网络安全 – 网络犯罪

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

支付安全

《网络安全法》

常见的网络犯罪

提升安全意识

支付安全

支付安全案例

2020年10月12日，在成都眉山某大学就读的张灵（化名）发现自己手机被盗。在手机被盗后9小时内，对方转走了手机号绑定的银行卡中的全部余额，并通过其手机使用京东白条消费7300元。

2020年9月，网友“老骆驼”手机丢失后，通过手机中的App，黑产组织获取了大量个人信息，包括身份证号码、银行卡号等。黑产组织使用“老骆驼”的身份证信息在多个平台开户，并且在各个平台申请了数目不等的贷款。案件暴露出一些银行和互联网平台还存在安全漏洞。这些漏洞给了犯罪分子可乘之机。

网络支付安全现状

过去丢手机，可能损失的只是一部手机的钱；如今丢了手机，可能搭上“全部身家”甚至因此背上贷款。

“弱验证”成为互联网金融安全的一大隐患。

- **为了提高便捷性，快速绑卡、一键注册等操作应运而生，认证方式上人脸识别等验证手段优先级下降。**
- **如果仅凭身份证、短信验证码、银行卡号等信息就支持用户进行各类操作，很可能导致在识别认证的过程中，“个人信息”代替“真人”做决定，严重威胁账户安全。**
- **对互联网金融而言，安全性是底线，便捷性是锦上添花。没有安全的便捷，只会给不法分子留下漏洞与可乘之机。**

——《新华时评：网络支付安全为先》

网络支付安全现状

人均损失金额下降，但受骗人群范围有所扩大

- **调查显示，受损群体人均受损金额降低约270元，但受骗人群占比较2020年增加6%，约占总人数的1/7。**
- **其中00后、60岁及以上留守老人、农民、网店店主、企业主、自主创业者、服务业等人群受损比例较高。**
- **从欺诈方式来看，主要表现为网络直播和虚拟币投资。**
- **数据显示曾遭遇过网络直播诈骗的受访群体占比约为11%，平均损失金额超过3500元，其中老年群体遭遇大额欺诈损失比例较高。在参与虚拟币活动群体中，45岁以上人群、小微企业主、自主创业者、学生等群体的占比排名靠前，上述群体因此而发生损失人群比例也高于平均水平。**

——中国银联《2021移动支付安全大调查研究报告》

开通小额免密免签功能的银行卡遗失怎么办？

与正常的银行卡扯失一样，拨打发卡银行服务热线速行电话挂失或者前往银行柜合办理挂失手续。对于挂失之前72小时内发生的小额免密免签盗刷交易，在挂失后按照发卡银行流程申请赔付。

发卡银行在接收到持卡人中请赔付的5个工作日内向中国银联提交补偿申请对于审核确认的，中国银联在2个工作日内将资金返还至持卡人账户。

如何有效保护银行卡信息安全?

- 妥善保管好自己的身份证、银行卡、网银U盘、手机，不外借他人使用，一旦丢失立即挂失
- 开通银行账户变动短信提醒，仔细核对和关注账户变动情况，定期检查账户资金交易明细和余额
- 不要随意丢弃银行卡刷卡消费或使用ATM设备的交易凭条
- 不轻信、不回拨收到的异常信息或电话，如接到银行、支付机构打来电话，应重新拨打客服电话进行核实
- 谨防木马病毒

手机丢失怎么办？

- 挂失手机卡
- 冻结手机网银账户
- 冻结微信账户
- 冻结支付宝账户

《网络安全法》

《中华人民共和国网络安全法》

《中国人民共和国网络安全法》（以下简称《网络安全法》）是我国第一部全面规范网络空间安全管理方面问题的基础性法律，由全国人民代表大会常务要员会于2016年11月7日公布，自2017年6月1日起施行。

《网络安全法》知识讲解

发现网络运营者违反《网络安全法》相关规定，侵犯个人权益的，我们有哪些权利?

- 有权要求网络运营者删除个人信息，发现网络运营者收集、存储的个人信息有错误的
- 有权要求网络运营者予以更正

《网络安全法》禁止哪些个人和组织网络行为?

- 不得危害网络安全，不得利用网络从事危害国家安全、荣誉和扬恐怖主义、极端主义利益的事情
- 不得宣，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序
- 侵害他人名誉、隐私、知识产权和其他合法权益等活动

法案如何更有效保护公民个人信息安全

《网络安全法》第四章在全国人大常委会《关于加强网络信息保护的决定》的基础上用较大的篇幅专章规定了公民个人信息保护的基本法律制度。

这之中有四大亮点，引人注目:

1.网络运营者收集、使用个人信息必须符合合法、正当、必要原则。

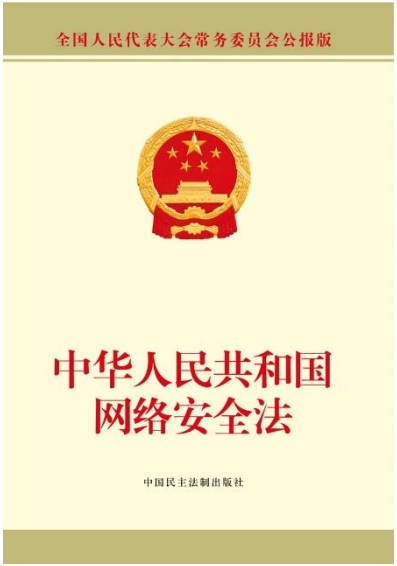
2.网络运营商收集、使用公民个人信息的目的明确原则和知情同意原则。

3.公民个人信息的删除权和更正权制度，即个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息。

4.网络安全监督管理机构及其工作人员对公民个人信息、隐私和商业秘密的保密制度等。

对网络安全法的认识

- 《网络安全法》的制定旨在保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展。
- 《网络安全法》主要适用于在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理等事宜。
- 《网络安全法》基本制度内容涉及网络安全支持与促进、网络运行安全、关键信息基础设施、网络信息安全、监测预警与应急处置以及法律责任等方面。



安全攻略

常见的网络犯罪

- **电信诈骗**：电信诈骗指通过**电话、网络和短信**方式，编造虚假信息，设置骗局，对受害人**实施远程、非接触式诈骗，诱使受害人打款或转账的犯罪行为**

- **伪基站**：伪基站是不法分子**利用计算机与通讯技术**伪装成运营商的假基站，通过**留用他人手机号码**强行向用户手机**发送诈骗、广告推销等短值息**

常见的网络犯罪

- **钓鱼Wifi：钓鱼WiFi是不法分子部署的与免费WiFi相似的假WiFi，当受者人连接钓鱼WiFi后，手机会自动下载木马病毒，不法分子可据此截取手机中的信息，包括银行卡、微信、支付宝、游戏等账号和密码都有可能被记录下来**

- **二维码诈骗：二维码诈骗是不法分子通过替换商户的收款码、共享单车二维码、罚单二维码等方式更改收款账户，或发布隐藏有木马病毒的二维码一旦受害人扫码支付，使可轻松获取受售人的钱财。**

常见的网络犯罪

- **恶意充电宝：病毒充电宝是被不法分子植入木马病毒的充电宝，通常放置在公共场所，一旦受害人连接充电，手机便会自动下载木马病毒，不法分子通过读取受害人通信录、银行卡、支付宝等的信息实施诈骗、勒索等非法活动**

- **移动支付诈骗：移动支付诈骗是用户在使用移动终端进行支付时，不法分子利用黑客技术、终端漏洞或用户疏忽等，盗取用户信息，骗取受害人钱财的行为**

常见的网络犯罪

- **指纹识别诈骗：**指纹识别诈骗是不法分子利用受害人使用的**指纹锁和指纹支付过程中的漏洞实施诈骗行为**

- **网购诈骗：**网购诈骗是不法分子**利用受害人在网购过程中的疏忽实施的诈骗**

身边的网络犯罪

- **东西湖警方破获一起特大电信网络诈骗案，19人被刑拘**

用正规股票交易软件进行投资，无法满足某些股民“以小博大”的赌博心态。狡猾的诈骗分子看准了这个机会，炮制具有“十倍杠杆”的股票软件，并通过反向荐股、虚拟交易的手法诈骗股民资金，不少人被骗的血本无归。

东西湖区警方通过3个多月的侦查，于2020年1月9日将该荐股诈骗团伙一网打尽，共刑拘19名嫌疑人，涉案金额500余万元。

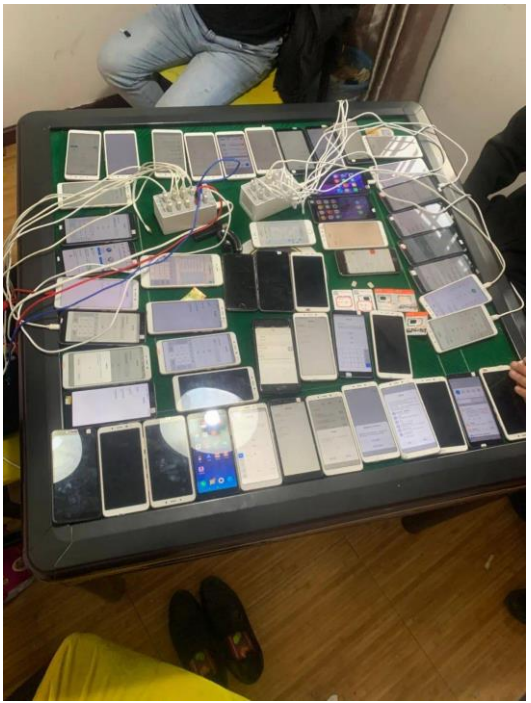
身边的网络犯罪

➢ 东西湖警方重要提醒！已有人被骗80000元！

2020年11月，东西湖区公安分局反电诈专班捣毁一情感咨询诈骗团伙，此类诈骗方式被公安机关打击尚属全省首例。

“痴男痴女”们在网上添加情感导师的微信后，却被告知要收取4800元费用，才能进行一对一的专业专项指导。

在当事人犹豫不决时，情感导师又主动说先收取2400元的入门费，见到成效后再支付余下尾款。打消顾虑的咨询男女，一步步入其套路，最后为图安宁，又不得不付清尾款，独自面对人财两空的伤心境地。



提升安全意识

提升安全意识，培养良好习惯

- 经常用于网络支付的银行卡不要存放太多资金，设置每日网络消费、转账限额
- 签约短信通知服务和盗刷保险服务，可以为资金财产安全保驾护航
- 不同网络支付账号建议设置不同密码
- 用于网络支付的电脑或移动终端应安装安全软件，并定期进行扫描
- 不要点击来历不明的链接，在进行网络支付或退款等操作时应登录正规网站
- 不要告诉他人网络支付的密码和验证码等关键信息
- 不要登录非法网站，避免电脑或移动终端被植入木马病毒

谢谢!