安全意识培训

绿盟科技

NSFOCUS

CONTENTS

目 录

NSFOCUS

01

安全态势

1. 互联网现状
2. 案例

NSFOCUS

1.1

互联网现状

我国互联网现状

8.02亿

中国网民规模

57.7%

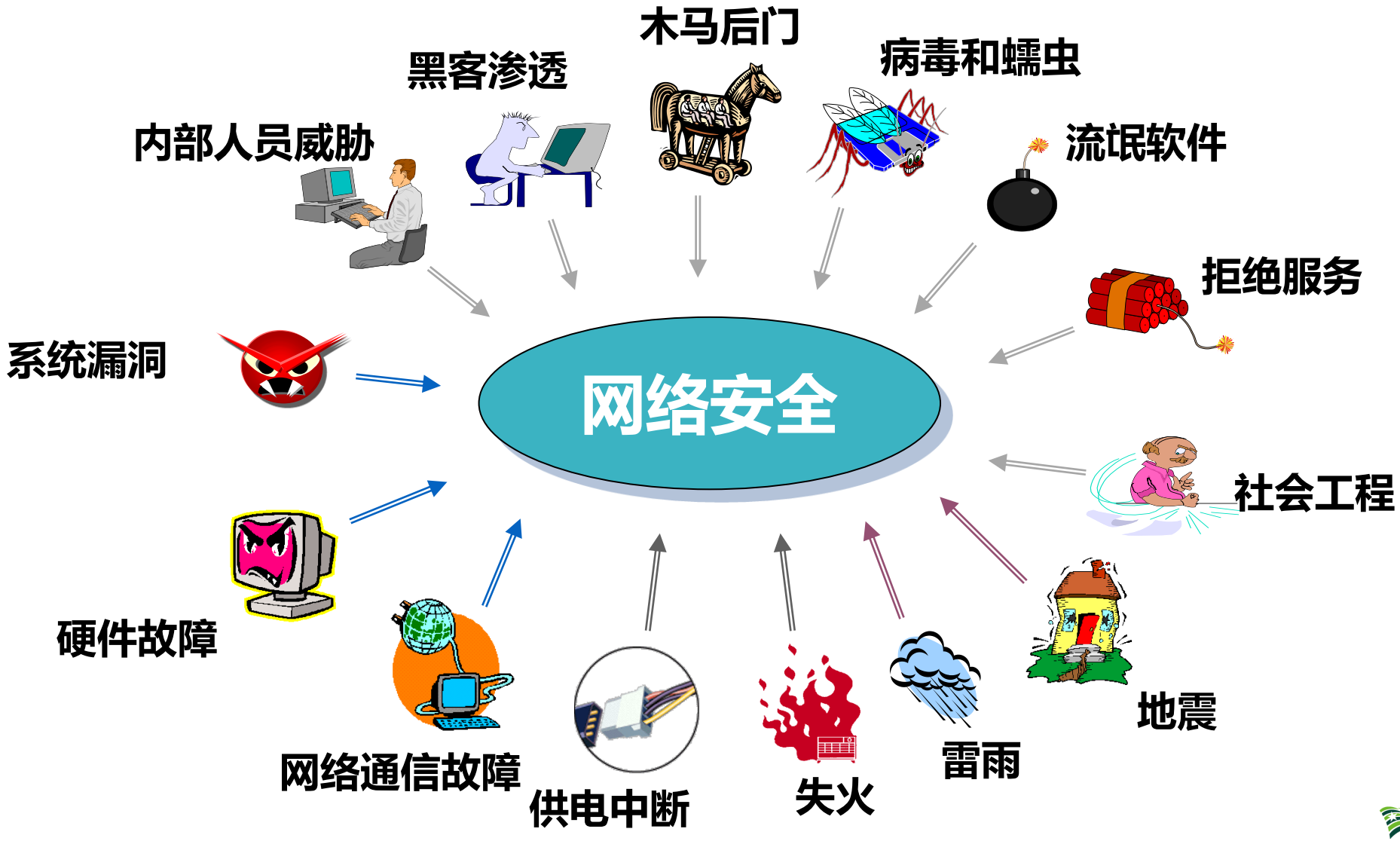
互联网普及率

27.2万亿元

数字经济总量，占GDP总量32.9%

我国正由网络大国向网络强国不断迈进

层出不穷的网络安全威胁



2019年数据泄露调查报告

数据泄露原因

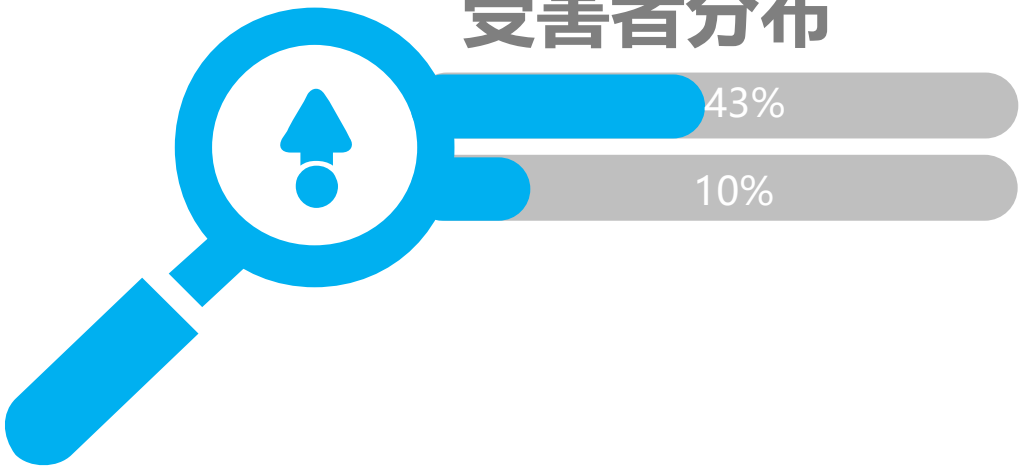
黑客攻击

52%的数据泄露与黑客攻击有关。

弱口令

81%的数据泄露涉及到撞库或弱口令。

受害者分布



小型企业

43%的数据泄露影响的是小企业；

其他行业分布

公共部门16%；医疗保健行业15%；金融行业10%。

NSFOCUS

1.2

案例

万豪客户信息泄露

- **时间：**2020年3月
- **事件：**万豪国际集团官方网站发布公告称，约520万名客户的资料可能被泄露，泄露的资料包括客户的姓名、地址、电子邮箱地址、电话号码、账户和积分余额、生日、偏好等。
- **影响：**万豪国际（MAR.O）股价大跌，跌幅7.57%，市值蒸发约18.34亿美元

Zoom爆重大安全漏洞

- **时间：**2020年4月
- **事件：**Zoom存在的重大安全漏洞：数以万计的私人Zoom视频被上传至公开网页，任何人都可在线围观。
- **影响：**数据泄露、安全隐患、漏洞频出……令大好形势在前的Zoom遭受当头一棒，受此影响，Zoom股价一路开盘下跌逾7%。

02

信息安全基础知识

1. 信息安全概念
2. 如何保障

NSFOCUS

2.1

信息安全基础知识

小测试

- 您离开家每次都关门吗?
- 您离开办公电脑每次都锁屏吗?

如果您记得关家里的门，而不记得锁屏办公的电脑，

说明您可能对电脑的安全认知度不够。

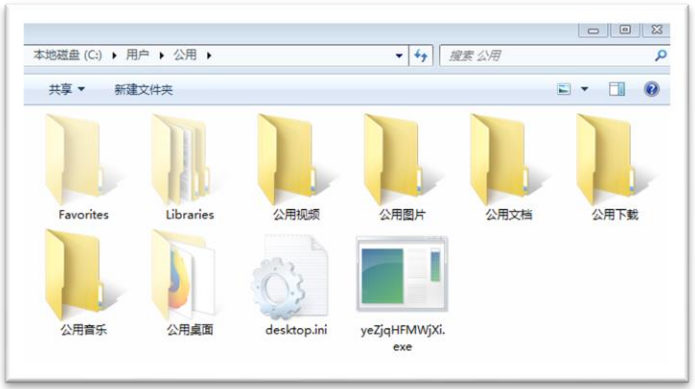
- 您的保险箱设密码吗?
- 您的电脑设密码吗?

如果您记得给保险箱设密码，而不记得给电脑设密码，

说明您可能对信息资产安全认识不够。

什么是信息?

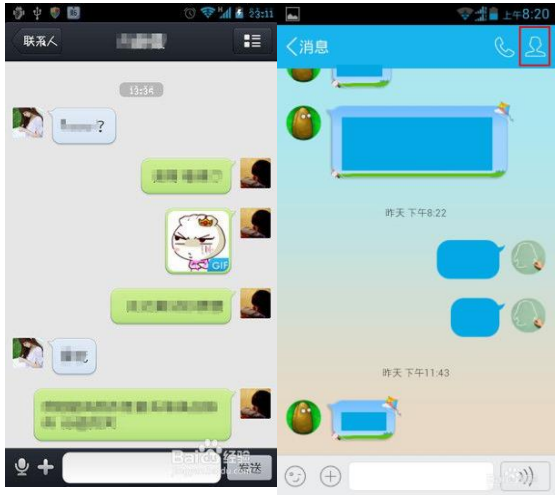
- 电脑中存放的一份文件



- 网站上的一条新闻

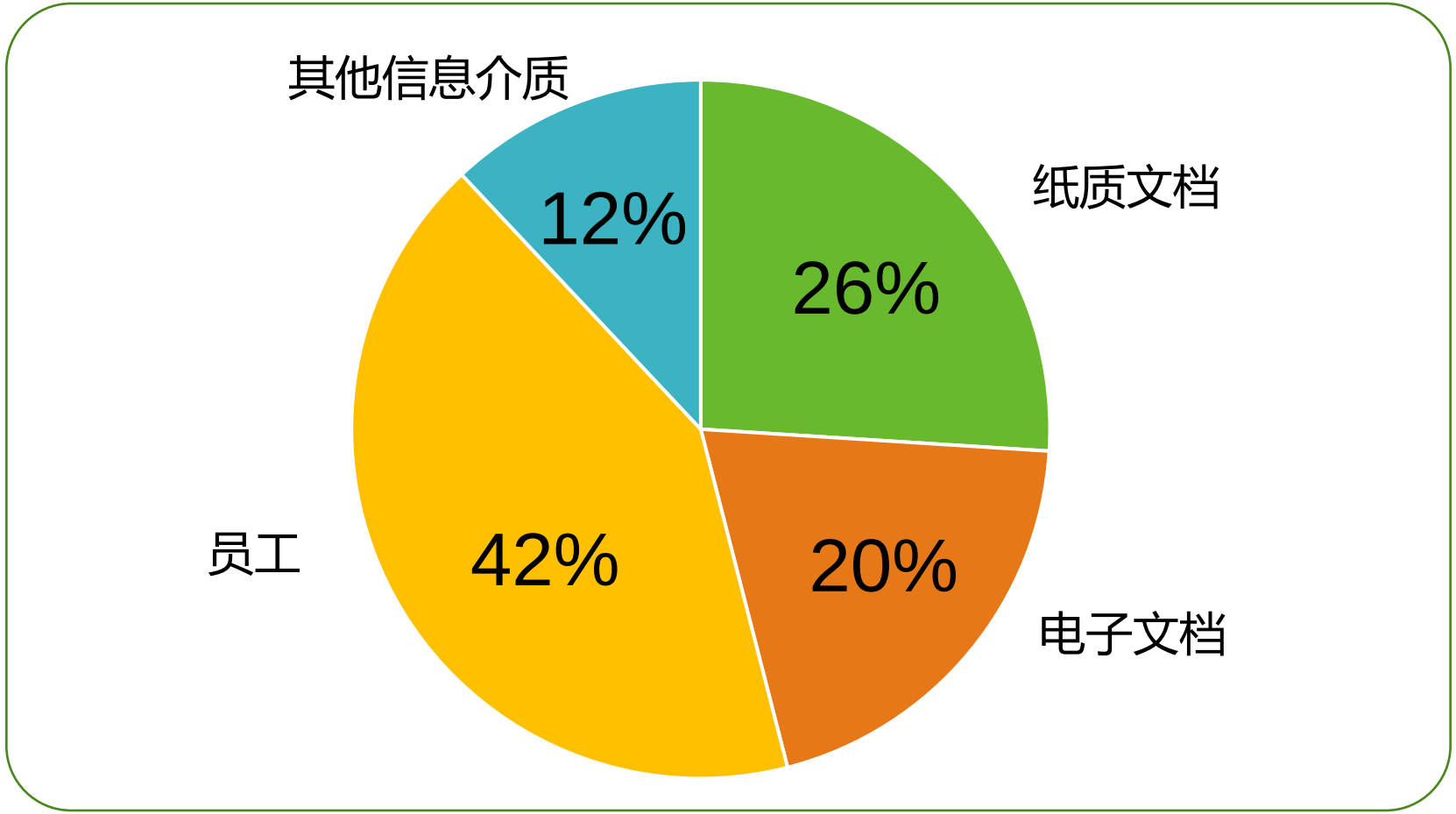
- 电视中的天气预报

- 手机上的一段聊天记录



什么是信息资产?

由企业拥有或者控制的能够为企业带来未来经济利益的信息资源



信息安全目标

Confidentiality（机密性）

确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。

Integrity（完整性）

确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。

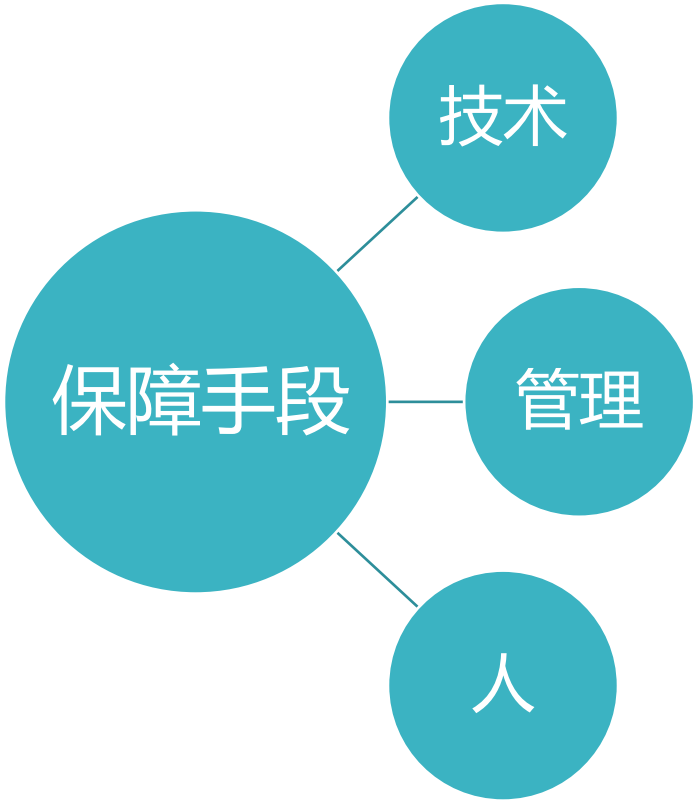
Availability（可用性）

确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

2.2

如何保护信息安全

如何保障信息安全?



物理安全、系统安全、网络安全、应用安全、数据加密、认证授权、访问控制、审计跟踪、防杀病毒、灾备恢复

业界最佳实践——ISO/IEC27001/27002

人员意识、人员技能

安全不是产品的简单堆积，也不是一次性的静态过程，它是人员、技术、管理三者紧密结合的系统工程，是不断演进、循环发展的动态过程

03

护网简介

1. 护网简介
2. 护网行动目的

NSFOCUS

3.1

护网行动简介

护网行动简介

公安部牵头组织，关键基础设施企业为目标，多个专业队伍参与的网络攻防演练活动。

目标不固定，采用随机方式选择，攻击手段不限制（拒绝服务等对正常业务有影响的方式除外），以获得业务系统数据和网络资产权限为目，攻防双方分别进行评分排名。

护网行动简介

得分标准：

蓝队（攻击队）：获取权限、穿透网络隔离、发现被控线索。

红队（防守队）：发现木马、钓鱼邮件、溯源、应急处置。

3.2

护网行动目的

护网行动目的

有效检测关键基础设施的安全状况，发现现实中存在的网络安全问题，增强运维人员安全能力，为做好安全防护工作提供指导，提升网络安全保障水平。

主要考核监测发现能力、应急处置能力、配合协调能力。

04

信息安全意识

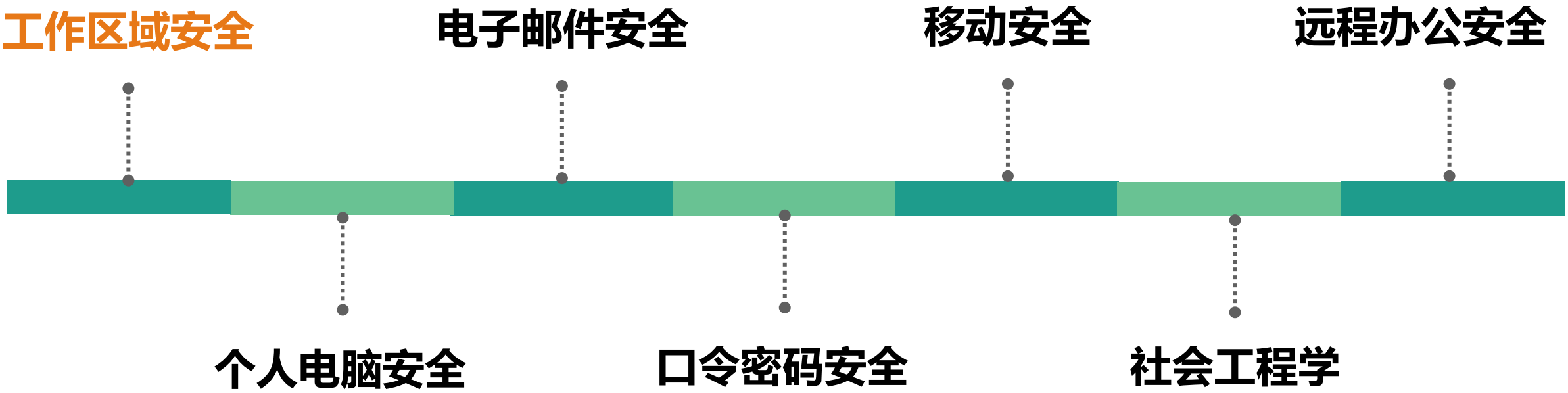
- 工作区域安全
- 个人电脑安全
- 电子邮件安全
- 口令密码安全
- 移动安全
- 社会工程学
- 远程办公安全
- 护网安全

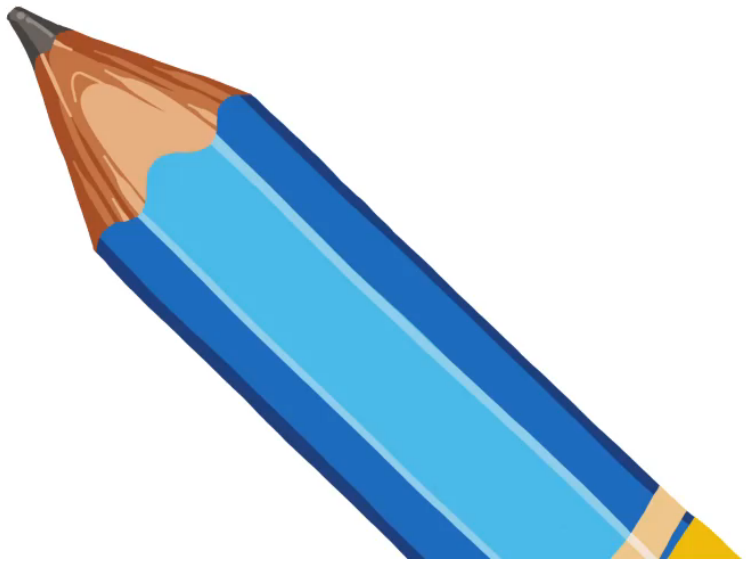
NSFOCUS

4.1

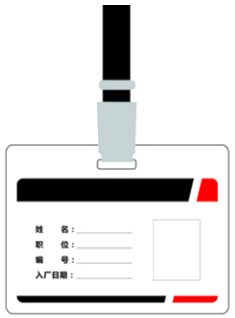
信息安全意识

信息安全意识及防范





工作区域安全



钥匙和门卡仅供本人使用，注意随手关门

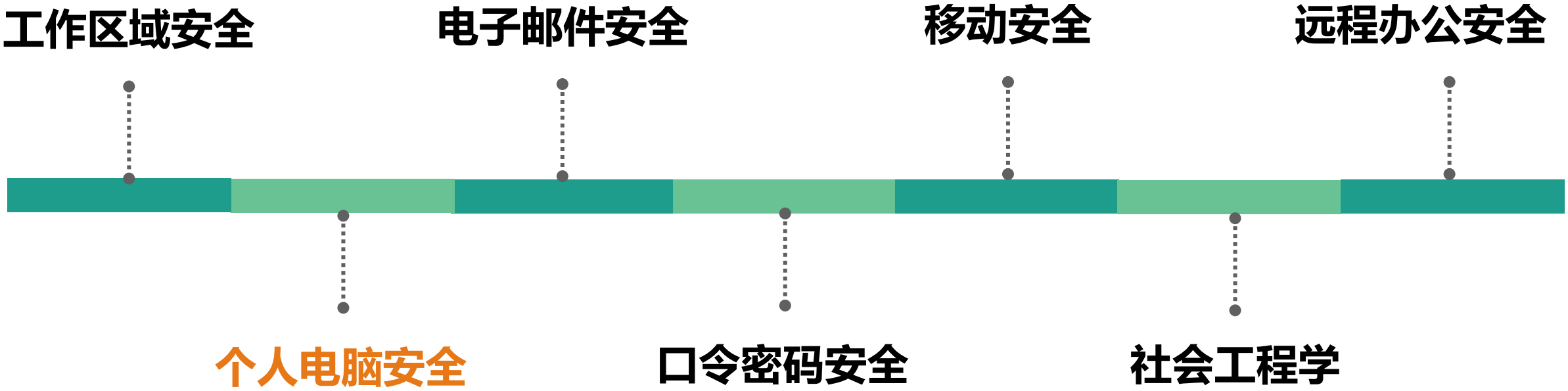
外来人员需登记，勿随意出入

个人工位不应随意摆放敏感资料

复印/打印时，禁止将敏感资料遗留在复印机/打印机旁边

对不再使用的资料，应使用碎纸机将其清理

信息安全意识及防范



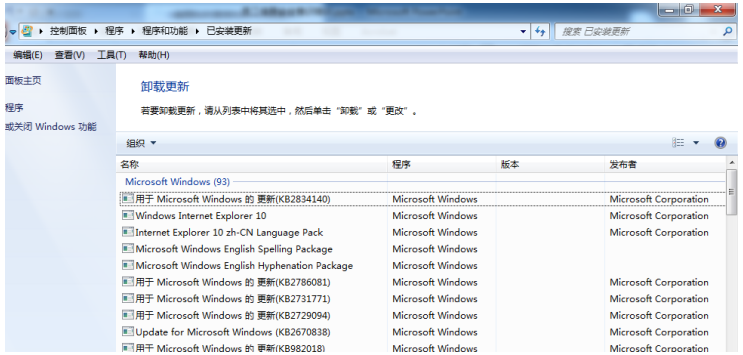
个人电脑安全

- 防病毒软件安装与及时更新
  - ✓ 可根据个人使用习惯来选择
  - ✓ 及时升级病毒库

NSFOCUS

个人电脑安全

- 操作系统补丁自动更新
  - ✓ 设置自动更新
    - – 【控制面板】→【自动更新】
  - ✓ 检查补丁安装情况
    - – 【控制面板】→【添加或删除程序】
    - – C:/WINDOWS/



NSFOCUS

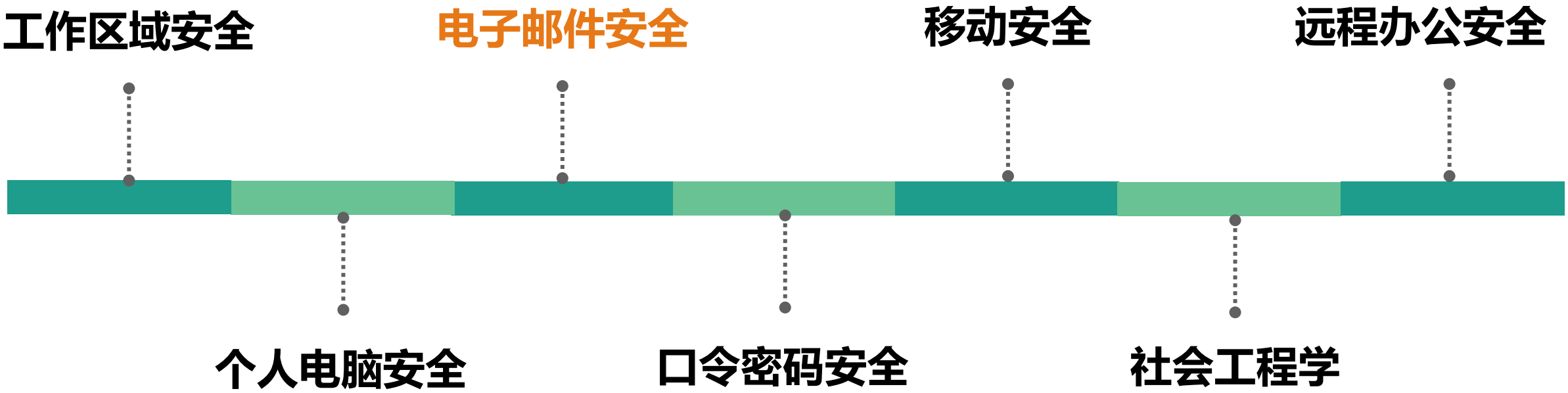
个人电脑安全

- 移动设备的安全使用
  - ✓ 未知U盘、移动硬盘等存储设备使用需谨慎
  - ✓ 存储设备使用前应先查杀病毒
  - ✓ 不要将重要的信息存储在U盘中；确需存储时采用加密U盘
  - ✓ 注意保管、防止丢失；若丢失应立即通知相关部门
  - ✓ 废弃设备应及对存储信息进行彻底可靠的销毁

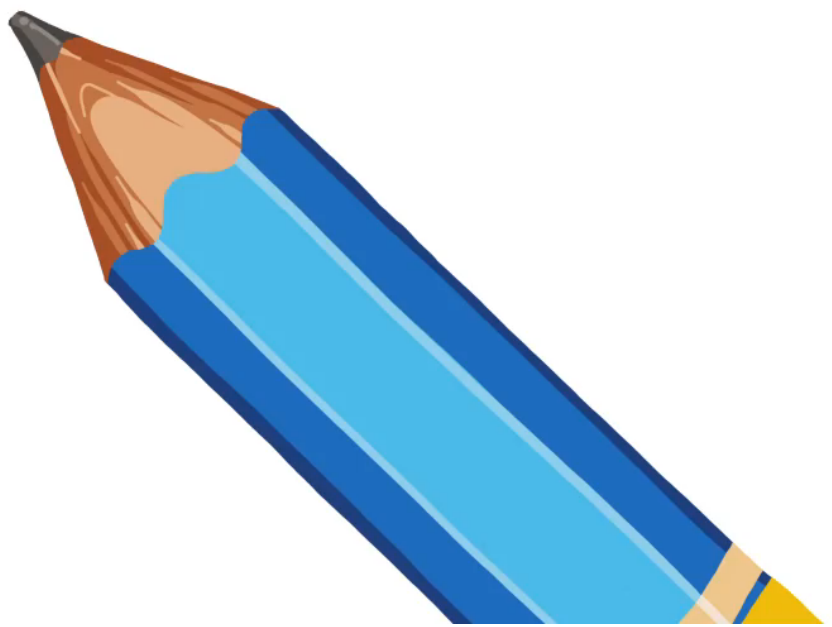
个人电脑安全

- 在暂时离开电脑时，需锁屏（Win+L）
- 设置10分钟自动锁屏
- 重新进入电脑桌面时需要密码认证

信息安全意识及防范

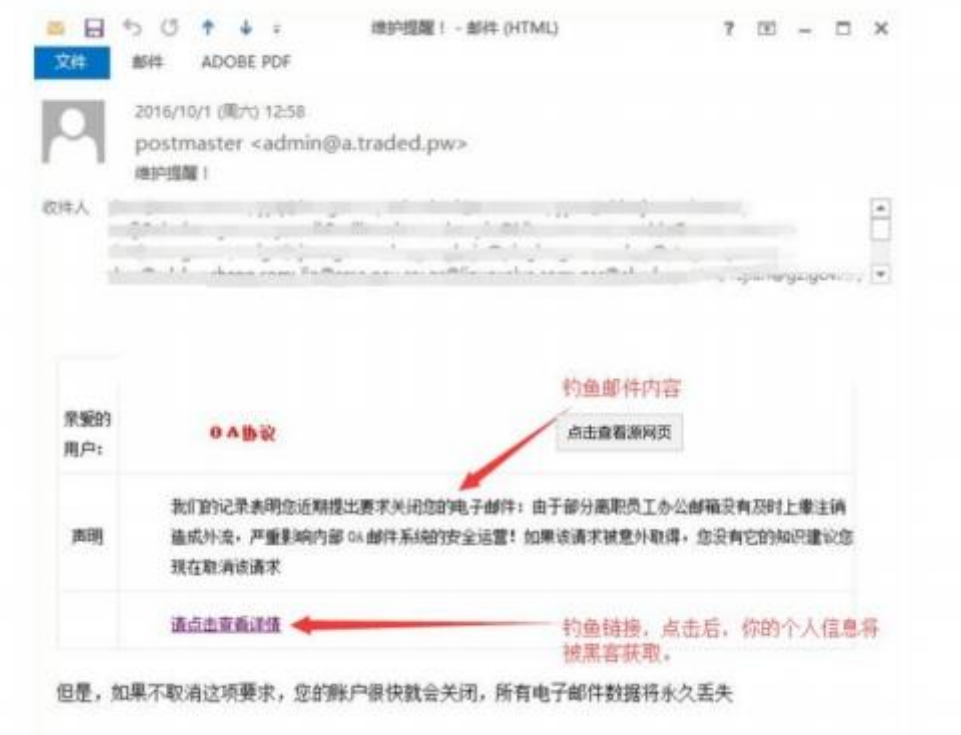


NSFOCUS



电子邮件安全

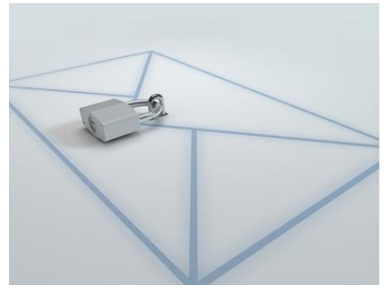
- 钓鱼邮件指利用伪装的电子邮件，欺骗收件人将帐号密码、口令等信息回复给指定的接收者；或引导收件人连接到特制的网页（这些网页通常会伪装成和真实网站一样，令登录者信以为真），输入帐号密码等信息从而盗取接收者信息。



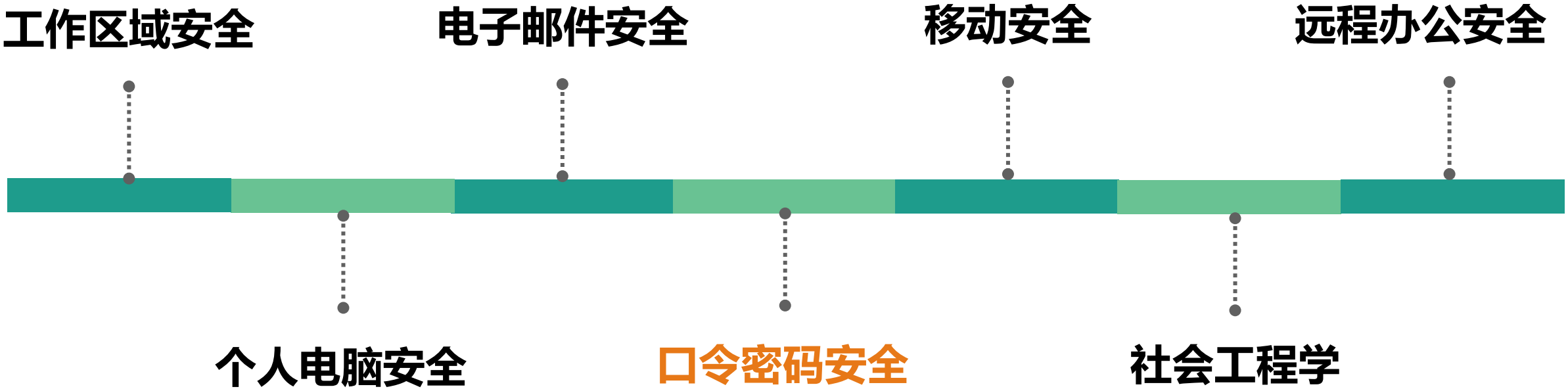
- 钓鱼邮件特点
  - 1、邮件标题多以“xx 会议通知”、"xx 办重要通知”、"xx 工资表”之类，对收件人具有很强的吸引、迷惑性。
  - 2、查杀逃逸
  - 3、诱导性提示，引导下一步动作

电子邮件安全

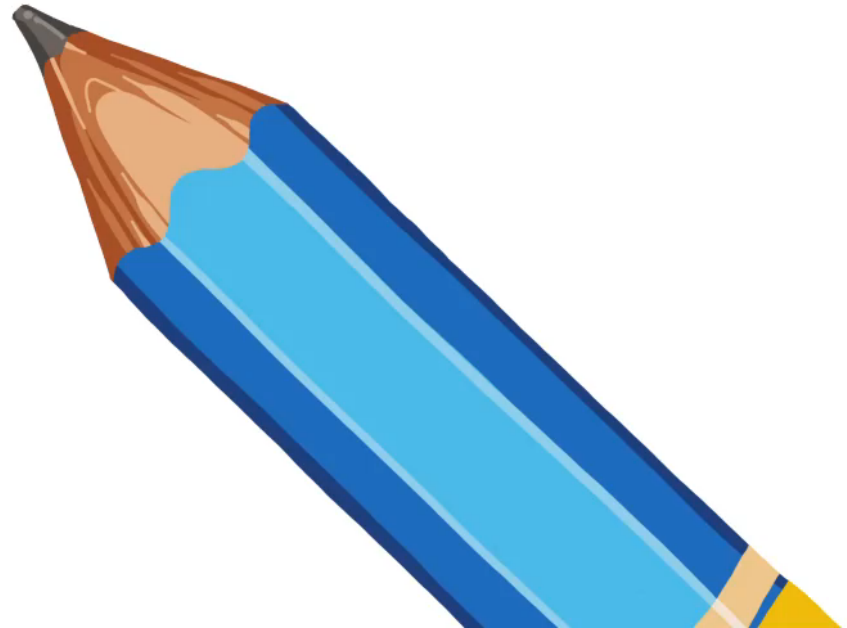
- 工作邮件均通过公司邮箱发送和接收
- 发邮件前应检查确认收件人，机密文件切勿群发
- 机密文件应加密后发送，密钥不得随邮件发送
- 重要邮件建议加密存储
- 切勿点击陌生邮件的附件或连接，删除与业务无关的邮件
  - 绝对不要打开任何以下文件类型的邮件附件：.bat, .com, .exe, .vbs
  - 绝对不要打开任何未知文件类型的邮件附件，包括邮件内容中到未知文件类型的链接
  - 如果要打开微软文件类型（例如 .doc, .xls, .ppt等）的邮件附件或者内部链接，务必先进行病毒扫描



信息安全意识及防范



NSFOCUS



口令密码安全

最烂密码

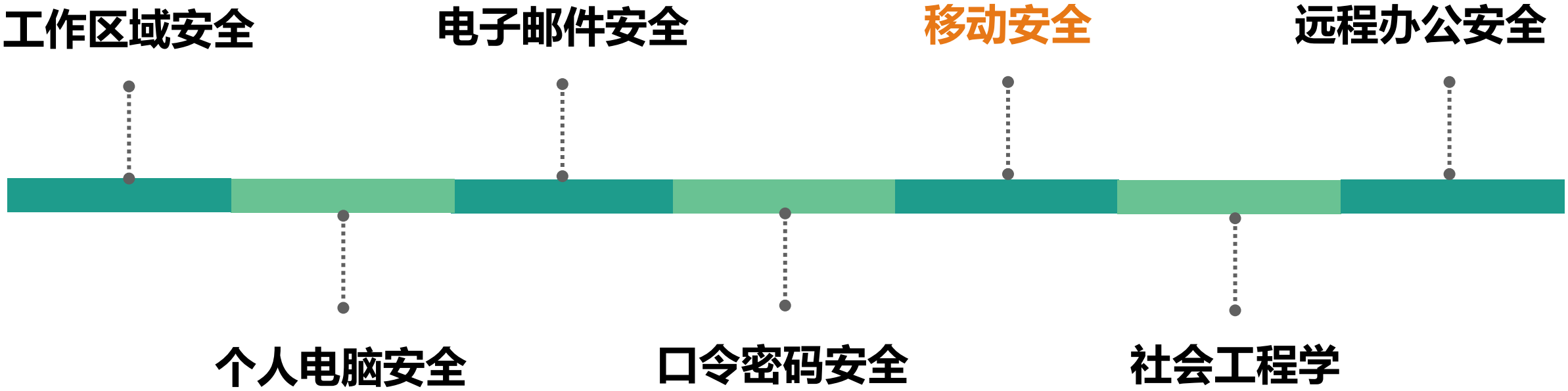
2018年12月15日安全服务公司SplashData公布了2018年度100组最不安全的密码榜单：

1、123456 (这组密码已连续三年登榜首)
2、password(与2017年排名相同)
3、123456789(去年排名第6)
4、12345678(排名比去年下滑一名)
5、12345(与2017年排名相同)
6、111111 (前十大排名新进榜)
7、1234567(排名比去年上升一名)
8、sunshine (前十大排名新进榜)
9、qwerty(去年排名第4)
10、iloveyou(与2017年排名一致)

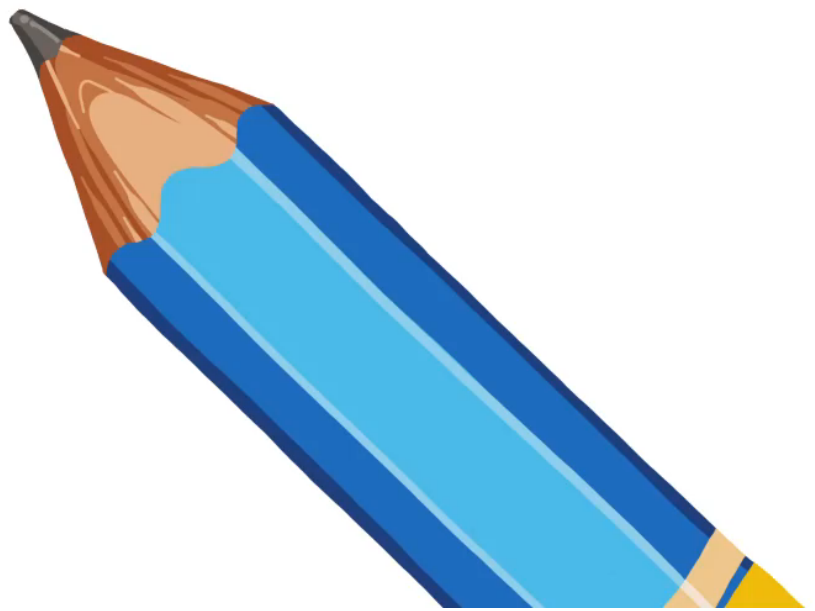
口令密码安全

- 使用大写字母、小写字母、数字、特殊符号组成的密码
- 妥善保管
- 长度不少于10位
- 定期更换，如三个月或半年
- 不同的账号使用不同的密码，分级管理
- 不使用敏感字符串，如生日、姓名关联
- 离开时需要锁定计算机

信息安全意识及防范



NSFOCUS



移动安全

Request | Response

Raw | Params | Headers | Hex

```
POST /mbc/svt/login.shtml HTTP/1.1
Content-Length: 311
Content-Type: text/plain; charset=UTF-8
```

使用网络嗅探或中间代理工具，抓取数据包

```
Cookie2: $Version=1

{"TranCode":"IBSQ0001","DeviceDigest":"A3PjFVhyCr9Tq4B3fwuk8wn4MbU=","LoginName":"123456","P
assword":"aaaaaaa","Reverse":"0","TransId":"bhbc.ClientLogin","DeviceInfo":"000000000000000|
android|android|2.3.3|android","imageCoder":"4059","DeviceType":"Android","TermSeq":"1212222
","Flag1":"1","Platform":"android"}
```

? < + > Type a search term 0 mat

移动安全

张先生是做家具定制生意的，近几年生意越做越大，他也开了一家网上旗舰店，双十一期间生意特别好。

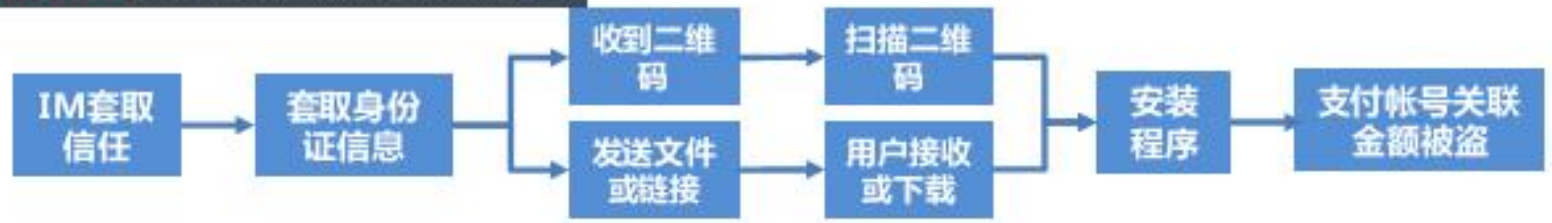
“前几天，有个人说他家里要装修，想定制些家具。那个人就和其他前来咨询的客人一样，没什么特别。”张先生每次回想这个事情，都特别懊悔。

“只是聊着聊着，那个买家突然说，他在外面，手机流量有限发不了那么多图，让我**扫描一个二维码**，下载后可以看到他想要的家具的图片和尺寸。”张先生说，“现在都流行扫一下二维码，我之前扫描过，很方便，就拿手机扫了一下。但是扫描后，我啥也没看到。”

“后来我又和买家沟通了一会，他说先付些订金，问我要了姓名、身份证、银行卡、手机号等信息，说晚上回到家再汇款就下线了。”

晚上，张先生登录网银，看看买家的订金到账没有，却震惊地发现**银行卡内少了好几万**。张先生马上意识到自己被盗了，赶紧冻结了银行卡并向警方报案。

共同案情回放：

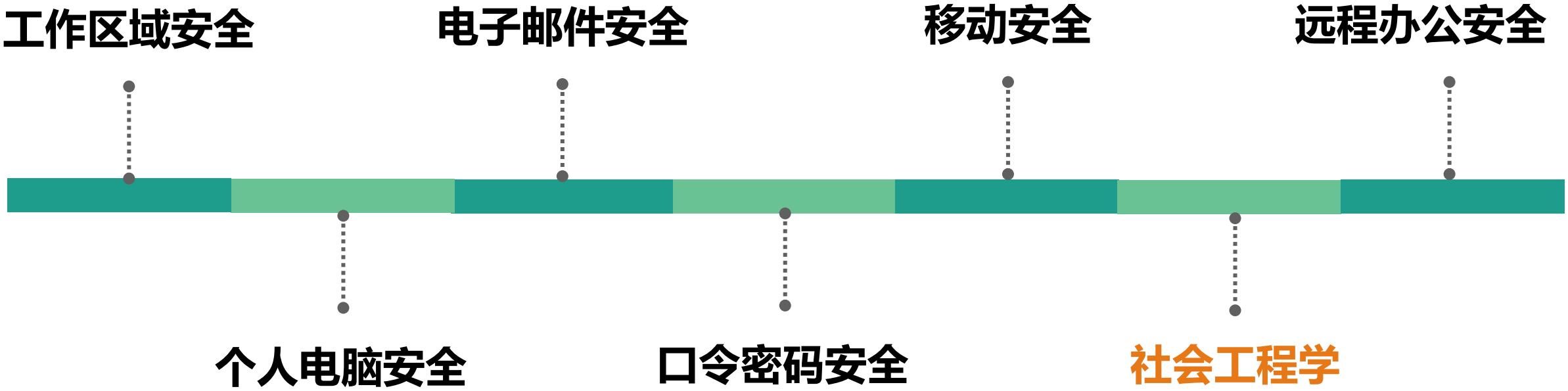


NSFOCUS

移动安全

- 连接WIFI时，仔细确认WIFI名称
- 免费WIFI请慎用
- 在传送公司机密文件、移动支付时请使用运营商4G网络
- 扫描前先判断二维码发布来源是否权威可信
- 通过二维码安装软件时，先杀毒再安装
- 苹果系统不越狱，安卓系统不root（不打开调试模式）

信息安全意识及防范



社会工程学特点

通过对受害者

本能反应、好奇心、信任、贪婪

等心理弱点进行如欺骗和伤害等攻击手段

社会工程学的攻击，成功于人们

普遍的对信息安全实践上的无知！

	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

社会工程学的一般攻击过程

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，或者攻击者期望的任意角色。

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。

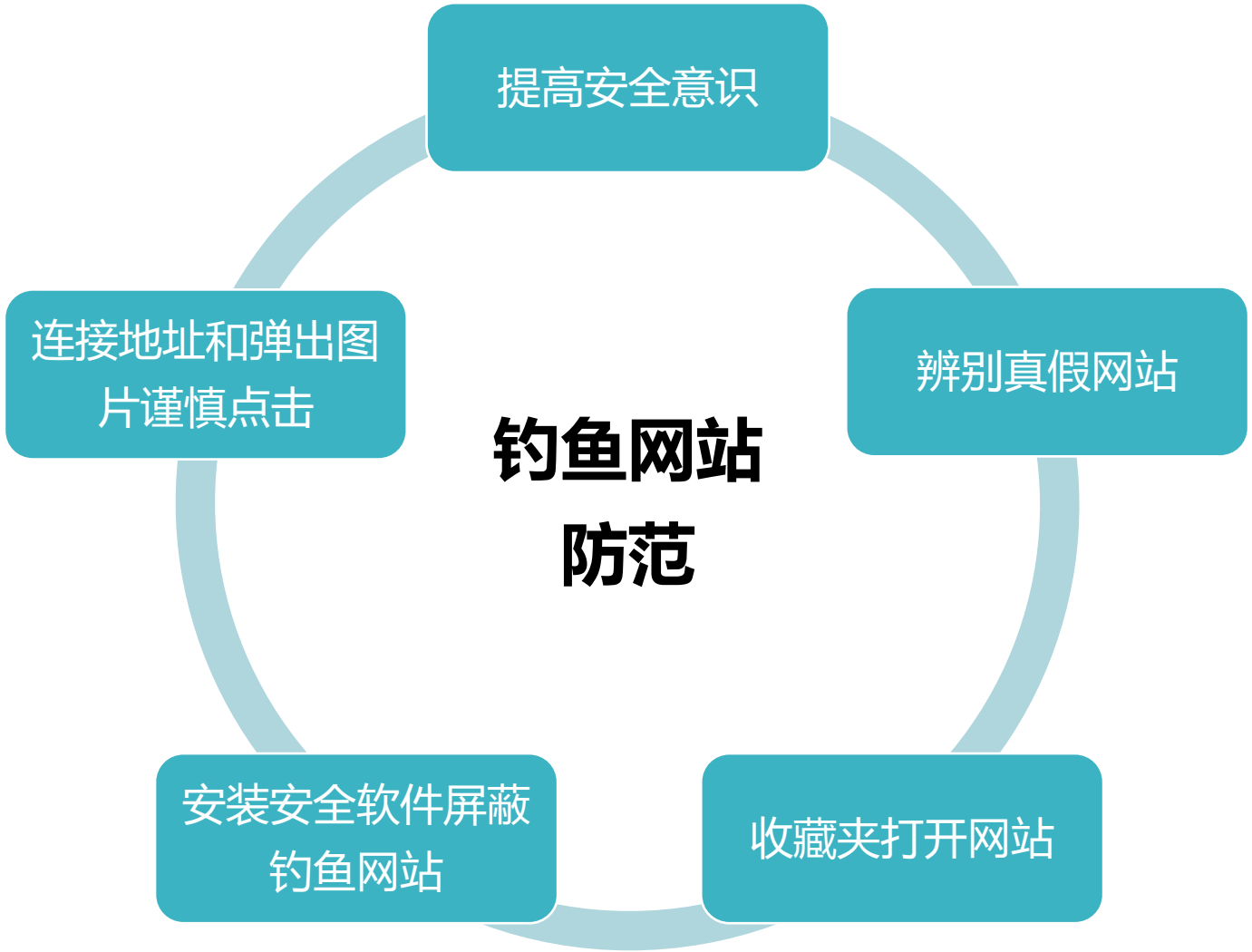
社会工程学常用手段及防范

- 钓鱼网站

社会工程学常用手段及防范

- 域名唯一，仔细辨别
- 制作粗糙，观察细节

社会工程学常用手段及防范

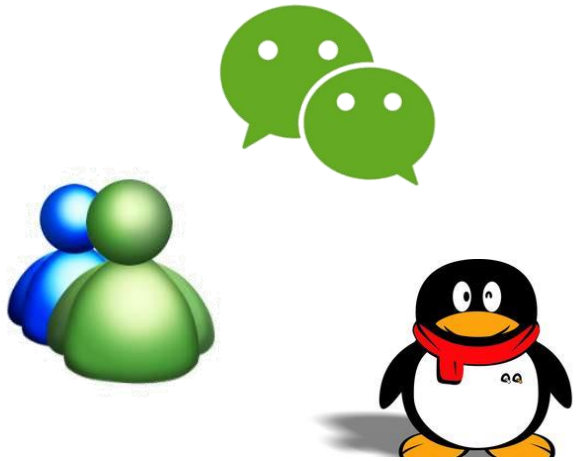


社会工程学常用手段及防范

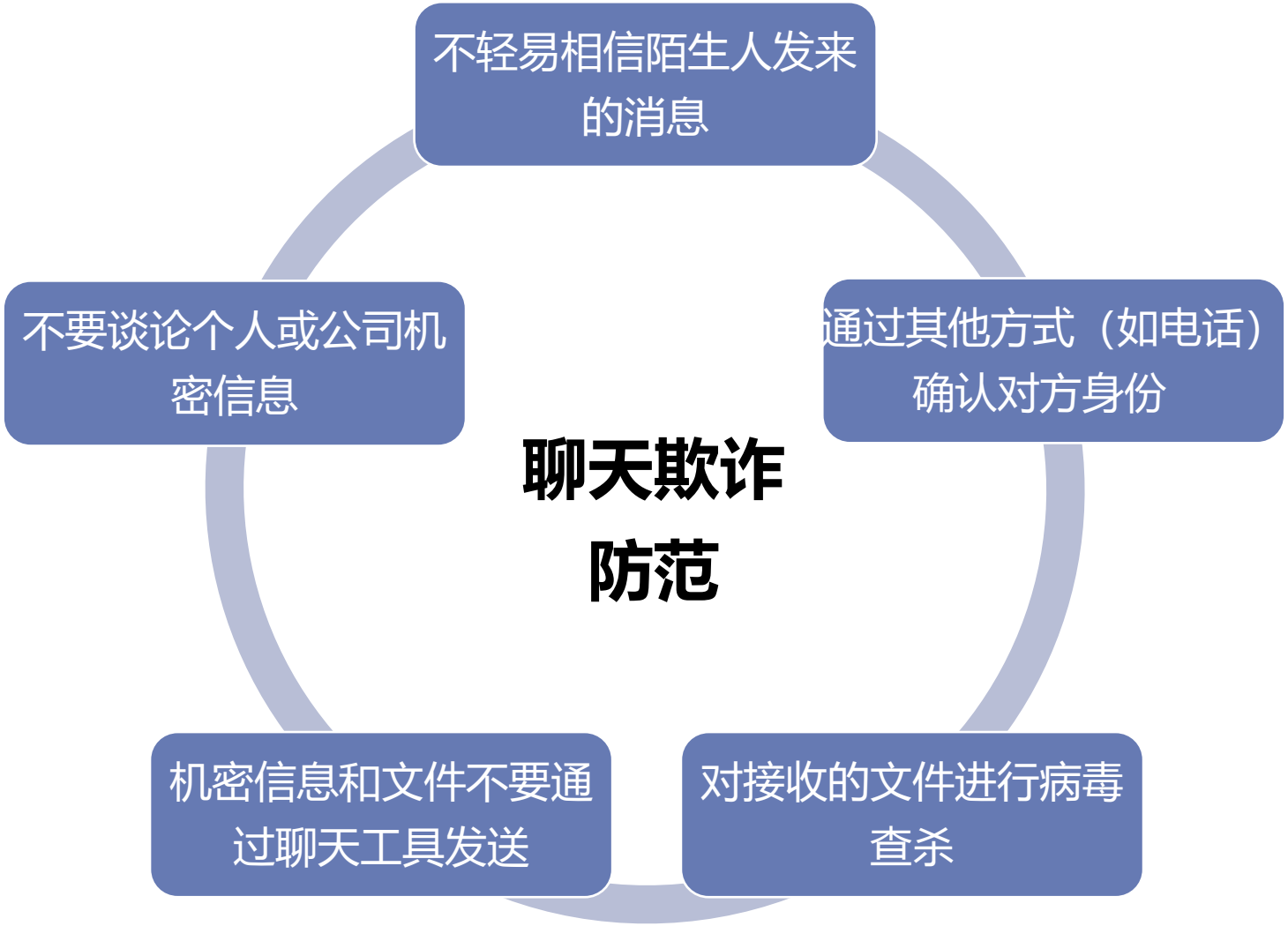
- 聊天欺诈

只要你一打开QQ，可能就会收到某个好友的留言，例如：
1：介绍你访问一个很好的xxx网址。
2：在XXXX网址发现了你的相片，让你快去看看。
3：说有急事，先帮忙往他的朋友银行帐户汇款，晚上再转帐还给你。
4：让你拨打一个电话号码，听他给你的留言和给你点的歌曲。等等。

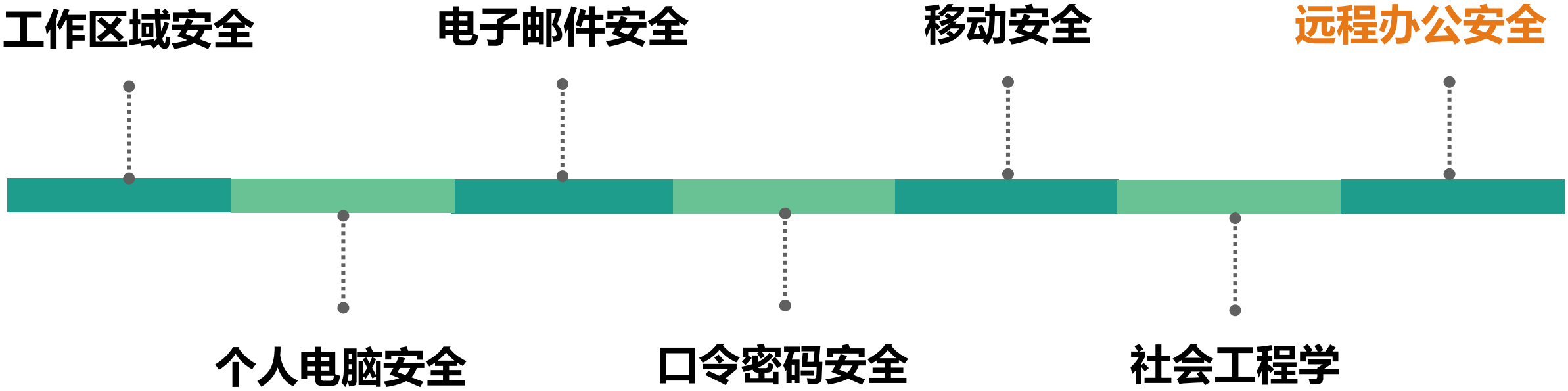
请大家不要相信，这些都是你的好友中了QQ病毒自动发送的，如果你访问了提示的网站可能就会中同样的病毒。汇款和打电话听留言是骗钱的



社会工程学常用手段及防范



信息安全意识及防范



远程办公安全

- 远程办公软件安全

办公软件：钉钉、企业微信、蓝信、飞书
远程会议：好视通、263、Zoom
在线协作：石墨文档、腾讯文档、WPS+

防护建议

1. 建议将使用的远程办公软件更新至最新版本，避免低版本可能存在的安全漏洞；
2. 在使用云盘分享文件时，如果文件重要性较高，建议对文件进行压缩并加密，同时分享文件时需设置提取码；
3. 使用主流的知名办公软件，通过官方渠道下载安装。

远程办公安全

- 办公终端安全

防护建议

1. 尽量使用公司配备的电脑办公；
2. 安装防病毒等安全终端防护软件，并定期进行杀毒；
3. 及时更新家用电脑的操作系统和补丁程序，确保使用的是最新版本；
4. 将家中的Wi-Fi密码设置为强口令；
5. 不使用外部的公共Wi-Fi上网办公；
6. 对设备设置开机密码，防止丢失或者被窃而导致的企业数据泄露问题；
7. 安装移动APP时，请通过官方渠道下载。

远程办公安全

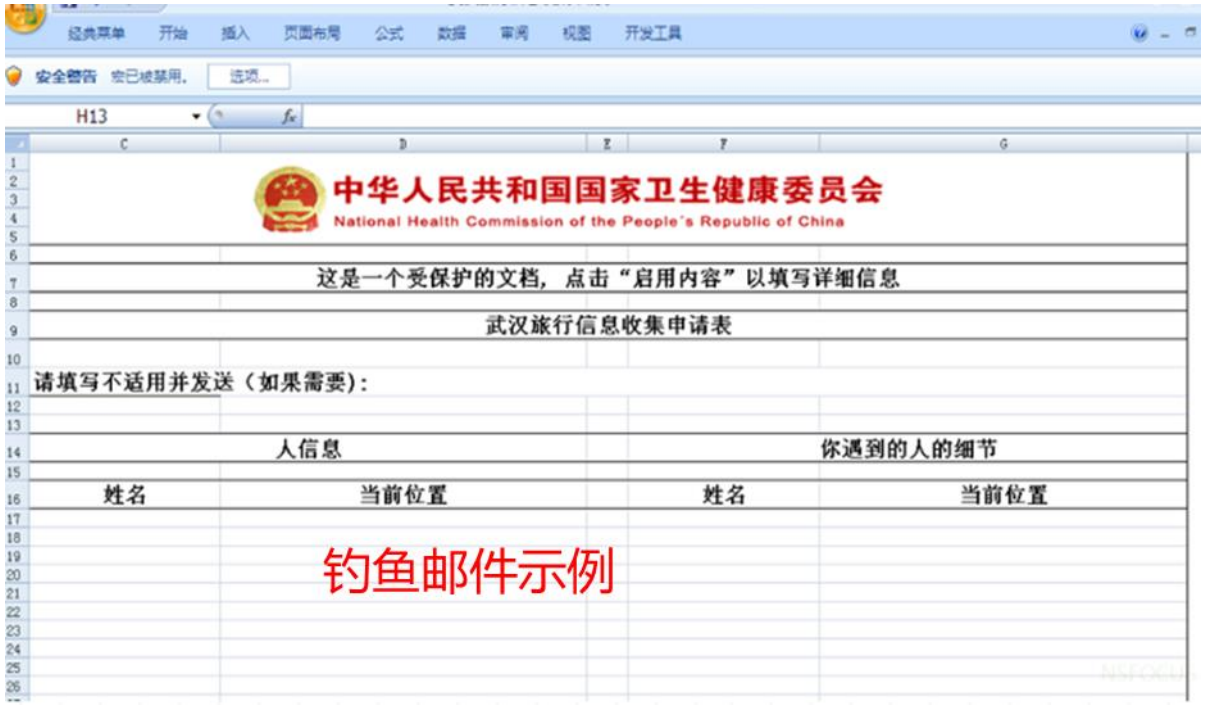
- 警惕疫情期间的钓鱼木马攻击

在国内，日前，有些黑客冒充“国家卫健委”，向政企用户有针对性地发送钓鱼邮件，“指导”其开展“新型冠状病毒肺炎疫情”的防控工作。为骗取政企用户的信任，黑客将邮件署名伪造为“中华人民共和国国家卫生健康委员会”。用户一旦点击这些邮件，就会成为钓鱼攻击的受害者。特殊时期，这种违法攻击行为所造成的影响极为恶劣。

钓鱼邮件示例

远程办公安全

- 警惕疫情期间的钓鱼木马攻击



防护建议

1. 自用电脑远程办公时尽量只访问办公相关地址。
2. 查看邮件时，一定要注意识别不明链接，不要打开来历不明的电子邮件或下载其邮件附件文件。
3. 不要轻易打开与疫情相关的可执行文件，如“.exe”“.bat”“.csr”等后缀的文件。
4. 注意关掉office中的宏。

NSFOCUS

4.2

总结

提升个人安全意识，培养安全办公习惯

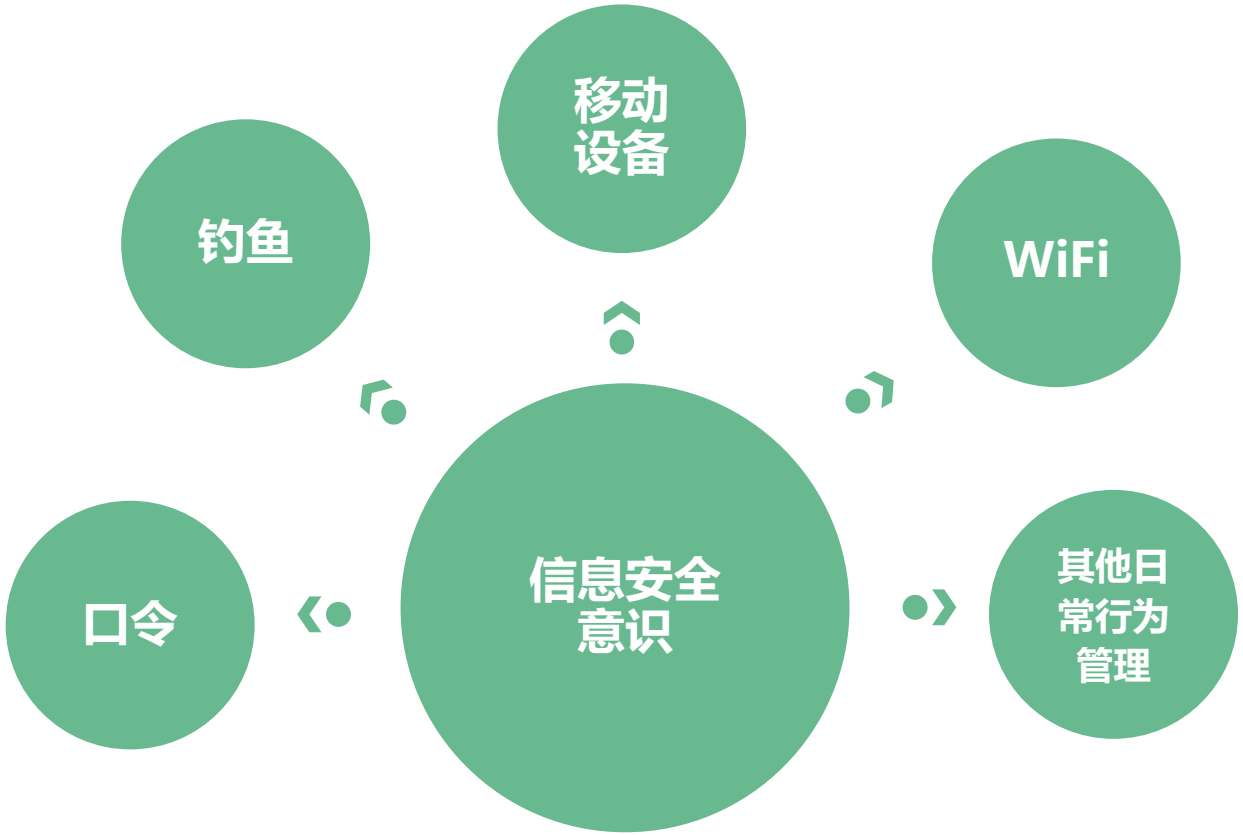
- 进入大门、闸机时主动阻止陌生人尾随进入；
- 废弃的纸质资料应该进行充分粉碎（碎纸机）；
- 敏感资料应妥善保管，在离开工位时锁入柜中；
- 电脑及时更新打补丁，使用防病毒软件；
- 避免弱口令，离开工位时对办公电脑进行锁屏；
- 不应使用来历不明的移动存储设备；
- 不应随意查看不明邮件中的附件；
- 机密信息和文件不要通过聊天工具发送。

NSFOCUS

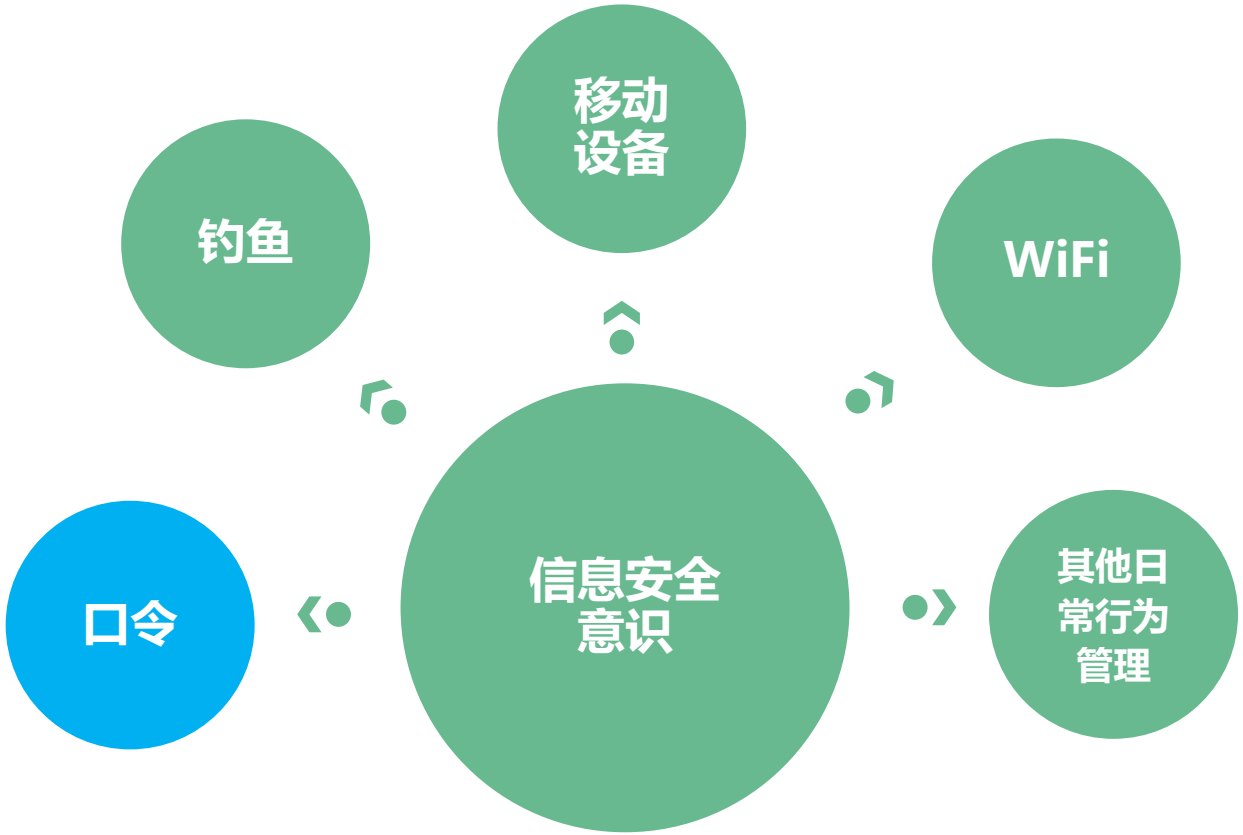
4.3

HVV信息安全意识

信息安全意识



信息安全意识



口令

所谓口令，就是一些过关的证据，由它来决定个人能否通过某个检测，例如过去抗战时期的暗语和暗号等等。口令并不真正具有机密性，除了你之外，银行本身也知道你卡的密码。

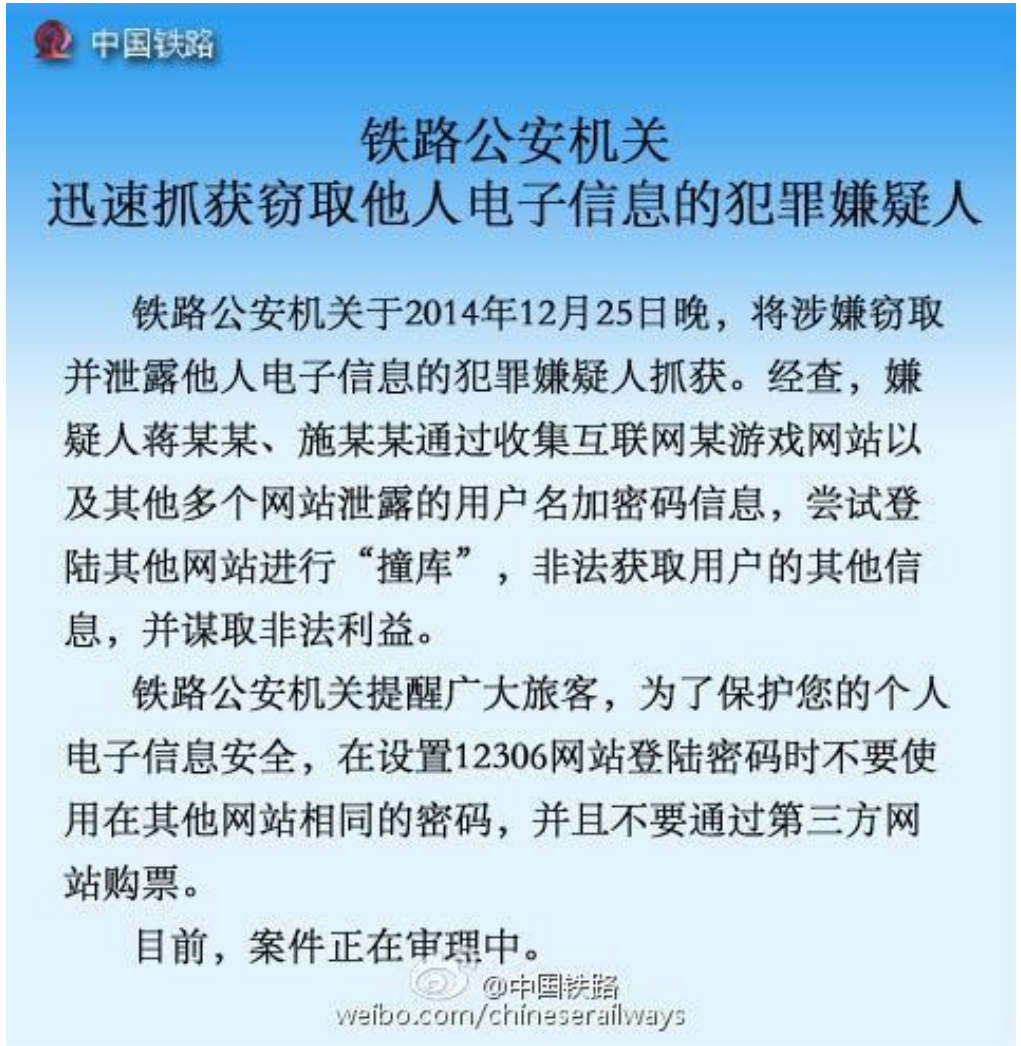
2011年中国互联网史上最大泄密事件

名称	修改日期	类型	大小
天涯数据	2011/12/29 0:41	文件夹	
7k7k2000万_2047.rar	2011/12/28 23:20	快压 RAR 压缩文件	198,876 KB
178(1000w)_3087.rar	2011/12/28 21:44	快压 RAR 压缩文件	105,991 KB
766_16368.rar	2011/12/28 21:20	快压 RAR 压缩文件	103,761 KB
766+开心.rar	2011/12/28 20:59	快压 RAR 压缩文件	111,850 KB
1000W+IS2_16436.rar	2011/12/28 23:25	快压 RAR 压缩文件	161,556 KB
17173_6208.rar	2011/12/29 0:05	快压 RAR 压缩文件	582,382 KB
CSDN-中文IT社区-600万.rar	2011/12/22 14:53	快压 RAR 压缩文件	107,366 KB
test.txt	2011/12/29 0:44	文本文档	2 KB
weibo.com_12160.rar	2011/12/28 20:27	快压 RAR 压缩文件	50,724 KB
xh-2.txt	2011/11/9 18:07	文本文档	160,129 KB
嘟嘟牛_66277.rar	2011/12/28 22:55	快压 RAR 压缩文件	210,613 KB
多玩网_800W.rar	2011/12/28 22:33	快压 RAR 压缩文件	222,112 KB
猫1000W_8228.rar	2011/12/28 20:39	快压 RAR 压缩文件	94,152 KB
人人网500W_16610.rar	2011/12/22 16:35	快压 RAR 压缩文件	50,752 KB
天涯数据.kz	2011/12/28 23:08	快压 KZ 压缩文件	386,143 KB

黑客在网上公开CSDN网站的用户数据库，导致600余万个注册邮箱账号和与之对应的明文密码（即用户密码什么样，网站数据库就存成什么样）。之后网上曝出人人网、天涯、开心网、多玩、世纪佳缘、珍爱网、美空网、百合网、178、7K7K等知名网站的用户密码遭网上公开泄露。最新监测数据发现，目前网上公开暴露的网络账户密码超过1亿个。

NSFOCUS

2014年12306数据泄露



撞库的原因及防御方法

原因

1. 广大网络用户为了方便记忆，所有网站都使用同一套用户名和密码。
2. 网站登录的安全措施不够

防御

1. 在满足复杂度的前提下，将密码中某一段与当前系统/网站联系起来，形成每一套系统不同的密码
2. 不使用弱口令

严禁使用弱口令

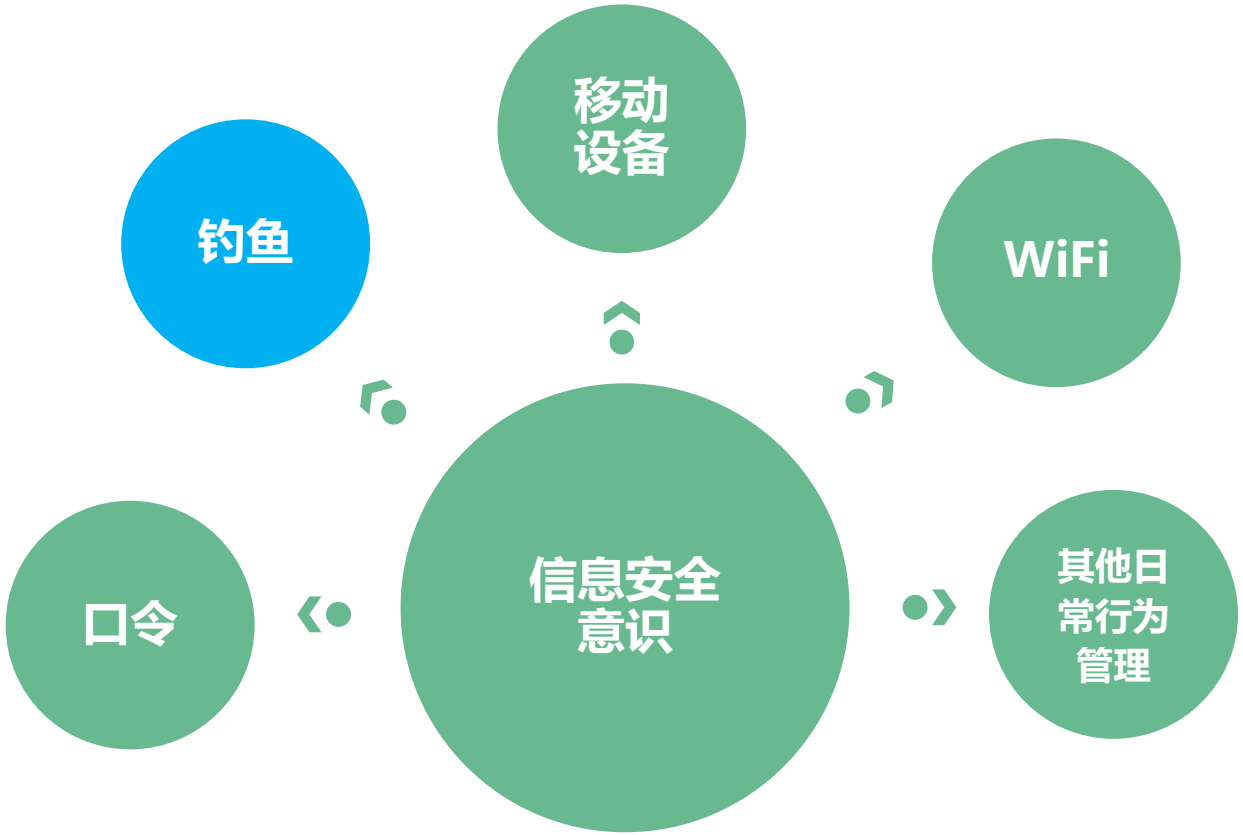
- **员工应注意保管好自己的帐号密码等，不应向其他任何人员透露。**
- **办公电脑应关闭 guest 和匿名帐号，及时删除长期不用的系统帐号和测试帐号。**
- **个人办公帐号的口令应满足以下安全强度要求：**

  a) 8 个字符以上；

  b) 使用以下字符的组合：a-z、A-Z、0-9，以及!@#$%^&*()-+。

  c) 口令每三个月至少修改一次。
- **办公电脑应设置屏幕密码保护的用户界面，屏幕保护时间不应超过 10 分钟。**

信息安全意识



几种常见的钓鱼手段

电子邮件

假冒网站

诈骗

看个例子

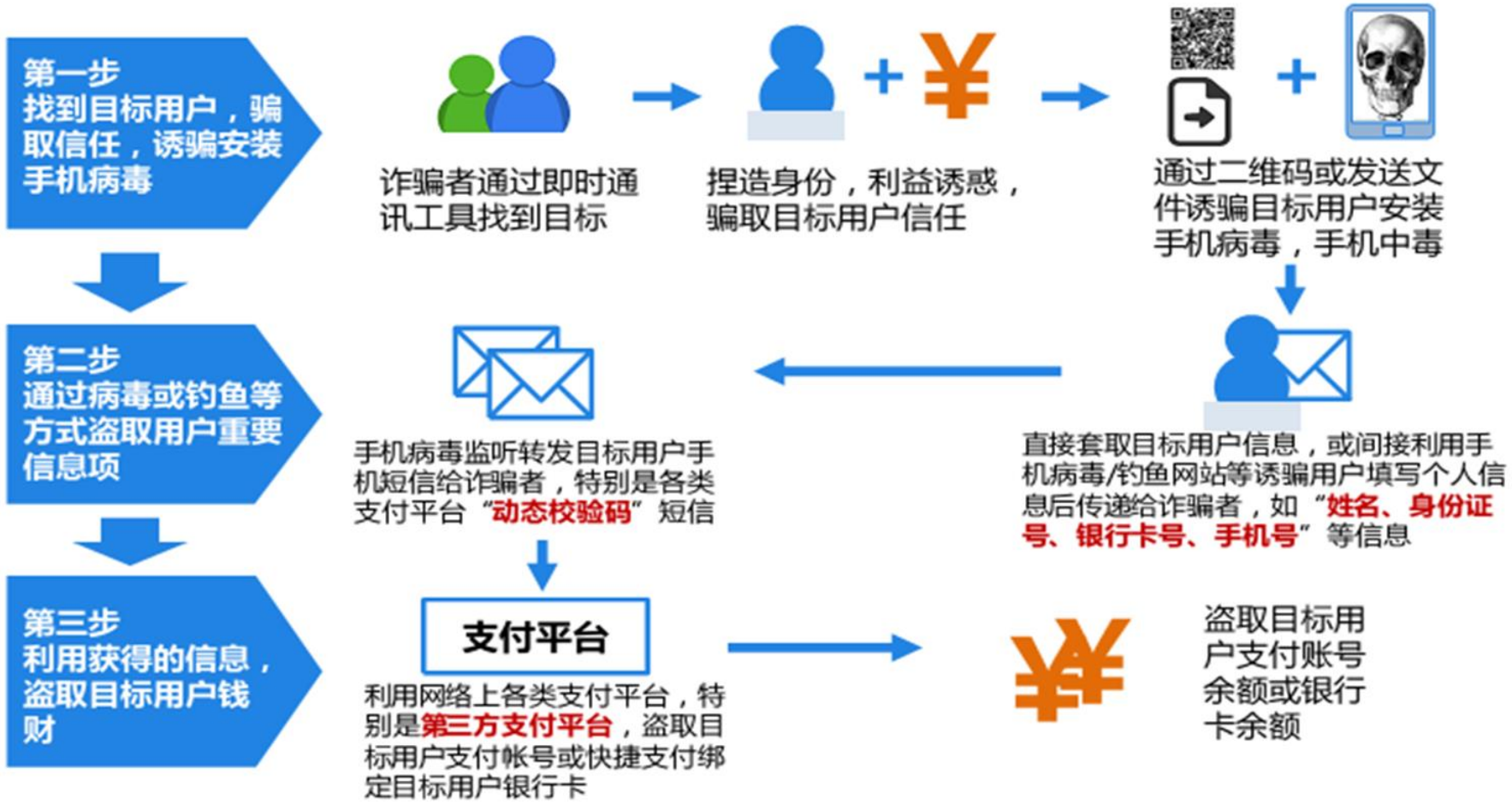
1- ATM 一切如常吧?

看个例子

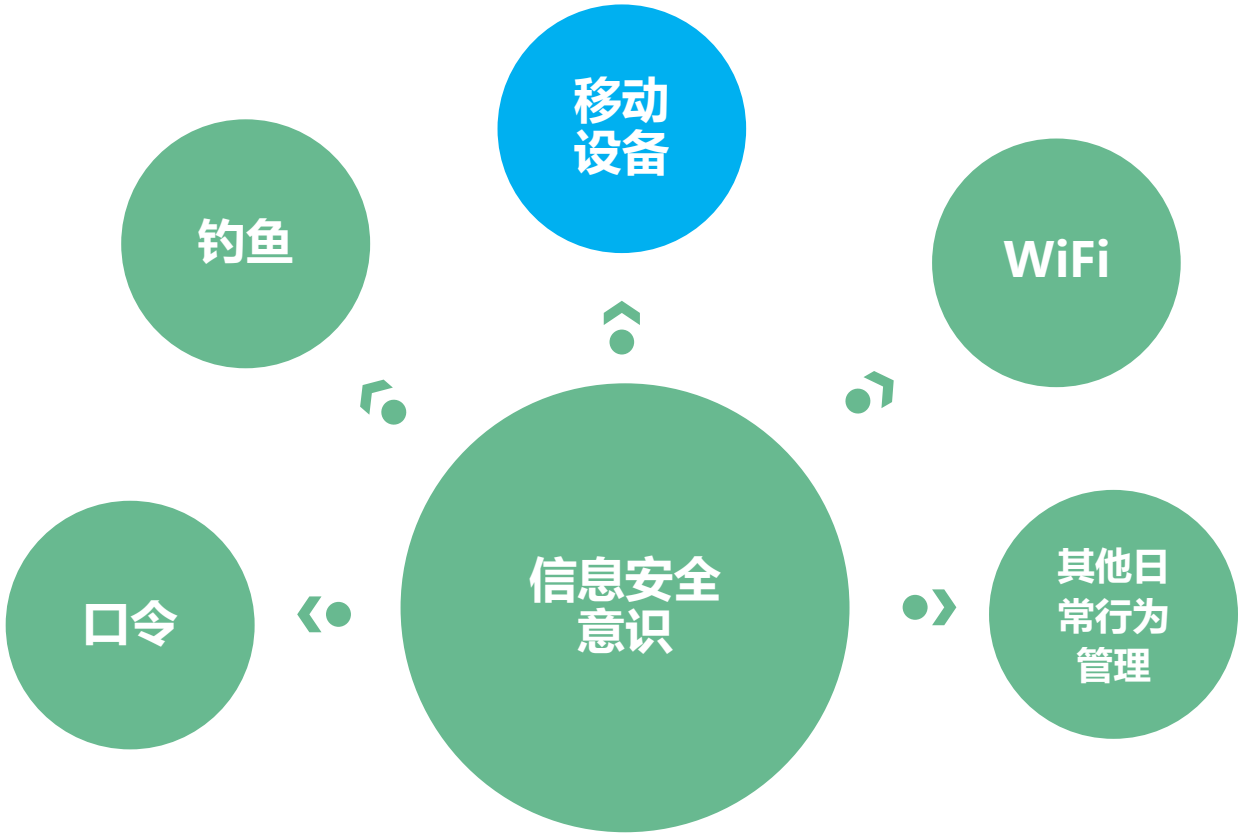
2- 这儿多出一个卡的插口?

假的插口固定在原来真插口的位置。假插口内部有另外一个卡的信息读写装置，可以复制卡上全部信息。

利用病毒木马窃取数据


第一步
找到目标用户，骗取信任，诱骗安装手机病毒
诈骗者通过即时通讯工具找到目标
捏造身份，利益诱惑，骗取目标用户信任
通过二维码或发送文件诱骗目标用户安装手机病毒，手机中毒
第二步
通过病毒或钓鱼等方式盗取用户重要信息项
直接套取目标用户信息，或间接利用手机病毒/钓鱼网站等诱骗用户填写个人信息后传递给诈骗者，如“姓名、身份证号、银行卡号、手机号”等信息
手机病毒监听转发目标用户手机短信给诈骗者，特别是各类支付平台“动态校验码”短信
第三步
利用获得的信息，盗取目标用户钱财
支付平台
利用网络上各类支付平台，特别是第三方支付平台，盗取目标用户支付帐号或快捷支付绑定目标用户银行卡
盗取目标用户支付账号余额或银行卡余额

信息安全意识



震网病毒

震网病毒是一种首次发现于2010年的恶性蠕虫电脑病毒，攻击的目标是工业上使用的可编程逻辑控制器（PLC）。震网病毒感染了全球超过20万台电脑，摧毁了伊朗浓缩铀工厂五分之一的离心机。震网病毒的感染途经是通过U盘传播，然后修改PLC控制软件代码，使PLC向用于分离浓缩铀的离心机发出错误的命令。

震网病毒只会感染Windows操作系统，然后在电脑上搜索一种西门子公司的PLC控制软件。如果没有找到这种PLC控制软件，震网病毒就会潜伏下来。如果震网病毒在电脑上发现了PLC控制软件，就会进一步感染PLC软件。随后，震网病毒会周期性的修改PLC工作频率，造成PLC控制的离心机的旋转速度突然升高和降低，导致高速旋转的离心机发生异常震动和应力畸变，最终破坏离心机。在2009年11月到2010年1月之间，震网病毒就摧毁了伊朗1000多台离心机。

BadUSB

BadUSB主要依靠USB拇指驱动器的构建方式，USB通常有一个大的可重写的内存芯片用于实际的数据存储，以及一个独立的控制器芯片。这个控制芯片实际上是一个低功耗计算机，并且与你的笔记本电脑或台式机一样，它通过从内存芯片加载基本的引导程序来启动。类似于笔记本电脑的硬盘驱动器包含一个隐藏的主引导记录(Master Boot Record)，内存芯片中内存单元的第一段包含让USB记录的编程。允许攻击者在不被检测到的情况下悄悄在USB设备中植入恶意软件。

BadUSB 有非常强大的攻击性：1. 它可以模仿键盘，得到用户的登陆权限。2. 它能够欺骗你的网络系统，并且改变你的 DNS 设定。3. 一个受感染的 U 盘或者其他的移动硬盘，能够监测到计算机的启动，并且释放一个小病毒，感染计算机的启动系统 （BIOS）。

BadUSB

Reddit 的一个帖子有点火，名字叫 “The Boss has Malware,again...”（老板的电脑又中病毒了）。点进去没有发现 “应该” 发现的东西，只看到了被感染和发现感染源的过程，不过也很有趣。

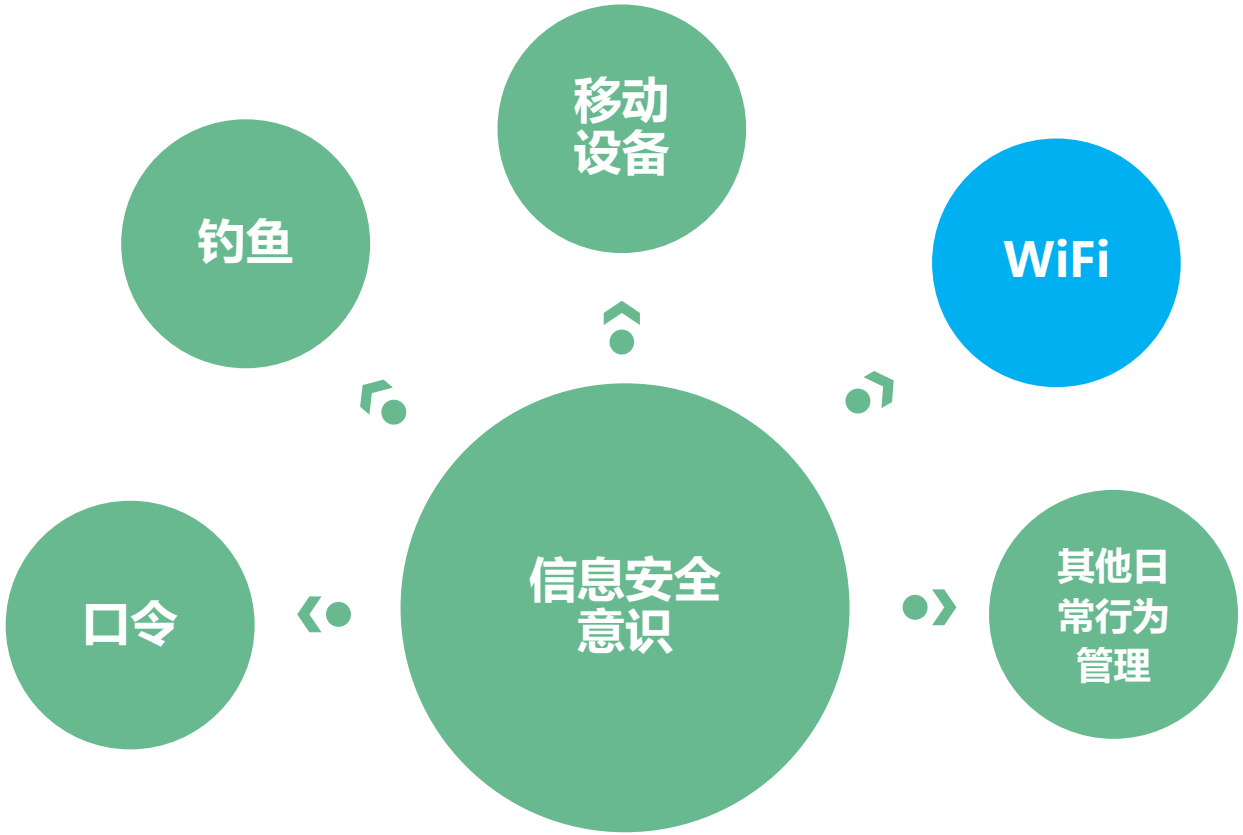
帖子讲述了发现感染源的过程，一个高管发现电脑感染了恶意软件，但无法确定来源。IT人员尝试了很多方法，但也一无所获。

后来 IT 人员发现，高管最近在生活上有一个小改变，用电子烟替代了实体烟。于是他们检查了高管的电子烟，发现里面含有恶意软件的源代码，当它连接到电脑的 USB 端口，就会植入电脑并感染系统。

通过 USB 感染电脑并不是新奇的事情。USB 的广泛传播得以于接口的多功能性，这让它能够满足很多不同的事情，例如数据传输、充电等等。在移动设备越发丰富的今天，很多人每天都要使用 USB 接口，其中就很可能把它接入到电脑中。

这当然会受到黑客的惦记。

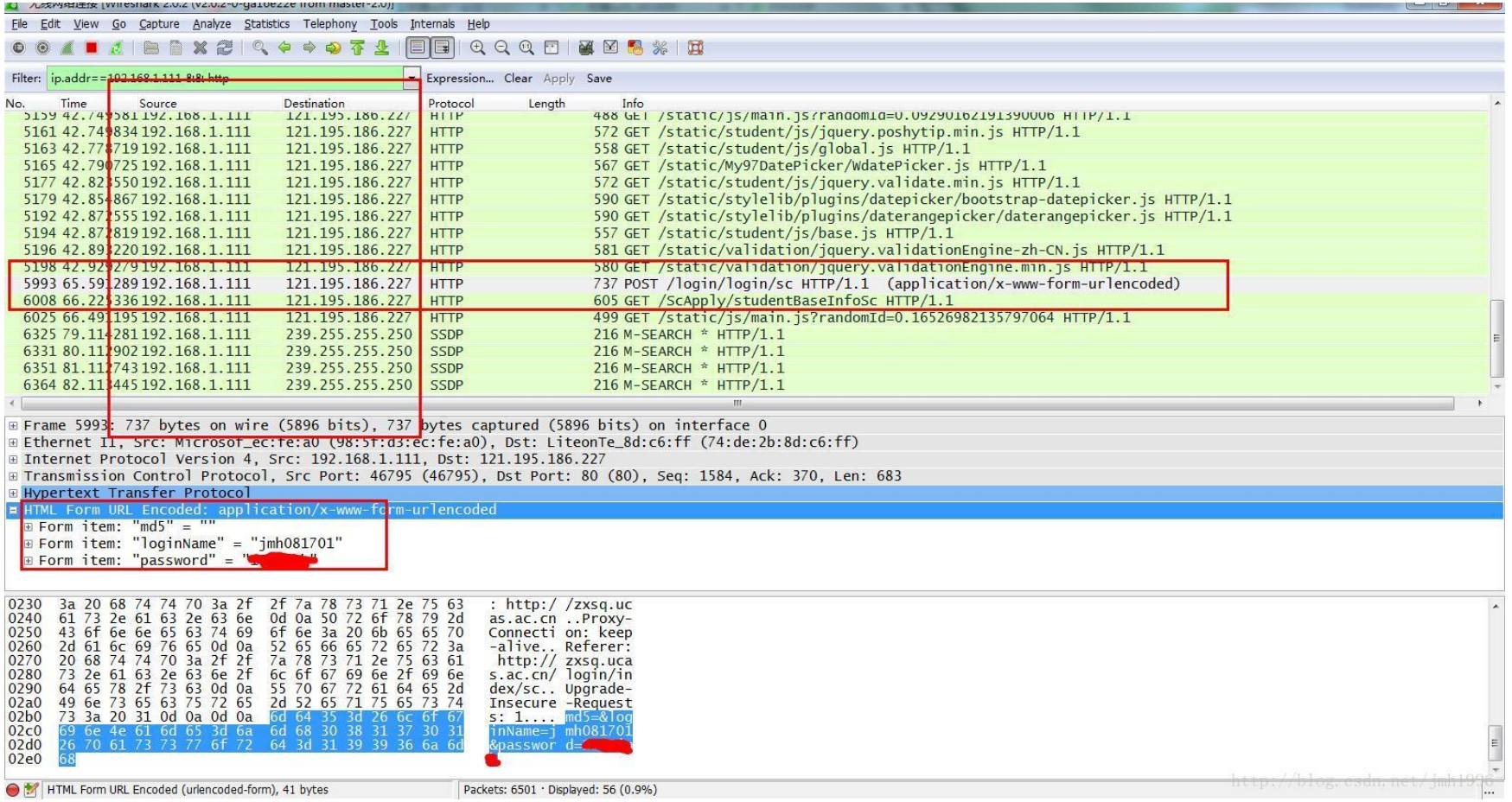
信息安全意识



钓鱼WiFi

一般就是在公开场合无需提供密码的AP热点，这个AP一般与正常的AP没有区别，连接上以后也能看似正常的进行网络链接。然而攻击者却可以轻松的得到用户的网络报文，更严重的是在钓鱼Wi-Fi的基础上设置钓鱼网站。普通用户一般缺乏安全意识，加上又有“蹭网”的心理，于是钓鱼Wi-Fi才有了其发挥作用的社工基础。

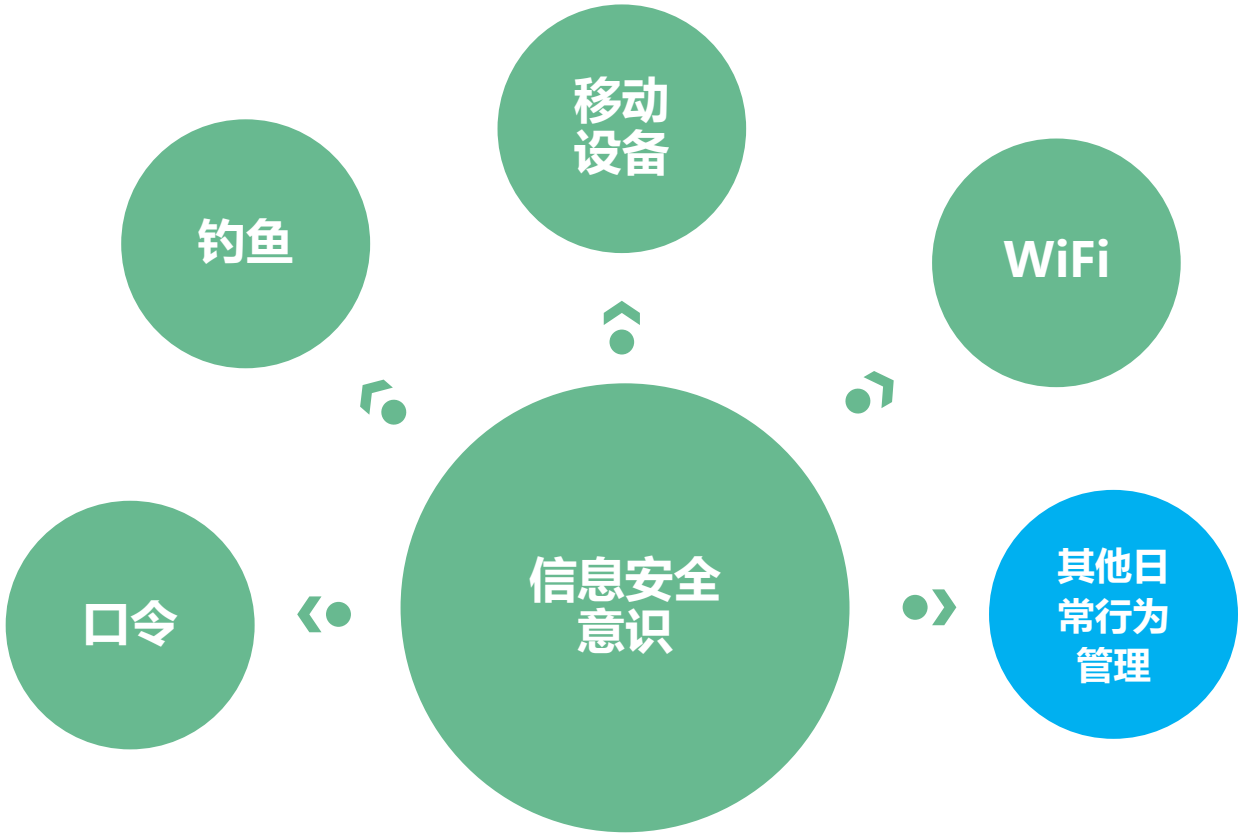
钓鱼WiFi


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.addr==192.168.1.111 && http
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
5161 42.749834 192.168.1.111 121.195.186.227 HTTP 572 GET /static/student/js/jquery.poshytip.min.js HTTP/1.1
5163 42.778719 192.168.1.111 121.195.186.227 HTTP 558 GET /static/student/js/global.js HTTP/1.1
5165 42.790725 192.168.1.111 121.195.186.227 HTTP 567 GET /static/My97DatePicker/WdatePicker.js HTTP/1.1
5177 42.823550 192.168.1.111 121.195.186.227 HTTP 572 GET /static/student/js/jquery.validate.min.js HTTP/1.1
5179 42.854867 192.168.1.111 121.195.186.227 HTTP 590 GET /static/stylelib/plugins/datepicker/bootstrap-datepicker.js HTTP/1.1
5192 42.872555 192.168.1.111 121.195.186.227 HTTP 590 GET /static/stylelib/plugins/daterangepicker/daterangepicker.js HTTP/1.1
5194 42.872819 192.168.1.111 121.195.186.227 HTTP 557 GET /static/student/js/base.js HTTP/1.1
5196 42.893220 192.168.1.111 121.195.186.227 HTTP 581 GET /static/validation/jquery.validationEngine-zh-CN.js HTTP/1.1
5198 42.929279 192.168.1.111 121.195.186.227 HTTP 580 GET /static/validation/jquery.validationEngine.min.js HTTP/1.1
5993 65.591289 192.168.1.111 121.195.186.227 HTTP 737 POST /login/login/sc HTTP/1.1 (application/x-www-form-urlencoded)
6008 66.225336 192.168.1.111 121.195.186.227 HTTP 605 GET /ScApply/studentBaseInfoSc HTTP/1.1
6025 66.491195 192.168.1.111 121.195.186.227 HTTP 499 GET /static/js/main.js?randomId=0.16526982135797064 HTTP/1.1
6325 79.114281 192.168.1.111 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
6331 80.112902 192.168.1.111 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
6351 81.112743 192.168.1.111 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
6364 82.113445 192.168.1.111 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 5993: 737 bytes on wire (5896 bits), 737 bytes captured (5896 bits) on interface 0
Ethernet II, Src: Microsof_ec:fe:a0 (98:5f:d3:ec:fe:a0), Dst: LiteonTe_8d:c6:ff (74:de:2b:8d:c6:ff)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 121.195.186.227
Transmission Control Protocol, Src Port: 46795 (46795), Dst Port: 80 (80), Seq: 1584, Ack: 370, Len: 683
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "md5" = ""
Form item: "loginName" = "jmh081701"
Form item: "password" = "[redacted]"
0230 3a 20 68 74 74 70 3a 2f 2f 7a 78 73 71 2e 75 63 : http:/ /zxsq.uc
0240 61 73 2e 61 63 2e 63 6e 0d 0a 50 72 6f 78 79 2d as.ac.cn ..Proxy-
0250 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 Connecti on: keep
0260 2d 61 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 3a -alive.. Referer:
0270 20 68 74 74 70 3a 2f 2f 7a 78 73 71 2e 75 63 61 http:// zxsq.uca
0280 73 2e 61 63 2e 63 6e 2f 6c 6f 67 69 6e 2f 69 6e s.ac.cn/ login/in
0290 64 65 78 2f 73 63 0d 0a 55 70 67 72 61 64 65 2d dex/sc.. Upgrade-
02a0 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 Insecure -Request
02b0 73 3a 20 31 0d 0a 0d 0a 6d 64 35 3d 26 6c 6f 67 s: 1.... md5=&log
02c0 69 6e 4e 61 6d 65 3d 6a 6d 68 30 38 31 37 30 31 inName=j mh081701
02d0 26 70 61 73 73 77 6f 72 64 3d 31 39 39 36 6a 6d &passwor d=[redacted]
02e0 68
HTML Form URL Encoded (urlencoded-form), 41 bytes
Packets: 6501 · Displayed: 56 (0.9%)

钓鱼WiFi

可以发现，对于http这种协议的网站，POST报文里面直接就可以看到用户的关键信息，比如这里的用户名密码。但是采用https协议的网站则是不然简单的分析出来了，但是钓鱼wifi的威力还是很强的。比如可以制作一个QQ空间的登录钓鱼网站，并使用iptables将所有访问QQ空间主机的http请求重定向到预先写的钓鱼网站，以此即可拿到QQ账户与密码。

信息安全意识



个人办公区域

1. 员工办公区域内用于存放敏感性资料的抽屉和柜子均应配锁。
2. 办公桌面不应堆放敏感性资料。
3. 员工离开个人办公区域时，应检查并确保存放有敏感性资料的抽屉和柜子均已上锁、桌面无任何敏感性资料；并锁定电脑桌面。
4.员工禁止在公开领域发布公司相关的工作内容。

安全防范

1.个人办公电脑必须启用安全自动更新或定期检查，及时安装安全补丁。
2.个人办公电脑必须安装并启用防病毒/木马软件，开启实时（文件系统、电子邮件和移动 存储等）监控功能，保证病毒库每周至少更新一次。
3.个人办公电脑不应开放任何网络共享。
4.定期备份系统或重要数据

4.4

总结

总结

- 不要轻易相信陌生人给你发送的文件、软件等。
- 将自己使用的口令修改为强口令，且定期修改。
- 不轻易将自己的账号借于他人使用。
- 办公终端及时杀毒，并定期检查。
- 打开网页以及邮件，注意观察地址栏以及发件人。
- 在办公区域，不私接个人热点。
- 在公共区域，免费WIFI请慎用。
- 使用U盘等连接办公电脑设备需确保安全。
- 离开办公位置收好敏感文件，电脑锁屏。

谢谢观看

NSFOCUS