否则只能越陷越深。

确认自己的财产损失，确认是否认识对方账号的主人。

（2）立即复盘，复盘被骗经过，时间、地点、人物、事由，清楚自己的钱原来在哪？是通过什么方式转出去的？每一笔被骗资金准确流出的时间、金额、自己的账号、对方的账号……

（3）立即报告，迅速梳理完上述问题后，拨打 58736110 或保卫处防骗宣传教育老师 18651680803 咨询求助。按照上述动作，受害者可以配合学校保卫处、校园警务室将涉案信息报告给警方，等待案件侦办结果。

21．对于反诈劝阻成功的行为，南京市公安局和学校会如何奖励？

答：首先，南京市见义勇为基金会会给予专项奖励。2023 年南京市公安局、南京市见义勇为基金会出台《南京市防范打击电信网络诈骗犯罪见义勇为专项奖励办法》，在全市范围内组织开展“全民反诈”专项奖励活动。其次，学校会对劝阻成功的师生给予“校园反诈先锋”荣誉表彰，并给予相应的物质奖励。

在本市行政区域内积极参与防范电信网络诈骗，经公安机关查证属实的，依据情节和贡献大小，由市、区见义勇为基金会给予奖励。

对主动发现、及时劝阻正在向电诈犯罪嫌疑人转账汇款、有效避免他人遭受财产损失或提供举报线索并查证属实的，将给予100-5000元不等的奖励。

22．哪些行为可以获得专项奖励？

答：（1）主动发现并及时劝阻、制止他人向电信网络诈骗犯罪嫌疑人转账汇款，有效避免他人遭受财产损失的；

（2）提供线索举报电信网络诈骗犯罪嫌疑人，协助公安机关破案或抓获电信网络诈骗犯罪嫌疑人的；

（3）提供线索协助抓获公安机关上网通缉的电信网络诈骗犯罪嫌疑人的；

（4）提供线索举报开贩涉通讯网络诈骗电话卡或银行卡，嫌疑人被采取刑事强制措施的；

（5）提供线索帮助公安机关抓获出境从事电信网络诈骗犯罪嫌疑人，嫌疑人被采取刑事强制措施的；

（6）提供线索帮助公安机关打掉电信网络诈骗犯罪窝点的；

（7）直接抓获电信网络诈骗犯罪嫌疑人或犯罪团伙，嫌疑人被采取刑事强制措施的。

23．防范电信网络诈骗必备利器有哪些？

（1） 国家反诈中心 APP，国家反诈中心 APP 是一款集诈骗预警提示、报案助手、线索举报、反诈宣传等多种功能于一体的手机软件，可以有效帮助用户识别预警诈骗信息、快速举报诈骗内容、高校提取电子证据、了解防骗技巧切实提升用户的识骗防骗能力。

（2）预警劝阻专线：96110，96110 是反诈预警专用号码，紧急劝阻预警极易被骗人员或正在被骗人员，发现群众正遭遇电信网络诈骗或者属于极易被骗人员，公安机关将通过该专线及时预警劝阻。如果遇到疑似电信网络诈骗活动，群众可以拨打该专线求助咨询。

（3）涉诈预警劝阻短信 12381,12381 系统可根据公安机关提供的涉案号码，利用大数据、人工智能等技术自动分析发现潜在被骗用户，并通过 12381 短信端口向用户发送预警短信，提示用户可能遭遇电信网络诈骗。

（4）全国移动电话卡“一证通查”，“一证通查”服务打通了 93 家省级基础电信企业和 39 家移动电信转售企业相关数据，师生只需要使用自己的居民身份证，即可通过线上线下多种渠道查询本人名下持有的全国移动电话卡数量，专用短信口 10699000 将在 48 小时内，向预留手机号反馈结果，真正实现了全国移动电话卡的统一便捷查询。

（5）云闪付 APP“一键查卡”，人民银行指导中国银联股份有限公司联合商业银行基于银行业统一 APP 云闪付试点“一键查卡”功能，打造统一查询途径，向境内公众提供银行卡数量、每张卡的银行名称、借贷记属性、脱敏卡号等信息的查询，在确保信息安全的前提下，便利公众掌握自己名下银行卡信息，强化自身银行卡管理。

（6）反诈名片，反诈名片是国家反诈中心、工信部反诈中心联合中国电信、中国移动、中国联通、中国信通院推出的一项反诈来电提醒服务。手机用户接听国家反诈部门的预警劝阻电话时，同步弹显国家反诈中心、工信部反诈中心温馨提示，让手机用户能够有效甄别号码真伪，快速、安心、接听反诈预警电话，大幅提升公安机关预警劝阻电话的接通率，更有效地预防电信网络诈骗犯罪发生。

（7）全国互联网账号“一证通查 2.0”，服务用户凭借手机号码和身份证号后六位，便可查询本人名下手机号码关联的互联网账号数量，切实解决防范用户不知情注册互联网账号等带来的涉诈风险。

24. “国家反诈中心”APP 如何下载使用？

答：下载方法一：长按识别下方的二维码直接下载“国家反诈中心”APP。

下载方法二：在安卓、苹果手机应用市场，搜索“国家反诈中心”即可下载。

“国家反诈中心”APP 如何注册？

（1）安装完成后进入“国家反诈中心”APP

（2）注册账号

如遇到“未能找到指定主机名的服务器”问题，解决方案是：切换网络、飞行模式后恢复或重启。

（3）完善个人信息（注意：实名验证后，才能使用 APP 全部功能）

（4）在 APP 首页，打开“来电预警”

（5）点击立即开启，请授权：照片访问、视频访问等所有权限，就可以开启诈骗预警功能

（6）开启后，就可以受到诈骗预警保护

25. 如何关闭境外呼入功能？

答：（1）移动用户：拨打 10086，或关注“中国移动高频骚扰防护”微信公众号：——业务设置——骚扰拦截设置——国际及港澳台拦截——开启。

（2）电信用户：拨打 10000 号，或关注“天翼防骚扰”微信公众号——个人中心——我的专属服务——智能拦截设置——国际长途电话——开启。

（3）联通用户：拨打 10010，或关注“智慧沃服务”微信公众号——手机管家——号段拦截——“国际电话”智能拦截设置。

26. 开展了这么多反诈宣传，为什么依旧有师生被骗？

答：第一，这些诈骗分子极其善于洞察人性，利用一些人轻信、贪婪、大意、恐惧的心理，让其在不知不觉中陷入他们精心设计的圈套。

第二，个别师生侥幸心理严重，总认为电信网络诈骗不会发生在自己身上，自以为是，不主动学习防诈知识，对于诈骗的思想认知与诈骗现实存在巨大偏差，仍然不重视防范电信网络诈骗。部分被骗师生认为电信网络诈骗会通过打电话、找借口等方式，诱骗钱财。殊不知，在网络购物、网络中奖等网络行为中，悄无声息地就容易遭遇电信网络诈骗，面对历次宣传，而从不入心入

脑，至今对非正常购物（不通过网络购物平台买卖物品、脱离购物平台交易）、网络中奖、网络兼职、刷单返利等诈骗陷阱明知故入。

第三，师生个人信息泄露严重，给了诈骗分子可乘之机。个别师生没有警惕性，随意扫描二维码，随意点击链接，轻易泄露个人信息，给了诈骗分子大量可乘之机。

27. 哪些人容易被骗？

答：我们通过梳理分析被骗群体发现：有钱的学生会被骗，贫困的学生也会被骗（和钱多少没关系）；本科生有被骗，硕士生有被骗，博士生有被骗，教师也有被骗（和学历、智商没关系）；男生有被骗，女生也有被骗（和性别没关系）。

我们通过一案一复盘、一案一反查发现被骗的师生往往有如下特点：爱占小便宜、想不劳而获、自律意识差、侥幸心理严重、无所事事、毫不设防、自以为聪明、做贼心虚、想破财免灾、好奇心重、胆小怕事、心有不甘、轻信他人等特点。（详见附件 4）

28. 电信网络诈骗发案这么高、被骗钱款那么多，被骗钱财难以被追回，高校师生应该如何加强防范呢？

答：电信网络诈骗万变不离其宗，最终的落脚点就是受害人的钱，只要做到“要钱不给，给钱不要”，心不贪、利不占还是能防得住的，做好防诈需要做到三不一多：陌生来电不轻信、未

知链接不点击、个人信息不透露、转账汇款多核实。电信网络诈骗是完全可以防得住的，特别提醒网络购物一定要全链条在网络购物平台完成。另外要熟练掌握高校师生常见诈骗类型特点（详见附件 3），做到举一反三。

29．出租、出售本人名下账户有哪些危害？

答：《反电信网络诈骗法》第三十一条 任何单位和个人不得非法买卖、出租、出借电话卡、物联网卡、电信线路、短信端口、银行账户、支付账户、互联网账号等，不得提供实名核验帮助，不得假冒他人身份或者虚构代理关系开立上述卡、账户、账号等。

《反电信网络诈骗法》第四十四条 违反本法第三十一条规定的，没收违法所得，由公安机关处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足二万元的，处二十万元以下罚款，情节严重的，并处十五日以下拘留。

典型案例：2023 年 1 月 30 日至 2 月 1 日，庞某（17 岁，高校在校学生）在明知犯罪嫌疑人利用网络实施犯罪的情况下，仍提供其持有的银行卡及手机银行 APP 帮助其收款、转账，为诈骗团伙提供人脸验证、支付结算等服务，交易金额达 67 万余元，庞某获利 4900 元。庞某等人已被依法处罚。

30．什么是“两卡”犯罪？

答：“两卡”犯罪，是指非法出租、出售、买卖“两卡”的违法犯罪活动，其中“两卡”指的是手机卡和银行卡。非法买卖个人电话卡、银行账户和企业对公账户，可能涉嫌帮助信息网络犯罪活动罪，妨害信用卡管理罪，侵犯公民个人信息罪，掩饰、隐瞒犯罪所得、犯罪所得收益罪，诈骗罪，直接带来牢狱之灾。极个别师生出租、出售手机卡、银行卡，帮“网络好友”（诈骗分子）代收款，从而沦为“两卡”类“帮信罪”的工具人，被公安机关处理，给人生染上污点。

31．非法制造、买卖、使用 GOIP、猫池等设备，为实施电信网络诈骗活动提供支持或帮助，会面临什么处罚？

答：《反电信网络诈骗法》第十四条 任何单位和个人不得非法制造、买卖、提供或者使用下列设备、软件：

（一）电话卡批量插入设备；

（二）具有改变主叫号码、虚拟拨号、互联网电话违规接入公用电信网络等功能的设备、软件；

（三）批量账号、网络地址自动切换系统，批量接收提供短信验证语音验证的平台；

（四）其他用于实施电信网络诈骗等违法犯罪的设备、软件。

《反电信网络诈骗法》第二十五条 任何单位和个人不得为

他人实施电信网络诈骗活动提供下列支持或者帮助。

（一）出售、提供个人信息；

（二）帮助他人通过虚拟货币交易等方式洗钱；

（三）其他为电信网络诈骗活动提供支持或者帮助的行为。

《反电信网络诈骗法》第四十二条 违反本法第十四条、第二十五条规定的，没收违法所得，由公安机关或者有关主管部门处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足五万元的，处五十万元以下罚款，情节严重的，由公安机关并处十五日以下拘留。

典型案例：2022 年 12 月，董某通过境外聊天软件进入组织发送诈骗短信的群组，根据群主提供的信息向他人发送诈骗短信，发送完成后将操作过程的录屏及支付宝收款码提供给群主，便能获得 20-150 元不等的佣金。2022 年 12 月至 2023 年 2 月，董某组织本地多名中学生多次帮助诈骗分子发送诈骗短信，共计获利 3779 元。董某及其他涉嫌违法的学生被公安机关依法处以行政处罚。

《反电信网络诈骗法》第三十六条 对前往电信网络诈骗活动严重地区的人员，出境活动存在重大涉电信网络诈骗活动嫌疑的，移民管理机构可以决定不准其出境。因从事电信网络诈骗活动受过刑事处罚的人员，设区的市级以上公安机关可以根据犯罪情况和预防再犯罪的需要，决定自处罚完毕之日起六个月至三年以内不准其出境，并通知移民管理机构执行。

32．我校下一步防诈工作的基本思路是什么？

答：通过全校师生的共同努力，我校防诈工作取得明显成效，发案数量、被骗金额大幅下降。经防诈专班研究，从 2024 年 9 月起，学校防诈工作转入常态化阶段，仍然作为二级单位党组织书记工作范畴，但由学工书记主抓，把新生的防诈作为重点，教工和老生主要根据发案情况针对性地开展提醒工作。本《指南》资料作为常态化防诈工作的主要指导。

33. 如何发挥“枫桥经验”，预防电信网络诈骗？

答：学校开展“枫桥经验”进校园（详见附件 5），对校园警务室业务功能进行拓展，由提供基础法律服务增加法律专家（律师）服务，工作日每周三下午邀请法律专家（律师）为师生开展法制宣传教育，预防案事件（尤其是电信网络诈骗）发生，也是学校探索更高水平的平安校园创建创新性举措。

“枫桥经验”进校园，就是要充分发挥党建引领作用，坚持“组织建设走在工作前，预测工作走在预防前，预防工作走在调解前，调解工作走在激化前”，实现“小事不出院，大事不出校，矛盾不上交”，充分发挥各学院、各单位党支部战斗堡垒作用，调动各级党组织、分工会工作人员、安全网格员等主体主观能动性，“以师生为本”，服务下沉，加强本学院、本单位内部预防案事件（尤其防范电信网络诈骗）工作，早发现，早调解，早预防，将电信网络诈骗案件扼杀在萌芽状态。

附件 1：

南京信息工程大学文件

校发〔2023〕153 号

关于成立南京信息工程大学防范电信网络诈骗工作专班的通知

各单位：

为深入学习贯彻习近平总书记关于打击治理电信网络诈骗犯罪的重要指示精神，进一步增强保护全校师生员工财产安全的能力，切实压降我校电信网络诈骗发案数量，根据《省教育厅关于成立打击治理电信网络诈骗“百日行动”工作专班的通知》要求，经研究决定，成立南京信息工程大学防范电信网络诈骗工作专班。成员名单如下：

组　长：韦忠平　金自康

副组长：周显信　袁　敏　李　健　付兆锋

成　员：（按姓氏笔画排序）

丁媛媛　马革兰　王贤芳　巨传友　文亚平　成　芳

朱伟军　朱庆峰　关　辉　孙再春　李　岩　李　霞
杨春艳　吴广宇　张广磊　张明菊　张京波　张昳丽
陈一虹　陈相勤　周淑琴　周　斌　庞章军　屈家安
俞书平　耿小雷　贾　冰　徐志勇　殷跃峰　郭　雨
崔维军　章　胜　葛昕明　蒋元春　焦　冶　詹筱茹

专班办公室设在保卫处，负责专班日常工作。工作职责为全面统筹我校预防电信网络诈骗“百日行动”各项工作；督促各单位落实工作任务，指导开展形式灵活多样的反诈防诈宣传；加强与党委教师工作部、研究生工作部、学生工作部、国际教育学院等部门的协同，定期研究解决工作推进中遇到的突出问题；承办各级主管部门打击治理电信网络诈骗交办的其他事项。

南京信息工程大学
2023 年 8 月 31 日

南京信息工程大学党委校长办公室　　2023 年 8 月 31 日印发

附件 2：南京信息工程大学防范电信网络诈骗知晓书

学院：_____班级：_____ 辅导员：_____

防范电信网络诈骗，我已知晓并做到**（请在横线上抄写括号内文字）**：

1.非正常购物类：受害人通过抖音、微博、QQ、微信等添加好友，委托代购，支付完成后，对方始终不发货。嫌疑人通过“闲鱼 APP”购物平台、QQ 或微信向受害人发送其它虚假收付款二维码或链接（与官网高仿），付款成功后，杳无音讯而被骗。

（购物到正规平台，所有平台之外的链接、交易都有被骗风险）

2.裸聊敲诈、做刷单任务、免费约炮类：骗子通过短信、电话、网络广告等形式发布黄色网站或招嫖信息，诱导受害人点击链接或者下载 APP（含有木马病毒）观看视频，通过木马病毒盗取其手机内通讯录，利用裸聊视频/照片、个人头像 PS 合成不雅视频，以发送给亲友或曝光相要挟。诈骗分子在各大社交平台发布黄色网站信息或免费找小姐信息，称可以提供各种“服务”，诱导受害人下载 APP。然后客服主动联系称需注册账号购买套餐才可以使用，接着让受害人领取刷单、押注任务，并称“会有导师带领，包赚不亏还可以换取美女免费上门机会”。

（**所有裸聊约炮都是诈骗**）

3.冒充特定人员类：冒充熟人/领导：骗子通过盗取熟人（家长/同学/老师/领导等）信息（/QQ/微信/微博号等）联系受害人，谎称亲属车祸、生病住院，微信转账受限，发送银行卡转账给受害人截图（PS），请受害人帮忙中转费用，或自己因各种原因无法付费，请受害人代为付款。

（骗子编造各种借口不方便接听电话，遇到“熟人”要求转账时，务必与“熟人”核实）

4.冒充公检法：骗子通过电话联系，自称是公检法、社保局等政府机关，以受害人身份信息被盗用，涉嫌洗钱、贩毒、社保/医保卡账号诈骗等为由，甚至发送虚假“警官证”“通缉令”，要求受害人将其资金转入指定“所谓安全账户”配合调查或转账至指定账户验证清白进行诈骗。

（**真正公检法不会电话、网络视频办案**）

5.冒充金融、快递、网购平台客服类：骗子通过非法渠道获取买家订单信息，冒充电商客服人员以“商品质量问题召回、退款”或以“取消 VIP 铂金会员业务，否则每月扣款”“快递物品丢失给予赔偿”为由诱导受害人进行转账行骗；或冒充淘宝、支付宝等银行、金融客服人员准确报出学生个人信息，以“注销清空贷款记录及账号、账户冻结/解冻、影响个人征信、花呗开通提

额、注销京东白条、利用借贷产品提高积分等或以缴纳手续费、保障金等为由行骗。骗子伪造虚假网站，要求受害人填写银行账号、密码、验证码等信息。

（**验证码就等于银行取款密码，为啥你要把你的银行卡密码交给别人？**）

6.游戏装备类：受害人在正规平台交易买卖游戏账号或装备时，骗子隐藏在正规平台内冒充买家或卖家，以平台手续费太贵等为由，要求在平台之外交易行骗。

（**所有平台之外的买卖游戏装备都有被骗风险**）

7.刷单、刷信誉、做任务返利类：骗子在网上发布虚假兼职广告，以“操作简单、日赚百元”为诱饵，诱导受害人添加“QQ 客服”或者下载虚假 APP，进行预先垫资类“网络刷单”；如今刷单已经演变为给抖音点赞、做简单手工赚快钱，免费领礼品等方式，把当事人拉到群里，群内的人都是“骗子的托”，在群里做任务奖励红包。前期返蝇头小利给受害人，然后继续刷单骗大钱。

（**做简单任务返还小利为诱饵，预先垫资的都是诈骗，所有刷单都是诈骗**）

8.诱导虚假投资理财、“杀猪盘”类诈骗：骗子通过网络交友，塑造虚假“白富美”“高富帅”形象，通过嘘寒问暖、虚假恋爱获取信任，抓住受害人心理，诱导其虚假投资理财类网站或APP 投资，甚至诱骗受害人网络贷款再投资。通过“取得信任、怂恿投资，小额回报、大量投入、无法提现、销声匿迹”“放长线、骗大钱”方式实施诈骗。网上炒比特币等虚拟货币、虚拟数字藏品击鼓传花式买卖也是诈骗！

（所有没见过面的人邀请你投资的，都有被骗风险）

9.网络贷款、校园贷类诈骗：骗子利用急用钱、月息低、无抵押/担保、或仅提供个人身份信息及照片等理由，轻松下款，利用先预交利息、手续费、保证金、保险费等名义诈骗。骗子会花言巧语提供 APP 贷款链接，诱骗受害人网络贷款，贷款是需要还的！校园贷已让不少学生陷入高利贷，无法正常学习和生活！

10.其它诈骗类别：点击带有诱惑性/异常不明链接的信息，下载 APP 投资、聊天软件被引诱转账行骗；钓鱼红包、木马病毒植入盗取受害人淘宝/支付宝/银行卡等账号、密码等个人信息后行骗；利用奖助学金、女生九价疫苗等名义行骗；其它引诱型、恐吓型、传销型、非常规校园上门推销型、代写代发论文/科研实践报告类诈骗等。

（转账汇款前，一定要核实，坚持：要钱不给，给钱不要，方能免受诈骗之害）

理性消费，克制贪念。涉嫌被诈骗，及时向辅导员、学校保卫处求助！（校园报警电话 025-58736110，学校防骗专员徐蒙田 18651680803）

莫让身边其他同学被骗的经历在你身上重演，请您反思：

刷单返利前问问自己：动动手指就能致富的好事情，为啥那些比你聪明还辛苦工作的人不去做？

遇到自称客服理赔时问问自己：是对方主动退款理赔，为啥要你自己一大堆操作，到底谁主动？为啥理赔还要自己出钱？

冒充公检法的人出示通缉令时问问自己：抓人还要提前通知，是生怕坏人跑路跑得不够快？

投资理财前问问自己：他和你非亲非故，为什么要带你挣钱？那么高的回报率如果是真的，为什么银行还没有倒闭？

非正常网络购物前问问自己：为什么不走有保证的正规平台购物？为什么要轻易相信网络上的陌生人？为什么点重新发送的、可能带有木马病毒的链接？

网恋的时候问问自己：肤白貌美的美女和帅气逼人的帅哥，为啥找不到对象，偏偏要在网上找你谈恋爱？

陌生人问你要验证码的时候问问自己：验证码就等于银行取款密码；为啥你要把你的银行密码交给别人?

（把银行卡、手机卡出租、出借、出卖给他人涉嫌什么犯罪？答：帮助信息网络犯罪活动罪。法律面前人人平等，务必知法懂法守法，大学生违法犯罪同样受到法律惩处；自媒体网络发言需谨慎，不妄议国家方针、政策，不参与、不传播情况不明的敏感热点话题，不随意发布侵犯他人隐私的信息，引发负面影响或不良后果将予以追究。）

学号：_____ 知晓人：_____ 年 月 日

附件 3：高校频发的电信网络诈骗类型及特点

1、非正常购物类：受害人浏览“闲鱼”“ 小红书”“拼多多”等交易平台，看到博主出售相关物品信息，诈骗分子通常以各种理由诱导添加微信、QQ 好友脱离平台交易，诱导不在平台完成付款（发送虚假链接、微信转账、银行卡、支付宝转账方式），诱导买家提前收货后杳无音讯（始终不发货），选择网络购物平台需谨慎。

2、裸聊敲诈、色情引诱+做刷单任务诈骗类：骗子通过短信、电话、网络广告等形式发布黄色网站或招嫖信息，诱导受害人点击链接或者下载 APP（含有木马病毒）观看视频，骗子通过木马病毒盗取手机内通讯录，利用裸聊视频/照片、个人头像 PS 合成不雅视频，以发送给亲友或曝光相要挟，受害人为了维护声誉没完没了地被骗子敲诈勒索支付封口费。或以同城免费约会约炮等为诱饵，诱导做刷单（押注）任务换取美女免费上门，对男生诱惑极大，极易上当受骗。【裸聊招嫖既违反法律、又违背道德还违反校纪校规】

3、游戏装备类：受害人在正规平台交易买卖游戏账号或装备时，骗子冒充平台客服以需要缴纳手续费、保证金为由，要求在平台之外交易。所有脱离平台的交易（交易猫、闲鱼等交易平台）都有被骗风险！

4、冒充特定人员类：冒充熟人/领导：骗子通过盗取熟人（家

长/同学/老师/领导/亲戚等）QQ、微博，联系受害人，谎称车祸、生病住院、话费充值、开会不方便接听电话等理由，要求借款转账或代为付款等。

冒充公检法等政府工作人员：一般通过电话联系，自称是公检法、社保局、银保监会等政府机关工作人员，以受害人身份信息被盗用，涉嫌洗钱、贩毒、社保/医保卡账号诈骗或涉嫌影响个人征信等为由，甚至发送虚假“警官证”“通缉令”，要求受害人将其资金转入指定所谓“安全账户”配合调查进行诈骗。实际上公检法不会电话、网络视频办案。

冒充金融、快递、网购平台客服类：骗子通过非法渠道获取买家订单信息，冒充电商客服人员以“商品质量问题召回、退款”或以“取消VIP铂金会员业务”“快递物品丢失给予三倍补偿”为由行骗；或称报警人名下网贷平台（微粒贷、京东白条、京东金条等）利率违反国家标准，如不按照要求调整会影响报警人个人征信，诱骗报警人将资金转入其指定的“所谓安全银行账户”行骗；或冒充京东、淘宝、支付宝等银行、金融客服人员准确报出报警人个人信息，以“注销清空贷款记录及账号、账户冻结/解冻、影响个人征信、花呗开通提额、利用借贷产品提高积分等或以缴纳手续费、保障金等为由进行诈骗。

5、刷单（刷信誉）做任务返利类：骗子在网上发布虚假兼职广告，以“操作简单、日赚百元”为诱饵，诱导受害人添加“QQ客服”或者下载虚假APP，进行预先垫资类“网络刷单”，如今

刷单已经演变为给抖音点赞、做简单手工赚快钱，免费领礼品等方式把当事人拉到群里（其实群内多数人是“骗子的托”或骗子操纵多个 QQ 或微信聊天），在群里做任务给红包。前期返蝇头小利给受害人，然后继续刷单骗大钱。所有刷单做任务都是诈骗！

6、诱导虚假投资理财、“杀猪盘”类诈骗：骗子通过网络交友，塑造虚假“白富美”“高富帅”形象，通过嘘寒问暖、虚假恋爱获取信任，诱导受害人在虚假投资理财类网站或 APP 投资，甚至诱骗受害人网络贷款再投资。通过“取得信任、怂恿投资（小额回报）、大量投入、无法提现、销声匿迹”“放长线、骗大钱”方式实施诈骗。网上炒比特币等虚拟货币、虚拟数字藏品击鼓传花式买卖也是诈骗！

7、中奖返利类诈骗：骗子以报警人所购物品中奖返利为由，但须先交个人所得税、转账流水、快递费等各种名义的费用行骗。或以免费会员、免费赠送礼物为诱饵，诱导受害人点击链接后，会被自动免密支付，之后联系退款又被以验证退款渠道为由再次被骗。

8、新型诈骗类型：

（1）免费收到快递礼品（洗衣液、电饭锅、加湿器、杯子等）并扫二维码或刷单获取更多礼品、返利类诈骗：收到上述之类物品的快递（本人并未购买任何东西），同时附有扫码宣传单，请千万不要主动扫码添加对方为好友，否则会被拉入各种福利群，群内有大量的托，声称完成刷单任务可以返利，前期一两笔可能

小额提现，后期对方会要求完成几连单操作才能返现，不少人会继续转账，从而上当受骗，请务必警惕这种非常具有迷惑性的刷单诈骗引流方式，不要贪小便宜造成大损失！

（2）手机屏幕共享类诈骗：利用可以看到“受害人手机共享屏幕”的会议软件（钉钉会议、腾讯会议、ZOOM 等）与受害人语音通话，指挥受害人操作。骗子会利用公检法或各种客服平台，利用掌握的受害人信息实施精准诈骗。不和陌生人实行共享屏幕，否则所有操作都会被骗子获取，密码、验证码等一览无遗。

（3）支付宝小荷包类诈骗：非正常购物类买卖物品时，骗子让受害人联系“客服”收款，客服以流水不足为由，诱导受害人开通小荷包，将钱转入“小荷包”内，邀请“客服”加入“小荷包”，“客服”将受害人转入“小荷包”的钱转走，受害人发现被骗后，骗子已将受害人拉黑。（小荷包可以实现一起攒钱，一起花钱，债务共同承担）

（4）刷单形式多样化诈骗：所有刷单都是诈骗，千万不要被蝇头小利迷惑，最终报警人投入的本金都要不回来。刷单诈骗的引流骗术：a、社交 APP 上看到兼职广告“给淘宝、京东撰写商品评论，佣金秒到账”或抖音点赞奖励。b、刷到直播间带有“做兼职赚零花” 此类音频信息时， 切勿加 QQ 联系。c、美女主播称扫码打赏可线下约会诱导下载诈骗软件。d、未按要求操作导致数据瘫痪，需补单修复才可提现。e、色情博彩类诈骗。 “约爱平台客服称完成‘猜字任务’方可约见美女”“激活四次即可获

得美女信息”“完成三次数据认证，得终生服务卡”是色情博彩诱导转账行骗惯用骗术。f、诱导点击网络“色情”弹窗约爱导师指导做任务得返利的，一定是诈骗。

9、其它诈骗类别：无故收到并点击带有诱惑性/异常不明链接的信息，下载 APP 投资、聊天或转账；钓鱼红包、木马病毒植入盗取受害人淘宝/支付宝/银行卡等账号、密码后行骗；利用奖助学金、女生九价疫苗等名义转账或获取个人信息类；其它可能出现的哄骗引诱型、恐吓型、传销陷阱型、上门推销型、代写代发论文/科研实践报告类诈骗等。

附件 4：致全校师生防范电信网络诈骗的一封信

亲爱的老师和同学们：

近些年，学校各级虽然想了很多办法，但师生电信网络被骗仍有发生，损失还不小，让人很心疼。我们时常在想，骗子的骗术并不高明，那为什么会被骗、到底是哪些人容易受骗呢？通过梳理分析发现：有钱的同学会被骗，贫困的同学也会被骗，说明与钱多钱少没关系；本科生有被骗，硕士生有被骗，博士生有被骗，教工也有被骗，说明与智商学历没关系；男生有被骗，女生也有被骗，说明与性别没关系；有年轻人被骗，也有老年人被骗，说明与年龄没关系。那么到底与什么有关系呢？通过一案一复盘、一案一反查，我们总结归纳出十二类易被骗人群，给师生们看一看，请大家对照着反思反思：你是这十二类人吗？你想当这十二类人吗？如不想，希望您能耐心看完，用心体会，谨防又双叒叕落入诈骗的陷阱。

类型一：想不劳而获或爱占便宜的人

2023 年 11 月 30 日晚上 7 点左右，一名大四女生收到微信“好友”信息：现在有一个购物活动，下单后便可获得抽奖的机会。该“好友”说自己的微信好友有 4000 多个顾客，并发送了证明微信“好友”数量的视频，让该生进一步相信其有足够的顾客群体，该生放松了戒备。随后，该“好友”又发送截图证明“幸

运粉丝”确实有抽奖获益的情况，该“好友”说活动就剩最后几天了。自此，该生为了获得抽奖机会，按照“好友”引导加链接、点小程序、预付税款、看对方的视频、看截图、加另一个好友、扫二维码等，进行了一系列操作，最终被骗 10297 元。

【启示】天上不会掉馅饼，想“不劳而获”必然会被骗。切记不要相信任何带有“抽奖”“免费”“赠送”“领奖”等活动。小红书免费领物、短视频平台免费领优惠券、领奖等都是此类骗局。贪占便宜也是如此。比如刷单返利就是最常见的诈骗形式。一开始施以小利，让你尝到甜头，同时也暗示你“投得越多赚得越多”，等你真正投了一大笔的时候，再也见不到返利了。刷单返利诈骗的变化形式多样，“杀猪盘”、以色情为诱饵下注（投资）、做简单充值任务赚快钱、需要先交钱的网络兼职都属于此类。虽然人人都知道这些都是骗局，但总有人不信，往往会被一开始的小恩小惠诱惑着掉入陷阱，想想挺可悲的。

类型二：自律意识差的人

2024 年 3 月，某学院一名大四男生点击了一个链接，下载了一款名为“TAP”的约炮 APP，对方让该生充值会员，该生向对方提供的二维码扫码支付了 68 元注册会员。进入 APP 后客服让该生完成 3 次认证就可以加“小姐”的微信，接着就给了该生 3 个任务，第一个任务是在这个 APP 群里向对方提供的二维码付款 88 元，第二个任务向对方提供的二维码扫码转账 198 元，第三个

任务向对方提供的二维码扫码转账 998 元。并在线上签一份所谓的约炮之后互不打扰对方生活协议，该生全部照做。第三次付款后，骗子以操作失误、充值错误等各种理由让其继续转帐，最后该生被骗 25353 元。

【启示】该案例过程较长，不再详述。无外乎是给你描述多么美妙，让你欲罢不能，一次次转帐，最终一场空。年轻人应增强自律意识，洁身自好，抵制不良信息和诱惑。对于网络上的不道德和违法行为，应保持距离，切莫参与，约炮招嫖等不仅被骗风险极高，即使成功也是违反法律、道德、校纪校规，后果是很严重的。

类型三：无所事事的人

2024 年 6 月 15 日 17:00 左右，某学院研二男生利用休闲时间在工位打三国杀游戏（因自己科研进展顺利，小论文已经基本完成），游戏中有人添加他为游戏好友，主动向他购买“三国杀”游戏账号，他答应出售，买家添加他为 QQ 好友（此时已经脱离游戏平台），买家建了包含他本人和买家两个人的 QQ 群，买家愿以 1100 元购买他的游戏账号，双方约定通过交易猫平台交易。为了完成这笔交易，在“好友”引导下，该生通过看虚假截图、联系客服、加链接等一系列操作，最终被骗 2000 元。

【启示】有的同学或考试结束、或论文完成、或周末休闲、或课程不紧、或一时对学习不感兴趣，总之有大把时间，没事就

刷网。要知道，常在河边走，难免不湿鞋。所有被骗案例中，无所事事、整天刷网、盲目点击的人占有较大比例。请此类人员重视主业，把主要时间用到学习工作上，业余生活也应该丰富多彩，不要全部放在刷手机上。

类型四：毫不设防的人

2023 年 3 月的一天，一名大二男生接到陌生电话，称他的快递丢失，需要给其理赔，并通过“微议 Pro”APP 进行语音会议，开通屏幕共享功能，全程引导他进行操作。对方以验证理赔银行账户真实性为由，诱导该生使用农业银行 APP 向指定银行账户转账 2495 元，该生按要求操作后许久，意识到被骗，为时已晚。

【启示】这样的案例其实很低级，陌生电话怎能轻信？即使信一回，理赔也是他给你赔钱，怎么向你要钱呢？请大家对要求下载不明软件、共享屏幕、建立小荷包或购买购物卡等行为，应视为高度可疑，极有可能是诈骗行为。除此案例外，还有中奖充值兑奖、冒充熟人、冒充同学、冒充领导、冒充老师、冒充客服等类似的情况。

类型五：自以为聪明的人

【案例】2024 年 4 月，某学院大二学生在小红书上看到有关免费领手机的消息，抱着试试看的心态，加入了一个 QQ 群（其实群内都是骗子），骗子 1 联系他，免费领手机需要支付 50 元

运费，问他能否接受？“别信他们，他们都是骗子，我曾在抖音成功领取过手机。”骗子 2 跟该同学说，并发送了领取手机的照片，成功获取了他的信任，并推荐只需要 20 元运费不需要一分钱就可以获得 iPhone15 的 QQ，对方声称是深圳苹果专营店的，以需要核实信息为由，让其在应用商店下载 Todusk 软件并开启屏幕共享，之后骗子诱导受害人打开银行软件查询流水，要受害人用支付宝扫描跳转陌生链接，又让该同学将对方报的数字（其实是转账）填入方框内，该生先后填入 9 次数字，直至其银行卡内仅剩 70 多元时，对方把他 QQ 拉黑才意识到被骗，累计被骗 2 万多元。

【启示】我是大学生，不可能受骗。大家要知道，现在的诈骗分子不是一个人，而是一个团伙。在这个团伙中，有策划、剧本、导演、化妆、演员，有网络专家、理财专家、心理专家等等，他们既有分工又有配合，组织严密技能高超，一旦落入圈套，你所谓的聪明将不堪一击！自以为聪明的人们，醒醒吧！

类型六：胆小怕事的人

2024 年 2 月 18 日深夜，某学院大四男生在宿舍上网时收到陌生 QQ 好友申请，加好友后对方发来该生的身份信息、银行卡账户跟密码和不雅视频与照片，要求该生向其转账，否则会将其隐私内容传播出去,该生担心自身名誉，先后 5 次向对方转账，累计被骗 33096 元。

【启示】目前，AI 技术高度发达，诈骗分子用此技术进行换脸、模拟声音、制作照片，甚至制作视频，用以要挟目标人群。遇到此类现象，大家切不可以破财消灾的办法来处理，那样只会越陷越深。只要内心坦荡，就不怕鬼敲门。除此案例外，诈骗分子还会以公检法办案等形式予以恐吓。请不要轻信，公安办案一般都是面对面，法律文书也是在面对面办案之后才会发出，大家切勿上当。

类型七：做“贼”心虚的人

2023 年 3 月 9 日凌晨 1 时许，大三男生通过手机推特与对方认识，对方用推特发送“凤凰城”APP（可以访问并窃取通讯录、相册等信息），谎称有情趣视频让该生下载注册，该生下载注册后，通过 QQ 视频与对方进行裸聊，不久对方以将裸聊视频发送给他的通讯录好友相要挟，勒索该生转账 1000 元。

【启示】骗子利用裸聊截图进行恐吓，让你破财消灾，这种案例在学生中的发生比例比较大。在网络社交中，不要轻信陌生人的邀请，尤其涉及裸聊等私密内容时，需警惕色情诈骗。一旦遭遇诈骗，如被裸聊视频、照片等威胁，要及时与校园警务室或校园报警中心 58736110 联系，一定要相信学校和警察会以很稳妥的办法帮助你的。从根本上来讲，规范个人生活，严守纪律法规，才能从根源上杜绝此类敲诈。

类型八：好奇心重的人

2024 年 6 月 17 日 12:00 左右，某同学在小红书上看到一个帖子“可以免费领取裙子”（对方说可以随机挑款式，该生好奇想看看有什么款式），如愿领取可以添加图片里的 QQ 群。该生就按照指引添加了 QQ 群，群内有一张图片，显示“企业代付操作流程”（该生不知道企业代付，好奇想看看到底是什么），她按照操作流程进行操作。首先是打开淘宝，搜索“充值中心”，然后在充值中心给她自己的手机号充值了 300 元后，去找 QQ 群里的管理员，让管理员把 300 元退给她。管理员让她跟财务联系，财务说需要银行卡过一遍流水，方能退钱（此时该生陷入了对方的圈套），然后就发给该生一个二维码。该生扫描之后，显示是转账页面，对方跟她说需要输入 3000 元，该生按照要求转账 3000 元后，财务跟她说，流水还没结束，又接连 3 次分别让她输入 2 次 3000 元、1 次 4000 元。该生转账后，等待对方退款，对方给她发送了一个退款成功的记录截图，上面显示给该生转账 13328 元，该生一直刷新银行卡页面，始终没收到对方的退款。累计被骗 13000 元。

【启示】这位同学从好奇进入骗局，到被骗结束。为了退款需要过流水，这是什么道理？过一次还不够，还要多次，不被骗才怪！好奇心害死人！除此案例外，还有游戏代练要求玩家先行支付部分费用、免费赠送游戏皮肤等类似的骗局。

类型九：心有不甘的人

2023 年 9 月，某学院大一新生在开学来校报到的路上，参加刷单返现，前几笔返现占了小便宜，后来被套住 1000 多元心有不甘，打算扳本后，就不再刷单了，最终越陷越深，被骗 37500 元。

【启示】很多被骗者都是在被骗一定数额后心有不甘，总想把本钱扳回来，被骗越多越想扳本，甚至到处借钱、网络贷款来扳本。希望大家在发现被骗后悬崖勒马，虽然损失了一些，但能避免更大损失。

类型十：轻信他人的人

2024 年 6 月 26 日 9：23，某学院研二女生在南信大租房 QQ 群内看到有人发帖：帮房东发布招租信息，有需要的添加房东 QQ。该生打算换房所以添加了房东 QQ 为好友。房东给她发送了盘新家园 2 栋房间的视频，该生看了以后，认为房子非常干净，所以同意租赁（并未看房、并未与房东见面，就相信了对方），双方约定房租每月 900 元，按付三押一方式付款。房东说还有另外 5 人预约看房，让她先交订金 400 元，为其预留房源。房东又发送了一个竞争租房的转账记录截图，声称竞争者预付了 4 个月的房租，让她补齐 4 个月的房租。她给对方支付宝转账 3200 元，补齐了 4 个月的房租。房东紧接着又发送了竞争者半年房租的截图，

让他补齐半年的房租。该生打算给对方补齐剩余房租，等到支付宝、微信给对方转账时，微信和支付宝分别提示转账有风险，就没有转账了。再向房东联系看房，发现自己已被拉黑。

【启示】为了师生的学习、生活方便，校园有一些热心者建立了一些民间服务群，如二手货交易市场QQ群、南信大租房QQ、阳光代跑、考试作弊群等。诈骗分子利用技术手段潜入群里，甚至潜入官方工作群，以提供服务为由实施诈骗。避免此类被骗的最简单有效方法，就是向同学、辅导员、校内防诈群核实一下即可，寻求校外服务也应如此。

类型十一：装睡不醒的人

2023年9月12日，一大二女生将自己的《开间小屋》游戏账号挂在平台上出售，在平台内有一“买家”跟她联系打算买她的账号，添加她QQ好友，通过QQ跟她说想在交易猫（通过应用商店可以下载，打消受害人疑虑）交易，待该生将游戏账号以500元价格挂在交易猫后，对方发来一张成功付款的记录截图，并发来一张二维码（客服），请该生扫码与“客服”联系发货，“客服”要求缴纳2000元保障金才能进行下一步业务，该生起初不想交保障金，“买方”称也支付了2000元保障金并且支付了游戏账号费用，此时，同宿舍同学提醒她，买卖游戏账号可能是电信网络诈骗，但该生自以为是，缴纳了2000元保障金，客服又以“信用值太低”导致资金冻结为由，要求转账8000元解冻金，

该生没有这么多钱，跟“买方”商量双方各交 4000 元，该生又交了 4000 元，累计被骗 6000 元。

该生已经多次参与防范电信网络诈骗宣传教育，签订并且朗读了防诈骗知晓书，屡次接受教育而不入心入脑。

【启示】在与被骗师生复盘反查时，被骗人说的最多的一句话就是“在没被骗之前，总认为电信网络诈骗不会发生在自己身上，抄写、朗读防诈骗知晓书时，就想赶紧应付了事，每次看到群内发布的防骗消息时，扫一眼又是防诈骗的，根本不去阅读内容，更甭提举一反三了”，历次防骗宣教都不当回事，即使有人提醒，他们也听不进去，这些装睡不醒的，公安说称他们为“天生被骗人”。希望大家不要做这样的人。

类型十二：想快速致富的人

某高校女教工 2021 年准备卖一套房子，因为房子面积大、不好卖，就将自己的个人信息和房产信息挂到“58 同城”网上，有好多人陆陆续续地给她打电话咨询买房子的事情。到了 2022 年 5 月底，有一个陌生男人添加她为微信好友，她以为是要买房子的，但是经过聊天得知他是卖房子的，微信里经常跟她谈论卖房子的事。平日里经常嘘寒问暖，聊的时间长了就有好感了，双方建立了男女朋友关系。对方让该教职工帮助操作一个 APP，做一些投资，声称自己家亲戚在里面是操盘手，按亲戚说的时候买进、卖出，非常赚钱。该教工心想自己跟他认识这么久了，又建立了

男女朋友关系，就想跟着对方赚些钱。对方教她下载了一个名为“OCBC”投资理财 APP，让她在上面买黄金期货，前几笔都获利了。该教职工想赚更多钱，于是就在 2022 年 6 月 9 日，投资了 176 万到这个 APP 客服提供的银行卡号，6 月 10 日投资了 120 万左右，6 月 11 日投资了 100 万左右，等到要退出时，出现 APP 提示系统有漏洞，无法提现，累计被骗 300 多万。

【启示】这是一个外校老师的案例，我校曾经也发生过教职工理财被骗的案例。手头有些余钱，做些投资理财很正常。但快速致富、一夜暴富的心理本身就有问题，即使有这样的好事也是违法的（当然炒股例外，但炒股的风险也大）。快速致富、一夜暴富的想法要不得，如果碰到有人提供这样的机会，也不能相信，肯定是骗局！

老师们、同学们：以上这十二个被骗类型，并没有涵盖所有被骗类型，有的被骗案件，是上述十二种因素中的好几个因素综合发挥作用而引发的。据公安同志讲，被抓获的诈骗分子自信地说，63 种款式（骗局），总有一款适合你。

面对电信网络诈骗，仅仅依赖学校的力量是远远不够的。请大家切记：电信诈骗的终极目标是“钱”，只要我们牢牢抓住“钱”这个核心要点，不但做到“要钱不给”，还要做到“给钱不要”（给你小钱是为了要你的大钱），就能护好自己的“钱袋子”。为此，规范自己的电话和上网行为：不轻易相信陌生人的电话、短信或邮件等信息，不随意点击陌生链接，不轻易透露个人信息

和银行卡信息，任何交易都在正规平台上完成，这样，就不会给诈骗分子以可乘之机！

最后，提醒大家在遇到可疑情况特别是在转帐打款前慎重再慎重，一定要及时向周边人（饭搭子、结对人、网格员、辅导员等）咨询求救，相信会得到帮助的。

祝愿每位师生都能擦亮慧眼，守住自己的“钱袋子”！

南京信息工程大学团委 保卫处

2024 年 7 月

附件 5：关于“枫桥经验进校园”的通知

各学院、各单位：

枫桥经验是 20 世纪 60 年代初期，浙江省诸暨县（现诸暨市）枫桥镇干部群众创造的“发动和依靠群众，坚持矛盾不上交，就地解决，实现捕人少，治安好”的经验。习近平总书记要求“坚持和发展好新时代枫桥经验，为推进更高水平的平安中国作出新的更大贡献”。今年上半年，学校保卫处、工会、法学与公共管理学院、学校有关部门与江北新区公检法司等单位以党建为引领，在中苑基嘉楼警务室设立“枫桥经验工作站” （电话：58699778、58731657），每周三下午邀请法律专家为师生提供法律咨询、矛盾调解、法律服务，积极主动化解校内矛盾纠纷。为不断创新发展新时代“枫桥经验”，发挥党建引领作用，坚持“组织建设走在工作前，预防工作走在事发前，调解工作走在激化前”，实现“小事不出院，大事不出校，矛盾不上交”，推进更高水平的平安校园建设，经研究，现将“枫桥经验进校园”相关事项通知如下：

一、学校部门统筹协调

保卫处负责统筹协调推进枫桥经验进校园各项工作，工会充分发挥桥梁纽带作用，依法维护教职工的合法权益，教师工作部、离退休办、学工处、研工部、国际教育学院等相关职能部门分别负责工作对象涉法问题、矛盾纠纷化解、预防案件情况汇总、上情下达、下情上达、集体会商等指导工作。

二、二级单位主动工作

各学院、各单位党组织充分发挥党建引领作用，调动安全工作人员、分工会工作人员的主观能动性，坚持以“以师生为本”，服务下沉，加强本学院、本单位内部矛盾纠纷化解、涉法事件排查、预防案事件，要把预防电信网络诈骗纳入平安校园建设重要内容，做到问题早发现，早调解，早预防。对于排查出的隐患风险、矛盾纠纷、案发事件，坚持“本学院、本单位自己能解决的，自己解决；解决不了的，汇报给机关所属部门和主管部门”的原则，实现“小事不出院，大事不出校，矛盾不上交”的任务目标。

三、校地形成联动机制

学校积极协同江北新区综合治理局、人民法院、人民检察院、公安分局、律师协会建立“联防、联处、联创”机制，开展法律法规宣传，联动处置突发事件，协同调处矛盾纠纷，共创共建平安校园。学校持续关注校情、改善民生、发展民主、维护安全、促进和谐，调集校内校外各种资源把矛盾和纠纷尽可能地化解在学校内。

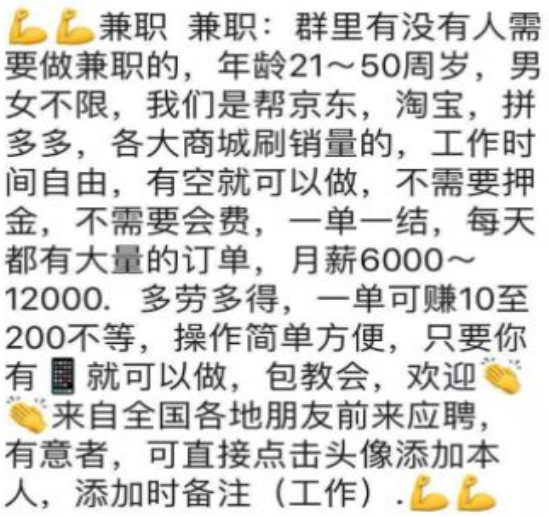
保卫处 工会 法学与公共管理学院

2024 年 7 月 21 日

附件 6：南京信息工程大学“慧眼识诈”能力测验

一．单选题（共 40 题，每题 1 分）

1．有人发送兼职刷单广告，下面说法正确的是（　　）。



A 这么轻松的网络兼职，赶紧试试

B 京东、淘宝、拼多多是正规购物平台，因此可以放心刷单

C 这是典型的刷单返现诈骗，不要轻信，更不要参与

D 有福同享，这么好的兼职大家一起试试

2．学生刘某接到自称是上海市公安局警察的电话，说他涉嫌犯罪，并让他登录网站查看网络通缉令。对方称刘某名下的一笔账户存在非法交易，要依法对他的账户及所有交易进行监管审查，请他将账户内全部资金于限定期限内转移至指定安全账户。下面

说法正确的是（　　）。

上海市虹口区人民检察院

刑事通缉命令

案号：2016年度(侦)字0212号

姓名	赵[illegible]	性别	男	
身份证号码	320382198811[illegible]	出生日期	1988年11月21日	
户籍地	江苏省 徐州市 邳州市	职业	张保 原法戊钱堂	

通缉个案内容

案件保密级别：

二级保密案件，指自通风报信，泄露案情者，将判处最严厉刑责，泄密罪最高可处三年以下六个月以上有期徒刑。

简要案情：

此人涉及重大金融刑事案件，与犯罪主嫌 张保 共谋作为同伙，提供银行帐户协助嫌犯进行违法洗钱犯罪活动，涉案情节特别严重，最高人民检察院二级检察官下令交由经侦科 高峰 科长通报上海市上海港公安局成立专案组负责侦办此案。

备注：

《公安部B级通缉令》对抓获犯罪逃犯或者提供关键线索的有功单位或个人，由公安部给予奖励，其家属不得窝藏、隐瞒此人犯罪资产，经发现作为共犯处理。

应解送处所	上海市公安局刑侦大队配合押解至上海市虹口拘留所
附　　记	全国公安机关及当地公安部门予以配合捉拿涉案嫌疑人逮捕归案。

经侦科科长　高[illegible]

二级检察官　张宝[illegible]

中华人民共和国上海市人民检察院

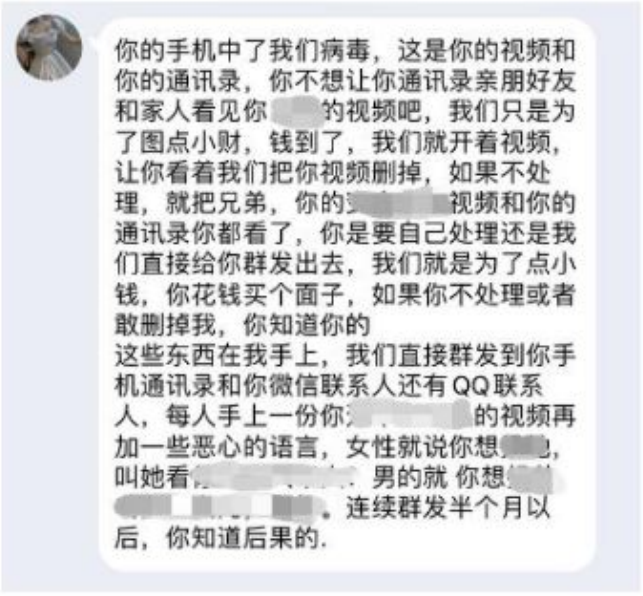
A 相信对方，并配合警察的调查

B 为了自证清白，应该尽快将全部资产转移到安全账户

C 警察不会骗人，对于对方下达的指令要坚信不疑

D 公安不会电话或网络办案，这是典型的冒充公检法诈骗，千万不要转账

3. 小马遭遇了裸聊敲诈，对方向他发送了以下信息，正确的做法是（　　）。



A 立刻转账，保护个人声誉

B 这件事太丢脸了，不能让别人知道，所以不要报警

C 坚决不转账，立刻向学校保卫处或公安机关求助

D 少转一些钱，先稳住对方再说

4. 如果你在网上预定了一张火车票，随后接到自称是票务工作人员的电话，告知你交易出现问题，需要申请退款并发送了一条含有退款链接的短信，你会怎么做？（　　）。

A 随手点开链接，按指令操作

B 登录官网或拨打 12306 核实

C 订票情况说的很准确，点开

D 服务挺到位，点开链接看看

5．小丽在淘宝上购买了一件价值 200 元的衣服后，接到了一个陌生电话，对方自称是淘宝客服，声称其购买的衣服存在质量问题，将赔付她 300 元。客服称已经通过支付宝“备用金”向其转了 500 元，需要小丽退还多收的 200 元。根据对方的指导，小丽的卡上果然多了 500 元。对方称，由于小丽个人原因导致理赔通道无法关闭，如果不关闭每个月都会扣除 2000 元，因此需要小丽从贷款平台贷款转入指定账户关闭理赔通道，然后再将钱退还回去。如果你是小丽，应该怎么做（　　）。

A 既然是淘宝客服打来的电话，就应该按照对方说的去做

B 这是天上掉馅饼的好事，不要白不要

C 联系淘宝官方客服，警惕购物退款诈骗

D 既然 500 元都提现到银行卡上了，就应该相信客服，贷款转入指定账户，关闭理赔通道

6. 你被同学拉入一个“活动通知群”，自称是教务处老师的人说：为了拓展大家的知识，提升同学们的综合素质，学校将和培训机构开展合作，请群内的学生邀请本班同学加入 QQ 群。你该怎么做？（　　）。

A 这个是好事儿，按照老师说的做

B 既然是同学拉进来的，就不用担心

C 反正是免费课程，学学总不是坏处

D 为防止网络诈骗，不要轻信加入陌生 QQ 群，也不要拉别人入群；如果是学校组织的活动，相关部门肯定会通过学院来通知，因此，这个教务处老师肯定是假冒的

7．东东收到短信“代办大额信用卡，无抵押，额度 5 万元起。有需要的请联系李经理 138********”，做法正确的是？（　　）。

A 这可能是诈骗陷阱，不予理会

B 无抵押且额度较高，赶快办一张

C 打电话过去咨询后再决定是否办理

D 反正不需要抵押，可以办一张试试

8．以下关于出租、出借、出售个人银行账户的表述，正确的是?（　　）。

A 账户出租、出借、出售之后，发生法律纠纷与我无关

B 银行账户属于个人私有财产，账户所有人可以自主决定出租、出借、出售

C 出租、出借、出售账户给亲人或朋友，肯定不会有问题的

D 出租、出借、出售银行账户是违法行为，严重影响个人征信记录，且要承担相应的法律责任

9. 阿华在游戏充值后，收到一条短信：“由于您填写的信息有误，之前充值金额已被冻结，请回拨此号码进行解冻操作。”，正确的是做法是？（　　）。

A 这是游戏充值诈骗，回拨过去看看对方想要怎么行骗

B 这是游戏充值诈骗，不予理会

C 应该是自己充值时操作有误，立刻回拨电话进行解冻操作

D 回拨电话后，在对方提供的网站中重新填写自己的账户密码

10. 刘某是要毕业的大学生，愁于毕业设计的作业，偶然间看到同学群里有人提供代写代做服务，于是刘某立刻添加对方为好友并且按照对方要求支付了劳务费，然而却没有拿到代写好的作业，且无法联系上对方。此时刘某才意识到自己上当受骗，他接下来应该怎么做？（　　）。

A 立刻向学校保卫处或公安机关报警

B 自认倒霉

C 自己的行为违纪，不报警忍气吞声

D 再找其他人代写

11．学生刘某在网上与女网友聊天，并互加 QQ 好友。对方称自己是女主播，并发裸露的私密照片，同时要求刘某下载某直播 APP（实为木马软件）。刘某按照对方要求下载软件后，并未发现任何信息，但他的手机通讯录已被上传。随后，女网友通过 QQ 与刘某进行在线裸聊，并录下整个过程。不久，女网友以裸体视频照片要挟付某转账 3888 元，否则将照片发给他通讯录里的成员。刘某接下来该怎么做？（　　）。

A 先转一点点钱，稳住对方再说

B 3888 元不算多，可以按照对方的要求转账，总之坚决不能让不雅视频泄漏出去

C 跟骗子说自己没钱，用真情打动对方

D 保持镇静，不要转账，保存和对方的聊天记录和下载的 APP，向学校辅导员、保卫处或公安机关报警

12．李某接到电话，称其参与微博转发抽奖活动，中了特等奖十万元，但需缴纳个人所得税后才可领奖，他该怎么办？（　　）。

A 立即与对方联系

B 通过对方提供的官方网站进行查询是否中奖

C 按对方提示缴纳个人所得税后等待领奖

D 这是诈骗电话，不要相信，同时告诫周围好友加以防范

13. 学生小方接到境外来电，对方称自己是某金融平台客服，由于小方有一笔校园贷款账户未注销，将影响其个人征信。客服称受中国银监会的委托，可以帮助小方注销校园贷。随后，客服发送了一张下方的图片，要求小方将自己的银行账户余额和网贷平台借款转入指定账户来注销校园贷账户。下面说法正确的是（　　）。

A 该文件有中国银监会盖章认证，因此可以相信对方

B 不怕一万，就怕万一，如果自己曾经真贷过款，就可以按照对方要求进行操作

C 这是典型的注销校园贷款账户诈骗，骗子以虚假的授权书和个人征信截图为幌子，骗取受害人信任，因此要立刻挂断电话、不要转账，立即向学校或公安机关报警

D 感到慌乱，询问对方如何注销校园贷

14．网络赌博中庄家永远不会输的“秘诀”是（　　）。

A 参与者普遍运气不好

B 庄家较参与者更为熟悉游戏规则

C 庄家“网络出千”，可以在后台直接修改赔率

D 玄学，很难讲

15．96110 是什么电话号码？（　　）。

A 遇难求救全国统一报警平台

B 反电信网络诈骗专用号码

C 全国统一短信报警电话

D 全国统一森林火警电话

16．你这个月生活费紧张，一直在找兼职。一天下午，在宿舍里你收到了一条兼职刷单的短信：刷单后公司将会返还商品费用和 5%左右的佣金，刷越多返越多。如果你刷 50 元返 52.5 元，那么刷 5000 元会返多少？（　　）。

A 250 元

B 2500 元

C 0 元

D 5250 元

17. 小马发现拼多多 APP 上有砍价免费拿活动，但缺少助力无法提现，遂到 QQ 群搜索“拼多多代砍”，并添加了一名“代砍人员”。该“代砍人员”发送给小马一个付款二维码，并告知小马此二维码为拼多多付款程序的破解程序，按照程序给定指示完成不扣费付款即可拿到拼多多的活动礼品。小马信以为真，进行转账操作，最终被骗了 400 元。小马接下来该怎么做？（　　）。

A 400 元太少，报案了怕警察不受理，应该主动联系该诈骗分子，继续转账以达到公安机关立案标准，方便抓捕诈骗分子

B 保留 QQ 聊天记录等证据并立即向保卫处或公安部门报案

C 吃一堑长一智，这次自认倒霉，全当花钱买了个教训

D 此代砍不靠谱可再找一位

18. 小胡收到一条信息，内容是:只要在“蚂蚁花呗”“借呗”等贷款平台套现转给我，就可以立即获得 10%的月利息，次月到期还款前归还本金。小胡认为这是遇到了生财之道，当其套现转款后，不光没有返现，就连电话也打不通了。（　　）。

A 不着急，等待下个月再查看利息的到账情况

B 反正钱不是小胡用的，因此不用管

C 这是网络投资理财诈骗，马上向学校保卫处或 110 报案

D 自认倒霉，不让别人知道，避免被嘲笑

19．关于“约炮”，下列说法不正确的是（　　）。

A “约炮”容易得艾滋、梅毒等性病

B 就算对方知根知底，也不可以“约炮”

C 这是不正当不安全的行为，应当杜绝

D “约炮”不用花钱，相比于“嫖娼”而言更省钱是好事

20．小李刚考上大学，入学前几天，她接到一个电话，对方自称是政府工作人员，能说出她的姓名并知道她刚考上了某某大学。对方表示，其家庭情况符合国家相关政策，现在要给她发放“助学金”5000 元。这时小李正确的做法是（　　）。

A 根据对方要求登录某网站申领助学金

B 根据对方指示到 ATM 机上进行操作领取助学金

C 按照对方要求提供自己的身份证号、银行账号、联系电话等信息

D 不要轻信，挂断电话，向相关政府部门进行核实

21．你接到一个自称是你老师的电话，对方说：“你明天早上到我办公室。”第二天一早，你又接到那位老师的来电：“我现在在院里开会，你过来一趟，顺便帮我买两个信封。”当你来到院里致电老师后，老师说他出去办事了。老师接着说，他现在约了上级领导在吃饭，需要钱“打点”一下，让你先打点钱过去，回头再还给你。你应该（　　）。

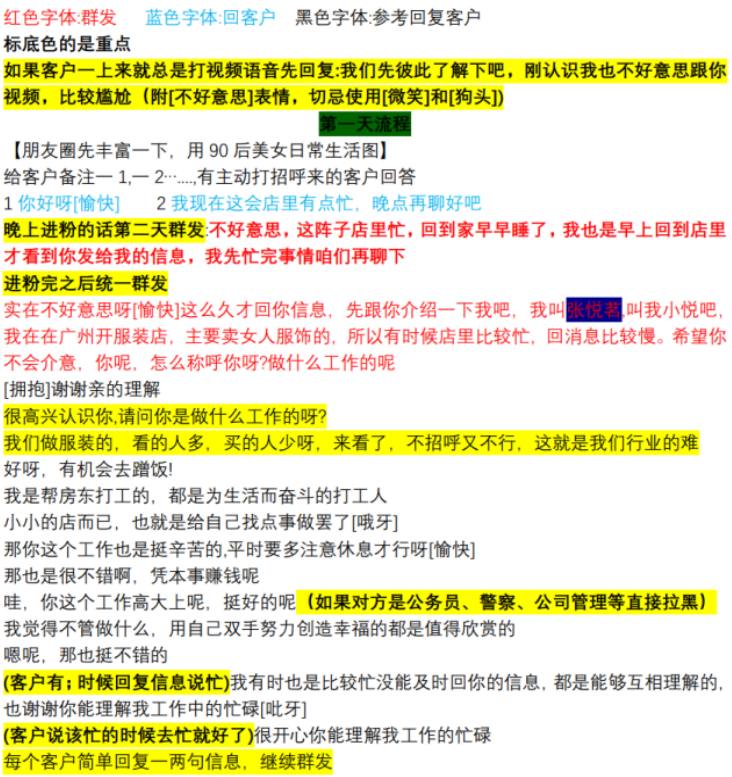
A 既然老师有急用，应该助人为乐，直接汇钱

B 如果跟这个老师比较熟悉，就可以汇款

C 这是典型的冒充身份诈骗，应该立即挂断电话，向学校或公安部门举报

D 先给一点敷衍下

22．根据图片内容，下列选项中说法错误的是？（　　）。



A 网络交友需谨慎，诈骗往往来敲门

B 这是普通的戏剧剧本，在现实生活中一般是不会遇见的

C 诈骗是团队作战，诈骗手段防不胜防，因此我们更应当提高警惕

D 这是经典的杀猪盘类诈骗的脚本

23．小明想利用课余时间赚取零花钱，某天他加入了“推广任务”兼职群，在群内看到了如图所示的兼职任务，以下说法正确的是？（　　）。

A 抖音是正规平台，因此这份兼职工作一定不会是骗局

B 完成推广任务后若收到佣金，则可以相信这份兼职工作是正规的

C 在“兼职”过程中，应当配合接待员，完成对方的要求

D “抖音任务”的实质很有可能是刷单诈骗，应当退出该群

24．小张是某校非全日制研究生，因床位紧张，学校未安排统一住宿。为方便学习生活，小张在学校百度贴吧发布求租床位的帖子，不久有一名自称是该校本科生的人联系了小张，并出示了他的校园卡、宿舍及床铺照片。对方说自己因为实习，住在校外，可以将床位租给小张，并要求小张先付 1000 元定金。下面说法正确的是（　　）。

A 私下里租用床位违反学校住宿管理规定，因此不可取，另外对方身份很难确定，搞不好就是诈骗分子

B 只要学生信息和校园卡是真的，就可信

C 只要宿舍信息和宿舍照片是真的，就可信

D 为确保安全，最好让对方写个收条

25．关于“裸聊”，说法错误的是（　　）。

A 在日常网上社交活动中，如果遇到有陌生女子主动添加联系方式和邀约时，首先要自觉提高警惕，洁身自爱，以免不法分子有可乘之机

B 不要轻易相信并接受陌生人的“激情”邀请，不要轻易安装陌生人发来的 APP

C 一旦遇到类似“裸聊”敲诈勒索发生时，一定要冷静分析，不回复对方信息，不接受私了，不转账，不删除，立即并坚持报警处理，防止上当受骗而导致经济损失

D 为防止“裸聊”视频流出，受害人应第一时间花钱消灾

26．以下不属于游戏装备诈骗套路的是（　　）。

A 骗子登录各种游戏交易平台、贴吧、Q 群、论坛等，寻找游戏装备卖家，然后留下自己的 QQ 号

B 骗子声称“无息贷款”，以证明还款能力为由，要求被害人打钱

C 当 QQ 联系上以后，骗子首先假装很关心装备的情况，接着再讨价还价，让卖家信以为真

D 骗子伪造一个支付页面，让卖家误以为资金已交到第三方监管手中，安全有保障

27．一日刘某闲来无事，便在聊天软件上寻找乐趣，他通过附近的人等途径添加了许多身材火辣的美女，其中一位自称已成年的女子，在聊天中声称可以提供“特殊服务”，并与刘某约好在某酒店进行色情交易。当刘某到达约定酒店再联系对方时，被要求先付“诚意金”800 元，刘某打款过去后对方却不再回话。下列说法不正确的是（　　）。

A 刘某应在酒店耐心等待，美女马上就会来了

B 刘某这种行为是不正确的，是不自尊自爱的表现

C “美女”只是来骗钱的，并不会如约而至

D 对方涉嫌诈骗，刘某应立刻报警，描述真实情况

28．杨某通过某探与一女子相恋，对方言语挑逗热情似火，并主动提出裸聊进行深入交流，杨某喜出望外，当即下载了女子提供的 APP 开始了裸聊，结束后“美女”开始暴露真实面目，摄像头背后原来是一位中年男子，通过 APP 掌握杨某姓名电话通讯录等个人信息后，以裸聊视频要挟杨某向他转账三万元。此时杨某应当（　　）。

A 立马转账，不能让自己的丑事暴露

B 尽快报警，这是裸聊诈骗行为

C 自知这种行为不正当且丢脸，忍气吞声

D 女朋友的要求，当然要答应，转账

29．学生小王正在在手机上玩一款名叫球球英雄的游戏，有人添加其为好友，并表示想购买其游戏账号，后两人互加 QQ，并约定交易价格为 500 元。买家很快发送付款截图，要求他在百度上搜索“赛偲游”，进入该游戏交易网站提现。在提现过程中，网站客服告知小王由于他输入的提现银行卡号错误，需要充值 500 元激活原账户。小王在支付 500 元后发现仍然无法提现，客服回复这是由于“充值金额未加零头”导致，并要求充值 4000.1 元激活账户。小王随后联系买家，怀疑两人串通好在欺骗自己，买家答应借 2000 元帮忙充值激活，剩下的钱由小王自己想办法。于是，小王又根据客服要求，向客服提供的银行账户充值 2000 元，但是账户仍然显示无法提现。客服称“已经交易过的账户，再次

激活必须充值 100%的激活资金进行激活”，并要求小王继续充值 5000.2 元。小王该怎么办？（　　）。

A 既然已经投入 2000 元，不激活的话，这钱就只能打水漂了，因此可以再相信客服最后一次，试着激活账户

B 可以激活。由于对方提供的是银行账户，有名有姓有账号，现在科技这么发达，即使被对方骗了也不用担心，警察会循着线索找到这个卡主，帮助找回损失钱财

C 游戏交易网站肯定是有备案的，即使被骗也不用担心，找到网站运营者，钱可以被追回来

D 绝不转账，这是典型的游戏交易类诈骗，购买游戏账号是假的，通过虚假支付平台骗钱是真，同时小王要立即向学校保卫处或公安部门报警求助

30．李某在网上看到招嫖信息，并立刻与其联系。对方向李某发送了“服务项目”，在网上谈好了价格。李某与“美女”相

约在附近的地铁站见面。随后，对方要求李某添加主管经理的微信，并被拉入某支付平台的聊天群。接着，该经理先后以交付定金、转账备注错误等为由多次要求李某群发红包。最后，对方以需要缴纳服务费体检费等为由，要求李某继续通过网银向指定账户转账 5 万多元。李某应该怎么办？（　　）。

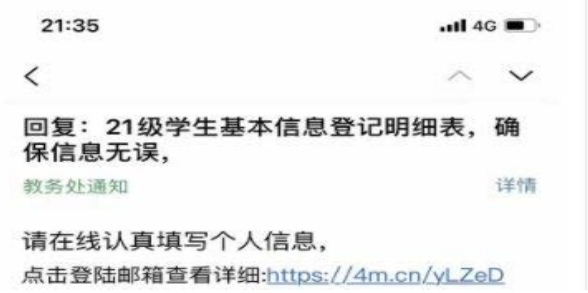
A 虽然这个是诈骗，但是嫖娼违法，还是不要报警为好

B 不要报警，骗子固然可恨，李某就当花钱买教训

C 这是网络招嫖诈骗，应该第一时间报警求助，并保留聊天记录

D 以报警为由恐吓骗子，试图把钱追回来，如果不行就到网上寻求网警帮助

31．当你收到一封名为“教务处通知”的邮件，下面说法正确的是（　　）。



A 陌生链接不乱点，这种网址通常是假的，主要用于收集 QQ 邮箱账号、密码 ，打开网址后会诱导你录入账号和密码

B 马上根据要求填写信息

C 即使账号信息被泄漏，只要手机在我身上，就没啥大问题

D 链接网址虽然有点奇怪，但既然是教务处发来的通知，而且知道我的身份，就应该不会有问题

32．你想买个手机，在网上搜索看到这款手机在某个网站上价格特别低，但是当你要购买时对方称要押金作为手机退税，该如何处理（　　）。

A 再砍砍价后再支付押金

B 反正押金是会退还的，先给他，拿到手机看看再说

C 不给押金，可能是诈骗陷阱，还是到官方平台购买比较好

D 这个手机是自己特别喜欢的，赶紧付押金购买

33．以下说法中错误的是：（　　）。

A 公安机关会通过短信、电话等方式提醒可能正遭受电信诈骗的群众

B 谁先联系我，我就相信谁是真警察，后联系或者上门的警察不能信

C 如果对警方的身份有疑问，可以拨打 110 或者到附近派出所核实身份

D 接到公安机关的提醒，要如实告知警方自己正在遭遇的事情

34．今天中午在淘宝上买了个小家电，下午突然收到了一个旺旺客服的消息，说他们的宝贝价格标高了，接着发给你一个链接，说是改价后的商品，让你重新拍下，旧的交易将会自动关闭，你会怎么做？（　　）。

A 直接点链接，重新拍下宝贝

B 旺旺客服发来的应该没错，点开看看

C 到自己购买小家电的商家主页上看看，咨询一下商家客服是否存在这种情况，如果存在，让他先退款然后再重新在店铺页面购买，不随便点任何人发来的链接

D 反正是客服发来的消息，应该不会是假的，点开链接，拍下宝贝

35．某日，小李手机短信收到一条 62000 元的信用贷款额度的消息，并附有一个网址链接，下面做法错误的是（　　）。

A 反正贷款已经到账了，不要白不要，点击链接提现

B 这条短信文字就不正规，这很可能是网络贷款诈骗短信，不能信啊

C 短信链接通常是一个虚假的贷款 App，客服会告诉你由于你银行卡号输入错误，导致你无法提现，然后让你再联系银行客服

D 银行客服会让你先打一笔钱解冻账户，谎称会退给你，当然，如果你真打了，对方是不会退的

36．小李闲来无事便打开 QQ 查看附近人，想与陌生人来场网聊消遣时间，突然一名性感美女引起了小李的注意。抱着试一试的心态，小李添加了对方的 QQ，没想到美女不仅同意添加好友，还主动搭讪。很快，小李与对方越聊越火热，聊天内容也极具挑逗性，不一会儿，美女又发出裸聊邀请，表示如果双方感觉好的话还可以线下见面。此时小李不正确的做法是（　　）。

A 保持警惕，不同意邀请

B 察觉不对劲，删除好友

C 天降好事，同意裸聊

D 不予理睬

37. 小张在二手交易平台进行交易时，看到低价好物询问卖家，卖家提出希望通过微信进行交易，会给予一定优惠，此时小张正确的做法是（　　）。

A 坚持通过平台交易

B 微信付款有优惠，同意请求

C 询问对方详细信息，并通过微信转账

D 及时购买好物，通过微信交易

38．M 男士玩抖音时刷到一个可以赚取佣金的视频，于是点击视频下方的链接下载并注册了 APP。随即客户向其发送了几张女子的照片，并声称办理会员并完成相应的刷单任务，就可以得到美女的联系方式。M 男士办理完会员后注册了“约炮”账号，并添加了“约炮指导”。按照“约炮指导”的要求完成了刷单任务，但“约炮指导”告知还需要完成几单任务才能认证成功，认证成功后就可以获得女子的联系方式。此时 M 男士的正确做法是（　　）。

A 继续努力垫资刷单，获得美女联系方式

B 办理刷单会员，加快刷单速度

C 及时止损，并报警寻求帮助

D 哀求“约炮指导”提供美女联系方式

39．近日李某需要购买一款品牌女包，便通过某书平台联系到了自称在韩国工作可以代购的王某，李某通过微信将 3 万余元货款转账给王某，但王某以缺货等理由拖延发货，后李某多次讨要货款，王某均未退款。李某现在应该做的是（　　）。

A 谩骂王某，要求他赶紧退款

B 及时报警寻求警方帮助

C 继续耐心等待

D 和王某争吵并拉黑他

40．某天小刘浏览网页时突然看见色情弹窗，没能抵制住诱惑点开弹窗查看，发现要下载一个 APP 才能免费观看视频，而下面评论全是好评，说这个 APP 是好东西，真的可以免费看，小刘心动下载后查看需要付 0.01 就能看所有视频，此时小刘不正确的做法是（　　）。

A 保持怀疑，不轻易相信此信息

B 发觉问题，及时卸载软件

C 向警方举报该 APP

D 1 分钱相当于免费，付款买下所有视频

二．多选题（共 30 题，每题 1 分，多选或者少选不得分）

41．请看下图，正确的做法是？ （ ）。

A 先稍微花点小钱，看看是不是真的

B 这是兼职刷单诈骗，不理会

C 这么好的事情，还不赶紧加入

D 肯定是骗子，果断举报

42．请问如果来电 96110 和 110，哪一个是真的？（　　）。

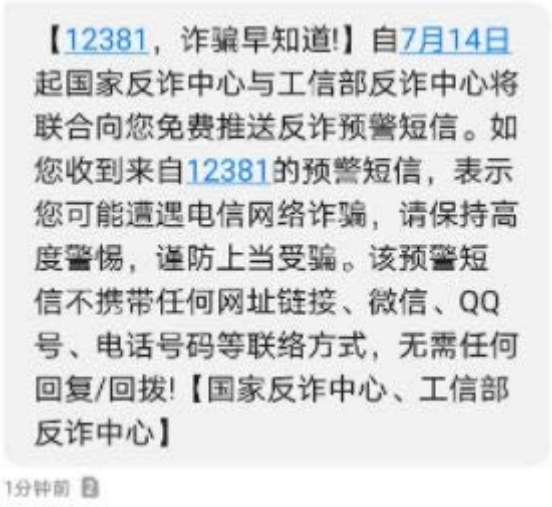
A 96110 是真的，这是国家反诈专用电话

B 96110 是假的，从来没听说过

C 110 是真的，要相信警察

D 110 是假的，警察不会线上办案

43．以下关于 12381 涉诈预警劝阻短信系统说法正确的是？（　　）。



A 12381 涉诈预警劝阻短信系统是由工业和信息化部联合公安部共同发起的反诈技术平台，是唯一的、 权威的

B 12381 涉诈预警劝阻短信系统可以根据涉案线索，利用大数据技术挖掘分析出潜在受害用户，并通过 12381 短信端口第一时间向潜在受害用户发送预警短信

C 当用户接收到 12381 涉诈预警劝阻短信时，说明正遭受网络诈骗侵害，用户应提高防范意识，避免个人财产损失

D 12381 涉诈预警劝阻短信系统可能会带有网址链接、微信、QQ 号、电话号码等联络方式

44．关于国家反诈中心 App 说法正确的是？

（　　）。

A 国家反诈中心填写个人信息、开放手机权限都是为了关键时刻能发出预警

B 国家反诈中心 APP 这款应用由公安部刑事侦查局组织开发，可以放心使用

C 国家反诈中心数据存储在公安部，拥有最高级别的安全等级保护

D 只要安装了国家反诈中心 APP，就不会被诈骗

45．小王收到一个陌生电话，对方自称是美团的工作人员，准确报出了小王的姓名、学校等基本信息。对方称小王有一笔校园贷未注销，如不清理会影响个人征信，并且还添加了小王的 QQ，发送了他的工作证件。此时，小王应该怎么做？（　　）。

A 相信对方，按照对方说的做

B 既然出示了工作证件，说明对方没有骗人

C 立刻挂断对话，询问官方客服

D 拨打保卫处电话 58736110 请求帮助

46．你在银行 ATM 机上取钱时发现出钞口被异物堵塞了，并贴有一张告示：“柜员机有问题，请联络维修人员，号码****”，正确的做法是（　　）。

A 拨打 110 报警，等待警方处理

B 拨打银行官方求助

C 拨打 ATM 机旁张贴的维修人员

D 提醒其他亲朋好友注意

47．周周接到一个陌生来电，称自己之前购买的商品存在质量缺陷，所以要进行赔偿 300 元。之后对方称由于操作失误，将钱打到了周周的支付宝备用金，并且多打了两百，周周应该怎么办？（　　）。

A 按照对方要求，将多的钱还给对方

B 很可能是诈骗，询问官方客服，是否存在此事

C 及时向公安机关咨询，并保留好对方身份信息

D 天上不会掉馅饼，怀疑退款一事的真实性

48．2022 年 5 月，我校某学生的朋友向其介绍一款“秀色”APP 约炮软件，后其在宿舍通过网址下载注册，客服以注册约炮会员、激活费、数据恢复费用为由要求其转账，下列做法错误的是（　　）。

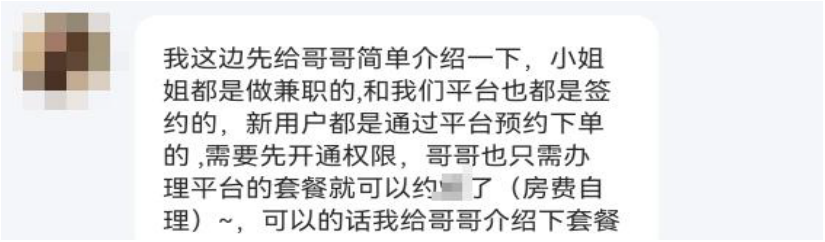
A 深信不疑，向客服转账

B 拒绝其转账要求，并立即卸载 APP

C 继续向身边好友推荐这款 APP

D 立刻拨打 58736110，寻求帮助

49．某天有人加了你的 QQ，告诉你可以根据他所提供的方式去一个安全的地方约炮，但是必须得先完成他的刷单任务，才能提供色情服务，并且保证这是保密协议，不会被其他人知道，你会怎么做（　　）。



A 是真的，询问情况

B 不能相信，并举报

C 远离删除这个 QQ 号

D 开通权限，预约下单

50．正在读大四的小王准备复习考研，决定卖掉自己的某游戏账号。没多久，就有人在交易平台上联系他。根据图片所示，说法正确的是（　　）。

A 主动联系对方

B 十有八九是骗子，平台就可以验证，干嘛要加 QQ

C 这种骗术通常是在QQ上发给你一个已经在交易平台付款的截图，并让你联系截图上的客服提现

D 实际上，付款截图是假的，假的客服还会以抵押金等各种名义让你交钱

51．小孟收到一条短信“您预定的航班由于机械故障已取消，请及时联系航班改签退款专线”，小孟应该？（　　）。

A 拨打过去，询问情况

B 认真辨别信息来源

C 拨打官方客服电话，询问是否有此事

D 拨打 96110 请求帮助

52．你通过电商平台购置了商品，下单成功后突然收到短信:“购置未成功需要退款，请按要求提供退款的账号和密码”。碰

到这样的情况应该（　　）。

A 按照对方的要求一步步操作

B 直接拨打询问卖家，或者在网站内询问

C 是真的，赶紧操作

D 好似有疑惑，还是询问其别人看看

53．小张在 QQ 上收到室友的消息，室友说他在去兼职的路上骑车撞了一位老人，现在急需 2000 元住院费，他此时身上没钱，让小张先给他指定的支付宝或微信账户转账，等他回到学校后再还钱给小张。这时候小张应该？（　　）。

A 拨打室友电话，确实是否有此事

B 要求对方视频或者语音聊天，进行互动，确认是否是本人

C 朋友有难，怎么能不帮助，立马转过去

D 可能是诈骗，立刻联系辅导员、保卫处或公安机关

54．兼职刷单诈骗在大学生中十分常见，兼职刷单诈骗的案件的特点有哪些？　（　　）。

A 犯罪分子先通过建立各种兼职群发布刷单信息、步骤、工资来骗取受害人信任

B 为了获取受害人信任，刷前几单时会如数返还货款并附上佣金

C 网上刷单全部都是诈骗，且刷单是违法违规行为

D 只有大平台刷单才能相信

55．一位学生收到了“刷信誉能赚钱”的兼职邀清。第一天要求你花 100 元购买商品，刷满信誉后，返还你 150 元。第二天花 300 元购买商品，返还 500 元。几天下来每天赚个一两百块。这天对方表示，随着等级升高需要花 5000 元购买商品，而后返还 10000 元，你碰到这种情况该怎么办？（　　）。

A 赚钱好容易，要刷下去

B 可能是陷阱

C 先尝点甜头再说

D 不予理睬

56．2023 年 3 月 9 日，笑笑在宿舍内通过手机推特与对方认识，对方用推特发送“凤凰城”APP 谎称有情趣视频让笑笑下载注册，笑笑下载后，用“凤凰城”APP 与对方裸聊，裸聊后对方以裸聊视频为要挟勒索笑笑转账，下列做法错误的是？（　　）。

A 是诈骗，不能相信

B 大好事，立马下载注册

C 使用支付宝扫码向对方转账

D 找身边好友一起

57．小明某天在大学生自建的物品交易群中看到自己喜欢的明星演唱会门票转让，转账后他却只收到了一组账号密码，被告知登录扫码即可，如果你是小明，你会如何做？（　　）。

A 立刻向学校保卫处报警

B 向群主反映情况，防止更多人被诈骗

C 按他说的即可，演唱会时登录扫码

D 这是遭遇诈骗了，为了减少损失，可以以相同方式转手卖出

58．小红接到一陌生电话，对方称小红的银行卡密码泄露，需要向“安全账户”紧急转移财产，对方还精确地报出了小红的多项个人信息，她该如何做？　（　　）。

A 没有所谓的安全账户，立刻拨打 110 报警

B 个人信息准确无误，该电话是官方的提醒电话，应当立刻转账至安全账号保护个人财产安全

C 对方能说出自己的个人信息，那肯定是官方人员，按照他说的做就行了

D 立刻拨打 96110 咨询，以免上当受骗

59．以下识别互联网上的官方正规网站方法错误的是？（　　）。

A 搜索排名第一的肯定是真官网

B 有 400***电话的肯定是真官网

C 搜索标有“推广”字样的网站

D 标有官方网站标识的搜索结果

60．符合游戏交易类诈骗特点的有？（　　）。

A 伺机下钩：骗子登录各种游戏交易平台、贴吧、Q 群、论坛等，寻找游戏装备卖家，然后留下自己的 QQ 号

B 佯装买家：当 QQ 联系上以后，骗子首先假装很关心装备的情况，加上一些讨价还价，让卖家信以为真

C 伪造支付：骗子伪造一个支付页面，让卖家误以为资金已交到第三方监管手中，安全有保障

D 假冒客服：这是最关键的一步，有了前面的铺垫。卖家一般不会拒绝“客服”提出的要求，将押金、保险费、提高信誉费、激活费等一次次扫码交到假客服账上

61．下列说法正确的是：（　　）。

A 未知链接不点击，不明电话不轻信，个人信息不透露，转账汇款多核实

B 凡是通过网络发送“逮捕令、通缉令”等法律文书，冒充“公检法”要求配合调查、自证清白的，都是诈骗

C 凡是要求通过网络媒介做笔录、做资金审查的，都是诈骗

D 凡是自称是公安机关人员的电话都值得被相信，我们应当积极配合

62．冒充公检法诈骗特点有（　　）。

A “我帮你把电话转接到公安机关”

B “你可以拨打 114，核实一下我的电话号码”

C “我们这个是专案，保密性非常强，绝对不能跟任何人提到，家里人也不行，别的警察也不行”

D 要把全部财产转移到“公安机关安全账户”

63．某天你接到一个电话，对方自称是某某公安局的警官，并直接报出你的名字和身份证号。警官称你的银行卡涉嫌洗钱罪，正在被警方通缉，如果要洗清嫌疑，需要把卡内的钱转到一个指定账户，核实排除嫌疑后，再把钱打回原账户，你应该怎么做？（　　）。

A 不相信，因为公安机关办案有严格程序，绝对不会在电话里办案的

B 对方知道我的名字和身份证号，应该是真的

C 按对方要求到银行柜员机去转账，尽快洗清自己的嫌疑

D 挂掉电话并拨打 110 报警

64．小李在网络上认识一位自称掌握内部信息的投资理财高手，对方向小李推荐了一款投资产品，称其收益高，稳赚不赔，并向小李收取 1000 元手续费，小李应该？（　　）。

A 无法证实对方身份，转账需谨慎

B 相信对方，转账 1000 元

C 一看就是骗子，拉黑此人

D 理财到正规平台，不相信陌生人

65．某日，张某被“一位美女”热情似火地追求，还收到了对方的照片，张某一看对方是肤白貌美大长腿的妙龄女子后，心情逐渐激动，慢慢放松警惕，与她循序渐进开始了裸聊，可视频一结束，对方就发来了刚才不雅视频的录像和张某亲朋好友的通讯录，不断威胁张某给指定用户打钱，否则就把其不雅视频发给家人和同事，对此，你会怎么做？（　　）。

A 只想快点破财消灾，花点钱把这件事瞒过去算了

B 立即报警，查询该用户号码

C 对方肯定会进行多次敲诈勒索，一定不能给他转账，立马寻求警方求助

D 放任不管，让她发，家人收到说不是我

66．关于电信网络诈骗说法正确的是　（　　）。

A 受害人基本上只能凭个人的智慧和经验来识别骗局，而施骗一方却是有预谋、有组织的团伙

B 诈骗团伙中有键盘手、话务员，他们按照既定的剧本，丝丝入扣地忽悠你往设好的套里钻

C 当受害人转账后，有操作员把诈骗到账的钱款天女散花地转到数百个账户，再由提款员背包扫大街似的到柜员机提现

D 骗子提到的现金，通过另外的途径汇到境外账户。所以，许多诈骗案件，即使案件破了，钱也追不回来

67．李某收到短信，称可以帮其升级信用卡额度，只要将信用卡账号发给对方，后来收到一个短信验证提示，对方说要短信验证码才能完成操作，李某将短信验证码发给了对方，结果被骗，李某该怎么做？（　　）。

A 打电话给对方，要求还钱

B 到银行修改信用卡密码

C 到银行先期冻结信用卡账户

D 打电话报警，求助警方，快速查找冻结对方帐户

68．周某在家中手机抖音刷短视频时看到一个女子跳舞的视频，周某想据评论里的提示下载“Telegram”APP，去看裸聊的美女，你会怎么做？（　　）。

A 有美女跳舞不看白不看，立马下载

B 不相信，美女不会随便跟我裸聊的，这肯定是假的

C 这个美女跳的好棒，为了支持她，立马下载

D 不相信，立马刷下一个视频

69．下列做法正确的是（　　）。

A 学生孙某在 QQ 上收到同学卢某的信息，对方称他的朋友受伤住院需要一笔医药费，由于微信限额无法转账，请他帮忙转钱应急。对方向孙某要了银行账号，随后发送“转账截图”，并以“跨行转账，到账延迟”为由，请孙某先转账到他朋友微信上。

孙某立即通过微信扫码向卢某朋友支付 2000 元

B 小马接到自称蚂蚁金服客服的电话，要求小马注销借呗，否则影响征信，让小马按其指令操作，小马不相信对方，挂掉了电话

C 小白通过交友软件认识一名“美女”，对方告知小白自己在做私密直播，并发送给小白“直播软件”要求他下载。小白识别出这是裸聊诈骗套路，拒绝安装软件并且删除好友

D 小王接到自称是李老师的电话，要求其前往办公室。路途中，小王再次接到李老师电话，知悉李老师临时急需用钱。小王考虑再三，转账了 1000 元

70．小李是一位彩民，在家上网时，点击登陆了一个名为“中国福利彩票 3D 专家预测网” 网站，小李中奖心切，立即与该网站联系咨询，对方称要交纳 2000 元咨询费。小李应该？（　　）。

A 先看看预测得准不准，准的话再给钱不迟

B 2000 元不算多，万一中奖了多划算

C 不轻信，不给钱，这是典型网络彩票预测诈骗

D 拨打 110 或 96110 举报

三．判断题（在你认为对或错的选项下打“√”，共 30 题，每题 1 分）

71．小苏收到短信，称其有快递被扣在快递站，让其回电。小苏回电后，对方称其包裹涉嫌私藏武器，直接将电话转接到公安局。小苏感到很恐慌，继续接听电话。

对☐　　错☐

72．小王接到电话，称其有一张法院传票。小王继续询问详情后，电话转接到一位警官处，对方称要通过电话做笔录。小王当即挂断电话，因为警方不可能通过电话来调查案件。

对☐　　错☐

73．根据聊天截图判断，这是典型的“杀猪盘”诈骗。

对☐　　错☐

74．根据下图的情境，一旦遭遇裸聊敲诈，只要删除视频就没事儿了。最好的办法应该是按照对方要求来。

对□　　错□

75．自称做私密直播的女孩给你发来一个手机直播软件，即使自己不小心安装了，只要不转账，就没事儿。

对□　　错□

76. 朋友圈有人在转发送校庆盲盒，开万元好礼的活动广告。很明显，这是虚假宣传。类似的还有锦鲤抽奖、校庆送礼品等活动，每年都会出现，大家一定要擦亮眼睛，不要盲目跟风转发。

对☐　　错☐

77. 某客服人员给你打来电话，声称受银监会委托，帮你核销贷款账户，还给你发送工作照，应该是可信的。

对☐　　错☐

78．接到自称是网贷平台工作人员的电话，务必提高警惕。遇到疑问时，应当及时向警方或者官方客服咨询核实，避免财产受到损失。不存在注销网贷账户的操作，只要你按时还清货款，就不会影响到个人征信。

对□　　错□

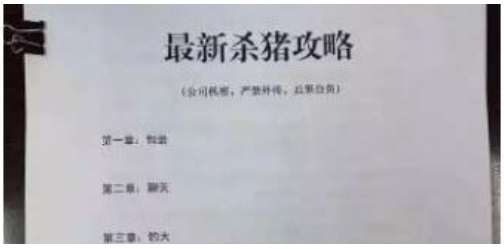
79．个人征信由中国人民银行征信中心统一管理非数据报送机构都无权删除和修改。凡是自称金融平台、网贷平台客服，提供注销不良网贷征信记录和账户的都是诈骗。

对□　　错□

80．学生小王准备在二手物品交易平台“闲鱼”APP 上购买一台平板电脑，一个卖家告诉他“由于闲鱼会偷换屏幕和原装配件”，建议他从“转转”二手交易网上购买，并发送了一个交易链接。因为“转转”APP 和“闲鱼”APP 一样是有平台担保的，因此卖家的话可信，可以放心购买。

对□　　错□

81.“杀猪盘”诈骗的套路是，先树立受害者所青睐的人设，在博得受害者的好感后，接着以“恋爱”“交友”为噱头，在受害者逐渐放松警惕时，他们开始忽悠受害者进行“投资”“赌博”等，最后导致受害者血本无归。所以大学生在交友时，一定要慎重对待!



对□　　错□

82．小明家境贫困，利用课余时间打工挣钱。有一天，小明在宿舍楼道发现一个打工兼职群二维码，扫码加入后看见有做淘宝刷单兼职的广告，操作简单，条件丰厚，遂添加广告中的 QQ 应聘刷单兼职。这种做法对吗?

对□　　错□

83．来电显示为“110”的一定是诈骗电话。

对□　　错□

84．自称是金融平台客服，受中国银监会委托帮助你注销校园贷账户，并给你发送个人征信截图。这一定是诈骗。

对□　　错□

85．民警办案、找当事人了解情况都是面对面的，不可能通过电话做笔录。因此，当你接到陌生电话，对方自称是“民警”，要加你 QQ 进行办案的，肯定是诈骗，不要轻信，更不要转账。

对□　　错□

86．小万单身 20 余年，渴望爱情。一日，小万在某 APP 上认识一女子小丽，后互加微信继续热聊。小丽在微信朋友圈中发的个人照片十分惊艳，小万顿时陷入爱河不能自拔。没过两天，小丽竟然答应做小万的女朋友。随着了解的深入，小万得知小丽白手起家，在一个赌博网站获利颇丰。小丽表示要带着小万一起发财，买房买车结婚步入人生巅峰。小万坚信不疑，认为小丽是真爱，不会欺骗自己。这种做法对吗?

对□　　错□

87．出差途中，突然遇到短信通知票务改签等事宜，应该立即跟短信里的客服联系改签。

对□　　错□

88．当你手机收到下图所示的信息，一定要高度警惕，有人正在登陆你的手机银行，可能你正在遭遇诈骗，要立即中断任何屏幕共享软件或卸载的模式软件，同时登陆手机银行 APP 查看或致电银行客服。

对□　　错□

89．“刷单返现”诈骗的通常套路是:“客服”会先让受害人先尝点甜头，骗取受害人的信任，然后再让受害人不停地刷下一单来返还上一单的本金和利息，如果不能完成“任务”就无法返还资金。而为了拿回本金的受害者，此时便不得不刷更大的一单。

对□　　错□

90．面对网络兼职信息，大学生要注意甄别真假，切不可轻信广告内容;想要从事兼职工作，一定要去正规平台应聘；不要轻易听信陌生人或下载陌生可疑的 APP；如果发现自己被骗，要及时拨打 110 报警。

对□　　错□

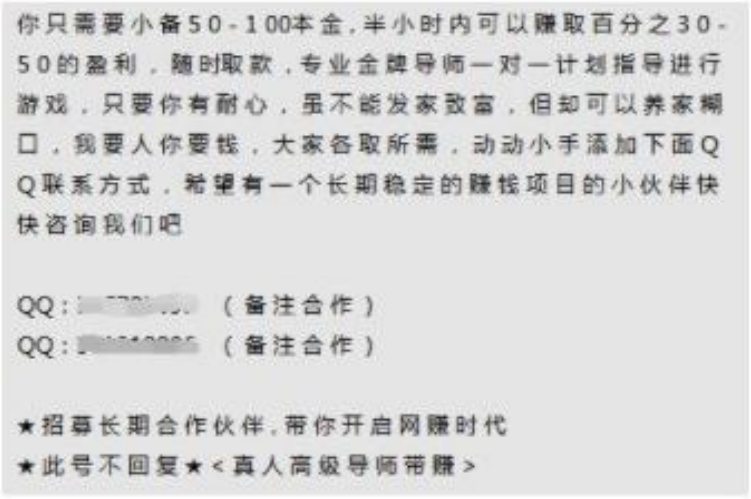
91．朋友圈有不少跟好友一起抢红包的活动，要求达到一定金额（比如 100 元）才能提现，参与此类活动一定要格外注意，很可能是一种吸引粉丝的骗局。

对□　　错□

92．当搞不清楚是否遭遇诈骗时，可以主动拨打 110 或 96110 进行咨询。

对□　　错□

93．朋友在 QQ 上给你发了一条信息，从下图来看，内容应该是可信的。



对□　　错□

94．小张同学（女生）在交友网站上认识一男子，通过 QQ、电话等方式与其相聊甚欢，后被该男子以各种理由骗取人民币 5000 元。小张发觉后，在盛怒之下将该男子的 QQ 号、手机号码全部删除。这种做法对吗?

对□　　错□

95. 小张是游戏骨灰级玩家，帐号里各类高级卡牌应有尽有。临近毕业，小张深感学业重要，打算将帐号出售一心学习，于是将帐号出售信息挂在闲鱼上。没过多久便有人联系小张，小张和卖家谈好价钱后，买家提出要在平台上进行交易，并发了一个平台链接给小张，让小张在平台注册帐号接受转账，小张虽然没听说过这个网站，但是还是照做了。小张把帐号信息录入平台后不久，帐号确实收到了相应金额的款项，但是怎么也无法提现。小张联系平台客服，平台客服表示等几天就可以了，于是小张开始耐心等候。这种做法对吗?

对□　　错□

96. 诈骗分子盗取小张 QQ 号，以要参加学校组织的国外培训为由，骗取了小张父母 2 万多元。小张找回 QQ 后气不过，想尽快找回损失，于是在百度上向“网警”寻求帮助，并添加了“网警“的 QQ。小张的做法对吗?

对□　　错□

97．小刘同学收到“双十一嘉年华”发来的短信，称其获得购物参与大奖，让其点击链接进入节目网站领取奖品。小刘非常兴奋，赶紧上网领奖。

对□　　错□

98．小刘同学近期在网上结识了一名异性网友，两人聊得甚是投机，发展迅速。有一天该网友突然提出要小刘为其开通支付宝亲密付，小刘出于对网友的信任，直接答应了。

对□　　错□

99．只要卡里没钱，就不用担心被诈骗。

对□　　错□

100．学生小王在某二手交易平台上看到转让闲置相机的信息，与卖家谈好价格后，卖家要求小王线下支付 300 元定金，小王付完定金后卖家将其收货递邮寄单截图发送过来，小王看后将剩余三千多元尾款转给对方。这种做法对吗?


¥3500 包邮
慢收！一台佳能200d二代，收的收的收的收的收的收的收的收的收的收的收的收的收的收的收的收的，别随便拍哦，这个价格是乱标的具体价格具体讨论
最好带小疫盖镜头哦！
感兴趣的话点"我想要"和我私聊吧~
#Canon/佳能
超赞
留言
收藏
管理

对□　　错□

“慧眼识诈”防骗能力随机测验链接