国际金融安全奥林匹克竞赛

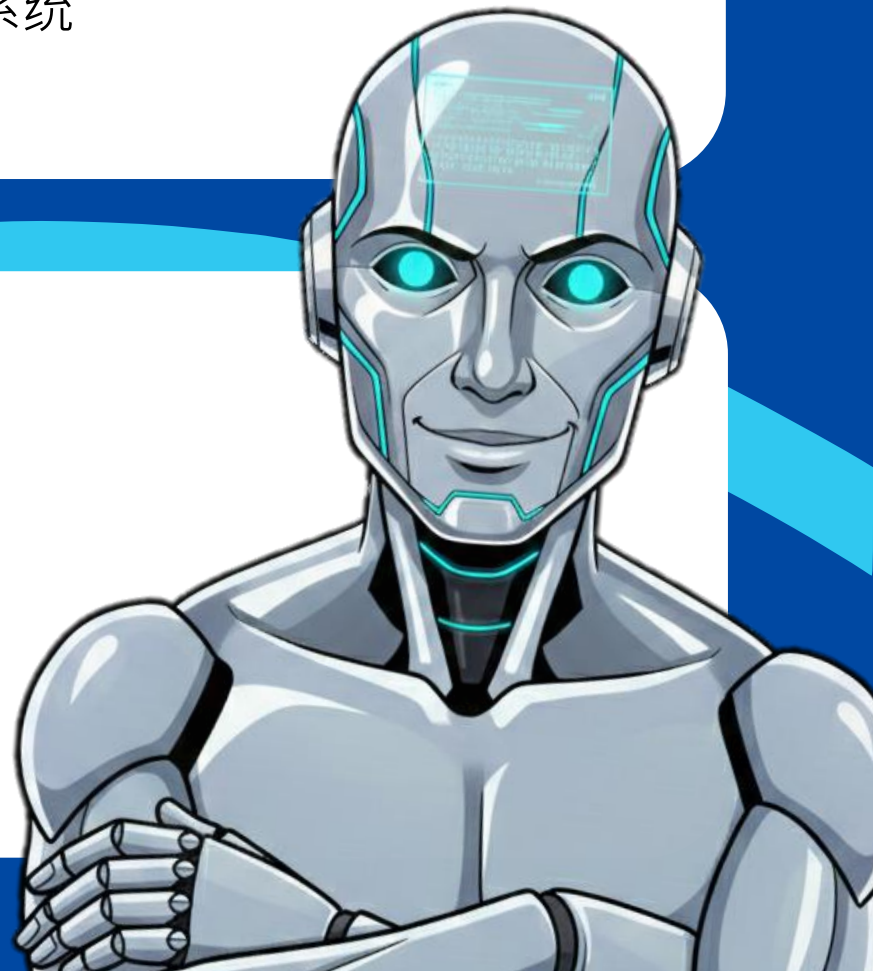
# 人工智能的

# 黑暗面

#人工智能

# 人工智能
# Artificial intelligence

能够执行人类智能特有任务的计算机系统



**人工智能是指使系统能够实现以下功能的技术：**

- •理解以自然语言表达的请求
- •分析、处理并查找所需数据
- •识别图像、符号和规律
- •在海量数据流基础上进行学习
- 做出决策并适应不同的环境

# 人工智能的应用领域

## 医疗卫生领域

- 个性化治方案
- 新药研发
- 数据分析

## 银行金融领域

- 自动化投资
- 信用评分与风险估计
- 即时决策

## 教育领域

- 基于学生特点的个性化材料的适配
- 知识薄弱点识别
- 编制额外练习

## 科学与研究领域

- 快速发现规律
- 加速科研进程
- 基于分析寻找解决方案

# 网络安全防护

**人工智能如何对抗诈骗者**

- •识别并拦截诈骗手段
- •**降低**对潜在受害者的风险暴露与实际损害


**例子：“网络奶奶”是移动运营商推出的人工智能模型**

- **以老年客**户名义与骗子交流
- **分散**诈骗犯的注意力，消耗其时间和资源

# 人工智能的另一面

**金融威胁：**

- **利用人工智能**实施的网络欺诈激增
- 资金和数据窃取
- **犯罪手段自**动化

**特别风险领域：**

- **未成年人受害者人数增加**
- **通**过电话与短信发起的攻击 (**学校、政府机构、**电信运营商)
- **与游**戏账户和国家统一考试（GIA）**相关的**诈骗

**未经客户同意的交易：**

**275** 亿卢布 — 2024 年

**210** 亿卢布 — 年前9个月

**已阻止的盗窃案件**

**2.22** 亿卢布

2025年11月

**应对措施：**

- **俄**罗斯联邦金融监控局
- **独**联体国家的金融情报**部**门
- **欧**亚反洗钱与反恐怖融资小组 (EAG)

# 洗钱

网络欺诈

虚假银行账户

多次转账，
资金混同

模糊资金流

加密货币平台

犯罪活动合法化 / 恐怖融资


威胁具有跨国性质

# 谁是钱骡？

## 钱骡

“钱骡”（Dropper）**是指利用自己的**银行卡对被盗资金进行**或中**转（进一步转移）的人。

# 青少年群体卷入风险

**哪些人会被卷入？**

- 14岁以上的青少年
- **在校大学生和中小学生**
- **失业者**

**超过一百万名“钱骡”**

俄罗斯问题的规模

*俄罗斯银行数据*

**诱骗手段（心理操控）：**

- **紧迫感** — "仅限今日"
- **简单性** — "谁都能干"
- **虚假合法性** — "完全合法"
- **渐进式诱导** — **从小额开始，逐步提高金额**
- **从众效应（社会证明）** — **"已有数百人参与"**

# 法律责任

## 直接刑事责任

针对“钱骡”**相关犯罪**链条，俄罗斯联邦刑**法典第 187 条修正案已明确**规定了相关刑事责任。

## 刑罚

- **最高3年监禁** — 转让银行账户信息
- **最高6年监禁** — 组织者（钱骡组织者）

## 司法应用实践

- 2025**年已**对钱骡组织者提起首例刑事诉讼
- 积极配合内务部调查是免除刑事责任的法定依据
- **通**过被捕“钱骡”**提供的关**键供述，成功锁定了幕**后**组织者

# 深度伪造：新型威胁

**深度伪造**

**（源自英文 deepfake — «深度伪造»）**，
**指由人工智能生成的**视频、音频或照片，其中人物**做出或**说出在现实中从未发生过的行为或言论。

**运作原理**

- **以**调查名义打电话并录制声音
- **人工智能复制人工智能复制人物面部特征及声音**
- **生成**语音深度伪造内容


**仅需数秒录音，即可生成**语音深度伪造

# 首个引发热议的案例

**英国，2019年**

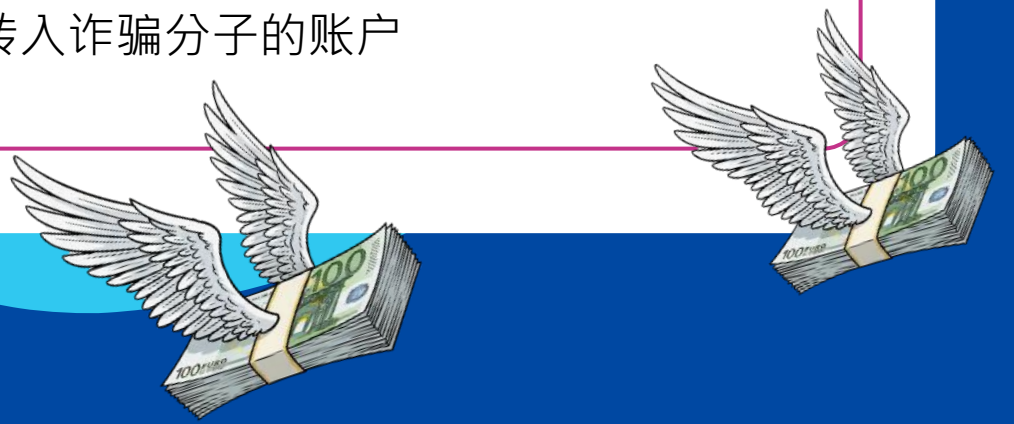
诈骗分子利用人工智能克隆了某能源公司**首席**执行官的声音

**运作流程**

“总监的声音”**致**电下属
**下达**紧急指令要求向供应商转账

↓

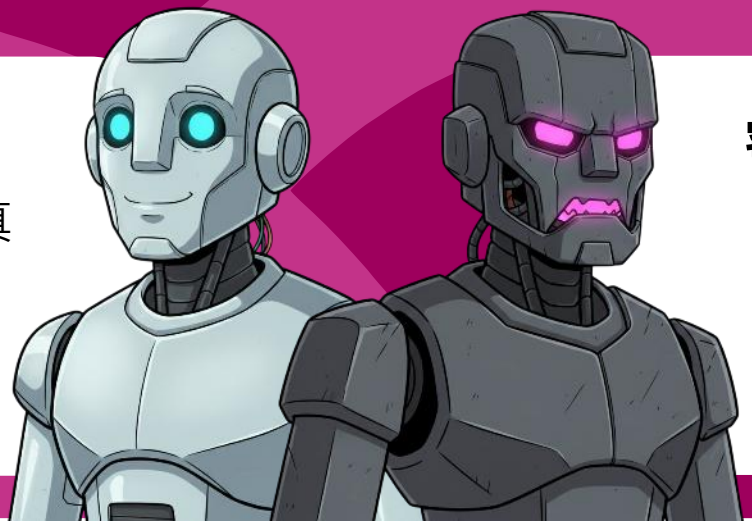
**22万欧元**
**已被**转入诈骗分子的账户



# «邪恶双胞胎»（Evil Twin）

**攻击本质**

伪造的 Wi-Fi 网络，复制真实网络的名称和设置



**窃取什么**

- **登**录名和密码
- 银行卡数据信息
- **通**讯记录和浏览器历史

**运作流程**

**网络克隆**：使用相同 SSID，**信号更强**

→ **受害者连接**：**咖啡**馆、**机**场、商场

→ **中间人攻击**：对全**部网**络流量进行拦**截和**监控。

**网络钓鱼**：伪造登录页面

# 机场中的«邪恶双胞胎»攻击

## 情境

- **一名女学生**连接了名称与机场相**同的** Wi-Fi 网络
- 该网络在列表中排在第一位
- 输入的验证码实为即时通讯软件**收到的一次性密**码

## 关键错误

- **忽略了关于非安全网**络的风险提示
- 输入了自己的手机号码
- 输入了来自通讯软件的验证码

## 结果

- **失去**对通讯软件的访问权限
- **个人数据被泄露**

## 重要提示！

WiFi **注册**时绝不会要求用户输**入来自通**讯软件的验证码

# 人工智能网路钓鱼

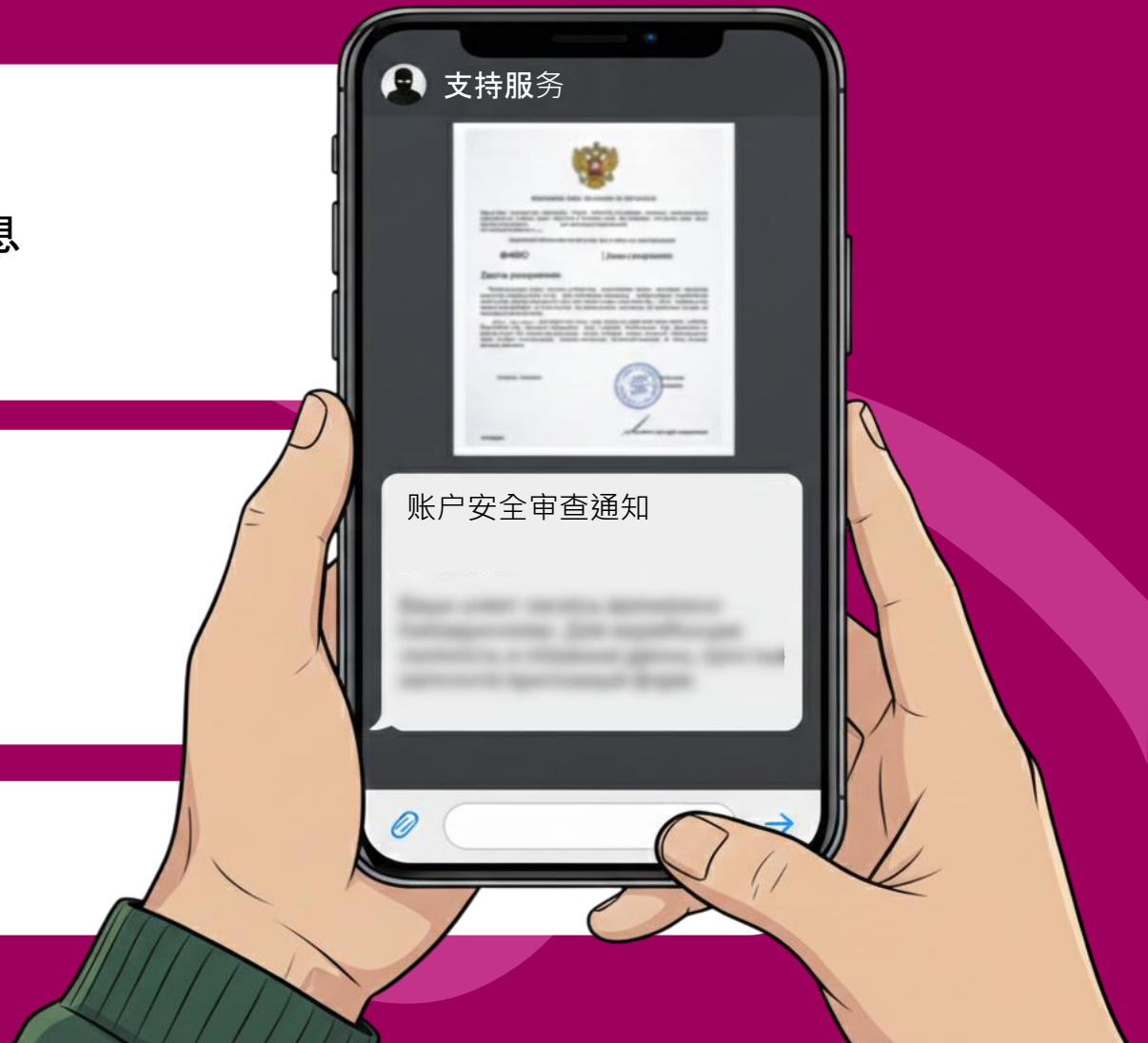
**在发起攻击前，人工智能系统会：**

- **分析来自社交媒体、网站以及数据泄露事件中的信息**
- **会生成“极具迷惑性”的**邮件与即时信息

**发送高度定制化的欺诈信息**

- **内容无**错，不套用常见模板句式
- **看起来与真**实的办公业务沟通毫无二致。

**最终结果 —— 资金损失**



# 人工智能语音钓鱼

**人工智能语音钓鱼**

（英文: **vishing = voice + phishing**）：即“语音钓鱼”

- **属于深度**伪造技术在语音维度的应用
- **人工智能**仅凭数秒的录音样本即可克隆人声
- **能**够与受害者进行实时对话交互


**人工智能将欺诈行为的真实感推至极致**

# 浪漫诈骗

## 攻击本质

- **人工智能可同**时与成千上万人进行对话
- **通**过分析社交媒体数据实现个性化交流，营造信任关系的**假象**

## 运作流程

聊天互动阶段
**涉及私人**话题、发送语音**消息**

→

**诱导投资阶段**
**博彩投注、加密**货币、传销**式金融**骗局

→

**展示“成功案例”阶段**
**通**过照片、**截**图、**礼物**营造获**利假象**

# 公共 Wi-Fi 安全指南

**不要使用不安全的网络**

“邪恶双胞胎”网络几乎总是开放的，没有加密保护

**仅访问HTTPS网站**

锁形图标 → 表示连接已通过端到端加密保护

**启用多因素认证 (MFA)**

密码 + 一次性验证码

**切勿输入密码和银行卡信息**

公共Wi-Fi环境存在流量被截获风险

**警惕系统安全警告**

此类警告通常意味着真实的网络威胁

# 不要惊慌！

**以下是防范人工智能语音伪造的简单且可靠的方法：**

1. **一旦**发现对方有任何可疑迹象，立即挂断电话
2. **从**电话簿中回拨亲友号码进行核实
3. **使用家庭内部**约定的代码口令验证身份
4. 询问仅限亲密家人知晓的个人化问题
5. （**例如**：“**我**们家养的狗叫什么名字？”）

# 保持良好的数字卫生习惯！

## 如何防止人工智能克隆您的声音

- **设置社交媒体访问权限** (仅限好友可见)
- **不要公开发布语音录音** (包括状态语音、直播、聊天工具)

## 控制情绪状态

- **任何激起**强烈情绪反应并要求立即行动的信息，**极有可能系欺**诈
- 与亲友商议核实

## 最重要的防护武器是批判性思维

请记住：政府机构（如俄罗斯央行、联邦安全局、税务局）不会通过电话处理“重要事务”

# 切断可疑联系

## 遭遇诈骗时的应对措施

- 一旦对方提及金钱、投注、加密货币，立即停止对话
- 运用批判性思维进行分析
- 将诈骗者拉黑或屏蔽
- ☒切勿向任何未曾线下见面的人员转账汇
- ☒如有必要——向执法机关和平台管理员举报

**情感浪漫诈骗是一场以信任为筹码的博**

但最终赌注是你的钱财

# 钱骡是诈骗金融方案中的中间人

## 什么是“钱骡”？

- **接收被盗**资金的人
- 为“**上**线人员”转账或提取现金
- **将个人**银行卡及其在线银行访问权限转交给他人使用

## 钱骡行为实际上构成刑事犯罪

**“非银行客户人员购买或转让银行卡”属于违法行为，针对此类违法行为，法律规定：最高可判处 6 年监禁，并处以罚金。**

*俄罗斯联邦刑法第187条《支付工具非法流通罪》*

# 俄罗斯联邦“钱骡”统计数据

**>100万**

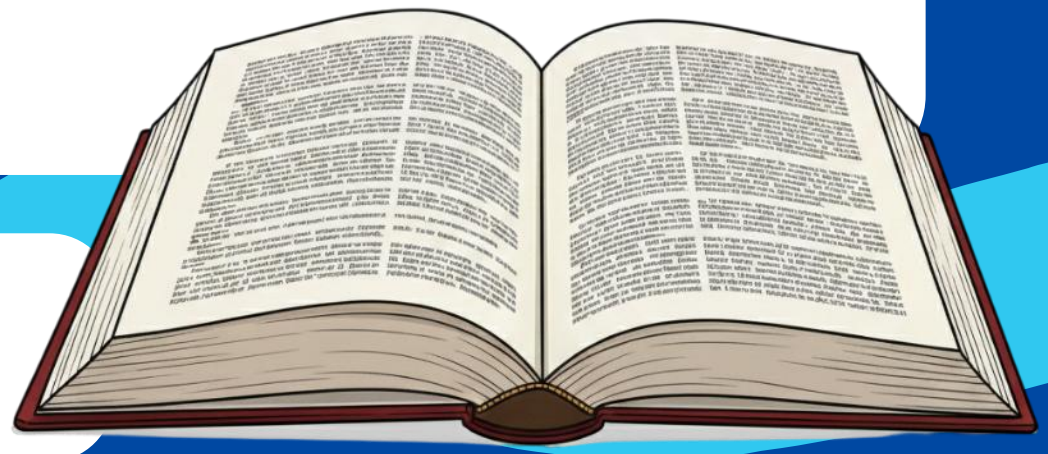
银行业务中的“钱骡”**客**户规模

**~20%**

**未意**识到法律后果的青少年

**“钱骡”是被盗资金“洗白”过程中的重要一环**

相关人员可能因触犯《俄罗斯联邦刑法典》**第174条——“对他人通过犯罪手段获得的资金或其他财产进行合法化（洗钱）”而被追究刑事**责任。



**提高警惕与风险意识**

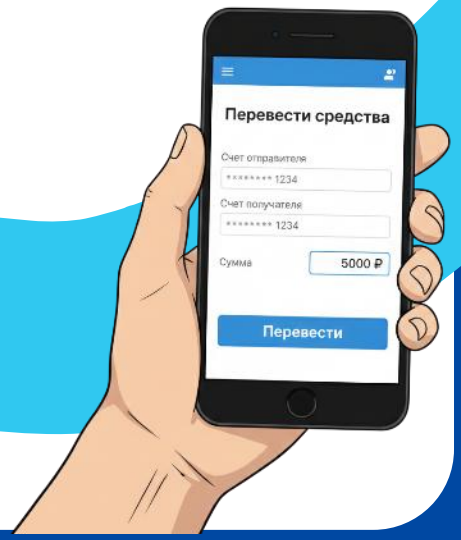
# 按职能划分的“钱骡”类型

## 资金“存入者”

- **接收**现金 →
- **存入**账户 →
- 继续转移

## 过渡“转账者”

- **接收**转账 →
- **将**资金转至其他账户或电子钱包




## 最终“取现者”

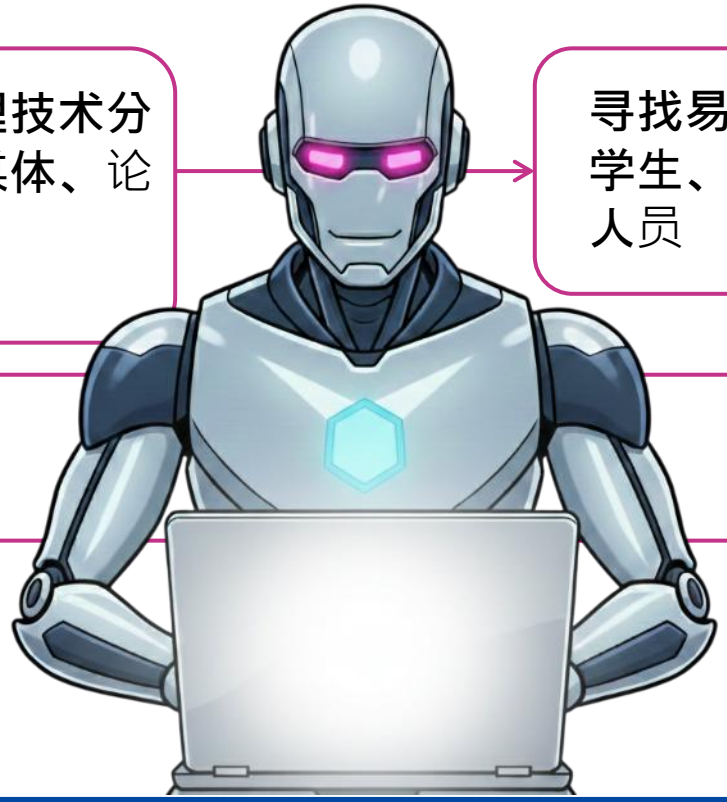
- **在自**动取款机取现 →
- **将**现金交付给组织者

# 使用人工智能招募“钱骡”

**招募链路解析**

**神经网络与自然语言处理技术分析公开信息来源（社交媒体、论坛、电商平台）**

**寻找易受害群体**
**学生、寻求"轻松赚钱"机会的失业人员**



**评估受害者心理特征**
**通过其发布内容和交流风格 → 判断其易受暗示性、逐利心理等特征**

**首次接触**
**利用聊天机器人，使用深度伪造的头像**

# «简单兼职»

**典型场景**

- **需相关工作**经验、无需学历背景
- **在家工作，每天只要2-3小时**
- **必**须拥有个人银行卡或开通网上银行（手机银行）。


**人们在不知不觉中成为"钱骡"，成为犯罪同谋**

# “银行转账错误”骗局

## 该诈骗链路解析

“意外”银行转账

到账

来电要求立即退款至"正确"账户

按犯罪分子提供的银行信息进行转账

## 唯一正确作法

- 立即联系银行
- 严格按照银行的官方指引操作

陌生号码发送的信息示例：“您的账户收到5万卢布。”

我不小心转错了，请把钱转回这个手机号。

# “彩票管理员”骗局

## 招募方式表现形式

- **提供«技**术性岗位»
- 职责——**向“中**奖者”**派**发奖**金**

## 实际是如何操作的

- **雇来的人成**为“钱骡”
- 银行卡中的资金为从其他受害人处骗取的赃款
- 转账被伪装为“**中**奖奖金”，**但**资金最终流向：

—— **其他**“钱骡”**或冒充的人**

—— 诈骗者本人

## “钱骡”的核心作用

- **拆分、“清洗”非法**资金流
- **极大增加**银行及执法机关识别犯罪方案的难度

# 通过社交网络招募

**如何寻找受害者**

- **人工智能分析社交网**络：求职类**帖文、参与抽**奖活动记录
- 筛选出易感人群

**典型的伪装身份**

- “**打**赏管理员”
- **博主或主播助理**
- 负责接收捐款的志愿者

**招募过程如何进行：**

- **使用盗用照片的“真人”**账号
- 发送兼职邀约、提供帮助或参与“**公益**项目”**等信息**
- **反复强**调该模式“**合法合**规”
- **要求通**过个人银行卡进行转账

**任何合法组织**
**都不会使用**
**陌生人的银行卡**

# 俄罗斯联邦的刑事责任

**涉及“钱骡”行为的相关法律条款**

- 《俄罗斯联邦刑法》第174条
- 《关于将他人通过犯罪手段获得的资金或者其他财产进行合法化（洗黑钱）的行为》
- 《俄罗斯联邦刑法第187条》
- 《支付工具非法流通》

**请牢记要点：**

- ”钱骡“并非“轻松赚钱”，而是会被依法追究刑事责任的犯罪行为
- 承担责任的不仅包括组织者，也包括普通参与者

# 安全准则

**如发现招募迹象：**

- **立即**终止与诈骗者的一切联系
- **切勿**进行任何转账操作，即使已收到可疑转账
- 冻结银行卡并通知银行
- **保留聊天**记录、收款信息、诈骗者电话号码
- 联系执法机关


**所有“轻松赚钱”的邀约均属可疑，**
**尤其是要求提供个人数据或**银行卡访问权限者。

# 历史与特点

## 什么是加密货币？

- **不依**赖国家银行的数字货币
- **基于区**块链运行，是一种去中心化的分布式账本

## 2009年1月3日

**生成了第一个比特**币区块 (Bitcoin)

## 比特币价格出现惊人增长

*2009年* | **1 分**

*2025 年* **$126 200**

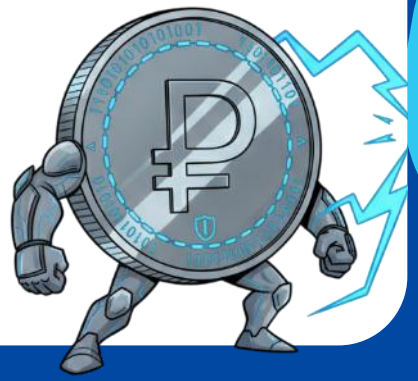
过去的收益 **≠ 未来的收益**

## *主流加密资产*

# 数字卢布 vs 加密货币

**数字卢布**

- 补充现金和非现金支付手段
- **由俄**罗斯联邦央行管控，通过移动应用及网**上**银行访问
- 强制执行KYC•(Know you customer)**程序，以防范**诈骗和洗钱



**国家管控资产**

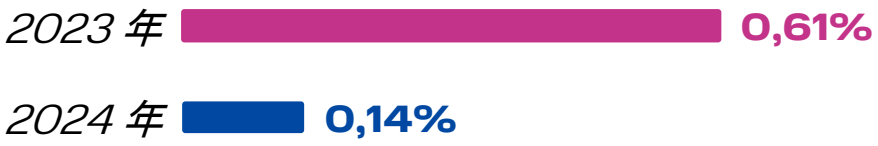
**加密货币**

- **去中心化——无**单一控制主体，不受国家或银行的干预
- **作**为资产**/**财产使用，不总是合法的支付手**段**
- 伪匿名性：与公开的区块链钱包地址绑定，**存在安全**风险

**一种去中心化、具有高波动性的数字资产**

# 加密货币与诈骗

## 犯罪交易占比




## 存在非法活动特征的实体

俄央行统计数据

| 3346 | 4183 |
| --- | --- |
| 2024年1月至6月 | 2025年1月至6月 |

## 犯罪分子利用手段

- **毒品**、赌博、侵犯知识产权
- **洗**钱、金融金字塔
- **加密**货币是一种以快速盈利为诱饵来吸引资金和投资的方式

## 加密货币对年轻人来说很方便

**然而，加密**货币也是一种诈骗工具，尤其在人工智能**技**术介入后，可实现大规模、自动化的欺诈操作

# P2P“三角诈骗”骗局

## 诈骗运作机制

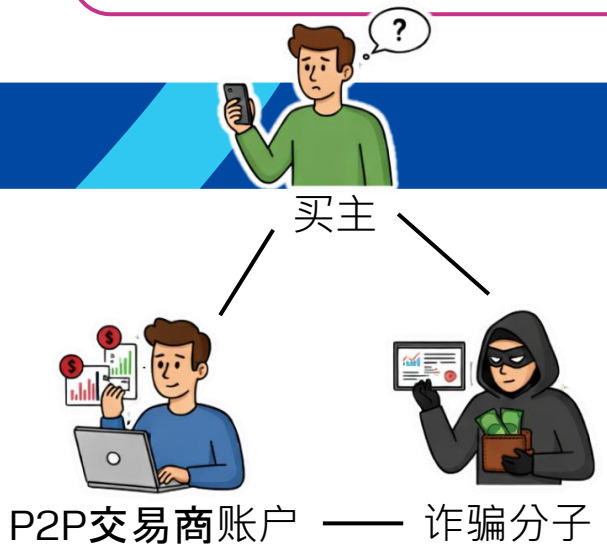
**虚假广告**
以明显低于市场价格的价格出售商品

→

**篡改收款信息**
指向P2P交易商账户，而非卖家本人

→

**资金转入P2P交易商账户**
为诈骗者购入加密货币




## 如何降低风险

- 检查交易对手的信用评级和历史记录
- 选用通用且可追踪的支付方式
- 仅通过正规、可信的交易平台进行商品买卖

# SQUID（鱿鱼币）加密货币骗局

## 事件经过

- **诈骗分子声称** SQUID （鱿鱼币）将用于一款基于热门电视剧**开**发的网络游戏。
- **两天内价格暴涨44,000%，最高达到2,860美元**
- **不久后**贬值至0
- **诈骗者卷走超300万美元，**40000**余名投**资者受害

## 风险信号

- **无法**卖出代币
- **未在主流加密**货币交易所上**市**
- **网站上存在**错误


## 重要提示

- **投**资前务必核查项目创建者背景及公开信息
- 审慎态度与批判性思维 = **防范金融**诈骗的盾牌

# Bitconnect 金融金字塔（庞氏骗局）

## 骗局本质

- **伪装成利用人工智能**进行交易的加密货币平台
- **承**诺低风险高回报
- **采用推荐奖励机制：从新投**资者的投入资金中**提取**7%–15%**作**为奖励

## 后果

- **来自40多个国家的投**资者遭受损失
- **一千七百万$**

## 诈骗机制

- **新投**资者的资金 → **用于向早期投**资者支付“**收益”和推荐**奖金 → **最**终流入组织者口袋
- **所**谓的“**交易机器人**”实际上并不存在

**“保本高收益”承诺 +**
**多层级推荐奖金**
**= 极其显著的金融诈骗信号**

# «FINICO»/ «非尼科»财政三角

**方案本质**

- **通**过投资**摆脱贷款**
- **使用** 《**数学模型**》**和人工智能来**《**降低**风险》
- **可以以市**场价的**35%购买公寓或汽**车
- **存款月收益率**为 **20–30%**

**特点**

- 车所有操作均以比特币和 Tether 进行
- **禁止用法定**货币充值账户
- 该计划因大规模《**有利可**图的》优惠而广受欢迎

**高收益 + 无法使用常**规货币 **= 明**显的欺诈信号

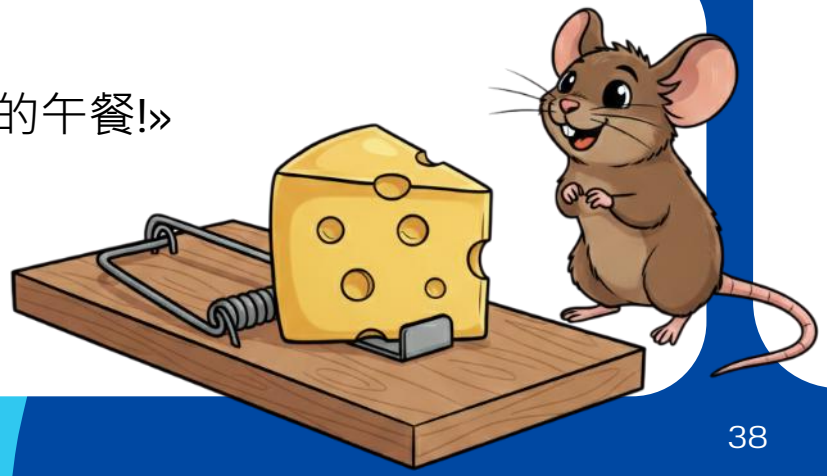
# 安全规则

**检查合法性**

- **所有金融机构必**须持有俄罗斯央行牌照
- **通**过以下目录进行核查:
  *cbr.ru/inside/warning-list*

**首要原则**

«**天下没有免**费的午餐!»



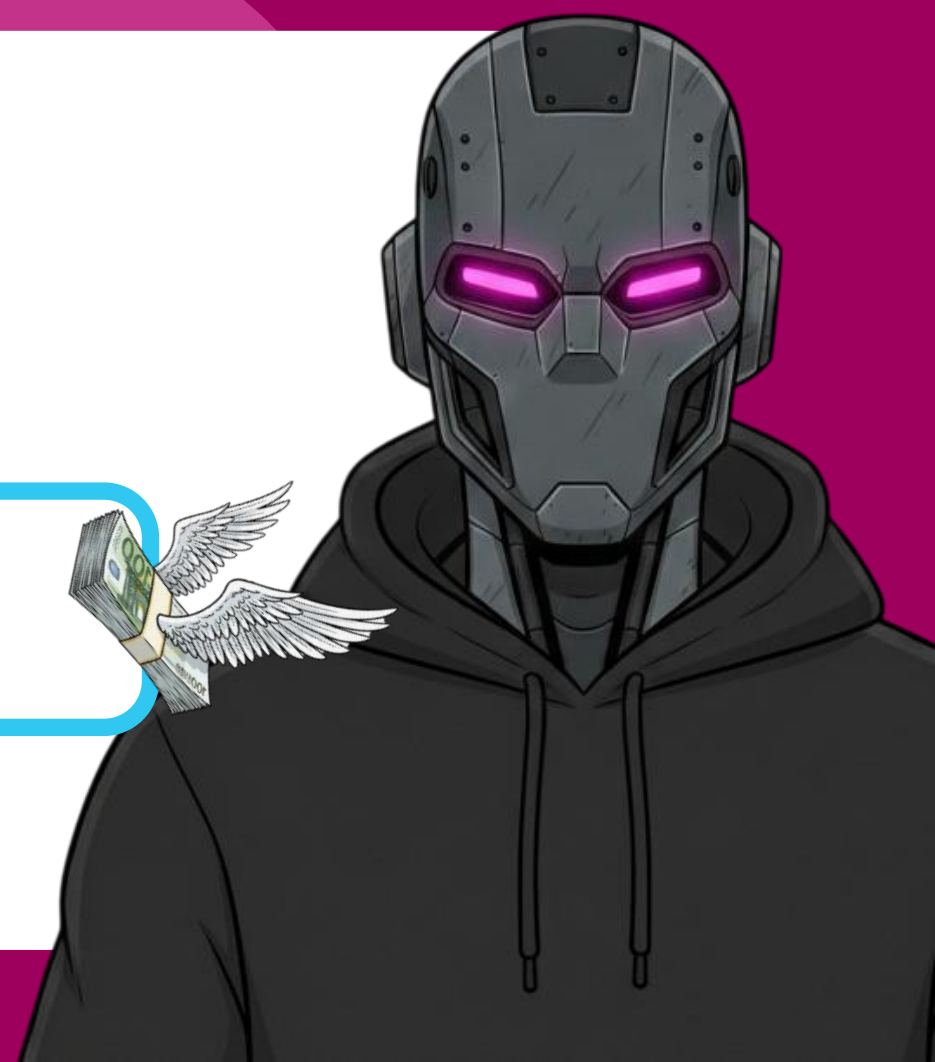
**金融庞氏骗局的特征**

- **承**诺不切实际、远高于市场水平的收益率
- 设有推荐奖励计划
- **缺乏牌照及相关**证明文件
- **激**进的广告宣传并制造紧迫感（“仅限今日！”）
- **不透明性**：**无管理**层或公司注册信息
- **无凭**证接收现金或加密货币

# 犯罪人的主要目标

**麻痹**牺牲者的警惕，
**使其**丧失批判性思维

诈骗手法不断变化，
**但本**质不变



# 线聊天钓鱼商店和网站

## 骗子的公式

骗子创网站，商店，航空公司， 银行的山寨

**把表示物品**，门票打折的旅游项目诱入陷阱

## 安全规则

**必**须用正式app买物品

**不要跟随**电子邮件的链接


**确保站点使用**https，**而不是**http


**网上**购物的单独卡

检查文本和站点名称中的错误

**使用防病毒**软件

# 鲜花配送与“国家服务”网站

## 诈骗分子方式

**“配送服务”来电**

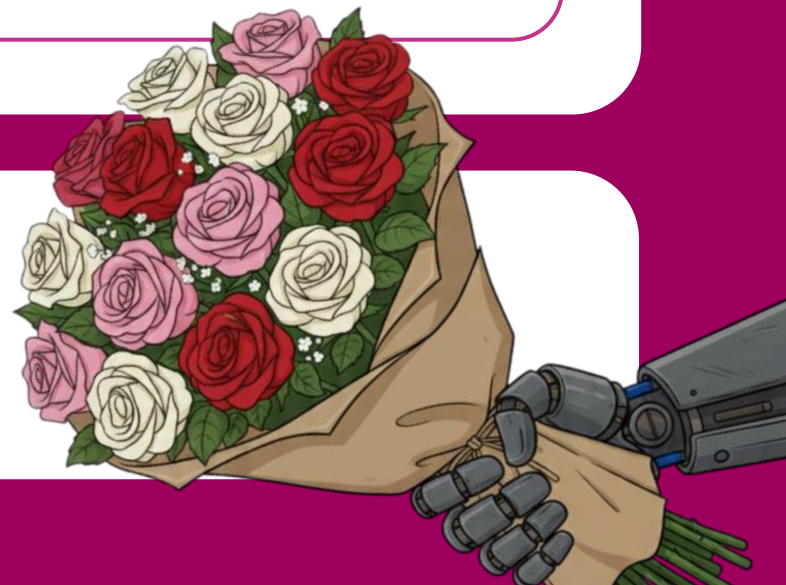
要求提供短信中的“确认”码

**“俄联邦通信监管局”来电**

通知存在不安全情况

**第二通电话“安全部门”来电**

帮助恢复“公共服务平台”网站访问权限



## 安全须知

- • **切勿告知短信**验证码 - 这是用于申请小额贷款的验证码
- •**自己**问自己：你是否在等快递？如果没有 → **是**骗子

# 基于人工智能的银行卡冻结

## 诈骗分子手段

**冒充“客户”给银行打电话**

提供个人身份信息，利用人工智能模仿声音

→

冻结银行卡

原因：挂失、被盗等

→

**威吓受害者**

索要钱财


## 安全规则

请仅拨打银行官方电话号码

**任何情况下都不要**转账

**把**这个计划告诉所有亲戚

# 全球性问题

## 世界成年人口

**57%**
被视为欺诈

**54%**
在网购中受害

**48%**
遭受投资诈骗

## 心理后果

**69%**
承受巨大压力

**14%**
家庭关系得到恶化

**17%**
失去自信

## 主要防线是批判性思维与数字素养

- 每四个自认为谨慎的人中，就有一个仍会上当受骗
- 骗子的手段不断翻新，仅靠基本的警惕性已经不够了

# 金融安全国际奥林匹克竞赛

**奥林匹克竞赛题目是根据程序编写的**

**高中学生**

- **数学**
- **信息学**
- **社会理论**

**大学生**

- **国**际关系，国外区域研究
- 经济，财政，经济安全
- **数学，信息安全**
- **法学**

## 奖品和优势

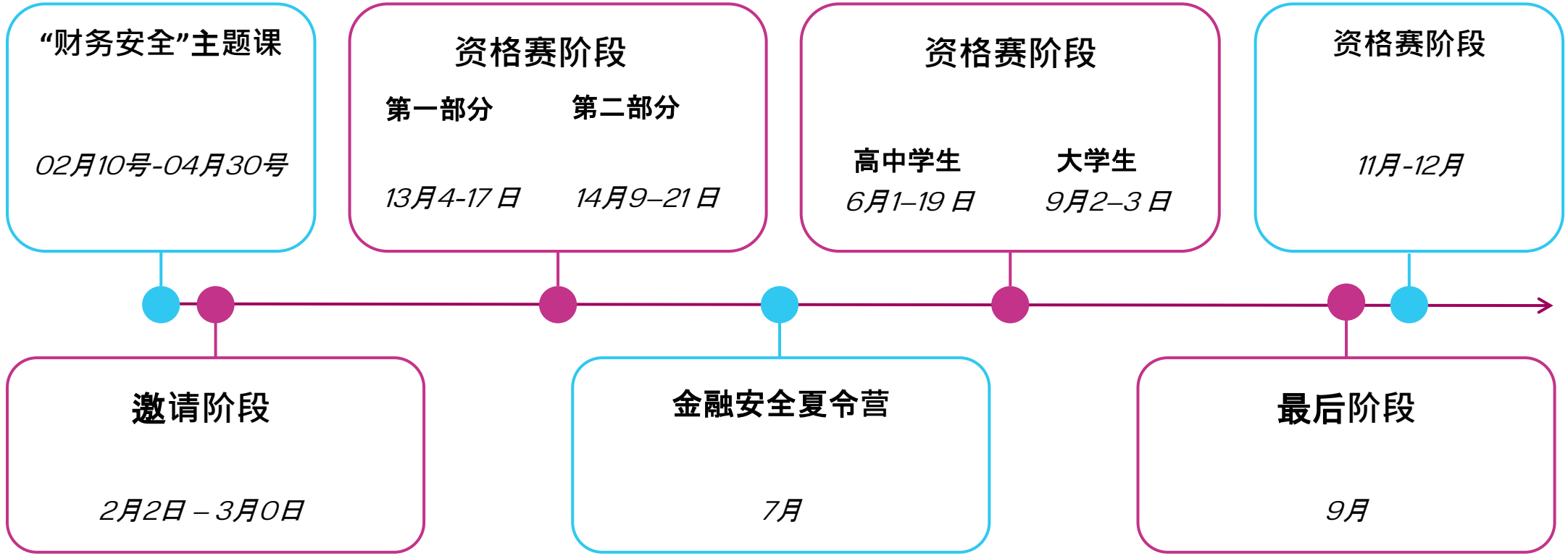
✓ **国**际网络学院高校入学**优惠政策（本科、**硕士、**博士**）

✓ **在俄**罗斯联邦金融监测局及其他机**构实习的机会**

rosfinolymp.ru

# 国际财务安全奥林匹克竞赛

sodrujestvo.org



# 伙伴

俄罗斯联邦金融监督局

俄罗斯联邦教育部

俄罗斯联邦内务部

俄罗斯人民友谊大学

俄罗斯联邦科学和高等教育部

МУМЦФМ

国际反洗钱和反恐怖融资教育训练中心

содружество

«Sodruzhestvo/协会»平台

ПСБ

俄罗斯工业建设银行

ЦЕНТР МЕЖОЛИМПИАДНОЙ ПОДГОТОВКИ

跨奥林匹克竞赛培训中心