教职工政治学习参考资料

（2024 年第 8 期）

苏州大学党委宣传部编

2024 年 11 月 1 日

教职工政治学习参考资料

（2024 年第 8 期）

苏州大学党委宣传部编　　2024 年 11 月 1 日

● 学习内容

网络安全专题学习

● 参考资料

培养师生正确网络安全观

目录

CONTENTS

01 日常办公用网注意事项

遵守网络使用规定

遵守学校或单位网络使用规定

了解并遵守所在学校或单位的网络使用规定，不违规使用网络资源。

不访问非法网站

避免访问含有违法、不良信息的网站，确保网络安全和信息安全。

不随意下载未知来源文件

不下载、不打开来自未知来源的邮件或文件，以防止恶意软件的入侵。

保护个人隐私信息

保护个人信息

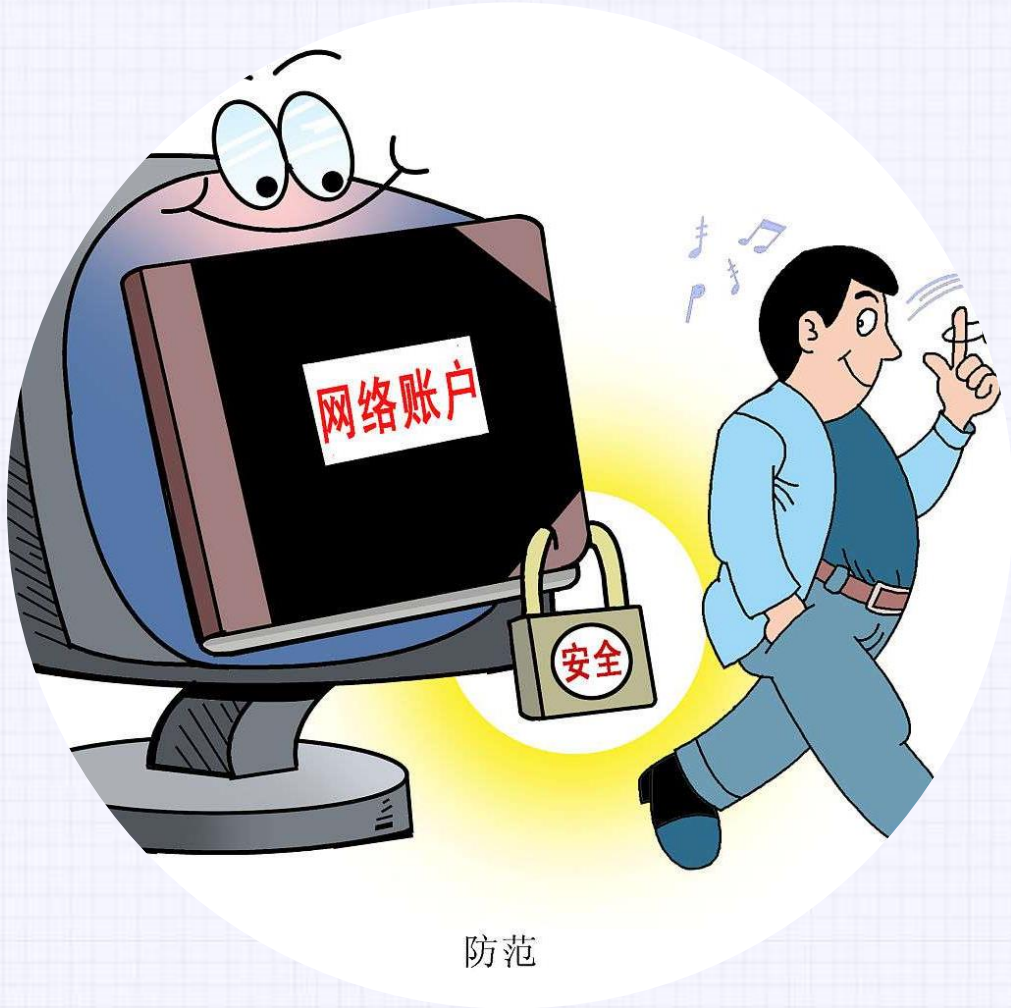
谨慎处理自己的个人信息，如姓名、身份证号、电话号码等，避免泄露。

不在公共网络环境下处理敏感信息

避免在公共网络，如咖啡馆、图书馆等场所处理敏感信息，以防被窃取。

使用加密技术保护数据传输

利用加密技术保护重要数据的传输，确保数据在传输过程中不被窃取或篡改。



防范

防范网络诈骗风险

提高警惕，识别诈骗信息

对于来自陌生人的信息或链接，要保持警惕，不轻易相信，不要提供个人信息或转账。

不随意点击不明链接

避免点击不明来源的链接，以防止恶意软件的下载和安装。

及时举报网络诈骗行为

一旦发现网络诈骗行为，要及时向相关部门举报，以维护自己和他人的权益。

定期更新密码策略

定期更换密码

为了防止密码被破解，应定期更换密码，并避免使用过于简单的密码。

使用强密码策略

采用包含大小写字母、数字和特殊字符的强密码策略，提高密码的安全性。

不在多处使用相同密码

避免在多个网站或应用上使用相同的密码，以减少密码泄露的风险。

02 网络谣言安全教育

识别谣言特征及危害

谣言特征

虚假性、夸大性、误导性、传播速度快。

危害分析

损害个人名誉、扰乱社会秩序、影响社会稳定、造成恐慌和不良后果。

增强信息甄别能力

01

培养批判性思维

学会独立思考，不盲目相信传闻。

02

多渠道求证

通过多个可靠来源获取信息，进行交叉验证。

03

关注官方信息

及时关注政府、权威机构发布的官方信息，了解事实真相。

不传播未经证实信息

慎重转发

对未经证实的信息，不轻易转发或分享，避免成为谣言传播的帮凶。

积极求证

对于不确定的信息，主动向相关部门或专业人士求证，确保信息的真实性。

净网守真

不因好奇心或博取关注而传播不实信息，维护网络空间的清朗。

积极举报网络谣言行为

举报渠道

了解并掌握网络谣言举报的途径和方式，如官方举报平台、电话等。

提供证据

在举报时，提供尽可能详细的信息和证据，以便相关部门及时查处。

配合调查

积极配合有关部门的调查工作，为打击网络谣言贡献力量。

03 抵制网络暴力行为倡导

了解网络暴力表现形式

人身攻击

通过网络平台对他人进行辱骂、诽谤、威胁等言语或行为上的攻击。

侵犯隐私

非法获取并公开他人的私人信息，如住址、电话号码、身份证号等。

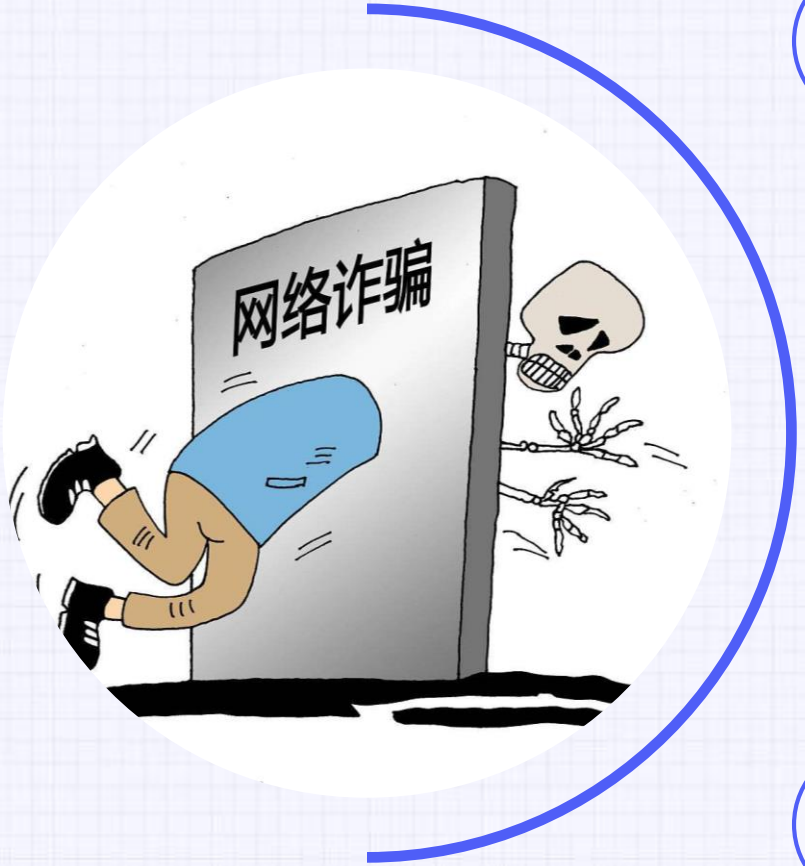
恶意造谣

捏造并散布虚假信息，损害他人名誉和利益。

网络霸凌

通过网络对特定个体或群体进行持续的、恶意的骚扰和欺凌。

自觉抵制参与网络暴力



01

增强法律意识

了解相关法律法规，明确网络言行的法律边界。

02

理性表达观点

保持冷静和客观，避免情绪化的言辞和行为。

03

尊重他人隐私

不传播、不询问、不评论他人的私人信息。

04

举报违法行为

发现网络暴力行为时，及时向相关部门举报。

关爱受害者提供心理支持

建立支持机制

学校、社会应建立网络暴力受害者支持机制，提供必要的帮助和关怀。

鼓励正面应对

鼓励受害者勇敢站出来，维护自己的合法权益，同时提醒他们注意保护个人隐私和安全。

心理咨询与辅导

为受害者提供心理咨询和辅导服务，帮助他们走出心理阴影。

加强宣传教育

通过宣传教育提高公众对网络暴力危害性的认识，形成全校共同抵制网络暴力的氛围。

倡导文明上网新风尚

树立文明上网意识

倡导以文明、理性、友善的态度参与网络活动。

推广网络道德规范

制定并推广网络道德规范，引导师生自觉遵守。

开展文明上网活动

组织各类文明上网主题活动，提高师生的参与度和认同感。

营造良好网络环境

共同努力营造一个健康、和谐、充满正能量的网络环境。

04 树立正确网络安全观念

认识网络安全重要性

信息安全

保护个人隐私不被泄露，确保个人信息安全。

财产安全

预防网络诈骗，避免经济损失。

社会安全

维护网络空间秩序，促进社会稳定和谐。

增强网络安全防范意识

01

警惕网络风险

时刻保持警惕，不轻易相信陌生信息。

02

识别网络陷阱

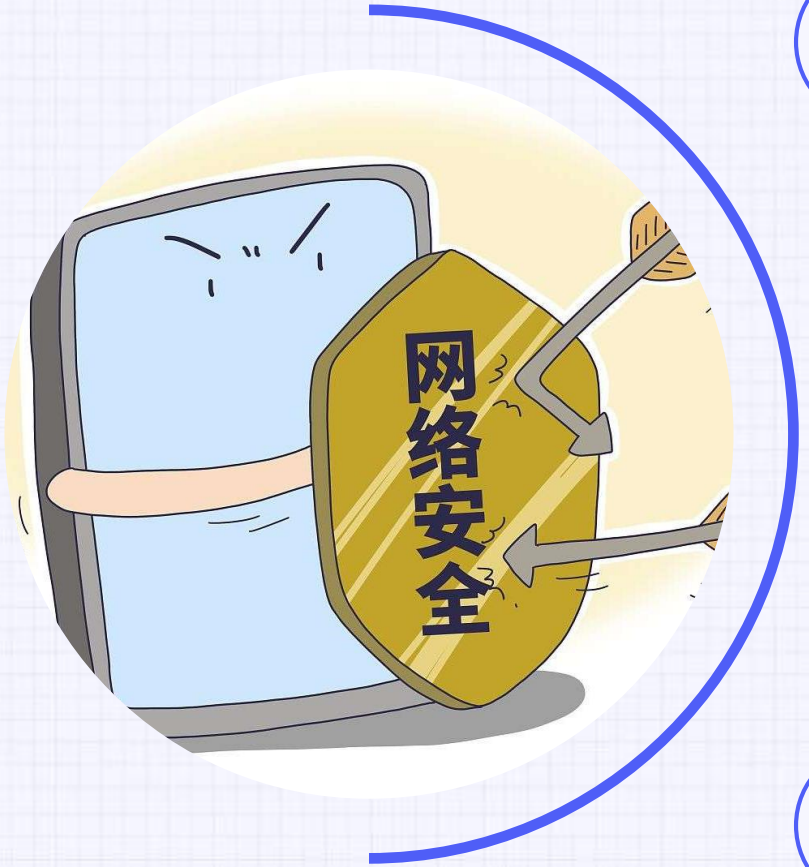
学会辨别网络诈骗、钓鱼网站等陷阱。

03

防范网络攻击

了解常见网络攻击手段，采取相应防护措施。

掌握基本防护技能方法



01

设置复杂密码

使用高强度密码，定期更换。

02

安装安全软件

安装防病毒、防火墙等软件，定期更新。

03

不随意连接公共WiFi

避免在公共WiFi环境下进行敏感操作。

04

保护个人信息

谨慎处理个人信息，不轻易透露给他人。

积极参与网络安全宣传

宣传网络安全知识

通过社交媒体、宣传栏等途径普及网络安全知识。

参与网络安全活动

积极参加各类网络安全主题活动，提高网络安全意识。

举报网络违法行为

发现网络违法行为及时举报，共同维护网络空间安全。

05 培养优秀网络安全素养途径

学习相关法律法规知识

了解国家网络安全法律法规

学习《网络安全法》、《数据安全法》等，明确网络行为的法律边界。

掌握个人信息保护规定

熟悉个人信息保护的相关法律条款，增强个人信息保护意识。

遵守网络道德规范

学习并遵守网络道德规范，维护网络空间的文明与和谐。

关注行业动态了解新技术

关注网络安全行业动态

通过阅读行业资讯、参加相关会议等方式，及时了解网络安全领域的最新动态。

如：中央网络安全和信息化委员会办公室官网

学习新技术和新知识

了解并掌握新兴的网络安全技术，如云计算安全、大数据安全等。

如：CSDN博客

提高对新型网络威胁的警惕性

关注新型网络攻击手段和防御方法，提高自我保护能力。

如：国家互联网应急中心官网

参加线上线下培训活动

参加学校组织的网络安全培训

积极参与学校举办的网络安全培训课程，提升自身网络安全素养。

参与线上网络安全教育

利用网络资源，学习网络安全相关课程，拓宽知识面。

如：教育网络安全服务平台

加入网络安全社团或组织

通过加入相关社团或组织，与同行交流学习，共同提升网络安全技能。

实践锻炼提升应对能力

参与网络安全竞赛

通过参加网络安全竞赛，锻炼实际操作能力，提高应对网络安全事件的水平。

进行网络安全攻防演练

模拟网络攻击和防御场景，提升实战经验和应急响应能力。

积极参与网络安全实践活动

通过参与网络安全检查、漏洞挖掘等实践活动，加深对网络安全的理解和应用能力。

感谢您的观看

THANKS

个人信息保护
——从意识到行动

目录

PART . 01

个人信息保护概念及法律责任解读

哪些信息是指个人信息?

《中华人民共和国民法典》第一千零三十四条：自然人的个人信息受法律保护。个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

个人信息的法定定义

什么是个人信息?

- **《个人信息保护法》第4条**：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

- 根据**GB/T 35273-2020《信息安全技术个人信息安全规范》**相关规定：个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

什么是敏感个人信息?

- **《个人信息保护法》第28条**：敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

- 只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

13类个人信息列举

类别	举例
个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等；
个人身份信息	身份证、军官证、护照、驾驶证、工作证、 出入证、社保卡、居住证等；
个人身份识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等；
网络身份标识信息	个人信息主体账号、 IP地址、个人数字证书等；
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、 医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、 以往病史、诊治情况、家族病史、现病史、传染病史等， 以及与个人身体健康状况相关的信息，如体重、身高、肺活量等；
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等；
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等） 、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等， 以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息；
个人通信信息	通信记录和内容、短信、彩信、 电子邮件，以及描述个人通信的数据（通常称为元数据） 等；
联系人信息	通讯录、好友列表、群列表、 电子邮件地址列表等；
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、 收藏列表等；
个人常用设备信息	指包括硬件序列号、设备MAC地址、软件列表、 唯一设备识别码等在内的描述个人常用设备基本情况的信息；
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等；
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等。

9类敏感个人信息列举

类别	举例
生物识别信息	个人基因、指纹、声纹、掌纹、眼纹、耳廓、虹膜、面部识别特征、步态等
宗教信仰信息	信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动、特殊宗教习俗等
特定身份信息	犯罪人员身份信息、残障人士身份信息、特定工作信息（如军人、警察）、身份证件号码等
医疗健康信息	病症、住院志、医嘱单、检验报告、检查报告、手术及麻醉记录、护理记录、用药记录、生育信息、家族病史、传染病史等
金融账户信息	银行、证券、基金、保险、公积金等账户的账号及密码，公积金联名账号、支付账号、银行卡磁道数据（或芯片等效信息）以及基于账户信息产生的支付标记信息等
行踪轨迹信息	实时精准定位信息、GPS 车辆轨迹信息、航班车票信息、特定住宿信息等
不满十四周岁未成年人个人信息	不满十四周岁未成年人的个人信息
身份鉴别信息	登录密码、支付密码、账户查询密码、交易密码、动态口令、口令保护答案等
其他敏感个人信息	网页浏览信息、婚史、性取向、通信内容、征信信息、未公开的违法犯罪记录等

《个人信息保护法》违法后果

停业整顿、 吊销业务许可（营业执照）、市场禁入

责令暂停或终止提供服务

三类处罚措施，最高处罚五千万或5%营业额

- 处理个人信息未履行个人信息保护义务的，由履行个人信息保护职责的部门**责令改正，给予警告，没收违法所得**，对违法处理个人信息的应用程序，**责令暂停或者终止提供服务**；拒不改正的，并处**一百万元以下罚款**；对直接负责的**主管人员和其他直接责任人员处一万元以上十万元以下罚款**。
- 处理个人信息未履行个人信息保护义务情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，**并处五千万元以下或者上一年度营业额百分之五以下罚款**，并可以责令暂停相关业务或者停业整顿、通报有关主管部门**吊销相关业务许可或者吊销营业执照**；对直接负责的主管人员和其他直接责任人员处**十万元以上一百万元以下罚款**，并可以决定**禁止其在一定期限内担任**相关企业的董事、监事、高级管理人员和个人信息保护负责人。

个人信息保护法主要内容

- **第四条** 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

  个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

- **第十五条** 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

  个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

- **第十六条** 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

- **第十七条** 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

  （一）个人信息处理者的名称或者姓名和联系方式；

  （二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

  （三）个人行使本法规定权利的方式和程序；

  （四）法律、行政法规规定应当告知的其他事项。

个人信息保护法主要内容

- **第十九条** 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。
- **第二十四条** 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。
- **第二十五条** 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。
- **第二十六条** 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。
- **第二十七条** 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。
- **第二十八条** 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

个人信息成为数字经济社会运行不可或缺的部分

技术进步

互联网和移动通信技术的飞速发展使得数据收集变得更加便捷。智能手机、智能穿戴设备、社交媒体平台和各类在线服务不断产生和记录大量个人信息。

数据驱动的商业模式

在数字经济中，数据通常被视为新型的资产和生产要素。企业通过分析用户的个人数据来优化产品和服务，实现精准营销，这对于提高运营效率和市场竞争力至关重要。

个人行为的数字化

人们越来越多的日常活动和交互都在数字平台上进行，从在线购物到社交互动，这些行为都在不断生成可用于分析的数据。

PART . 02

国内外个人信息泄露经典案例

全球视角下的个人信息泄露案例——Meta支付7.25亿美元 解决剑桥分析相关隐私诉讼

Oct. 12, 2023, 1:18 AM GMT+8

Facebook's $725 Million Cambridge Analytica Deal Gets Final OK

Christopher Brown
Staff Correspondent

- Court overrules objections to size, scope of deal
- Suit focused on data sharing with Trump-tied firm

Meta Platforms Inc. will pay $725 million to settle claims it violated Facebook users' privacy by sharing their personal data with Cambridge Analytica, a research firm tied to Donald Trump's campaign, during the 2016 presidential-election cycle.

The settlement, with an estimated class size between 250 and 280 million claimants, provides the largest data-privacy class action recovery to date, according to attorneys for the plaintiffs.

Judge Vince Chhabria of the US District Court for the Northern District of California issued an order giving the deal final approval Tuesday.

泄露数据：8700万 ***赔偿金额：7.25亿美元***

- 2018年3月，英国一家调查机构“剑桥分析”被曝出卷入美国总统选举和英国脱欧投票中。“窃取”5000 万选民的 Facebook 个人资料，利用这些资料构建了一个强大的软件程序来预测和影响投票箱中的选择结果！该公司依靠算法预测用户的政治倾向，借助Facebook的广告投放系统，定向给用户推送新闻，影响他们在美国大选中的投票行为。
- 此事件引起了全球范围内对个人隐私保护问题的关注，并引发了对Facebook公司数据安全措施的质疑。
- 后来，Meta经调查发现，最多有8700万用户的信息被剑桥分析公司不当分享。
- Meta Platforms及其用户已同意就一桩集体诉讼达成和解，和解金额为7.25亿美元。
- Meta 公司于 2022 年 12 月同意支付 7.25 亿美元（约 50.68 亿元人民币），以了结一起有关“剑桥分析丑闻”的集体诉讼。**美国地区 2007 年 5 月 24 日至 2022 年 12 月 22 日期间注册的 Facebook 用户，都有资格获得赔偿。**

全球视角下的个人信息泄露案例——因泄露 5.33 亿用户隐私， Facebook被罚 2.65 亿欧元

泄露数据：5.33亿 ***赔偿金额：2.65亿欧元***

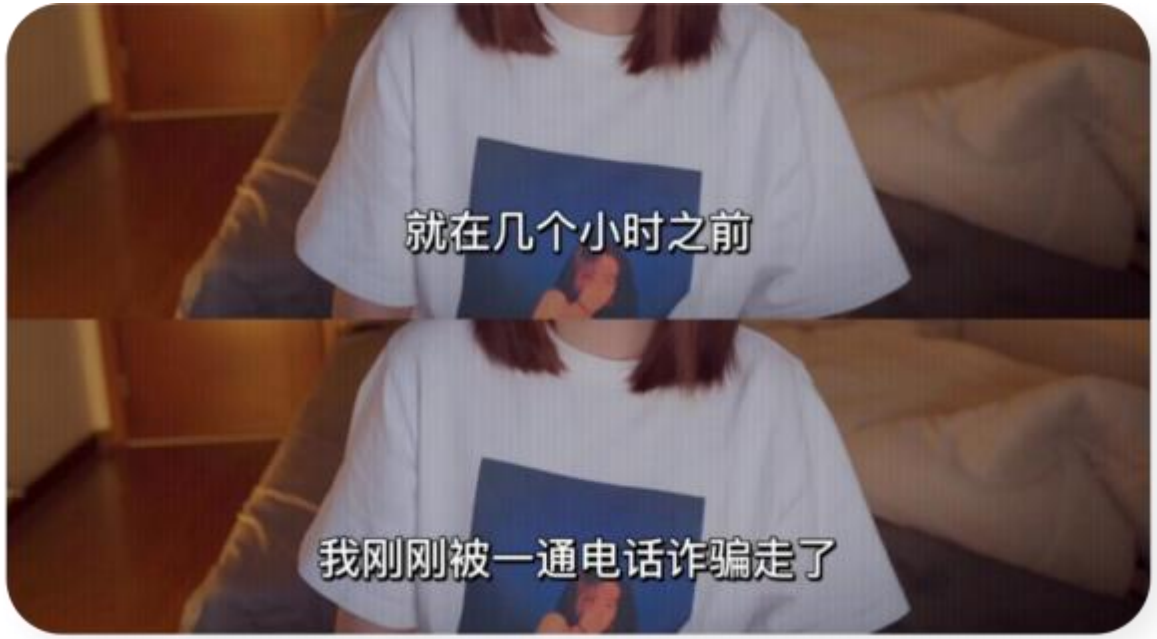
- 2021年4月，**黑客将5.33亿Facebook用户隐私数据泄露至黑客论坛**，其中包括了手机号码、Facebook ID、姓名、性别、位置、人物关系、职业、出生日期和电子邮件地址。

- DPC 于 2021 年 4 月 14 日正式启动了对 Meta 可能违反《通用数据保护条例》（GDPR ）相关规定的调查。爱尔兰数据保护委员会 (DPC) 因 **2021 年 Facebook 大规模数据泄露事件，向其母公司Meta开出 2.65 亿欧元（约20亿人民币）巨额罚单。**

- 根据DPC 的调查结论， Meta违反了 GDPR 第 25章第1及第2条：

25.1 数据控制者应实施适当的技术和管理措施，比如将数据进行假名化，并在处理过程中纳入必要的保障措施，以满足本规定的要求并保护数据主体的权利。
25.2 数据控制者应该使用适当的技术及管理措施，来保证在默认情况下，仅使用处理目的所必要的个人数据。 特别注意这类措施应确保在默认情况下，不应允许任何个人干预，同时只向有限数量的自然人提供个人数据。

物流行业个人信息泄露案例



百万博主遭遇诈骗细节，通话30分钟被骗16万元

- 2021年某日，一名音乐女博主发布了一个七分半的视频，自述了其在30分钟内被诈骗16万元。当天，该博主接到了一个自称某某快递员的电话，对方表示博主的“快递件丢失要给其予十倍赔偿”，**并且在电话中“快递员”准确地报出了她在快递单上留下的化名和快递单号及其住地地址，**并告知博主一会儿公司的“客服”会与她电话联系关于赔偿事宜，这个“快递员”的电话，使她认为这家快递公司还真“负责任”于是就放松了警惕。这位女博主心想“快递员说的”信息与她手机中商家发的信息都对的上，没什么可质疑的。

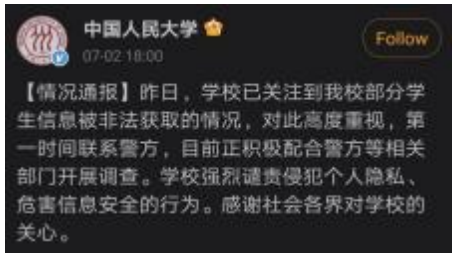
- 之后，“客服”很快就联系上了女博主，她开始一步步在某某快递公司“客服”的诱导下在某宝“备用金”申请所谓“丢失物品”的快递理赔。在操作过程中，快递公司“客服”称因女博主的操作失误，其某宝产生了借贷关系，贷款方向女博主的某宝自动转入了一笔95000元的借贷款。为解除其借贷关系，该快递公司“客服”要求她下载一款名为“某某会议”的APP加入“某某会议”与一个自称是“某宝客服”的工作人员联系。这名“某宝客服”称，女博主的某宝芝麻信用分不足，需向其指定的账户转账18万元进行信用担保，为让女博主继续相信，该“某宝客服”让她用某宝购买了一个“保险”。**于是女博主在“客服”引导下从其名下银行卡上向“客服”指定的账户转账16万元。**

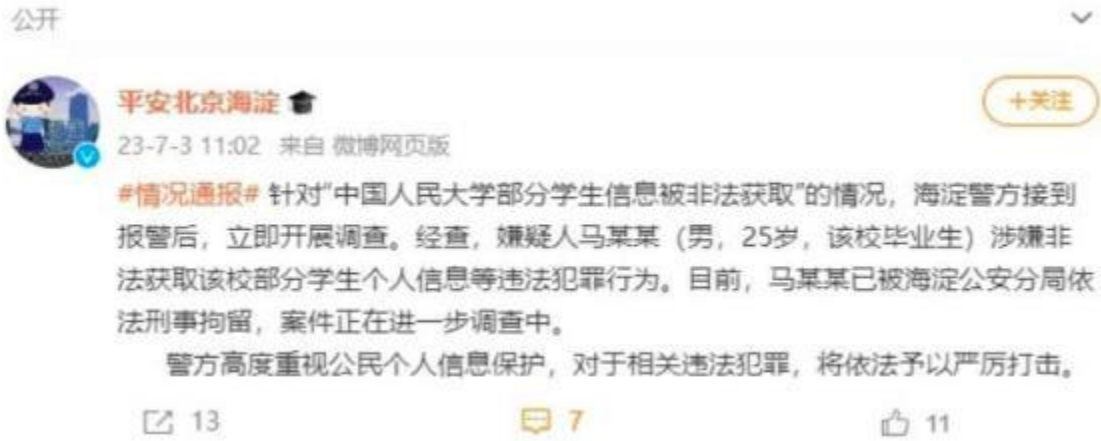
- 当她向朋友借2万想继续转账时，朋友提醒她是不是被骗了？女博主才如梦初醒发觉自己是被骗了。随后前往当地公安机关报案。办案民警迅速抓获了该电诈团伙。

高校个人信息泄露案例

人大万名在校生个人信息被盗取用于“颜值评分”，被刑拘！

- 2023年7月1日，有网友爆料称，中国人民大学一硕士毕业生盗取全校学生的个人信息，制作颜值评分网站供人查看，**被泄露的信息包含学号、姓名、学院、家乡、生日、照片等。**
- 其中，“美颜评分网站”的创建者被网友爆料为中国人民大学22级硕士研究生马某某同学。据大数据发现，自2020年10月以来，一个疑似马某某的个人交媒体平台上的账户**一直在使用非法手段取得了他人信息，创建这个“美颜评级网站”。**
- 7月2日18时许，中国人民大学官方微博发布消息：昨日，学校已关注到部分学生信息被非法获取的情况，对此高度重视，第一时间联系警方，目前正积极配警方等相关部门开展调查。学校强烈谴责侵犯个人隐私、危害信息安全的行为。
- 7月3日，警方，针对“中国人民大学部分学生信息被非法获取”的情况，海淀警方接到报警后，立即开展调查。经查，**马某某涉嫌非法获取该校部分学生个人信息等违法犯罪行为。目前，马某某已被依法刑事拘留。**





保险行业个人信息泄露案例

保险公司销售总监勾结柜面业务人员违规获得公司客户信息，触犯刑法

- 内外勾结的犯罪团伙，通过金钱的诱惑，拉拢保险公司能够接触到所有客户信息的柜面业务人员单某，从而违规获得本保险公司的客户信息。
- **单某将客户信息打印出来后，以一条30元的价格卖给了销售的团队总监李某**。在一年多的时间里，**单某靠贩卖客户信息，收取好处费59万元**。拿到这些信息后，销售团队总监李某指使他的助理童某，将这些名单分发给下级业务经理。总监李某获利不少，助理童某也获取了28万的新人补贴。另一方面，童某将客户的信息下发给业务经理后，业务经理周某就开始动员业务员让客户退保，然后购买新保单。通过这样的方法，周某利用非法获取的信息销售保单，共计获利74万。
- 2023年9月11日，**静安区人民检察院，以侵犯公民个人信息罪**，向法院起诉三名被告人，要求追究其刑事责任。
- 2023年9月26日，静安区人民法院对这起案件作出判决。**被告人单某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑三年，并处罚金60万元**，被告人童某犯侵犯公民个人信息罪判处有期徒刑两年，缓刑两年，并处罚金5万元，被告人周某犯侵犯公民个人信息罪，判处有期徒刑7个月，缓刑一年，并处罚金人民币3万元。

  判决后，三名被告未提起上诉，案件判决生效。随后三名被告缴纳了罚金，并在媒体上公开赔礼道歉。

航空行业个人信息泄露案例

航空APP泄露个人信息，80元可买明星行程

- 微信朋友圈流出了一张贩卖明星艺人航班行程的图片，微信昵称为“AAA帮你追星啊”的网友**在朋友圈爆出了二十多位明星的航班信息**。
- 媒体记者在支付了80元后，这位“追星小助手”果真发来了一份鹿晗5月17日从北京飞往捷克布拉格的行程。网上查询后发现，这份航班行程与鹿晗所参加的综艺节目《奔跑吧》最后一期录制场地完全吻合。
- “追星小助手”透露，**只要交50元学费，就可以查询到任何人的航班出行信息**。据了解，不法商家贩卖航班信息每月收入可达几千到上万，甚至近十万元。
- 黄牛或者粉丝贩卖明星隐私信息这种行为显然已经触犯了法律，情节严重的可能要被追究刑事责任。非法获取、售卖他人身份证等信息，**且售卖50条以上就属于“情节严重”的刑事犯罪**；另外，利用**购买的个人信息去查询明星的航班信息也是一种侵权行为**。

外卖行业个人信息泄露案例

你的订餐地址电话可能被出卖
万条外卖信息有人叫价2000

- 有市民反映，因为在一外卖平台订过一次外卖，他所住的酒店地址、房间号码 、 联系电话等隐私信息竟然全被泄露！

- 记者通过QQ群，联系上了贩卖数据的人陈xx。**这些数据， 全部都是来自外卖平台， 包括姓名、 电话、 性别和地址**。每一万条800元， 五千条起售。陈xx称其手上有来自北京 、 上海 、 广州等地， 最新最全的外卖平台客户 数据。

- 记者从表格中随机选取100个电话号码进行验证。其中有效号码61个，33名机主确认表格中的信息准确， **并确认自己近一两个月内， 在某外卖平台订过餐**。

- 记者调查发现，一些代理运营外卖店的网络公司也在售卖信息！记者联系上了一家成都地区， 代理运营外卖店的网络公司。 其负责人称手上有多家成都地区外卖店的顾客数据。 **姓名、 性别、 电话、 地址， 订餐次数都有， 售价为每条5毛， 保证准确率**。

来源： 新京报

教培行业个人信息泄露案例

兄弟二人里应外"爬"取数万条学生信息获刑

- 2022年9月初，**上海某教培公司员工纷纷反映，查询学生信息的内部系统网速极慢。**技术部门经分析发现，有一员工ID正疯狂查询学生信息，大量挤占网速，经排查，该ID已多次调出学生信息，在短短20天里发起查询数十万次，而持有该ID的员工是8月中旬刚刚入职的汪某甲。

- 9月8日，该公司经理到公安机关报警。据该经理介绍，汪某甲是公司的课程销售，负责协助家长买课、安排学生上课等工作，**有员工ID账户和密码，可以使用工作电脑登录内部系统查询学生信息。**该经理表示，“人工查询根本做不到一天查这么多次，我们认为是计算机程序黑进了公司内网。**按这种查询频率，实在不敢想象有多少学生信息遭泄露。**”

- **公安机关立案后，将正在公司上班的汪某甲抓获归案。**汪某甲交代了自己恶意获取学生信息的事实：“我之前从事过教育行业，知道该行业的工作人员能掌握一定的教育信息，入职公司后，我就通过网络联系技术人员帮我做了一款‘爬虫’软件，这样我用我的ID登录系统后，就可以通过软件大量获取公司内部信息。”该公司经理指出：“该异常ID登录的IP地址都在外地，而汪某甲却一直在公司上班，他一定有共谋！”警方顺藤摸瓜，很快将远在外省的汪某甲的亲弟弟汪某乙抓获，**并在汪某乙的电脑里找到已被下载存储的该公司学生信息2万余组。**汪某乙到案后，交代了和哥哥里应外、伙作案的事实：“哥哥入职后说平时接触到的客户数据有限，让我帮他一起多弄点客户资料出来。哥哥向我提供他的账户ID及密码等信息，技术人员做好软件后远程操作我的电脑查询。”
- **法院以侵犯公民个人信息罪分别判处汪某甲、汪某乙有期徒刑一年三个月和有期徒刑一年，各并处罚金2万元，禁止汪某甲自刑罚执行完毕之日起五年内从事校外培训机构工作。**

房产行业个人信息泄露案例

中华人民共和国中央人民政府
www.gov.cn

首页 | 简 | 繁 | EN | 登录 | 邮箱 | 无障碍

新华视点：数十万条信息泄露，内容精确到门牌号房屋面积——透视房地产信息地下产业链

2016-10-31 16:32 来源：新华社

字号：默认 大 超大 | 打印

新华社广州10月31日电（记者 孙飞 欧甸丘）近年来，各类手机骚扰信息令百姓不胜其烦，其中数量最多的包括卖房、装修和房贷等信息。日前，深圳警方开展了打击整治骚扰信息专项行动，对9家涉嫌侵犯公民个人信息、发送信息干扰正常生活的企业相关人员进行了刑事、治安拘留，并关停了200余个骚扰电话。

警方调查涉案企业发现，其中有数十万条无法解释合法来源的公民房产信息，内容甚至精确到业主门牌号码、面积。对于公民个人房产信息的非法泄露、售卖、使用，已形成一条地下产业链。

精确到门牌、面积！数十万条个人房地产信息被谁泄露了？

各类手机骚扰信息令百姓不胜其烦，其中数量最多的包括卖房、装修和房贷等信息。

- 警方调查涉案企业发现，**其中有数十万条无法解释来源的公民房产信息**，内容甚至精确到业主门牌号码、面积。对于公民个人房产信息的非法泄露、售卖、使用，已形成一条地下产业链。
- 经过审查，深圳警方**刑事拘留13人、治安拘留39人，依托三大运营商关停208个涉及骚扰的电话**。

用户买房后信息被泄露，检察机关启动公益诉讼

- 2017年12月，小朱刚刚买了一套婚房，没多久，便开始接到各种各样的推销电话，一天少则一两个，多则五六个，从售楼商铺到装修设计，从家居建材到小额贷款，**电话那头不但能准确地说出小朱的姓名，甚至连其购买的楼盘房号也一清二楚。**
- 忍无可忍的小朱向警方报案，警方展开调查后发现在诸暨某宾馆两个房间内有大量号码频繁拨打电话。经搜查，房间里竟然是某家居公司雇来的十几个人拿着厚厚的电话材料逐一拨打电话进行推销。同时，警察在现场扣押的u盘中发现85个文档，**每一个文档就是诸暨一个小区的业主信息，共计包含公民个人信息2万余条！**
- 通过审查发现，泄露这些信息的“上家”是装饰公司的设计师骆某，其在工作之余还做着倒卖楼盘信息的小生意。而骆某获取房产信息的“上家”有两个：一个是诸暨某房产公司的内勤财务处，另一个则是某房产公司前员工杨某处。杨某曾经是一家房产公司的员工，离职后自己开了中介公司，从前同事、公司数据员陈某手上免费拿到了大量公民个人信息。经统计，陈某共计提供公民个人信息8万余条！
- **陈某、杨某、骆某三人因犯侵犯公民个人信息罪**，均被判处有期徒刑三年，缓刑四年，并处罚金1万元。

来源：新华、诸暨检察公众号

个人信息泄露事件层出不穷

疑似45亿条个人信息泄露，电商物流行业数据安全警铃再响

网信秦皇岛 + 关注

非法买卖2亿余条公民个人信息 泰州警方摧毁犯罪团伙

人民资讯 2021-10-12 14:31

浙江破获特大侵犯公民个人信息案 逾7亿条信息遭泄露

山西警方侦破一起"暗网"贩卖个人信息案 涉及个人信息近9亿条

来源：新华网 | 2020年08月25日 15:13

广东警方重拳打击整治网络黑产犯罪 缴获被窃取公民信息58亿条

来源：广州日报 | 2019年11月15日 06:30

高中生窃取1亿条公民信息 黑客少年窃取的"数据帝国

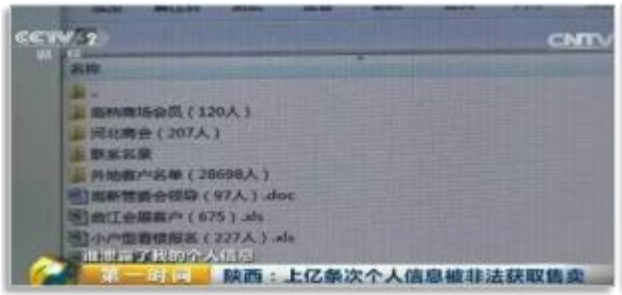
来源：中国青年报 | 作者：李超 | 时间：2019-10-29 | 责编：徐虹

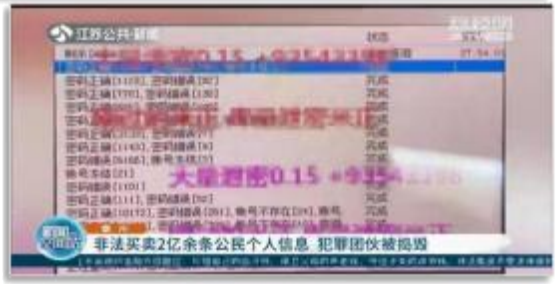
省级健康数据平台汇集个人健康信息1.2亿条 医疗信息百亿条

川观新闻 2020-07-23 15:44

男子非法收集16亿条公民信息 花72元就可查询

发布时间：2017-07-12 08:45:43 | 来源：检察日报 | 作者：佚名

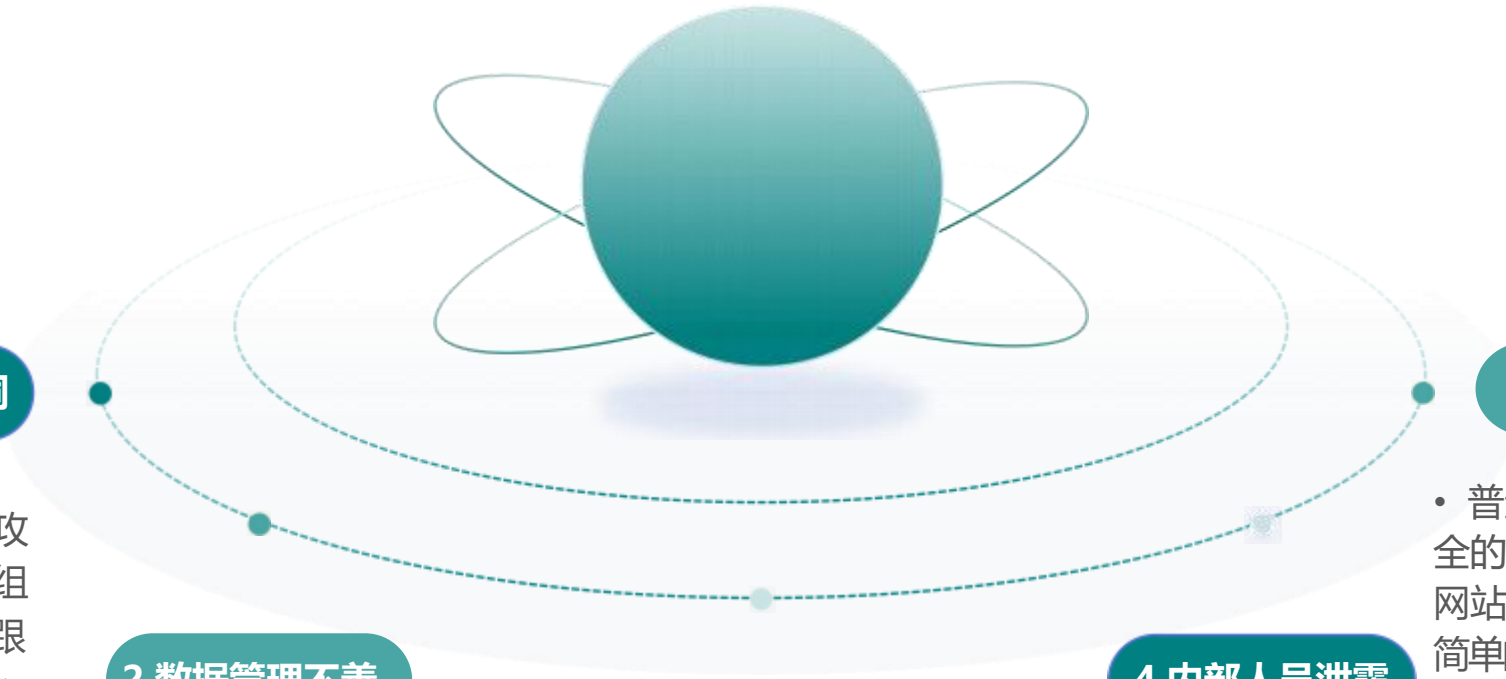




PART . 03

个人信息泄露的成因及后果

个人信息泄露的五大主要原因



1.技术安全漏洞

- 随着技术的发展，黑客攻击手段不断进步，很多组织的信息安全防护措施跟不上黑客技术的发展速度，导致安全漏洞频发。

2.数据管理不善

- 许多公司或组织在个人数据的收集、存储和处理方面存在管理不善的问题。

3.社工工程学攻击

- 黑客通过诱骗个人，利用他们的信任或好奇心理，巧妙地获取敏感信息。

4.内部人员泄露

- 公司或机构内部的员工因利益驱动或疏忽大意等各种原因泄露用户信息。

5.公众意识不足

- 普通用户对于个人信息安全的意识不足，在不安全的网站上录入个人信息，或使用简单的密码，使个人信息被盗取。

个人信息泄露的五大主要原因——技术安全漏洞

- **技术安全漏洞定义：**
  - 技术安全漏洞是指软件或硬件中的弱点，可被恶意利用以窃取、篡改或破坏个人信息。
- **技术安全漏洞重点：**
  - 漏洞通常存在于操作系统、网络服务、数据库系统及应用软件中，这些漏洞可能使个人信息面临泄露的风险。
- **技术安全漏洞造成个人信息泄露实例：**

eBay 数据泄露（2014年）

- 黑客通过公司网络的漏洞攻入eBay系统，泄露了约1.45亿用户的姓名、加密密码、电子邮件地址、邮寄地址、电话号码和出生日期。

Anthem Inc. 医疗保险数据泄露 (2015年)

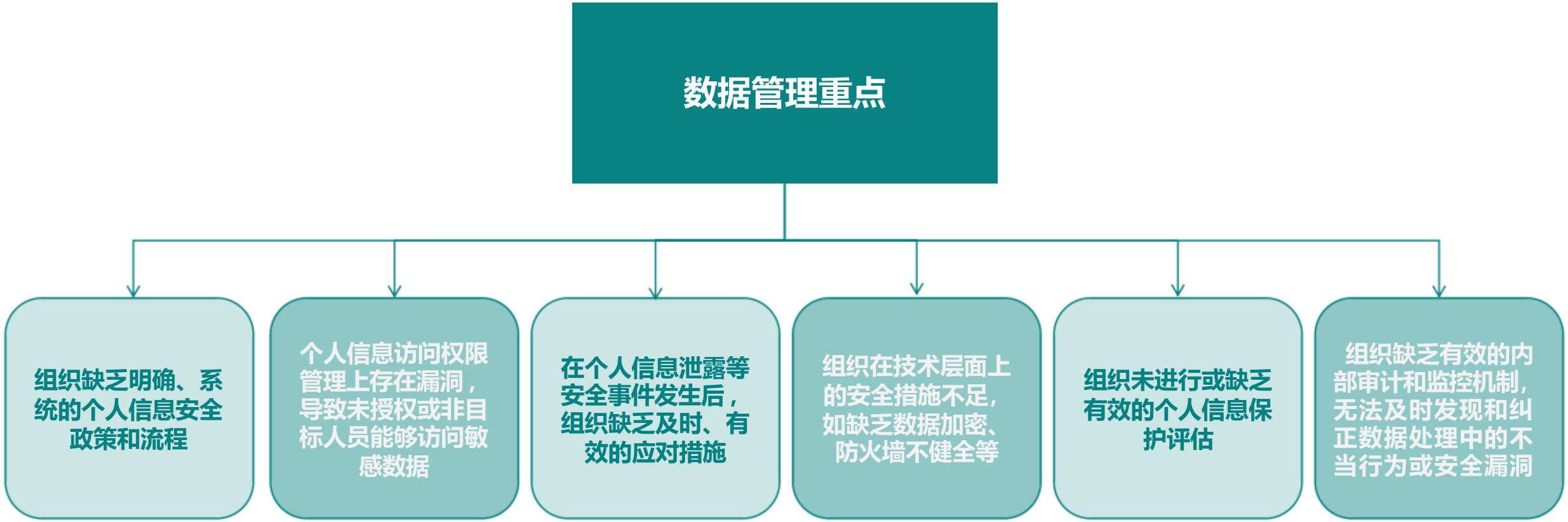
- 由于系统漏洞，美国第二大健康保险公司Anthem遭受重大网络攻击，影响了近8000万客户和员工的个人信息，包括姓名、生日、社会保险号、地址、就业信息和收入数据。

Capital One 金融数据泄露 (2019年)

- 黑客利用Capital One的云存储安全漏洞，泄露了1亿多美国人和600万加拿大人的个人信息，包括社会安全号码、银行账户信息和信用分数。

个人信息泄露的五大主要原因——数据管理不善

- **数据管理不善定义：**
  - 数据管理不善是指在处理个人信息过程中的组织、技术或流程缺陷，导致数据泄露、滥用或丢失。



个人信息泄露的五大主要原因——社会工程学攻击

- **社会工程学攻击定义：**
  - 社会工程学攻击是指攻击者利用人类的心理弱点，如信任、好奇心或恐惧，来操纵个人泄露敏感信息或执行特定操作。
- **社会工程学攻击重点：**
  - 这种泄露可能是由于内部人员的不满、贪婪或对数据保护措施的无知造成的。
- **社会工程学攻击的常见手段：**

网络钓鱼	捕鲸攻击	诱饵
转移盗窃	商业电子邮件妥协	短信钓鱼
交易交换	编造借口	蜜罐陷阱
尾随/搭便车	诱骗电话	冒充

- **社会工程学攻击造成个人信息泄露实例：**

案例：中科大发钓鱼邮件3500余人上当

- 2022年9月8日，中秋节前夕，有中国科技大学的学生发帖称收到“中秋免费月饼领取”的邮件，点开填写资料后月饼没领到，却发现是钓鱼邮件。
- 每年中秋节，中科大制作的特色月饼都会成为“抢手货”。谁料想今年“免费送月饼”竟成一场反诈演练
- 此次演练向全校师生发送模拟钓鱼邮件45000余封（其中学生38000余封，教工6000余封），截止9月8日上午，共有3500余人“上当”，其中学生3100余人，教工400余人。

个人信息泄露的五大主要原因——内部人员泄露

- **内部人员泄露定义：**
  - 内部人员泄露是指组织内部的员工或伙伴因疏忽、恶意或其他原因导致的敏感信息泄露。
- **行业“内鬼”为泄露公民信息的主要源头**

- **最高检：**发布数据显示，2021年，**检察机关起诉侵犯公民个人信息犯罪9800余人**，同比上升64%。公民个人信息泄露成为电信网络诈骗犯罪的源头行为。检察机关办案发现，有不少行业“内鬼”泄露个人信息。**检察机关起诉泄露公民个人信息的“内鬼”500余人**，涉及通信、银行、保险、房产、酒店、物业、物流等多个行业。

- **南方都市报：**南都记者通过中国裁判文书网梳理了2022年1月至2023年9月全国各地法院审结的436宗侵犯公民个人信息罪刑事一审案件。**经分析发现，行业“内鬼”为泄露公民信息的主要源头。**

个人信息泄露的五大主要原因——公众意识不足

- **公众意识不足定义：**
  - 公众意识不足是指普通人群在个人信息保护方面缺乏必要的知识和警觉性，导致了个人信息被轻易获取和滥用。
- **公众意识不足重点：**
  - 不安全的用网习惯、忽视隐私设置。
  - 无意中在社交媒体上泄露个人信息：发布带有地理位置信息的照片、透露生日信息、分享有关家庭成员的信息。
- **公众意识不足造成个人信息泄露实例：**

案例：公共Wi-Fi下的信息泄露

- 张女士在逛商场时，连接上了商场内一个没有设置密码的Wi-Fi，没过多久，张女士就连续收到了多条手机短信提醒，发现她的信用卡竟被盗刷了6笔！每笔的金额都在1500元以上，总金额高达9000多元！
- 市民李先生在餐馆吃饭时，用店里的免费Wi Fi登录了手机，可随后微信号就被盗了。李先生对记者说，从他们店里的Wi Fi上网跟朋友聊天，结果第二天有朋友给我打电话，问是不是向他们借钱。

AI视频换脸软件刷暴朋友圈，隐私谁来负责

- AI换脸APP刷爆微博和朋友圈，用户只需一张正脸照就可以将各种电影、电视剧视频中的主人公替换成自己的脸，官方声称“可以让你出演各种好戏”、“实现和爱豆同台”等等。APP才上线不到一天其背后的用户协议和隐私协议暴露着巨大的隐私泄露风险

个人信息泄露的影响分析——个人层面

隐私侵犯

- 个人信息泄露最直接的影响就是侵犯了个人的隐私权。敏感信息如住址、电话号码、电子邮件等一旦泄露，可能会被不法分子利用。

财产安全风险

- 银行账户信息、信用卡信息等一旦泄露，可能导致经济损失。诈骗分子可能利用这些信息进行盗刷或其他形式的欺诈行为。

个人安全风险

- 泄露的个人信息可能被用于跟踪、骚扰甚至更严重的犯罪行为，威胁个人安全。

社会信任受损

- 个人信息泄露已成为社会关注的焦点，它不仅对受害者造成直接损害，还深刻影响公众对信息安全的信任。

职业影响

- 在某些情况下，个人职业信息的泄露可能对职业生涯造成负面影响，例如泄露的信息被用于职场欺凌或不公正竞争。

心理压力

- 知道自己的个人信息被泄露，可能会对个人造成持续的心理压力和焦虑。

信用评分受损

- 如果个人信息被用来欺诈性地申请信用卡或贷款，这可能对个人的信用评分造成长期损害。

长期监控风险

- 在某些情况下，泄露的信息可能被用于长期监控个人行为，侵犯个人自由。

个人信息泄露的影响分析——社会层面

1 国家安全

- 涉及国家机密、关键基础设施和国家重要个体的信息泄露可能对国家安全构成直接威胁。

2 国际关系影响

- 跨国数据泄露事件可能引起国际纷争，特别是在涉及数据跨境传输和国际法律冲突时。

3 信任度下降

- 频繁的信息泄露事件可能导致公众对政府、企业和技术平台的信任度下降。

4 经济损失

- 信息泄露导致的金融诈骗和身份盗用可以给个人和企业造成巨大经济损失，从宏观层面影响国家经济。

5 犯罪率提高

- 个人信息泄露增加了社会范围内诈骗、身份盗用等犯罪活动的发生率。

6 社会不公

- 信息泄露可能加剧社会不平等，特别是当某些群体比其他群体更容易受到信息泄露的影响时。

PART . 04

增强个人信息保护意识的方法

加强个人信息保护对于推动数字经济的创新发展至关重要

数据安全是数字经济的基石

- 随着大数据、云计算等技术的发展，个人信息成为数字经济的核心资产。确保数据安全是维持数字经济健康发展的基础。

促进消费者信任

- 保护个人信息有助于增强消费者对数字服务的信任，从而促进数字产品和服务的广泛应用。

法律和法规要求

- 个人信息保护法等法律法规的实施，成为企业使用个人信息的重要前提。加强个人信息保护有助于避免法律风险和潜在的经济损失。

促进国际合作与交流

- 在全球化背景下，加强个人信息保护有利于不同国家间的合作与数据交流，促进全球数字经济一体化发展。

你在生活中是否犯过这些错误?

1	使用相同且规律可循的密码：在网银、电商网站、聊天软件、视频网站等使用相同的密码，这样一旦一个账户被破解，其他所有账户都会受到威胁。
2	随意连接公共WI FI：公共WI FI可能不安全，容易遭到黑客攻击，进而导致信息泄露。
3	轻信钓鱼网站的短信：这些短信可能会诱导你点击链接，进而盗取你的个人信息。
4	随意注册各种网站：在不可信的网站上注册时，你可能会不经意间泄露个人信息。
5	在办理会员或填写调查问卷时泄露个人信息：如手机号、住址等。
6	允许APP获取不必要的个人敏感信息。
7	随意扫描二维码：部分二维码可能会链接到恶意网站或下载含有恶意软件的应用。

你在工作中是否犯过这些错误?

1	在学校外部的不安全网络环境中处理工作文件：如在公共WI FI下处理含有敏感信息的工作文件。
2	使用简单密码或相同密码登录学校系统：这可能会导致系统遭到破解。
3	未经加密的远程办公：在非安全网络下远程访问学校系统，可能导致信息泄露。
4	不使用或不当使用安全软件：例如，不使用VPN（虚拟专用网络）来保护数据传输，或不使用防病毒软件来防止恶意软件侵入。这些措施对于保护工作中的敏感信息至关重要。
5	未经核实回复可疑的工作邮件或短信：这可能是钓鱼攻击的一部分。
6	忽视物理安全：例如，将带有敏感信息的笔记本电脑或移动设备无人看管地放置在公共场所，或者不使用屏幕隐私过滤器，从而使旁观者能够看到屏幕上的内容。在处理敏感信息时，物理安全同样重要。

个人角度：生活中，我们应该怎样做来守护个人信息?

- 使用强密码并定期更换：为每个账户设置独特、复杂的密码，并定期更换密码。
- 谨慎使用公共WIFI：避免在公共WIFI下进行敏感操作，如网上银行或购物支付。
- 警惕钓鱼信息：不要点击来历不明的链接，对可疑的短信和邮件保持警惕。
- 谨慎注册网站账户：仅在必要时注册，并尽量减少提供个人信息。
- 避免在不安全的渠道泄露个人信息：在办会员或填调查问卷时，不要轻易留下个人敏感信息。
- 使用官方渠道下载APP：避免Root或越狱手机，只在官方商店下载APP。
- 控制APP权限：仅授权APP访问必要的个人信息。
- 小心扫描二维码：只扫描来自可信来源的二维码。
- 处理快递单等含有个人信息资料的文件时，先抹掉个人信息再丢弃。
- 朋友圈晒照片，一定要谨慎，尽量不晒包含个人信息的照片。
- 一般情况下，简历只提供必要信息。家庭信息，身份证号码等不要过于详细。

个人角度：学习生活中，我们应该怎样做来守护个人信息?

① 在安全的网络环境中处理工作文件：在家工作时使用VPN等保护措施。

② 为办公所用系统设置强密码：且不要和个人账户共用密码。

③ 加强单位敏感信息保护：不在未授权的情况下共享工作数据。

④ 使用加密工具进行远程工作：确保所有远程连接都是安全的。

⑤ 小心处理工作邮件和短信：对可疑邮件和信息保持警惕。

⑥ 使用安全软件保护数据：安装并更新防病毒软件和其他安全工具。

⑦ 使用加密的通讯工具讨论敏感信息：选择安全的通信方式来处理敏感数据。

⑧ 注意物理安全：确保设备处于安全的环境中，避免在公共场所随意展示或遗留个人敏感信息。

应该如何提升个人信息保护意识?

01

■定期安全培训： 学校进行定期的安全培训，包括隐私保护、密码管理和识别网络钓鱼等。

02

■创建安全文化： 在校园内部推广安全意识，鼓励学生对信息安全采取主动和负责的态度。

03

■信息安全事件管理： 建立和维护一个明确的信息安全事件报告和响应流程， 确保师生知道在发现问题时应如何行动。

04

■演习和模拟测试： 定期进行安全演习， 模拟各种信息安全威胁， 训练师生的应急反应能力。

05

■强化政策执行： 通过监控和审计， 确保信息安全政策得到贯彻实施， 并对违反政策的行为采取措施。

06

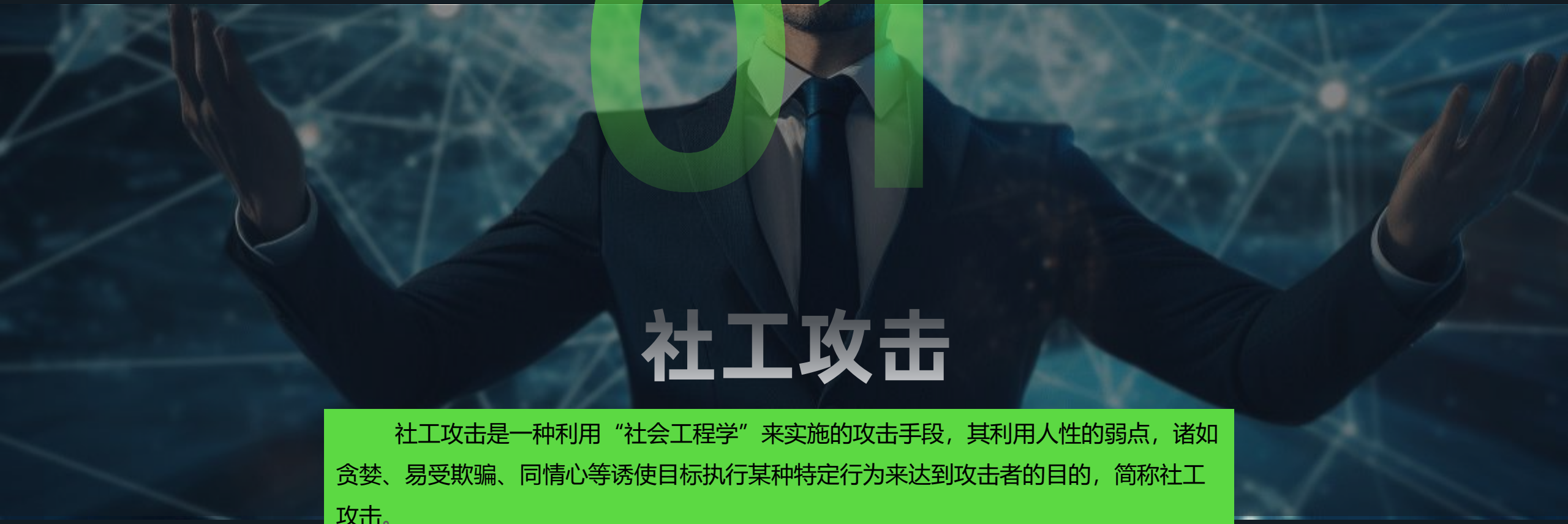
■激励和奖励机制： 设立安全奖励机制， 鼓励师生发现并上报安全漏洞和潜在风险。

谢谢观看

社会工程学及其防护手段

目录

CONTENTS



01

社工攻击

社工攻击是一种利用“社会工程学”来实施的攻击手段，其利用人性的弱点，诸如贪婪、易受欺骗、同情心等诱使目标执行某种特定行为来达到攻击者的目的，简称社工攻击。

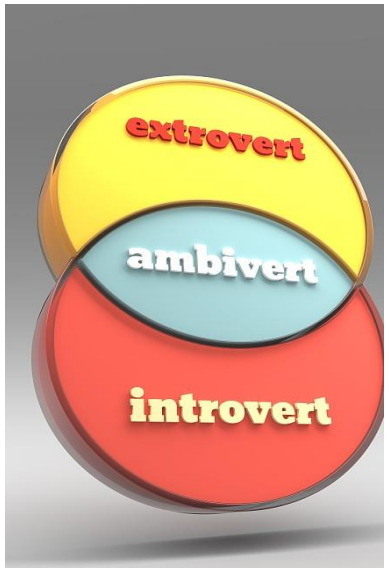
社工攻击的概念

利用人类行为模式的弱点

社会工程学攻击是一种独特的攻击手段，它并不依赖于高深的技术手段，而是利用人类行为模式的弱点，如贪婪、易受欺骗、同情心等心理特征，来诱使目标执行特定的行为。这种攻击方式的核心在于欺骗和操纵，攻击者通过精心设计的场景和故事，使目标在不经意间泄露信息或执行不安全的操作。

社工攻击的目的

社工攻击的主要目的是获取目标的信息、金钱或其他资源。攻击者可能会通过伪装成可信的实体，如银行、同事或朋友，来诱骗目标执行某些操作，如点击恶意链接、提供敏感信息等。这些信息可能包括个人身份信息、银行账户信息、学校内部资料等，对个人和学校都可能造成严重的损失。

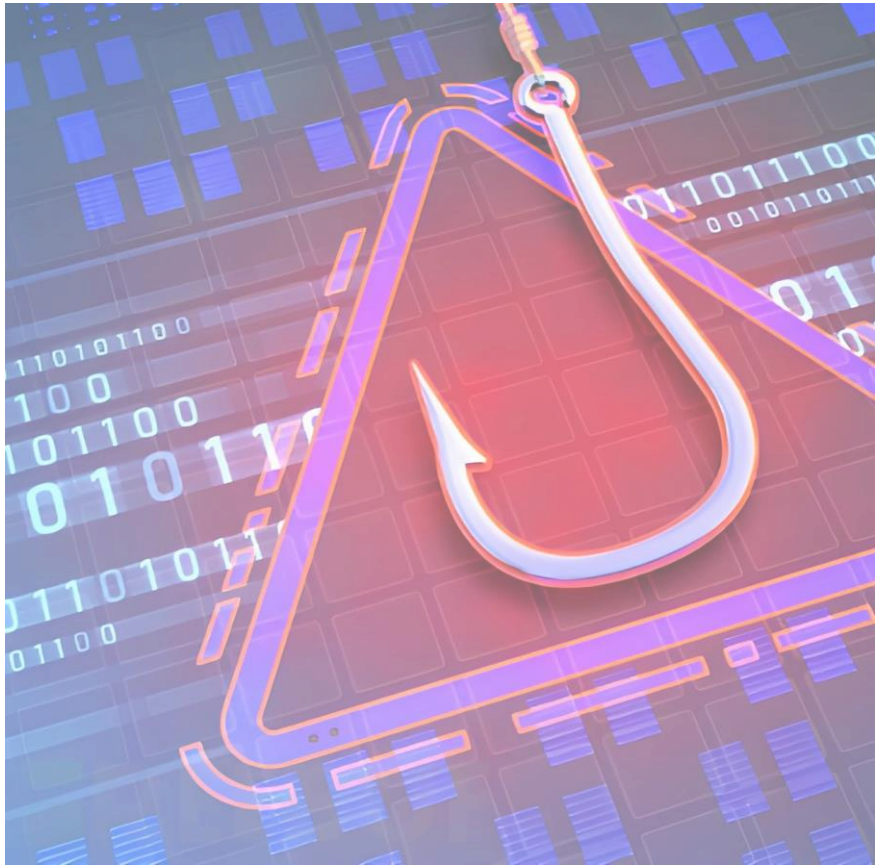


社工攻击的方式

——利用人性的弱点

学生帐号 一击致命

攻击者通过在QQ上搜索某高校群，假装是师兄师姐，等时机成熟，就会以想进学校的线上图书馆阅读一些书，借用一下帐号等理由，成功进入学校内网。而后就可在学校内网进行大规模的横向渗透，给服务器植入勒索病毒等.....

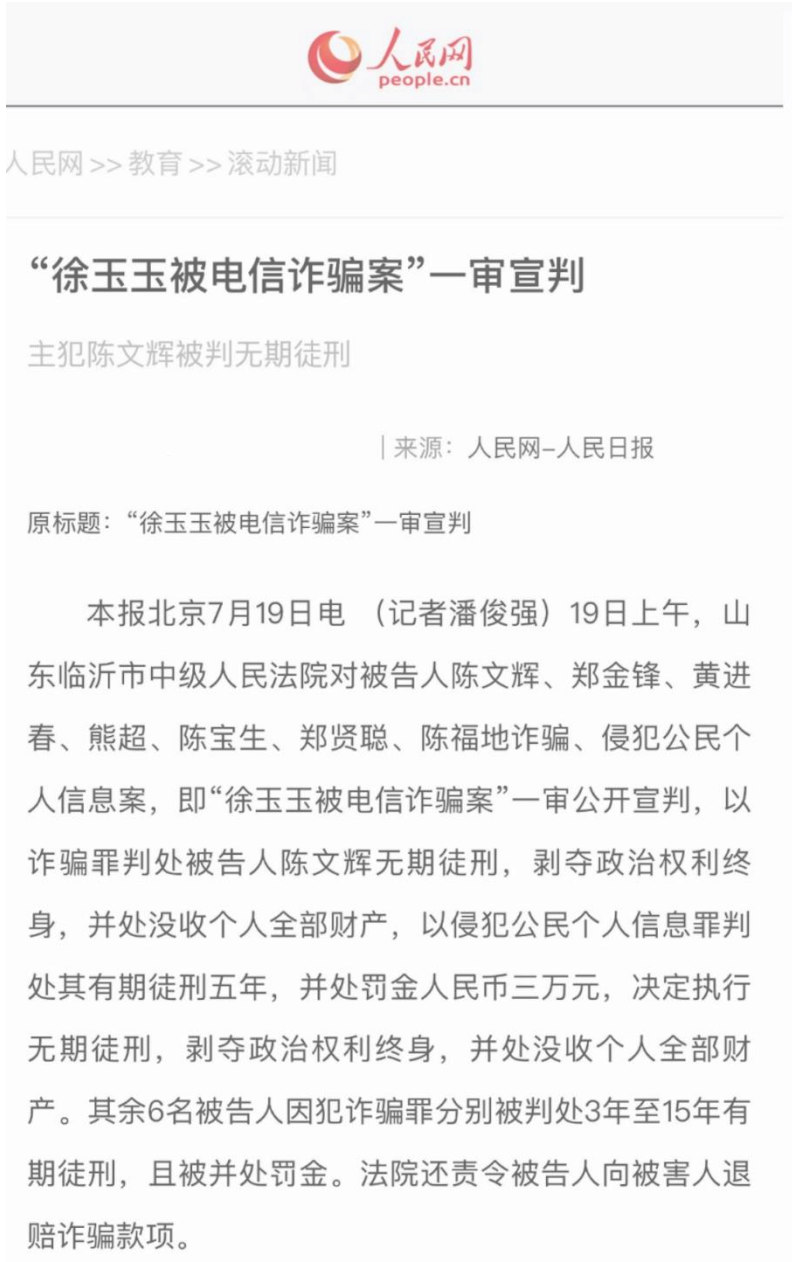


社工攻击的手段

——电信诈骗

冷静思考 识别手段

面对未知的电话、短信或网络消息时，请务必保持冷静与警惕。不要轻易相信陌生人的说辞，特别是那些涉及紧急情况、高额回报或要求提供个人敏感信息的请求。在做出任何决定之前，请务必通过官方渠道或可靠途径核实信息的真实性。保持谨慎，避免成为不法分子的目标，保护好自己的财产和信息安全。



人民网 people.cn

人民网 >> 教育 >> 滚动新闻

“徐玉玉被电信诈骗案”一审宣判

主犯陈文辉被判无期徒刑

| 来源：人民网-人民日报

原标题：“徐玉玉被电信诈骗案”一审宣判

本报北京7月19日电 （记者潘俊强）19日上午，山东临沂市中级人民法院对被告人陈文辉、郑金锋、黄进春、熊超、陈宝生、郑贤聪、陈福地诈骗、侵犯公民个人信息案，即“徐玉玉被电信诈骗案”一审公开宣判，以诈骗罪判处被告人陈文辉无期徒刑，剥夺政治权利终身，并处没收个人全部财产，以侵犯公民个人信息罪判处其有期徒刑五年，并处罚金人民币三万元，决定执行无期徒刑，剥夺政治权利终身，并处没收个人全部财产。其余6名被告人因犯诈骗罪分别被判处3年至15年有期徒刑，且被并处罚金。法院还责令被告人向被害人退赔诈骗款项。

社工攻击的手段

——电信诈骗

总案件数
2130,000 件

5 %

自2013年至2023年，电信诈骗案件在这十年间急剧增加，凸显出电信诈骗问题的严重性和复杂性，这些都是利用了社会工程学来制造的电信诈骗。

社工攻击策略应对

提升应对社会工程学攻击的能力，保护个人的财产安全和人身安全

02

攻击手法

不法分子利用伪装的电子邮件，欺骗收件人下载病毒附件或者点击钓鱼链接，引导收件人连接到特制的网页，让收件人信以为真，输入银行卡号码和账户密码等，从而实现其攻击目的。在频发的安全攻击事件中，钓鱼攻击往往是黑客的首选。

攻击手法

——钓鱼类型

03
二维码
利用定制的二维码
让受害者扫描

02
Wifi钓鱼
利用定制的wifi
让受害者连接

04
水坑攻击
挖掘受害者经常访问网站的漏洞，放入木马进行攻击

01
钓鱼邮件
利用邮件发送
恶意木马或病毒

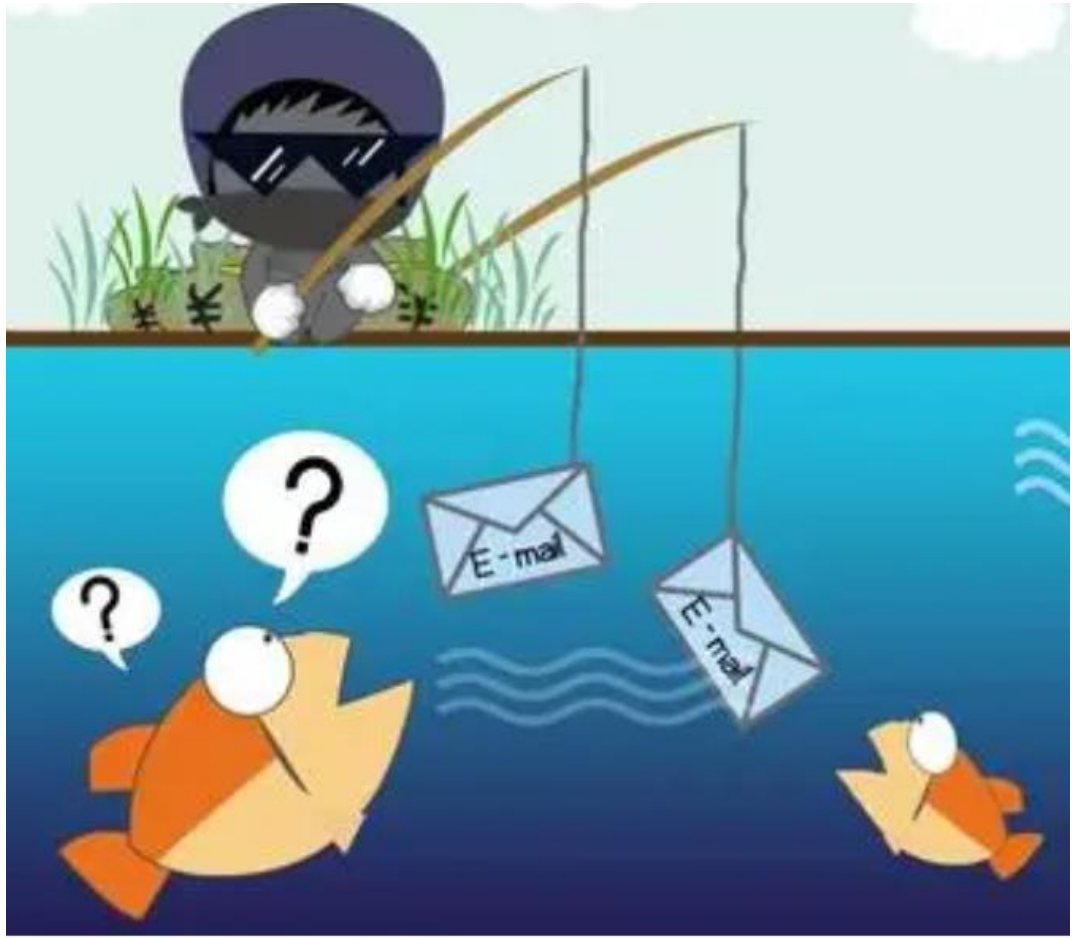
05
U盘钓鱼
利用定制的U盘让受害者插入自己的电脑

攻击手法

——钓鱼类型

钓鱼邮件

钓鱼邮件（Phishing Email）是一种网络诈骗方式，诈骗者通过伪装成可信的实体（如银行、知名公司或政府机构等）发送电子邮件，以诱骗收件人透露敏感信息（如用户名、密码、信用卡卡号等）或执行某些行为（如点击恶意链接、下载恶意软件等）。



攻击手法

——钓鱼类型

WIFI钓鱼

WiFi钓鱼（WiFi Phishing）是一种网络攻击，攻击者通过创建一个伪造的无线网络，诱使受害者连接到这个网络，从而获取受害者的敏感信息，如登录凭据、浏览记录和个人数据等。这种攻击也被称为“恶意热点”（Malicious Hotspot）或“蜜罐”（Honeypot）。

攻击手法

——钓鱼类型

二维码钓鱼

二维码钓鱼（QR Code Phishing）是一种网络攻击，攻击者通过伪造二维码并诱骗受害者扫描，从而引导其访问恶意网站或下载恶意软件等，以窃取个人信息或执行其他恶意操作。

攻击手法

——钓鱼类型

水坑攻击

水坑攻击钓鱼（Watering Hole Attack Phishing）是一种复杂的网络攻击策略，攻击者通过入侵受害者常访问的合法网站，将这些网站变成恶意软件的分发平台。受害者访问被感染的网站时，会不知不觉地下载恶意软件，或被重定向至钓鱼页面，从而被动泄露敏感数据等。

攻击手法

——钓鱼类型

USB攻击

BadUSB是一种网络安全攻击，利用USB设备的固件漏洞来执行恶意操作。固件是设备的低级控制软件，通常用户无法直接访问和修改。BadUSB攻击的原理是重新编译这些固件，使普通的USB设备，如U盘或键盘等，执行恶意攻击行为，而非它们原本的功能。

03

钓鱼案例

通过一些攻击案例，更直观地认识到钓鱼攻击在日常生活中的普遍性，以及其所带来的巨大危害性。

钓鱼攻击

钓鱼攻击的普遍性

钓鱼攻击是一种常见的网络攻击手段，它无处不在，无论是个人还是企业，都可能成为钓鱼攻击的目标。这些攻击通常通过电子邮件、短信、社交媒体等渠道进行，形式多样，难以防范。

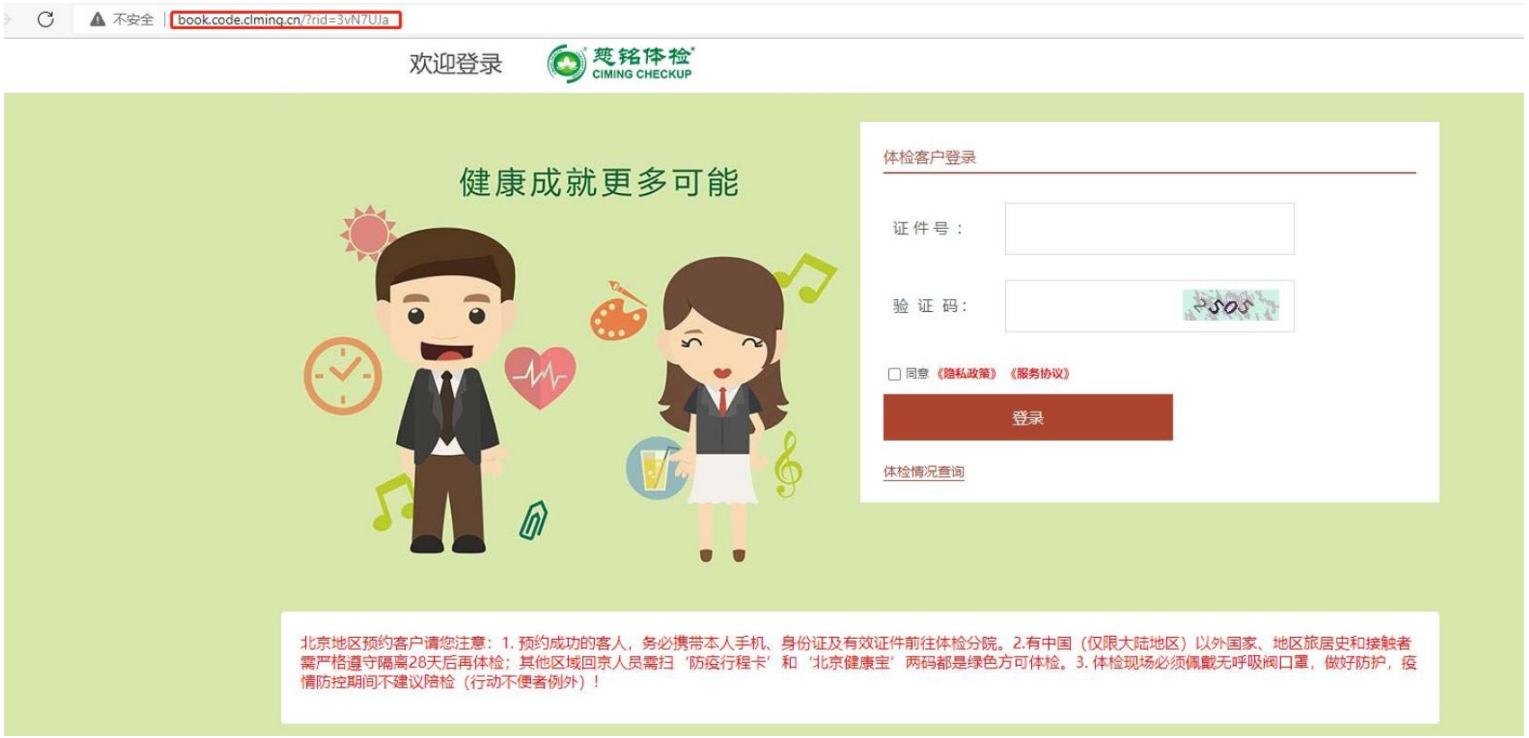
钓鱼攻击的危害性

钓鱼攻击的危害性巨大，它们可能导致个人信息泄露、财产损失、甚至身份盗窃等问题。一旦攻击者获取了目标的敏感信息，他们可能会利用这些信息进行欺诈、盗窃或其他犯罪活动，给受害者带来严重的损失。

钓鱼攻击的案例一

——广撒网链接钓鱼

黑客会对钓鱼邮件的发件人地址进行伪造，比如单位域名的邮箱账号或者系统管理员账号，让我们核实个人信息。收件人通过链接引导进入钓鱼网站，误填账号和密码。



钓鱼攻击的案例二

——二维码补贴诈骗邮件

攻击者在邮件中伪造二维码，诱使收件人扫描并访问恶意网站或下载恶意软件。这种类型的钓鱼攻击利用了人们对二维码的信任，一旦扫描了恶意二维码，受害者就可能泄露敏感信息或遭受其他形式的攻击。

诈骗案例

邮件主题： Re:2022人社部第三季度个人劳动补贴登统计
邮件附件： 2022人社部第三季度个人劳动补贴登统计相关补充材料.docx
诈骗手法： 通常结合**盗号**，向同域名其他邮箱发送；**通过二维码引导进入仿冒的国家部委网站**，骗取银行卡信息。

钓鱼攻击的案例三

——仿冒银行年检诱骗财务加入QQ群汇款

诈骗手法

1.以银行年检为话术，诱骗财务人员加入QQ群

2.在QQ群中冒充领导，要求财务人员转账

钓鱼攻击的案例四

——在知乎编写各种故事，吸引别人点击

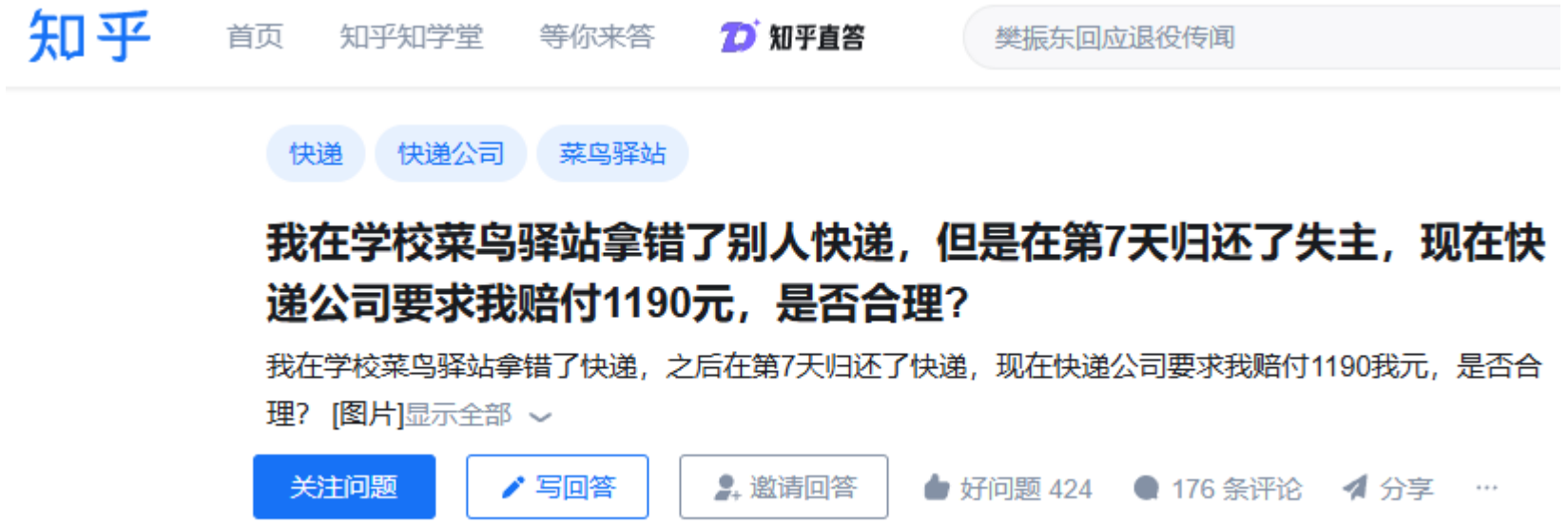
编了一堆故事

还做了 pdf

然后 pdf 不全

说去贴吧下压缩包

看完整版



04

防范意识

防范网络钓鱼：使用安全软件、启用浏览器防钓鱼功能，及时更新系统和软件、小心邮件附件和链接、验证发件人、启用双重认证、使用强密码、不在邮件中提供敏感信息等……

防范意识

——钓鱼类型：钓鱼邮件

钓鱼邮件的原理

钓鱼邮件是一种伪装成可信实体的邮件，旨在诱骗收件人透露敏感信息或执行恶意操作。这些邮件通常包含诱人的标题、伪造的发件人地址、恶意链接或附件等，旨在欺骗收件人进行不安全的操作。

钓鱼邮件的防范

识别钓鱼邮件的关键在于注意邮件的发件人、邮件内容、链接和附件等是否可疑。例如，邮件发件人的地址可能与可信实体不一致，邮件内容可能存在拼写错误或语法错误，链接可能指向不安全的网站等。

防范意识

——钓鱼邮件特征一

伪造身份且含有诱导性关键字：如下图【请点这里进行升级】诱导用户点击，但显示链接与实际链接不一致；或发信人地址与真实地址仅有细微差别；或通过修改“显示名”掩盖实际发件人（比如下图显示为admin，但实际为个人账号）

防范意识

——钓鱼邮件特征二

以标题吸睛：大量钓鱼邮件主题关键字涉及“通知”、“系统升级”、“发票”、“会议日程”等。收到此类关键词的邮件，需提高警惕，不要轻易点击链接或附件。

防范意识

——钓鱼类型：WIFI钓鱼

WIFI钓鱼的原理

攻击者通过创建伪造的无线网络，诱使受害者连接并获取其敏感信息。这些伪造的网络通常看起来与合法的公共无线网络相似，但实际上是由攻击者控制的。

WIFI钓鱼的防范

防范WIFI钓鱼需要谨慎连接公共无线网络，并使用安全软件保护设备。在连接公共无线网络时，应尽量使用加密的连接方式，避免在公共网络中进行敏感操作，如网上银行、购物等。

防范意识

——钓鱼类型：水坑攻击

水坑攻击的原理

水坑攻击是一种针对特定目标的复杂网络攻击，攻击者通过入侵受害者常访问的网站，将恶意软件植入其中。当受害者访问这些网站时，恶意软件就会自动下载并执行，从而实现对目标的攻击。

水坑攻击的防范

防范水坑攻击需要定期更新操作系统和软件，并使用安全软件检测恶意软件。此外，应避免访问不可信的网站，尤其是那些看起来可疑或来源不明的网站。

防范意识

——钓鱼类型：USB攻击

USB攻击的原理

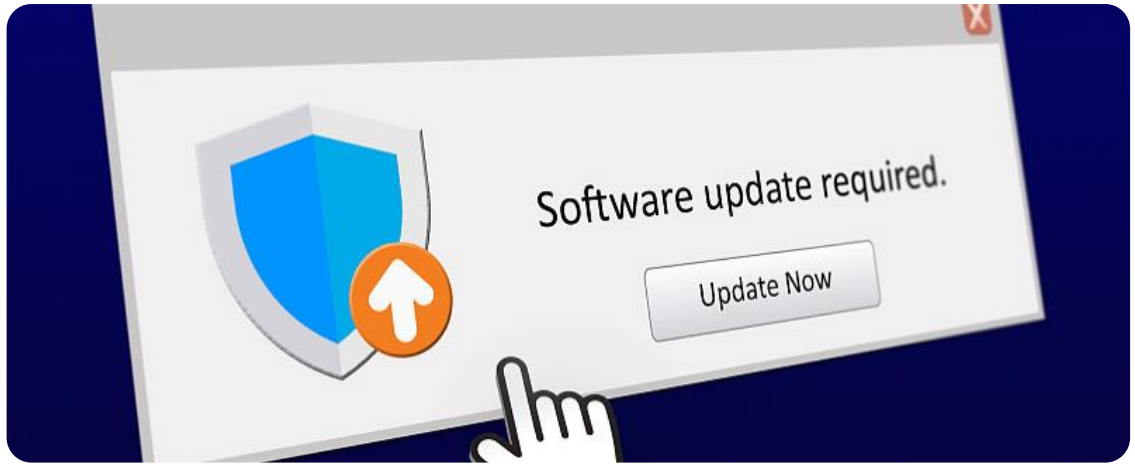
USB攻击利用USB设备的固件漏洞，执行恶意操作。攻击者可能会将恶意软件植入USB设备中，一旦受害者将USB设备插入电脑，恶意软件就会自动执行。

USB攻击的防范

防范USB攻击需要谨慎使用未知来源的USB设备，并定期更新设备固件。在插入USB设备时，应确保设备来源可信，并使用安全软件扫描设备以检测潜在的恶意软件。

防范意识

——使用终端威胁防御系统阻止钓鱼



- **终端威胁防御系统的作用**

使用终端威胁防御系统可以帮助识别和阻止钓鱼攻击，保护个人电脑和移动设备的安全。这些软件通常具备实时监控、恶意软件扫描、钓鱼网站识别等功能，能够及时发现并阻止潜在的威胁。

- **终端威胁防御系统的选择**

选择终端威胁防御系统时，应考虑软件的可靠性、功能性和易用性。应选择知名品牌的软件，并定期更新软件以保持最佳的保护效果。建议，安装学校购买的天融信终端威胁防御系统（http://sd.suda.edu.cn)。

防范意识

——启用浏览器防钓鱼功能

浏览器防钓鱼功能的作用

现代浏览器通常具备防钓鱼功能，可以识别和警告用户潜在的钓鱼网站。当用户尝试访问已知的钓鱼网站时，浏览器会显示警告信息，提醒用户谨慎操作。

浏览器防钓鱼功能的设置

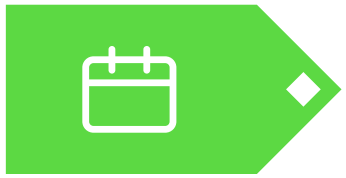
用户可以在浏览器的设置中启用防钓鱼功能。此外，还应保持浏览器的更新，以确保最新的安全功能得到应用。

05

安全意识提升

安全意识提升

——文件保护意识



加强重要文件防护

对重要文件进行加密和备份，以防丢失或泄露。加密可以确保文件在未经授权的情况下无法被访问，备份则可以在原始文件丢失或损坏时进行恢复。

设置强密码

使用强密码，并定期更换密码，以增加账户的安全性。强密码应包含字母、数字和特殊字符的组合，长度至少为8个字符。

安全意识提升

——陌生邮件防范

防范意识的培养

满足以下条件的陌生邮件，在确认邮件完全可信前，请不要点击网页链接或打开附件，也不要输入账号密码等敏感信息进行身份认证。网页链接很有可能是仿冒网站，附件也可能携带木马或病毒：

1. 发件人邮箱地址和发件人名称身份不一致；
2. 发件时间在半夜或凌晨；
3. 夸大事件、制造紧张气氛，造成恐慌；
4. 声称是官方邮件，但机构名称不规范；
5. 提及工资，补助，或者莫名收到的信息等；
6. 提醒用户系统升级、迁移、过期等。

安全意识提升

——日常行为规范

需要做

1. 公私邮箱要分离。
2. 安装杀毒软件，定期更新病毒库并进行全盘扫描。
3. 设置强密码并定期更换。
4. 重要文件加强防护。

不能做

1. 不要轻易点开陌生邮件中的链接，也不要轻易下载陌生文件。
2. 不要使用公共场所的网络设备执行敏感操作。
3. 不要放松对“熟人”邮件的警惕。
4. 不要将敏感信息发布到互联网。
5. 不要点击exe文件。

安全意识提升

——应急处置建议：如果不小心点了钓鱼邮件

1.密码修改

应第一时间对账号密码进行修改，包括邮箱的账号密码，也包括链接中输入的账号密码。

2.病毒查杀

如果点击了钓鱼邮件中的附件或链接，应立即对电脑进行全盘病毒查杀，如有必要需进行系统重装。

谢谢大家