新员工

网络信息安全意识培训

目录
CONTENTS

01

网络安全意识的重要性

我国实施国家教育数字化战略行动，网络安全防线成为重要支撑

推进教育数字化的战略目标。党的二十大报告中明确提出要进一步推进数字教育，为个性化学习、终身学习、扩大优质教育资源覆盖面和教育现代化提供有效支撑。我国已连续三年实施国家教育数字化战略行动，全力构建国家智慧教育平台，为教育现代化铺设了坚实的数字基石。

网络安全成为不可忽视的关键环节。随着教育数字化的深入推进，在加速教育数字化转型的同时，必须守牢安全底线，全面加强内容安全、技术安全、数据安全、算法安全的保障工作，构建安全可靠的教育信息网络安全体系。教育部在各类规划或指导文件中强调了网络安全的重要性。

- 2017年《教育行业网络安全综合治理行动》指出：高校开展以治理网站乱象、堵塞安全漏洞、补齐等保短板、规范安全管理为主要内容的教育行业网络安全综合治理行动，全面提升教育行业网络安全水平。
- 2019年《教育信息化和网络安全工作要点》指出：把网络文明、网络安全教育纳入学校教育工作内容。
- 2021年《教育信息化2.0行动计划》指出：深入开展网络安全监测预警，提高网络安全态势感知水平。
- 2022年《2022年工作要点》：深化信息技术与教育教学融合创新；建立信息化产品和服务进校园审核制度。

作为高校教育工作者，保护个人信息和敏感数据的安全不仅关乎个人利益，也关系到整个学校的信息安全。加强网络安全意识的培训和教育有重要意义，每位教职工做好网络安全防范，共同维护安全和谐的网络环境。

狭义安全：网络安全就是指网络信息处理和传输的安全

广义安全：网络系统的硬件、软件及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然或恶意行为而遭到破坏、更改或泄露

国家视角

“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”

高校教育单位视角

1.业务连续性、服务连续性

2.单位资产的保护

3.业务系统的合规性

4.关键信息基础设施等级保护

个人视角

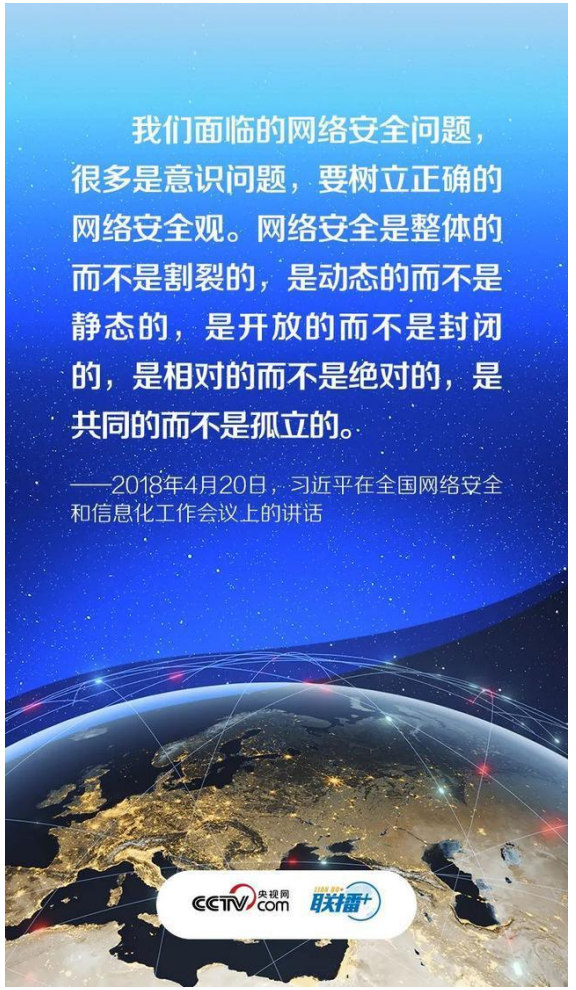
1、个人信息和隐私的保护；

2、个人从事网络活动的行为的规范

3、社会工程学

网络安全意识的重要性

“没有意识到风险是最大的风险。正所谓‘患生于所忽，祸起于细微’。”



02

网络安全形势分析

我们面临的网络安全形势

（一）近年来国外主要网络安全事件

2014年底，美国索尼影业网络被自称为“和平护卫队”黑客团体攻击事件，大量信息敏感被泄露。

2015年12月23日，乌克兰国家电力系统是被俄罗斯黑客组织“沙虫”攻击，导致100多万人停电4个多小时。

2016年12月23日，包括推特、脸书、亚马逊、Paypal、纽约时报、CNN、华尔街日报在内的美国知名大型互联网企业网络遭受黑客攻击，造成大面积瘫痪。

（一）近年来国外主要网络安全事件

美国前总统候选人希拉里搭建私人电子邮件服务器处理官方邮件，后来电子邮箱被黑客攻击入侵，电子邮件被泄露曝光。该事件成为导致希拉里败选2016年美国总统的主要原因之一。

2017年5月12日全球爆发的“永恒之蓝”勒索病毒事件。在我国很多电脑中毒，数据被加密无法打开。

（一）近年来国外主要网络安全事件

2013年斯诺登事件，某些西方国家长期对互联网实施监控、攻击、窃密。在“9•11”事件以后，西方国家实施了秘密计划，利用巨大影响力的互联网公司,对全球互联网及通信网络实施全方位监控。

境外反动黑客组织攻击破坏。不停攻击政府网站，发布爆恐音视频、张贴反动标语和违法有害信息等，影响极其恶劣。

我们面临的网络安全形势

（二）网络违法犯罪问题突出。计算机木马、病毒等恶意程序不断涌现。网络攻击违法犯罪活动十分猖獗，逐步形成黑色产业链条，给信息网络安全造成了很大的危害。网络安全事件事故时而发生，严重威胁我网络安全，侵害公共利益。

有关分析报告显示，每年网络犯罪就给国家造成了数百亿美元的经济损失。

黑客攻击破坏
侵害公民个人信息
网络诈骗
盗刷银行卡
网络赌博
网络招嫖

网络安全形势严峻

近年来，针对政府、金融、教育、医疗等关键信息基础设施的网络攻击更加常态化、专业化，针对性极强，造成了大量的经济损失。2018年开始，工业互联安全等引发关注，30%已上事件涉及黑色产业链，40%已上事件涉及国家背景的黑客组织，50%以上的事件导致规模惊人的信息泄露，80%以上事件有电子邮件的身影。

勒索病毒持续爆发

2020年12月对富士康的勒索病毒攻击。当时富士康位于墨西哥工厂的服务器遭到勒索病毒攻击，攻击者向富士康限期21天索要1804.0955枚比特币——按当时的汇率计算，约合3468.6万美元或2.3亿元人民币。

APT攻击愈演愈烈

世界范围内使用**SWIFT系统**的银行相继被曝出盗窃案件，从2015年厄瓜多尔银行损失1200万美元，10月的菲律宾银行，到16年2月孟加拉国央行曝出被盗窃8100万美元。

有组织有目的的攻击

黑客组织（**匿名者**）组织在2019年2月13日针对我国网站采取攻击，并列明了将被攻击单位的网站列表。其中不乏一些影响力比较大的主体，如360、电信云等。

西北工业大学遭网络攻击事件

- 2022年6月22日，西北工业大学发布《公开声明》称，该校遭受境外网络攻击。陕西省西安市公安局碑林分局随即发布《警情通报》，证实在西北工业大学的信息网络中发现了多款源于境外的木马样本，对此立案调查。

9月5日，国家计算机病毒应急处理中心发布了关于西北工业大学遭受境外网络攻击的调查报告，初步判明攻击活动源自美国国家安全局的“特定入侵行动办公室”，其使用41种网络攻击武器，对西北工业大学发起了上千次攻击窃密行动。技术团队经过持续攻坚，成功锁定了美国国家安全局（NSA）下属特定入侵行动办公室（TAO）对西北工业大学实施网络攻击的目标节点、多级跳板、主控平台、加密隧道、攻击武器和发起攻击的原始终端，发现了攻击实施者的身份线索，并成功查明了13名攻击者的真实身份。

美国网攻西工大另一关键图谋曝光！

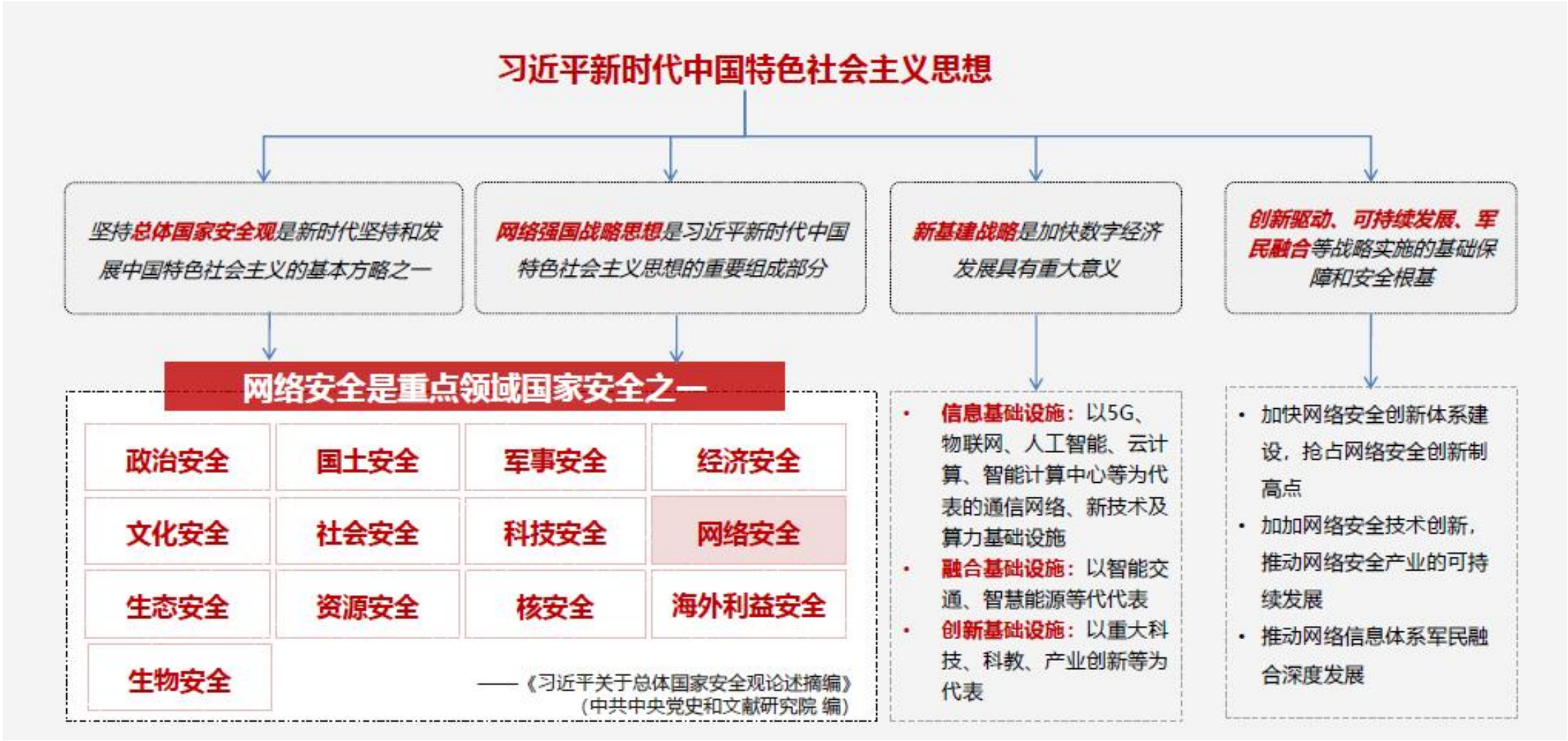
袁宏 环球网 2022-09-27 10:25 发表于陕西

美国网攻西工大另一图谋曝光：查询中国境内敏感身份人员信息

《环球时报》记者27日获得的最新调查报告进一步揭露了美国对西北工业大学组织网络攻击的目的：**渗透控制中国基础设施核心设备，窃取中国用户隐私数据，入侵过程中还查询一批中国境内敏感身份人员，并将用户信息打包加密后经多级跳板回传至美国国家安全局总部。**

- TAO网络攻击行动中先后使用了54台跳板机和代理服务器，主要分布在日本、韩国、瑞典、波兰、乌克兰等17个国家，其中70%位于中国周边国家，如日本、韩国等。

国家战略层重视网络安全发展



国家法律法规对网络安全的监管要求

2021年《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》《中华人民共和国个人信息保护法》等网络安全相关法律施行。《中华人民共和国反电信网络诈骗法》2022年9月2日通过，2022年12月1日起施行

- **2021年9月1日起施行《中华人民共和国数据安全法》**聚焦数据安全领域的突出问题，确立了数据分类分级管理，建立了数据安全风险评估、监测预警、应急处置，数据安全审查等基本制度，并明确了相关主体的数据安全保护义务，这是我国首部数据安全领域的基础性立法。
- **2021年9月1日起施行《关键信息基础设施安全保护条例》**，明确了关键信息基础设施的定义及认定程序，为我国深入开展关键信息基础设施安全保护工作提供有力法治保障。
- **2021年11月1日起施行《中华人民共和国个人信息保护法》**，中国第一部专门规范个人信息保护的法律，对我国公民的个人信息权益保护以及各组织的数据隐私合规实都将产生直接和深远的影响。

2017年6月1日正式实施的《网络安全法》

明确为了保障网络安全，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，制定本法。

✓“任何个人和组织应当对其使用网络的行为负责”法律责任包括治安处罚“警告、罚款、行政拘留”直至犯罪

✓“任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息”

✓“违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的处一百万元以下罚款”

✓“机构、组织、人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任”

还有其他已经施行的跟网络安全有关的法律，主要包括《刑法》、《治安处罚法》、《反恐法》、《国家安全法》、《警察法》等等。

违法有害信息：制作、复制、发布、查阅（浏览）或传播的危害国家安全、公共安全、损害社会管理秩序或经济秩序，或者侵犯个人、法人和其他组织的人身、财产等权利的信息。

网络安全责任：十分明确，“**谁主管谁负责、谁运用谁负责、谁使用谁负责**”。可以这么说，网络安全跟每个人息息相关，需要大家一起共同努力，共同维护。

03

生活中的网络信息安全

- 个人信息泄露
- 密码安全
- 免费WiFi
- 二维码
- ……

工作单位

网站浏览痕迹

家庭住址

网购记录

个人信息泄露

诈骗信息

垃圾信息

姓名

身份证号

通话记录

地理位置

学历

IP地址

软件使用痕迹

个人信息泄露渠道

八大个人信息泄漏渠道

手机

5月13日，腾讯移动安全实验室发布今年一季度手机安全报告，统计发现近470万个软件包中，有读取用户隐私权限相关操作的软件比例达到71%。

报考

据报道，不少报考研究生的考生，在网上报名后连续收到内容为“提供考前绝密资料”的短信，大家一度怀疑自己的考试信息被学校泄露。

酒店

国内安全漏洞监测平台乌云近日发布报告，称如家、汉庭等大批酒店的开房记录被第三方存储，并且因为漏洞而泄露。

航空公司

近日，陆续有消费者通过微博投诉，称订购机票后个人信息遭泄漏，涉及南航、东航、山东航空、深圳航空等多家国内知名航空公司。

网购

近日，“团委会团购网”的网页中出现了千余名会员的个人信息，内容包含会员名、电话号码及购买物品的内容等。

快递

近日，据央视报道，为了创收，圆通、申通、天天快递等快递公司会留存着单号等信息，价高就卖。

银行

余某为某银行职员，他将自己掌握的600余份客户信息出售，获利3万余元。这些个人信息被用作办理信用卡，并透支200余万。

保险公司

据央广报道，一家名为众宜风险管理机构的网站，可以随便在网站上查询客户投保信息，估计泄露的网页高达80万页。

“免费”WIFI不免费

无论在家中，或者外出，民众对无线上网的需求越来越高。而手机上网已成为网民上网的首选，截止目前，手机网民已超过6.3亿。值得注意的是，其中92%的手机网民使用WiFi接入互联网，平均每天每人连接WiFi时长1.1小时。由此可见，WiFi已经成为民众日常生活中不可或缺的一部分。

“免费”WIFI不免费

- **钓鱼WiFi：**

  在繁华的街道设立名字叫做“CMCC”、“KFC”的WiFi热点。

- **Karma：**

  伪装成受害设备以前连接过的公开WiFi热点。

- **ARP欺骗：**

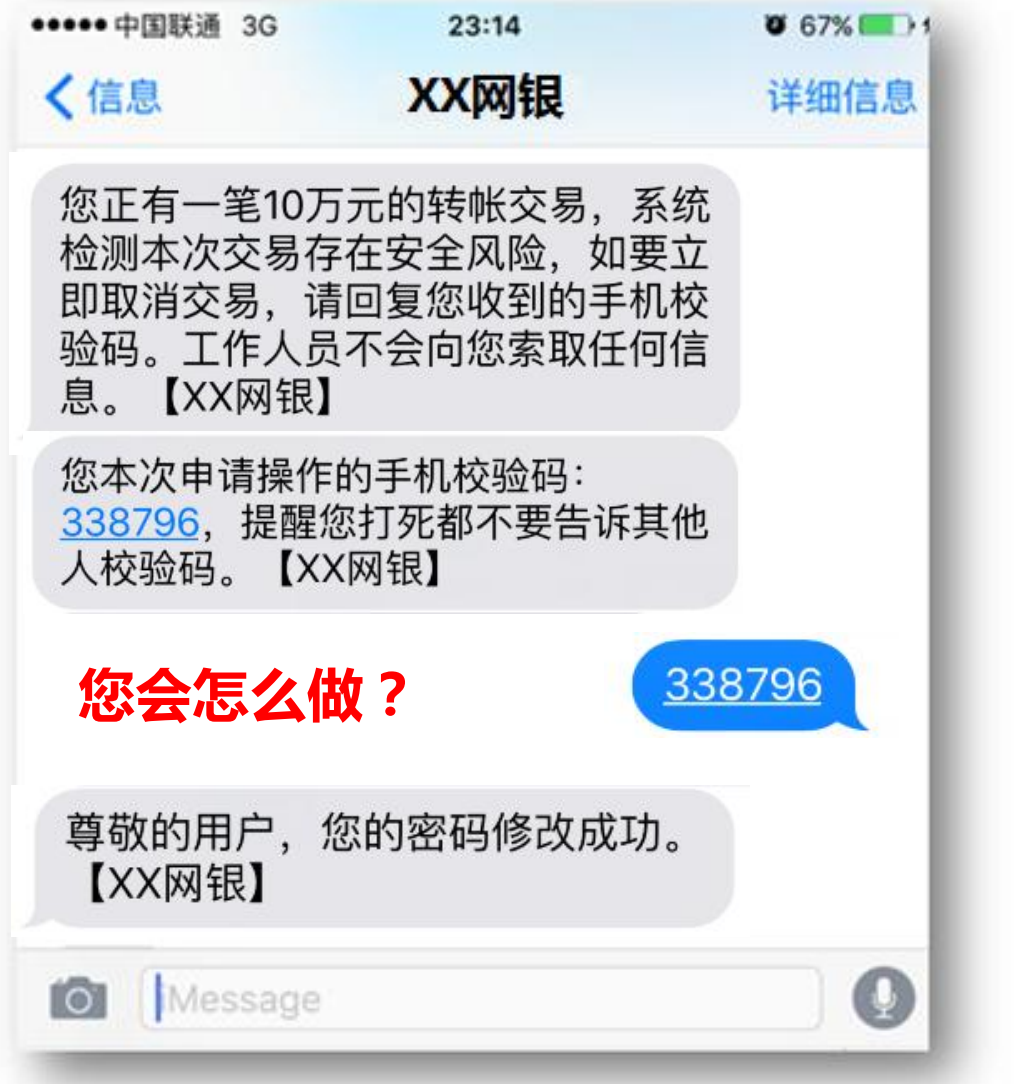
  攻击者与受害者接入同一个WiFi热点

  通过发送特定数据伪装成数据网关

二维码

用来存储信息的，信息既可以是**文本**、**网站链接**、**文件**、**图片**；也可以是**视频**、**软件安装包**等。

“善意”的短信



某天突然收到XX网银的短信提醒……

黑客使用伪基站发送伪造XX网银客服号码的短信

黑客在XX网银申请重置您网银帐号的密码

网银

黑客收到您发送的验证码，成功修改密码。

黑客的目标不是转账而是修改您的网银密码，然后再转账

看看你的手机

看看你的手机

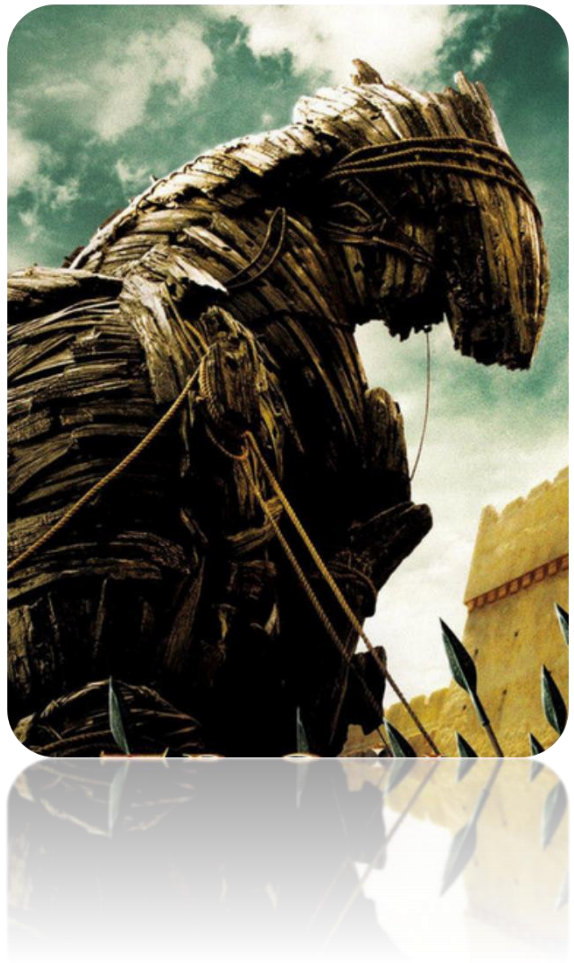
●●○○○ 中国移动 4G 15:01 87%

(1) +86 152-2191-2821 详细信息

短信/彩信
昨天16:46

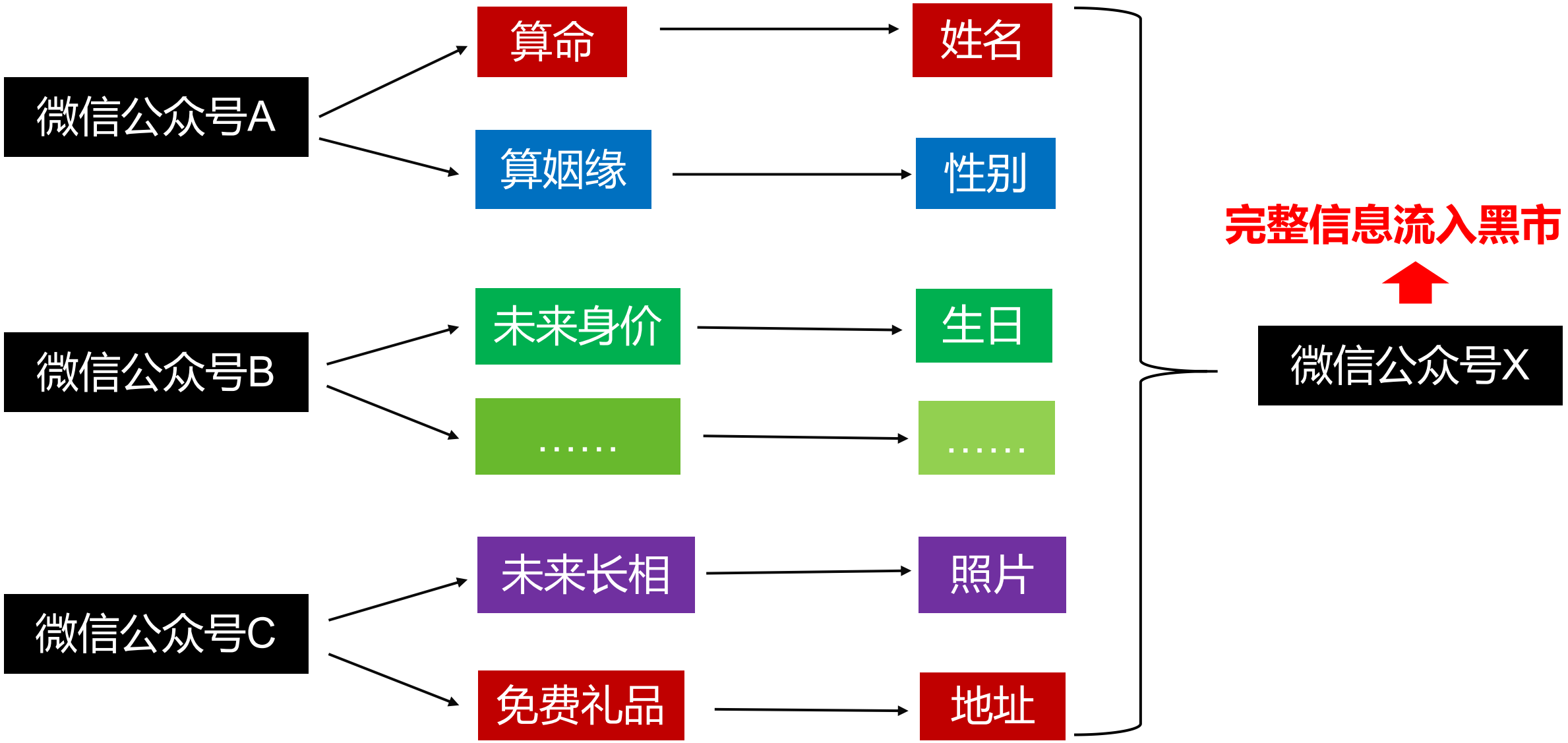
看你干的好事，自己打开看吧
72.52.83.228/zjx.apk
证据都在里面呢

短信/彩信 发送



“有趣”的游戏

“有趣”的游戏


微信公众号A
算命
姓名
算姻缘
性别
微信公众号B
未来身价
生日
……
……
微信公众号C
未来长相
照片
免费礼品
地址
完整信息流入黑市
微信公众号X

04

校园网网络安全介绍

- 弱口令
- U盘安全
- 钓鱼
- 勒索病毒
- 社会工程学

高校网络安全体系

领导责任制：网络安全和信息化委员会，为学校网络安全和信息化建设的管理与决策机构

信息安全制度：机构职责分工、安全管理制度、防护措施、监督检查、教育培训等。

信息管理系统：充分考虑网络安全因素。系统日常运维、业务连续性、数据灾备等措施

网络安全事件应急处置：网络与信息安全突发事件应急预案，按安全事件发生的性质分类指引

个人信息保护：重要数据和个人信息的采、传、存、用等采取了加密、脱敏、水印等技术措施

网络安全技术防护：基础网络结构，区域划分、安全控制策略、入侵及病毒防护、设备管理及日志分析等

应用系统安全防护：身份鉴别、帐号权限控制，审计信息保存及分析，系统管理及业务数据传输防护

智慧校园总体设计

用户与终端层

学生　老师　校领导　家长

PC端　手机　公众号　小程序

综合服务层

统一信息门户　统一信息服务　网上办事大厅　统一应用入口

应用系统层

智慧管理		智慧教学		智慧环境		智慧内涵	
教务管理	科研管理	数字化课程平台及资源		校园网络		专业建设	
学工管理	招生管理	虚拟仿真	虚拟现实	校园自助服务终端		校园文化	数据分析
人事管理	党群建设	实习管理	在线考试	智慧教室	校园广播	教学诊改	专业共建
协同办公	一卡通	实验实训室建设		云桌面/多媒体教室		数字图书	师资培训
资产管理	……	资源制作	……	录播教室	……	技能提升	……

平台支撑层

基础数据管理　统一身份认证　统一数据中心　统一权限管理　物联网集成　大数据决策分析

基础设施层

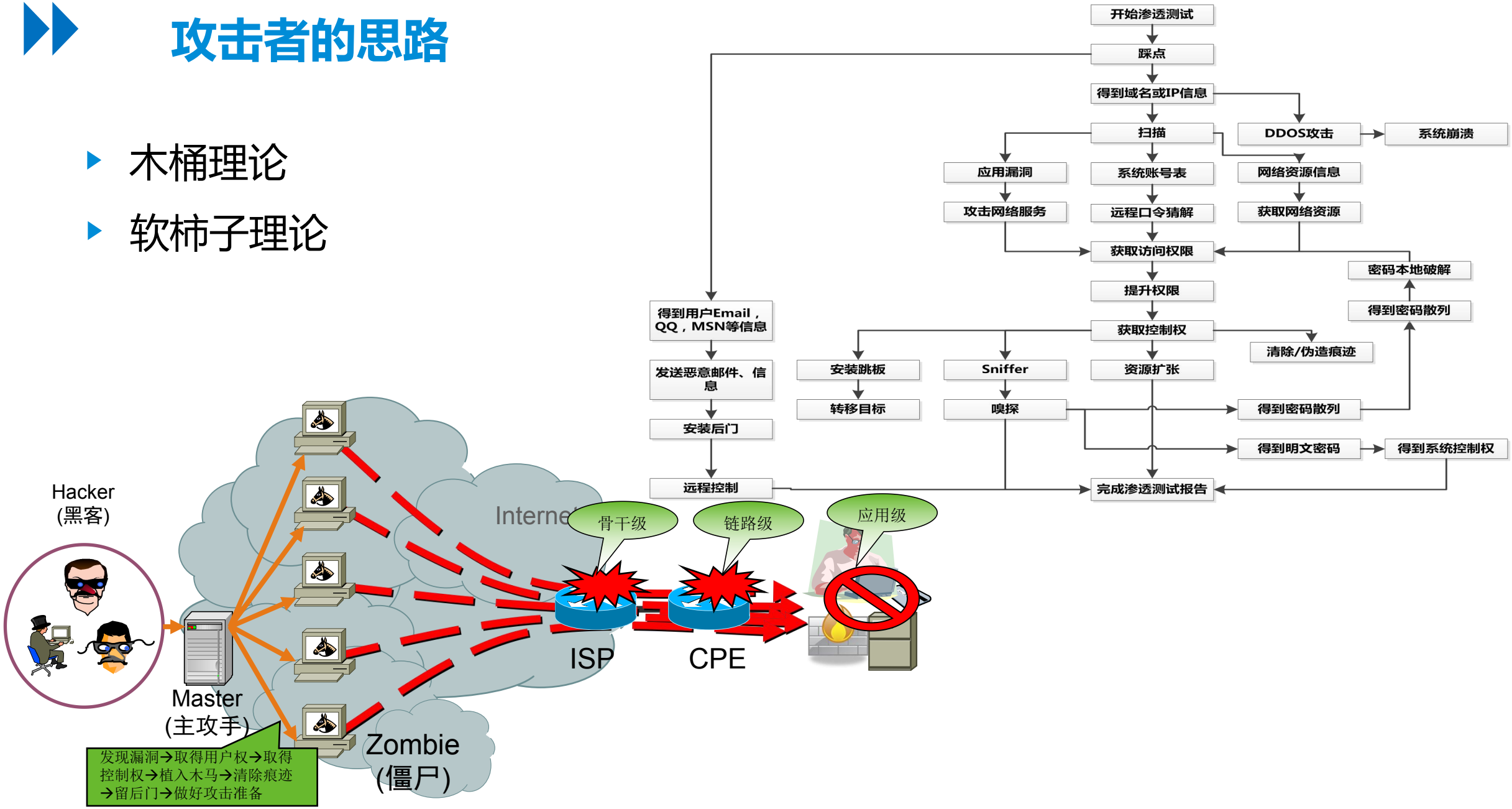
校园网络　无线覆盖　网络设备　校园云计算机平台　网络安全设备　数据库

教育信息化标准及信息安全体系

系统培训及终身服务体系

攻击者的思路

- 木桶理论
- 软柿子理论



网络安全技术

一个具有“工匠精神”的小偷是如何入室盗窃：

1. 伪装——隐藏小偷信息
2. 踩点——寻找目标并摸清人员规律、路线及场所入口
3. 开始入室——选择时机从不牢固或开放的入口进入
4. 盗窃——打开存放贵重物品的柜子
5. 寻找相邻目标继续作案
6. 达到主要目的——获取贵重物品
7. 预留通道——以便传递赃物或再次入室
8. 消除痕迹——如破坏监控数据

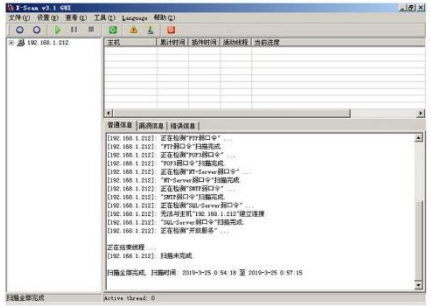
常见的攻击方式

- 社会工程 Social Engineering
- 病毒virus （蠕虫Worm ）
- 木马程序Trojan
- 拒绝服务和分布式拒绝服务攻击 Dos&Ddos
- ARP欺骗：IP spoofing, Packet modification ; ARP spoofing
- 邮件炸弹 Mail bombing
- 口令破解 Password crack

如何在攻击前封杀攻击者

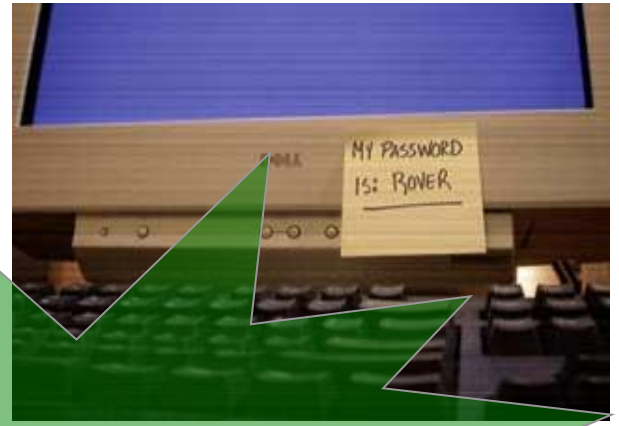
灰鸽子木马程序

运用X-Scan综合扫描器扫描系统



你的密码是”password” “123456” ？

- 口令强度不足
- 口令结构简单
- 口令保存方法不当
- 口令保质期过长



密码的常用破解方式：

- 猜测
- 木马程序
- 网络钓鱼
- 网络监听
- 暴力破解
- 撞库
- 社会工程学

密码安全绝对不是技术问题，而是意识问题！

常见的弱密码类型

- 设置口令别犯傻，生日姓名手机码
- 姓名、姓名变形、生日、常用英文单词、6位以下长度、手机号或个人邮箱、经常在各个不安全网站使用的密码

强密码类型

- 包含数字、大小写字母、特殊符号
- 重要密码不要与一般网站密码相同
- 至少每个月更新一次
- 不用曾用密码

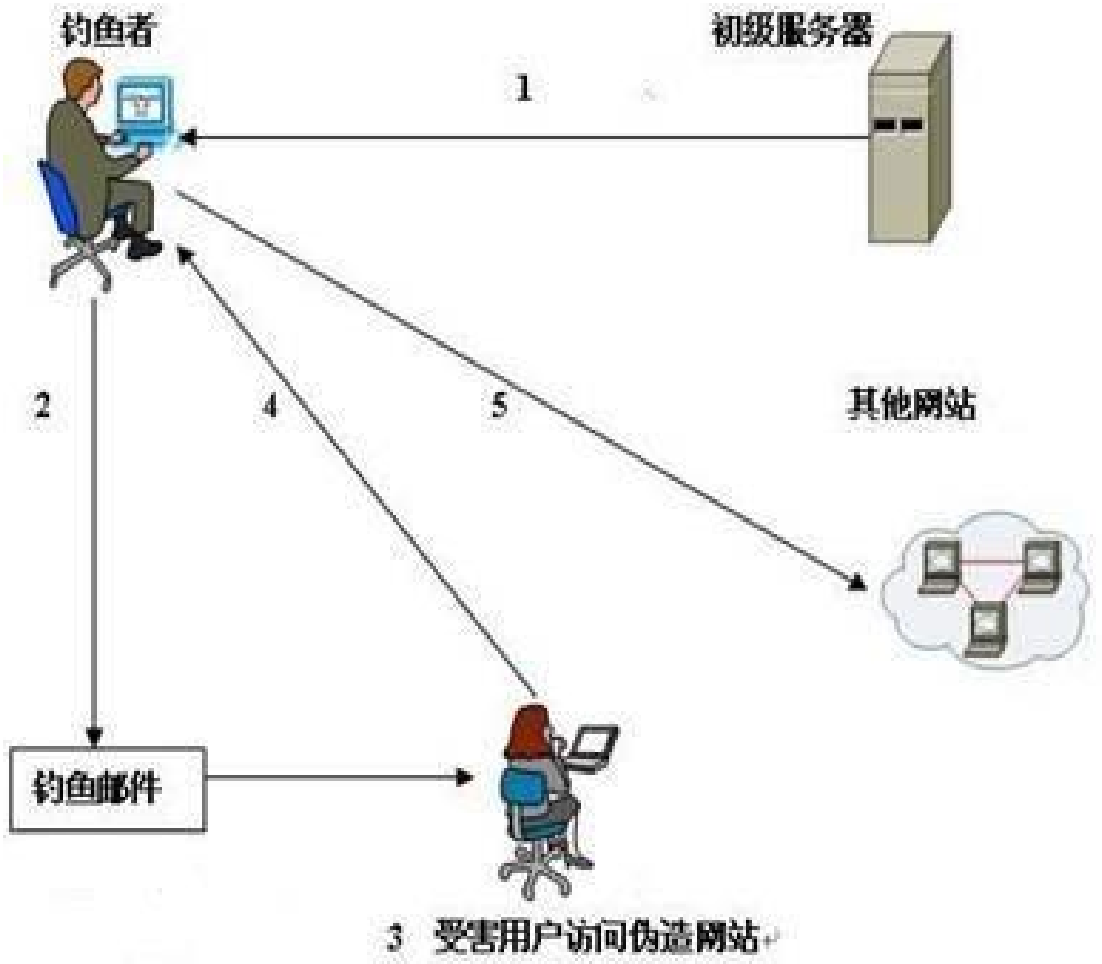
不定期更改你的密码。
只要有足够的时间，无论多高强度的密码最终都可被破解!
一般来说密码寿命最好不超过一个月。
键盘锁定

注意U盘泄密

- U盘病毒传播造成60%内网安全问题
- 运维时禁止使用U盘随意拷贝资料

网络钓鱼

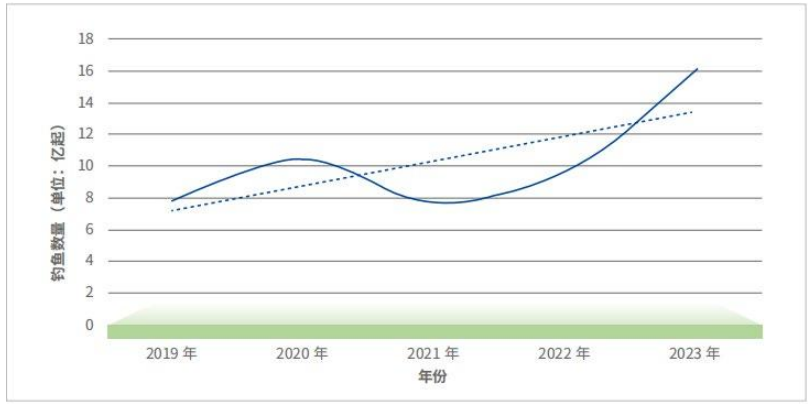
“姜太公钓鱼，愿者上钩”



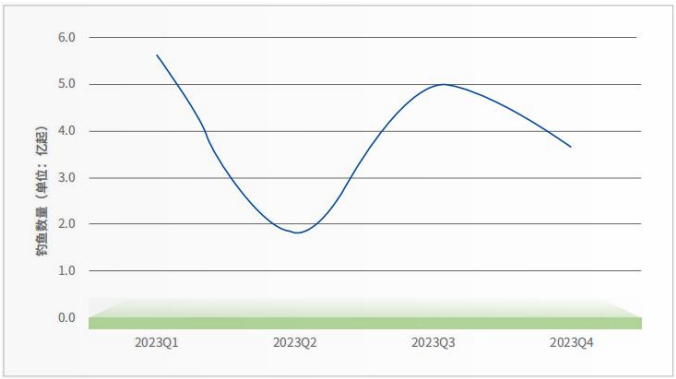
网络钓鱼（Phishing）攻击者利用欺骗性的**电子邮件**和伪造的**Web 站点**来进行网络诈骗活动，受骗者往往会泄露自己的**私人资料**，如信用卡号、银行卡账户、身份证号等内容

诈骗者通常会将自己伪装成**网络银行**、**在线零售商**和**信用卡公司**等可信的品牌，骗取用户的私人信息

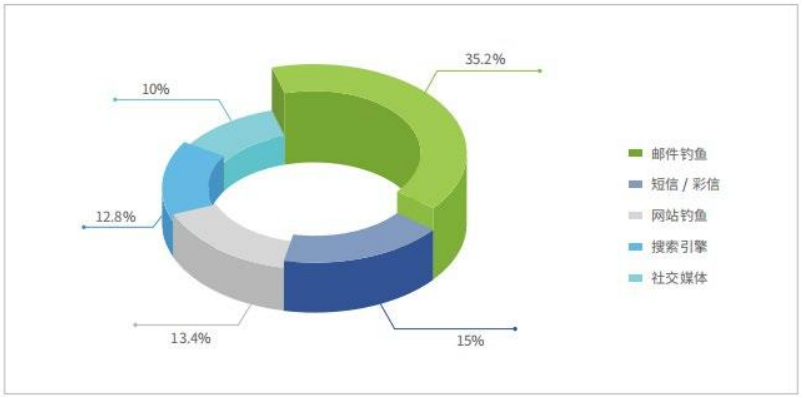
网络钓鱼趋势分析



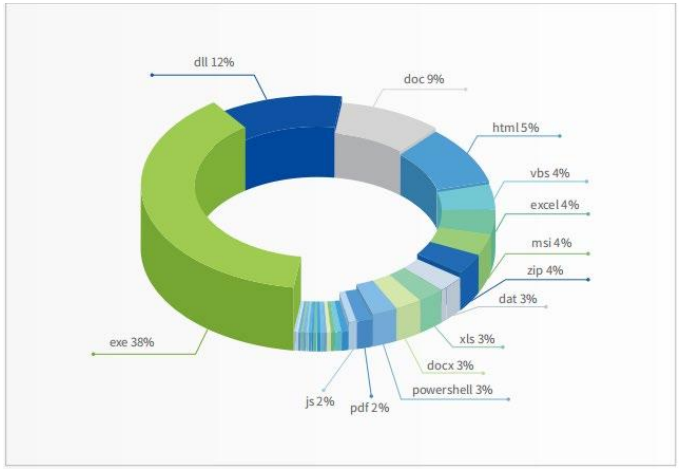
2023年，网络钓鱼攻击事件**总数约为16亿起，同比增长166%**。SlashNext 公司的报告显示，自2022年第四季度至2023年第三季度，网络钓鱼邮件数量增加了1265%，平均每天发送了约31,000封网络钓鱼攻击邮件。



时间分布上，网络钓鱼攻击**呈现季节波动特征**，一季度和 三季度出现两个高峰，可能受到了春节、国庆等假期热点影响。



攻击渠道上，**钓鱼邮件依然是最主要的攻击渠道**，利用短信 和彩信、创建钓鱼网站进行欺诈、利用搜索引擎投放诱导广告、利用社交网络和即时通讯软件发起钓鱼活动等手段也越来越普遍。



攻击形式上，犯罪分子使用频率最高的文件类型包括 **exe、dll、doc、html 和 vbs** 等。它们分别用于运行木马程序、 进行钓鱼网站攻击或释放/下载其他文件。这些手段不仅技术性强，而且极具欺骗性。

教育行业钓鱼分析

教育行业存储着大量敏感身份信息和前沿领域研究数据，因此成为不法分子的重要目标。这些不法分子经常伪装成政府机构人员、学校工作人员、学生或家长，发送虚假通知、恶意链接或虚假账户要求提供个人信息或转账，试图侵入校园网络系统。

最新数据显示，面向教育系统和师生员工的钓鱼攻击已占网络钓鱼总体的8%以上。教育行业拥有大量隐私信息，如学生、家长、教职员工的个人身份、家庭、考试、财产等详细信息，这些数据在黑市上价值不菲。然而，学校师生整体安全意识不足，对信息安全重视程度不高，对各种钓鱼手段缺乏了解，容易受骗。因此，教育行业亟需重视网络钓鱼等身份信息盗用犯罪问题，从安全教育、系统加固和攻击监测应急等多个方面入手，切实提高网络欺诈防御能力，保护敏感数据安全。

2023 年 11 月份，一名学生接到了自称是政府电信局工作人员的电话，对方声称该学生涉嫌参与电话卡洗钱活动，要求将钱款转至指定银行卡中。学生最终被骗走了超过 350 万元的巨额资金。

网络钓鱼的主要特点

网络钓鱼主要方式和特点

01 邮件依旧是传播钓鱼的主力

- 攻击者可以轻易获取大量收件人，发起大规模邮件攻击，而且发送钓鱼邮件只需要基础的技术即可完成；
- 利用成熟的社会工程学手段，攻击者可以轻松伪造发送人、主题和内容，这种低成本、低风险的攻击便利了网络犯罪分子；
- 长期高强度的邮件钓鱼攻击，让用户产生了防范疲劳，安全意识淡漠，容易被欺骗，也间接助长了此类攻击的持续活跃。

02 利用即时通讯软件钓鱼

- 攻击者通常会向受害用户发送包含钓鱼链接或附件的消息，利用各种社会工程学手段诱使用户输入个人信息或扫码转账汇款，从而非法窃取账号、资金和个人信息；
- 主要传播方式包括好友账号被盗后发送汇款要求、利用空群自动传播消息、创建假冒机构或客服账号发信、制作符合日常会话语境的信息等。

03 二维码钓鱼的广泛使用

- 攻击者利用二维码可以规避安全解决方案的检测，同时也能降低用户的警惕性；
- 用户对二维码支付和扫码认证存在盲信心理，意识不够警惕，为攻击者提供了机会利用假冒支付宝、微信等知名企业收款二维码进行诈骗的；
- 不法分子通过社交平台传播假冒业务延伸的钓鱼二维码，进行远程诈骗。一些攻击者还会在公共场所如餐馆、共享单车张贴含恶意链接的二维码，一旦扫描二维码可能会导致个人信息泄露、凭证失窃、资金被盗等风险。

“钓鱼邮件”安全提示

近期学校邮箱用户收到“钓鱼邮件”的情况时有发生，此类邮件多以仿冒我校师生名字、骗取个人账号口令、勒索钱财等为目的。为保护大家的邮箱安全，特提醒如下:

“钓鱼邮件”是指黑客伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户回复邮件、点击嵌入邮件正文的恶意链接或者打开邮件附件以植入木马或间谍程序，进而窃取用户敏感数据、个人银行账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动。

一、“钓鱼邮件”常见特征

1. 以邮箱停用、账号重新登记、账号备案、邮箱升级、系统升级、“数据迁移”等名义，诱导用户点击链接，并要求提供邮箱密码等个人信息。

2. 声称已通过植入病毒等技术手段获取了用户隐私、控制了用户电脑设备和摄像头，并进行恐吓、威胁和勒索。

3. 以各种“发放福利补贴”、“奖学金申请””保险到期”等理由和名义，催促、诱导用户点击链接、扫描二维码、下载邮箱附件，进而使用户设备感染病毒或木马程序。

4. 冒用或盗用领导、好友、同事或学校部门的邮箱，并以其名义要求借款、办事、加QQ群等。

5. 邮件主题包含“紧急通知”、“重要提醒”、“发票”、“会议名单”等明显特征的邮件。

6. 发件人将邮箱名称刻意修改为带有学校邮箱后缀，但实际邮箱账号域名为校外或国外域名的邮件均为诈骗邮件。

URL钓鱼方式

【邮箱安全通知】近期钓鱼邮件频发，请更新安全证书（重要）

发件人：[redacted]

时　间：2023年8月9日（星期二）下午2：06

收件人：[redacted]

纯文本 |

邮件可翻译为中文 立即翻译

各位领导、同事：

近日公司收到大量钓鱼邮件和垃圾邮件，经信息部分析，是由于个别用户邮箱被盗用导致，针对于此请完成如下操作：

1.未进一步提升邮件系统的安全性，信息部于今日陆续更新了用户邮件系统的安全证书，请用户及时迁移新证书。

2.凡未及时更新安全证书的邮箱账户，将暂停邮箱使用权限。

3.请于本周三（7月28日）18点前完成证书迁移，如有问题请联系科技部。

4.操作方式：请点击【证书迁移备案】，升级后用户名和密码均不变。

[redacted]综合

[redacted]

传真/Fax: [redacted]

邮箱/Email: [redacted]

地址/Add: [redacted]市教[redacted]

邮编/P.C. [redacted]

网站/Web [redacted].st.cn/

微博/Twitter: htt[redacted]

本邮件仅供指定收件人依法使用。任何单位或者个人未经许可，不得对邮件内容进行浏览、披露、存储、复制、散播或通过其它方式使用。如果您非指定收件人，请立即删除本邮件并告知发件人。谢谢合作。

This e-mail may contain confidential and/or privileged information. Any company or individual without approval shall not disclosure, save, reproduction, dissemination or use by other ways. If you are not the intended recipient, please advise the sender immediately by e-mail and delete this e-mail and any attachment without copying or disclosing the contents. Thank you for your cooperation.

[redacted]

二维码钓鱼方式

2023年员工的住房公积金基数调整确认 ☆

发件人：人力资源部综合 [redacted]

时　间：2023年6月30日（星期五）下午3：47

收件人 [redacted]

纯文本 |

各位领导、同事：

接国家人力资源和社会保障部通知，将会于7 月份调整 2023 年员工的住房公积金基数。

请各位同事于周五（7 月7 日）下班前在 OA 人力资源管理系统https[redacted]n/ **中填写相关信息或扫描下方二维码，确认 2023 年的住房公积金缴存基数。**

感谢各位同事的配合。

人力资源部 | Human Resource Dept.

[redacted]

2023 年 7 月 3 日

二、钓鱼邮件防范和处置措施

1.邮箱密码应使用至少8位以上并包含数字、字符等复杂度较高的强密码，并定期修改密码。

2.区分邮箱名称和邮箱账号，邮箱名称可以随意设置，但邮箱账号是邮箱的唯一标识；识别学校的邮箱域名stu.edu.cn(教职工)和alumni.stu.edu.cn（校友），发信人邮箱账号为其他域名的邮件均为校外邮件。

3.对于要求提供个人信息的邮件，请谨慎对待并再三确认内容的真实性，不要输入账号、密码等个人信息。

4.对于来历不明的邮件，不点击邮件中的链接、不扫描二维码、不安装文件、不提交密码！

5.对带有附件的邮件，不要盲目点击、下载、安装。

6.登录邮箱的终端设备应安装杀毒软件，并及时更新。

7. 做好数据备份。（1）及时清空收件箱、发件箱和垃圾箱内不再使用的重要邮件；（2）备份重要文件，防止被攻击后文件丢失；（3）重要邮件或附件应加密发送，且正文中不能附带解密密码。

勒索软件

- **什么是勒索软件？**
  - 对受害者电脑进行文件加密并进行勒索；
  - 只有支付赎金才可以正常使用原有文件；
- **勒索软件攻击流程**
  - 以钓鱼邮件的形式传播，邮件附件中往往包含经过伪装的恶意程序；
  - 受害者直接点击打开该恶意程序；
  - 恶意程序加密受害电脑上数据文件；
  - 在受害者尝试使用文件时弹出勒索要求；

勒索软件

I RECORDED YOU!

[redacted]@stu.edu.cn 下午12:35

Hello there!

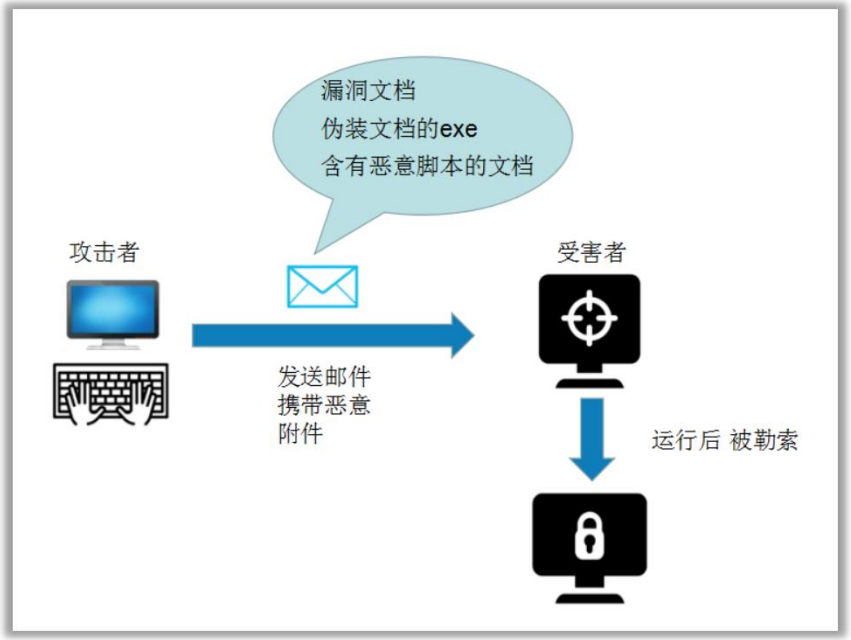
Unfortunately, there are some bad news for you.

Some time ago your device was infected with my private trojan, R.A.T (Remote Administration Tool), if you want to find out more about it simply use Google.

My trojan allows me to access your accounts, your camera and microphone.

Check the sender of this email, I have sent it from your email account.

You truly enjoy checking out porn websites and watching dirty videos, while having a lot of kinky fun.



社会工程学

- **什么是社会工程学攻击？**

搜集足够多的信息，以便于伪装成一个合法的雇员、合作伙伴、执法官员，或者任意角色。

我就是我所声称的那个人！

采集信息 → **选择目标** → **建立信任** → **实施攻击**

寻找组织、员工的明显弱点，寻求突破。

社会工程学与一般攻击的区别

	一般黑客攻击	社会工程攻击
攻击对象	 网络设备 主机服务器 应用程序 网络服务	 人 对人 只对人
攻击方法		 欺骗 诱导

05

校园网安全防范指南

No.1 安全使用公共WiFi

一、关闭WiFi自动连接功能。
二、谨慎使用陌生WiFi。
三、不使用公共WiFi进行网购、支付等操作。
四、关掉共享。
五、使用安全软件。

安全可信的网络环境：
一、学校建设的WiFi热点。
二、运营商移动网络（4G/5G）。
三、运营商的家庭WiFi热点

No.2 口令安全-设置建议

口令至少应该由8个字符组成

口令应包含大小写字母

口令应包含数字、特殊字符

不要使用字典中的单词

不要基于人的姓名、生日

例1：
183GRXChhl
183YYSYxyz

例2：
5tgb^YHN
7ujm*IK<

例3：
淘宝：183TzxnygrB
京东：183JzxnygrD
163: 1831zxnygr63

定期更新（90天）

No.3 电子邮件

接收邮件建议

- 不安全的文件类型：绝对不要打开任何以下文件类型的邮件附件：.bat, .com, .exe, .vbs
- 未知的文件类型：绝对不要打开任何未知文件类型的邮件附件，包括邮件内容中到未知文件类型的链接
- 不要打开未知的链接:未知的链接可能是含有病毒的网站和一次含有欺骗信息的钓鱼网站
- 微软文件类型：如果要打开微软文件类型（例如 .doc, .xls, .ppt等）的邮件附件或者内部链接，务必先进行病毒扫描
- 要求发送普通的文本：尽量要求对方发送普通的文本内容邮件，而不要发送HTML格式邮件，不要携带不安全类型的附件
- 禁止邮件执行Html代码：禁止执行HTML内容中的代码
- 防止垃圾邮件：通过设置邮件服务器的过滤，防止接受垃圾邮件
- 尽早安装系统补丁：杜绝恶意代码利用系统漏洞而实施攻击

No.3 电子邮件

发送邮件建议

- 如果同样的内容可以用普通文本正文，就不要用附件
- 尽量不要发送.doc, .xls等可能带有宏病毒的文件
- **不要回覆由匿名**寄件者寄来的邮件
- 不要在公开网站例如搜寻引擎、聊天室等披露你的邮件地址
- 发送不安全的文件之前，先进行病毒扫描
- 尽早安装系统补丁，防止自己的系统成为恶意者的跳板
- 可以使用口令或加密软件发送安全级别较高的的邮件

No.4 浏览器

浏览器为什么重要？

- 互联网入口
- 工作业务入口
- 生活需要入口
- 其他

No.4 浏览器

使用IE之外的安全浏览器！

chrome

Firefox

Opera

safari

- 使用新版本游览器
- 不要存储账号信息
- 升级最新的操作系统

No.5 即时通讯-使用建议

- 不要在公共电脑上保存个人的登陆密码
- 在与他人聊天过程中，轻易不要发送个人与财产尤其是银行卡、会员卡等信息
- 定期清除个人电脑的聊天备份文件
- 有陌生人加好友的邀请，不要不经过验证信息就添加
- 在聊天中若对方不在常用地区登录的话，要尤其注意不要轻易给对方发送个人的信息
- 不要发送公司或业务相关的机密信息

No.6 移动存储介质—安全建议

一 提高安全意识和保密意识

二 加大技术投入，构筑安全保密的“防火墙”

- 是不断完善技术保密的措施
- 制定有效的移动存储介质防病毒策略

三 强化管理，健全监督机制

- 根据实际情况，制定移动存储介质管理流程
- 针对移动存储介质使用者制定全面的监督制度
- 对于存储的重要信息要及时备份，定期杀毒
  做好重要信息的防丢失和防损坏工作

No.7 手机安全

伪APP以假乱真，导致手机支付泄密！

No.7 手机安全

1、不要相信那些赚钱、返利、应用推广的手机APP软件

2、要在正规的APP商城下载手机应用

- 案例：伪造的淘宝手机客户端

山寨手机app对你究竟有哪些危害？

1．窃取账号，窃取用户支付账号及使用行为；
2．购物欺诈，诱导用户去钓鱼网站进行支付；
3．恶意扣费，私自定制扣费SP业务；
4．远程控制，在用户使用后留取后门，远程控制并窃取用户手机中的资料；
5．窃取隐私，窃取用户通讯录，向用户推送购物广告；
6．骚扰用户，每天不定时无限制地向用户推送广告购物信息，并无法关闭推送。

- 安装淘宝手机病毒后诱骗“淘宝”手机用户获取Root权限，静默安装私自下载的恶意软件，订购一个名为"**业务 支付*元/月"的业务，同时病毒将会屏蔽运营商订购回复短信，在用户毫不知情的情况下，恶意扣取资费。

No.7 手机安全

手机安全使用手册

手机安全必须做到

①不轻信扫描生人发的二维码；
②不要把银行卡、身份证及手机放在一起；
③保持设置手机开机密码的习惯；
④更换手机号前，在微信设置解除捆绑；
⑤手机丢失，第一时间打电话给银行和第三方支付供应商冻结相关业务。

手机安全使用手册

被索要微信验证码，不要给！

有人伴装手机刷机，要求对方发送手机号与验证码给他，以通过好友验证，如果发送验证码，微信可能立马会被盗！一旦中招，可能波及到很多人！

手机安全使用手册

安装软件 少点“ 允许 ”

手机安装游戏等软件时，常被要求“使用你的位置”，一旦点击“好”，这些应用便可扫描并把手机信息上传到互联网云服务器，一旦资料泄露，别人就可能知道您的位置、跟谁通话，玩啥游戏，家在哪……

及时关闭手机 WiFi 功能

发现免费WiFi不要随便登录，这可能是黑客用来入侵你手机的工具！

江西一位先生使用没有设置密码就能直接登录的免费WiFi，并用手机输入自己网银卡号密码，结果发现账户被人转走了3.4万元！

手机安全使用手册

别随便晒孩子照片

有些家长爱在社交网络发孩子的照片，会提到孩子的名字、学校，图片也可能透露不少居住小区的线索。根据这些信息很容易汇总出孩子的名字、家庭住址、学校，可能会让孩子有潜在的安全风险。

网上测试小心有诈

“测测你的心理年龄”、“测测你前世是谁”、“测测你的出轨概率”……测试时输入的姓名、生日、手机号码等，会被存入后台，对其梳理，有可能拼凑出完整个人信息。小心！

手机安全使用手册

微信里的这些开关，关掉！

1、微信“ 附近的人 ”功能可定位你的位置，依次点击“ 设置—通用—功能—附近的人 ”，选择“ 清空并停用 ”，必要时可重新开启。

2、在微信“ 隐私 ”选项中关闭“ 允许陌生人查看十张照片 ”。

3、在微信“ 隐私 ”中关闭“ 通过 QQ 好友搜索到我 ”和“ 可通过手机号搜索到我 ”。

手机安全使用手册

手机号注销前要做的事

①将U盾、网银、手机银行、短信通知等银行卡业务解绑；
②将证券、基金账户等金融业务解绑；
③将淘宝、微信等第三方支付平台解绑；
④及时变更微信、微博、QQ等服务的关联电话

一定要完成所有业务解绑后再销号！

手机安全使用手册

手机丢了，这些事立刻做！

①致电运营商挂失手机号
中国电信：10000
中国移动：10086
中国联通：10010
并到运营商处补办手机卡

②致电银行冻结手机网银
工商银行95588 中信银行95558
农业银行95599 光大银行95595
中国银行95566 民生银行95568
建设银行95533 广发银行95508
交通银行95559 浦发银行95528
招商银行95555 华夏银行95577

③解除支付宝绑定：95188

④解除微信绑定：110.qq.com

No.8 网络钓鱼—安全建议

1、提高警惕，不登录不熟悉的网站，键入网站地址的时候要校对，以防输入错误误入狼窝，细心就可以发现一些破绽。

2、不要打开陌生人的电子邮件，更不要轻信他人说教，特别是即时通讯工具上的传来的消息，很有可能是病毒发出的。

3、安装杀毒软件并及时升级病毒知识库和操作系统（如Windows）补丁。

4、收到不明电子邮件时不要点击其中的任何链接。

5、登录银行网站前，要留意浏览器地址栏，如果发现网页地址不能修改，最小化IE窗口后仍可看到浮在桌面上的网页地址等现象，请立即关闭IE窗口，以免账号密码被盗。

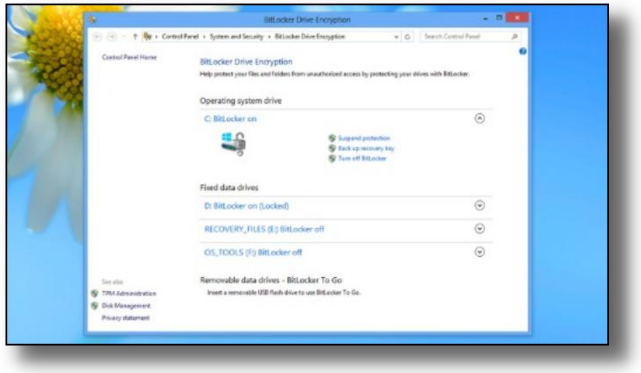
No.9 电脑安全—安全建议

1.木马病毒扫描防护能力

2.启用主机防火墙

3.及时更新系统补丁、软件升级

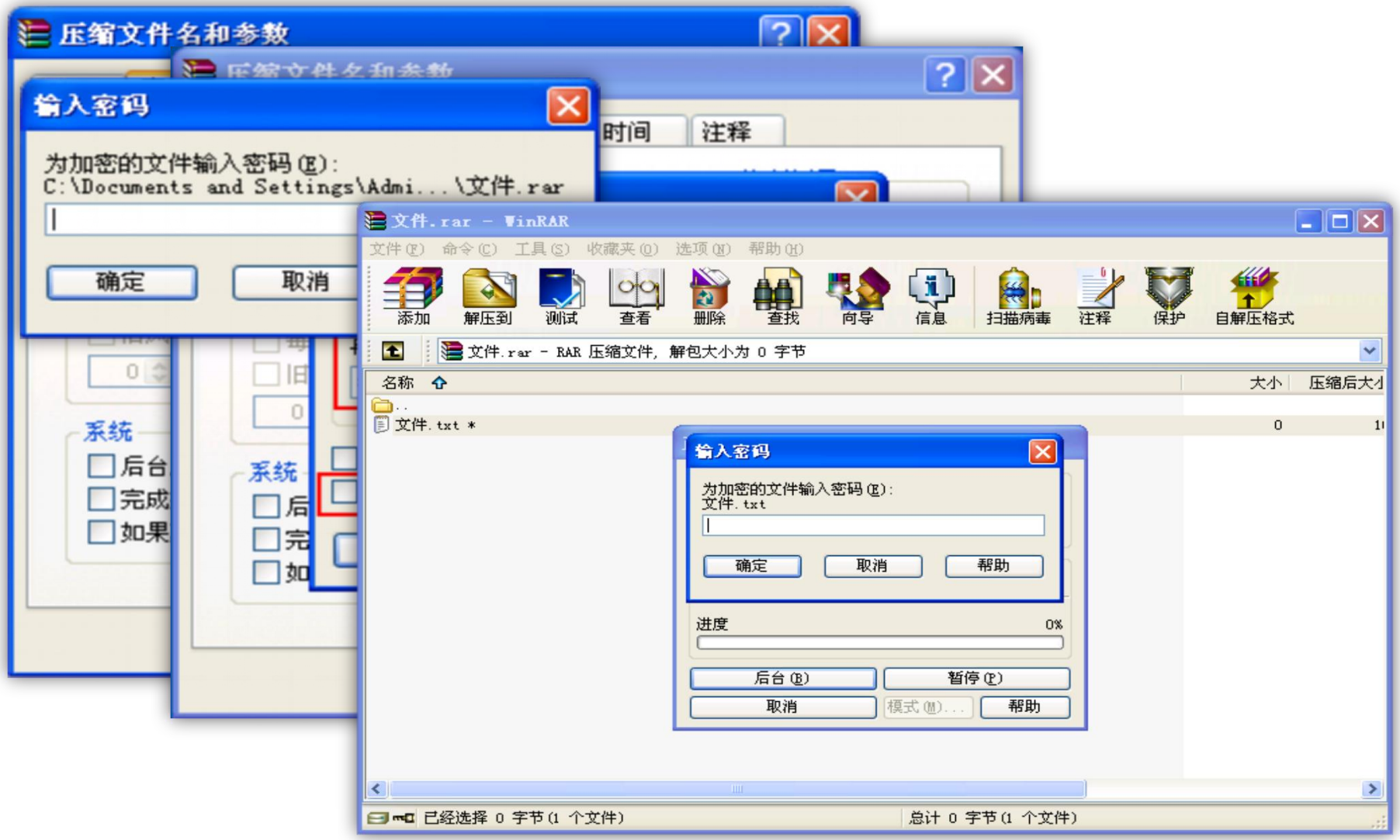
4.对敏感文件加密



5.重要文件备份

6. 维修期间做好硬盘数据保护

No.10 数据安全


压缩文件名和参数
输入密码
为加密的文件输入密码(E):
C:\Documents and Settings\Admi...\文件.rar
确定
取消
时间
注释
系统
后台
完成
如果
文件.rar - WinRAR
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)
添加
解压到
测试
查看
删除
查找
向导
信息
扫描病毒
注释
保护
自解压格式
文件.rar - RAR 压缩文件, 解包大小为 0 字节
名称
大小
压缩后大小
文件.txt *
0
为加密的文件输入密码(E):
文件.txt
确定
取消
帮助
进度
0%
后台(B)
暂停(P)
取消
模式(M)...
帮助
已经选择 0 字节(1 个文件)
总计 0 字节(1 个文件)

No.11 安全使用大模型和各种AI工具

AI时代奔涌而来，随着高校AI与教育的深度融合，AI技术在大学生学习、科研、生活中快速应用，大学生安全使用AI工具需兼顾“效率提升”与“风险防控”，建立对AI的理性认知，守住安全底线。把人工智能当成个人助手的同时，要防范数据隐私与信息泄露风险。

1. 避免输入敏感个人信息

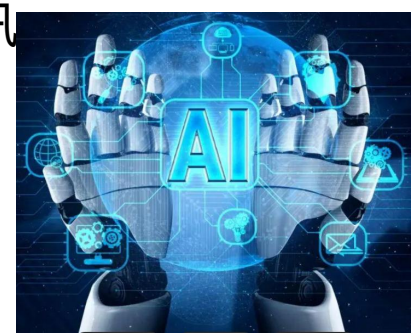
不向大模型提交身份证号、学号、银行卡信息、家庭住址、联系方式等私密数据，也不要上传含个人信息的文档（如简历、成绩单）。大模型可能会将输入数据用于模型训练或存储，存在信息泄露风险。

2. 谨慎分享校园/学术敏感信息

涉及实验室数据、未公开的研究成果、课程作业原稿、考试内容等，勿直接输入大模型，部分校园内部信息可能涉及知识产权或学校管理规范，泄露可能引发学术风险或纪律问题。

3. 注意账号与授权安全

避免使用校园统一身份认证账号登录非官方授权的AI工具，防止账号关联信息被窃取；慎用“第三方登录”功能，授权前仔细查看权限范围（如是否允许访问通讯录、文件等）。



No.11 安全使用大模型和各种AI工具

4.拒绝过度依赖AI导致学术不端

大模型生成的内容可能存在错误（如“AI幻觉”）或抄袭痕迹，直接用于作业、论文、报告等将违反学术诚信规定，可能面临成绩取消、处分等后果。使用时需人工校验、修改并明确标注AI辅助的部分。

5. 知识产权问题

大模型生成的文本、代码、图像等内容，其版权归属可能不明确，若用于公开作业、竞赛或发表，可能涉及侵权。避免直接使用生成内容作为原创成果提交。

6. 遵守平台使用规范

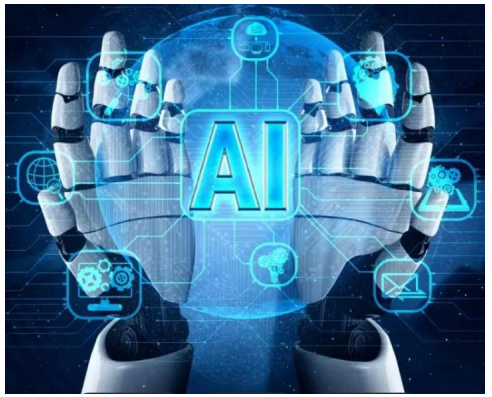
部分AI工具对学术用途有明确限制（如禁止生成考试答案），需提前阅读用户协议，避免因违规使用导致账号封禁或法律风险。

7. 防范钓鱼与恶意工具

只使用正规平台的AI工具，避免点击不明链接或下载来源可疑的“AI插件”“破解版工具”，此类软件可能捆绑病毒、窃取数据或控制设备。

8. 警惕算法滥用与伦理问题

不利用大模型生成违法违规内容（如虚假信息、恶意代码、侮辱性言论），也需警惕AI被用于诈骗（如模仿他人语气生成信息），增强对“AI生成内容”的辨识能力。



大学生利用AI技术违法犯罪典型案例

案例

在一场校园设计大赛中，学生小赵借助 AI 绘图工具创作参赛作品。他直接选用 AI 生成的一幅插画作为作品主体，未确认版权归属。赛后，该插画原作者发现并提出侵权指控。最终，小赵的参赛资格被取消，作品被收回，还可能面临原作者的进一步追责。

未经授权使用他人作品：用AI生成内容时，若训练数据包含未授权的文字、图片、音乐等，可能构成抄袭。例如，直接复制AI生成的论文段落而未核查原创性，可能侵犯原作者著作权。

案例

大学生小林和团队创业做APP，为节省成本，用免费开源AI图像识别库，未按协议保留原作者版权声明。APP上线后遭版权方起诉，不仅需支付赔偿金，创业项目也因信誉受损停滞，给团队带来巨大打击。

擅自使用受专利保护的AI技术：在创业项目中，若未经许可使用他人已申请的AI算法或技术框架，可能构成专利侵权。

案例

传媒专业的小吴，在短视频平台发布 AI 换脸短剧，未经原演员授权，擅自使用其形象。视频爆火后遭演员追责，小吴需公开道歉、下架视频，还因侵权面临平台处罚，极大影响账号运营 。

非法采集或泄露数据：使用AI工具时，若未经授权收集用户隐私数据（如人脸信息、行为数据），或未对数据进行脱敏处理，可能违反《个人信息保护法》。

大学生利用AI技术违法犯罪典型案例

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，非法入侵了学校某系统并获取两万余条该校学生个人信息。

为寻求刺激、炫耀技术，胡某通过之前发现的某小程序存在的技术漏洞，利用**Ai编写程序**，把其中盗取的**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淫秽内容发送至学生本人，对其进行**短信骚扰**。

总之，使用AI大模型时，应秉持“审慎使用、主动验证、守住底线”的原则，在享受技术便利的同时，筑牢个人信息、学术诚信和网络安全的防线。

让我们共同做好校园网络安全工作

- ✓ 万物皆可破，没有绝对的安全
- ✓ 安全防范没有任何捷径可走
- ✓ 好的用网习惯比技术更重要
- ✓ 信息安全并非一劳永逸，一直在路上