网络安全宣传周

瑞达基金管理有限公司

2022年8月

《中华人民共和国网络安全法》

2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过。2017年6月1日正式实施，构成我国网络空间安全管理的基本法律。

网民或个人，这些你不能做

不得危害网络安全，不得利用网络从事危害国家、传播暴力、编造谎言等。

不得窃取或者以其他非法方式获取个人信息，不得非法出售或非法向他人提供个人信息。

不得设立用于实施诈骗等违法犯罪活动的网站、通讯群组，不得利用网络发布违法犯罪活动的信息。

不得从事非法侵入他人网络、窃取网络数据等危害网络安全的活动。

不得设置恶意程序，不得含有法律、行政法规禁止发布或传输的信息。

网民或个人，这些你有权做

- 对危害网络安全的行为向网信、电信、公安等部门举报。
- 依法享有个人信息删除权与更正权。

办公信息安全

办公网络安全，方寸不容有失。

- 据统计，在所有的信息安全事故中，只有20%-30%是由于黑客入侵或其他外部因素造成的，而有70%-80%是由于内部员工办公的疏忽或故意泄漏造成的。而在企业数据泄露事故中，有78%是由于内部员工办公不规范。

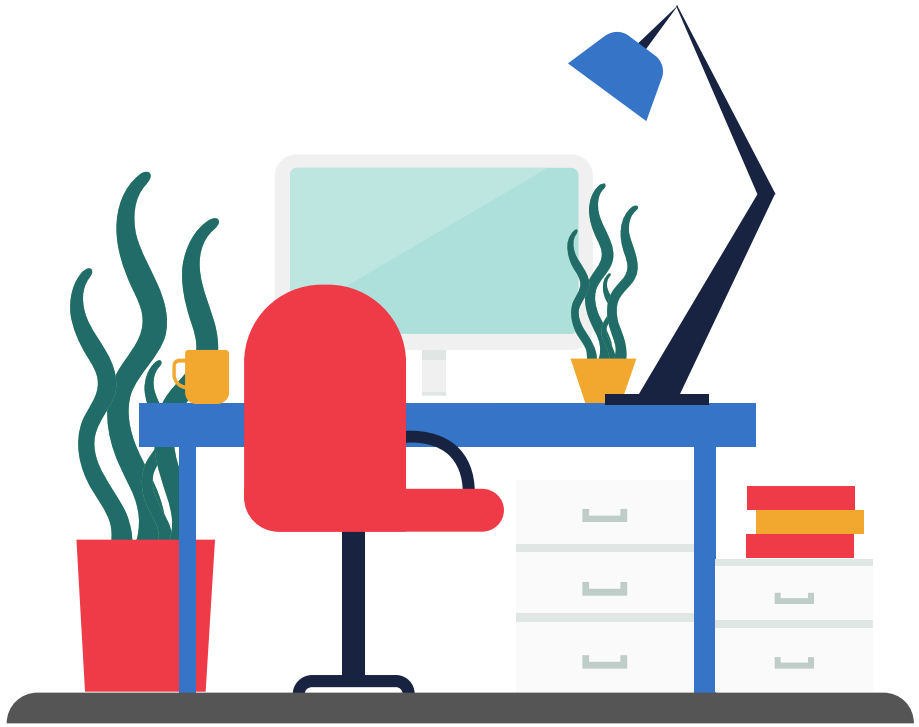
办公信息安全

说到办公网络安全的隐患，可谓不胜枚举。

- 电脑密码写在便签上贴在电脑上，被他人随意登陆电脑，数据泄露。
- 离开电脑没有锁屏，导致文件丢失、被窃取。
- 扫描、打印的文件未及时取走，被他人看到敏感信息。
- 办公室未锁门、门禁不严密，导致财产丢失、信息失窃。

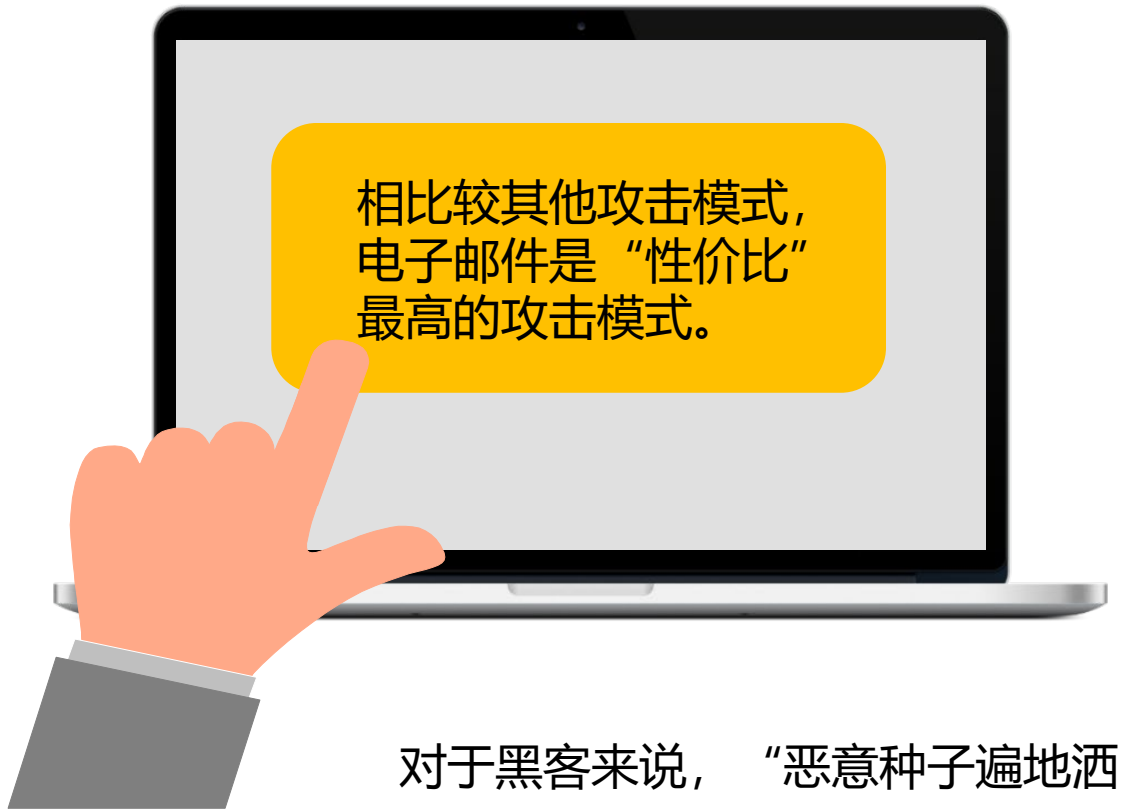
办公信息安全

- 不要把密码写在纸上或贴在键盘下面等可能被其他人获取的地方。
- 为屏保程序设置密码，离开机器时要锁屏（快捷键Win+L）。
- 在传真敏感信息时，必须事先通知收件人。
- 复印打印敏感信息时，待文档复印/打印后必须立即取走。
- 在离开办公桌时必须收拾妥当及锁好，避免信息泄露。
- 会议室及培训教室等公共区域使用完毕，使用者应及时将白板擦拭干净，关闭投影，并取走会议资料，防止敏感信息外泄。
- 门禁卡只能由本人使用，不得转借他人。
- 进门时要防止他人尾随。



邮件安全

黑客为什么喜欢攻击企业邮箱



攻击电子邮件对黑客“技能”要求低，也不需要耗费大量精力、资源和时间。

电子邮件有很强的指向性，容易被用于发动精准攻击。

电子邮件服务器端口往往是企业对外公开暴露的唯一网络端口。

企业邮箱发送垃圾邮件一般无数量限制。

对于黑客来说，“恶意种子遍地洒，总有一颗要发芽”的方式，无疑相对轻松许多。

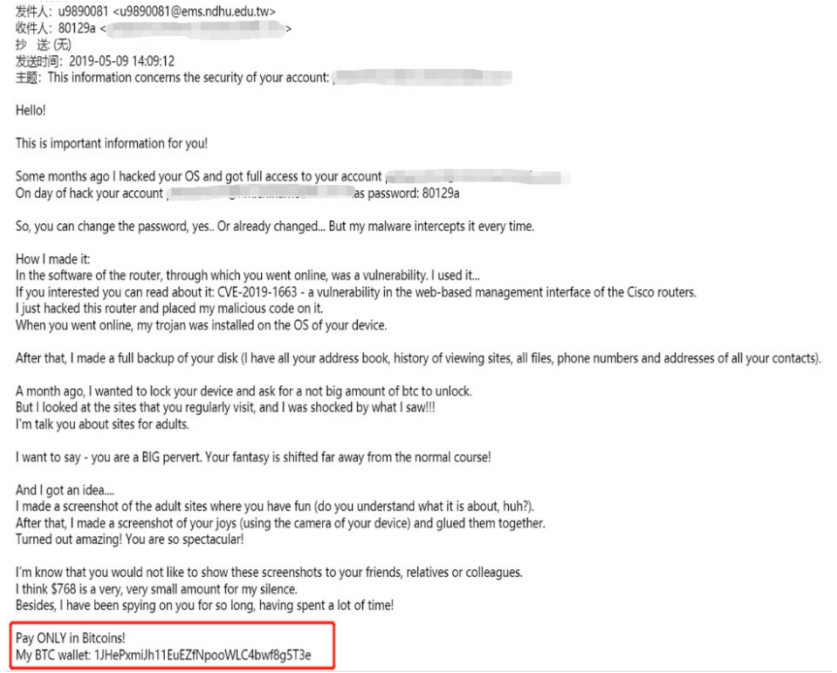
邮件安全

钓鱼邮件

天上不会掉馅饼

在邮件中加入恶意链接、附件，诱使收件人填写一些个人信息或账号密码等信息，回传给攻击者，导致信息泄露、系统账号密码泄露或邮箱被攻击者掌握利用。

以勒索之名行钓鱼之实



发件人: u9890081 <u9890081@ems.ndhu.edu.tw>
收件人: 80129a <[redacted]>
抄 送: (无)
发送时间: 2019-05-09 14:09:12
主题: This information concerns the security of your account: [redacted]

Hello!

This is important information for you!

Some months ago I hacked your OS and got full access to your account [redacted]
On day of hack your account [redacted] as password: 80129a

So, you can change the password, yes.. Or already changed... But my malware intercepts it every time.

How I made it:
In the software of the router, through which you went online, was a vulnerability. I used it...
If you interested you can read about it: CVE-2019-1663 - a vulnerability in the web-based management interface of the Cisco routers.
I just hacked this router and placed my malicious code on it.
When you went online, my trojan was installed on the OS of your device.

After that, I made a full backup of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.
But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!
I'm talk you about sites for adults.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....
I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).
After that, I made a screenshot of your joys (using the camera of your device) and glued them together.
Turned out amazing! You are so spectacular!

I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.
I think $768 is a very, very small amount for my silence.
Besides, I have been spying on you for so long, having spent a lot of time!

Pay ONLY in Bitcoins!
My BTC wallet: 1JHePxmiJh11EuEZfNpooWLC4bwf8g5T3e

邮件安全

应急处理

及时联系技术部门帮忙。

01

立即修改登录密码。

02

发现电脑异常应及时做全盘扫描杀毒。

03

发现病毒立即切断受感染设备的网络连接（拔掉网线或者禁用网络）。

04

邮件安全

- 仔细识别发件人，不对“熟人”松警惕；
- 杀毒软件要安装，扫描邮件和附件；
- 登录密码要保密，邮箱账号绑手机；
- 公私邮箱要分离，处理不同的事务；
- 垃圾邮件黑名单，使用邮件过滤器；
- 重要邮件要加密，定期备份更放心；
- 邮件地址要保护，垃圾邮件隐患多；
- 涉及款项和权限，务必线下确认清；
- 各种附件谨慎点，陌生链接勿点击；
- 钓鱼邮件时常有，识别套路无烦恼。

密码安全

你的密码之所以被盗，简单来说是：**密码太简单 + 多个账户使用同样的密码。**

18%的用户都遭遇过账户被攻击，但是很少有用户使用高效和明智的密码保护自身。

30%的用户会为不同的在线账户创建不同的密码。

20%的用户会为所有的在线账户使用同一个密码。

47%的用户会在密码中使用大小写字母组合。

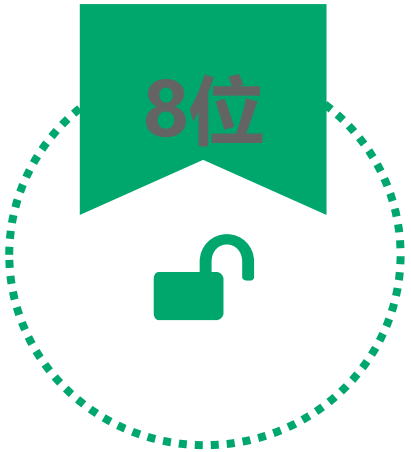
61%的用户喜欢使用人名、地名、字典词汇和纯数字来设置他们的密码。

22%的用户承认自己会在记事本上写下自己的密码，以便记住。

密码安全

养成良好的密码使用习惯对密码保护是至关重要的。

至少每90天更换一次密码。



系统要求密码长度设置不低于8位。

至少包含以下四类字符中的三类字符：

- 英文大写字母(A到Z)
- 英文小写字母(a到z)
- 10个基本数字(0到9)
- 非字母字符(例如!、$、#、%等)

更新时不得使用最近5次以内重复使用的口令。

计算机病毒防范

计算机病毒（Computer Virus）是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。

病毒

病毒（Virus）具有自我繁殖能力，寄生于其他可执行程序中，通过磁盘拷贝，文件共享和电子邮件等多种途径进行扩散和感染。

木马

木马（Trojan）是一种传统的后门程序，它可以冒充正常程序，截取敏感信息，或进行其他非法的操作。

蠕虫

蠕虫（Worm）不需借助其他可执行程序就能独立存在并且运行，通常利用网络中某些主机存在的漏洞来感染和扩散。

勒索软件

勒索软件（Ransomware）通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。用户数据资产包括文档、邮件、数据库、源代码、图片、压缩文件等多种文件，赎金形式包括真实货币、比特币或其它虚拟货币。

计算机病毒防范

计算机病毒造成的影响

03 控制用户设备，“占为”己用

02 破坏设备文件，无法运行

04 窃取用户数据，挪作他用

01 消耗设备资源，运行变慢

05 锁定用户数据，勒索钱财

计算机病毒防范

计算机病毒常见传播途径

01 通过电子邮件附件传播

02 通过网页木马传播

03 通过恶意软件捆绑传播

04 以社交网络中的.jpg图片为载体传播

05 可移动存储介质传播

06 文件共享网站传播

计算机病毒防范

计算机病毒防范措施

01 经常更新操作系统补丁和应用软件的版本。

02 安装防火墙和杀毒软件。

03 经常备份重要的数据。

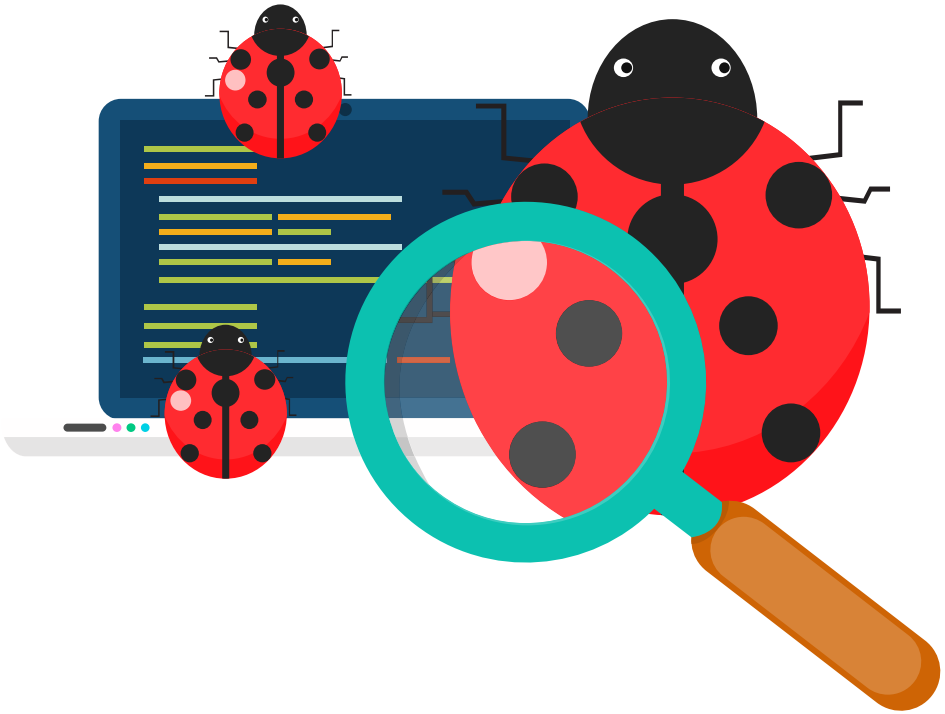
04 重要数据要加密。

05 使用复杂的密码。密码越复杂，被破解的几率越小。

计算机病毒防范

计算机中病毒后的处置措施

- 发现计算机感染病毒迹象后，首先断开网络连接。
- 打开杀毒软件对全盘进行扫描查杀。
- 清除完病毒后，导出重要的文件进行备份。
- 重新安装操作系统，彻底清理系统分区。
- 如果上述步骤执行过后，计算机系统仍然存在顽固病毒感染的情况，就得让专业人员来进行针对性清理查杀。



移动存储介质安全

移动存储介质包括：

实验数据：

- 17%的用户会在大街上捡到U盘后立即插入自己的电脑当中。在2016年4月进行的另一项研究中，一名安全研究人员故意在伊朗利诺伊大学香槟校区大学街上遗漏300个U盘，研究人员发现，98个U盘已经被捡走，其中有48%的U盘已经插入电脑，并且被打开点击其中文件。

移动存储介质安全

网盘安全防范措施

01

重要数据不上网

02

做好权限控制

03

做好数据加密

04

网盘密码要复杂

移动存储介质安全

- 取消U盘插入后的自动播放功能。
- 对U盘进行写入保护。
- 在安装有防病毒软件的机器上使用移动介质，并注意查杀病毒。
- 严禁在涉密领域和非涉密领域混用可移动存储介质。
- 涉密移动存储介质应遵循“集中管理、严密防范、确保安全”的原则。
- 及时查杀病毒、木马等恶意代码，防止其蔓延传播。
- 严禁将已报废的涉密移动存储介质转为非涉密载体继续使用。
- 对报废的涉密移动存储介质实行彻底的损毁。
- 定期数据备份。

无线网络安全

案例

- 江苏南京市民张先生使用公共场所的WiFi后，电脑被黑客入侵，在U盾、银行卡都在的情况下，他网银上的6万多被人在两天内盗刷69次，只剩下500元。而且他的手机还被黑客做了手脚，接收到消费提醒短信的功能也被屏蔽，所以发生的69次交易他根本没有收到任何短信提示，钱不知不觉就全被转走了。

  警方提示：曾错连钓鱼WiFi导致密码被窃取。

无线网络安全

公共场所藏风险，免费WiFi莫乱用

不要连接任何无密码的WiFi。

连接免费WiFi密码时，除了要你输入手机号码的信息时，例如身份证号码，QQ号码，这个时候最好就不要再连接WiFi，及时切断比较好。

切勿连接公共WiFi的情况下做网购，网银，支付操作。

在公共区域的时候，WiFi可以处于关闭的状态，等需要使用的时候再打开。

能不在公共场合使用WiFi时，尽量还是使用自己的流量比较好，防止会被不法分子利用。

无线网络安全

无线网络要保护，无线路由器是关键

更改路由器或者无线网络接入点的默认管理员密码。

确保用于连接到你的无线网络的密码是强密码并且不同于你的管理员密码。

更改默认的无线网络名称（也称为SSID），即你的设备扫描无线网络时搜索到的名字。

添加一个访客网络，确保开启WPA2安全机制并为其设置一个特殊密码。

确保只有你信任的人才能连接并使用你的无线网络，而且这些连接都是加密的。

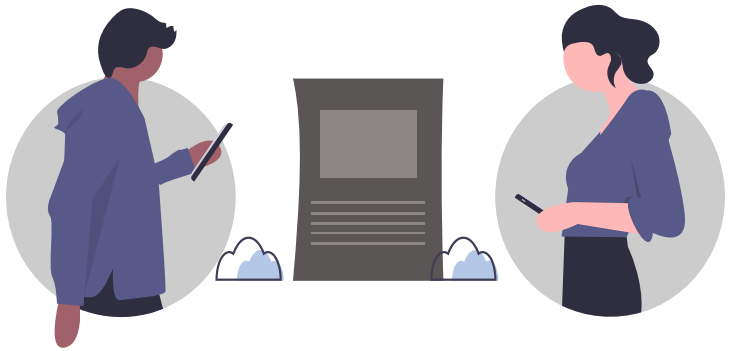
启用WiFi安全防护设定，禁止新设备可以不需要密码就能连接网络和更改设置的机制。

为了确保您的无线网络安全，更改网络设备默认设置并开启密码保护。

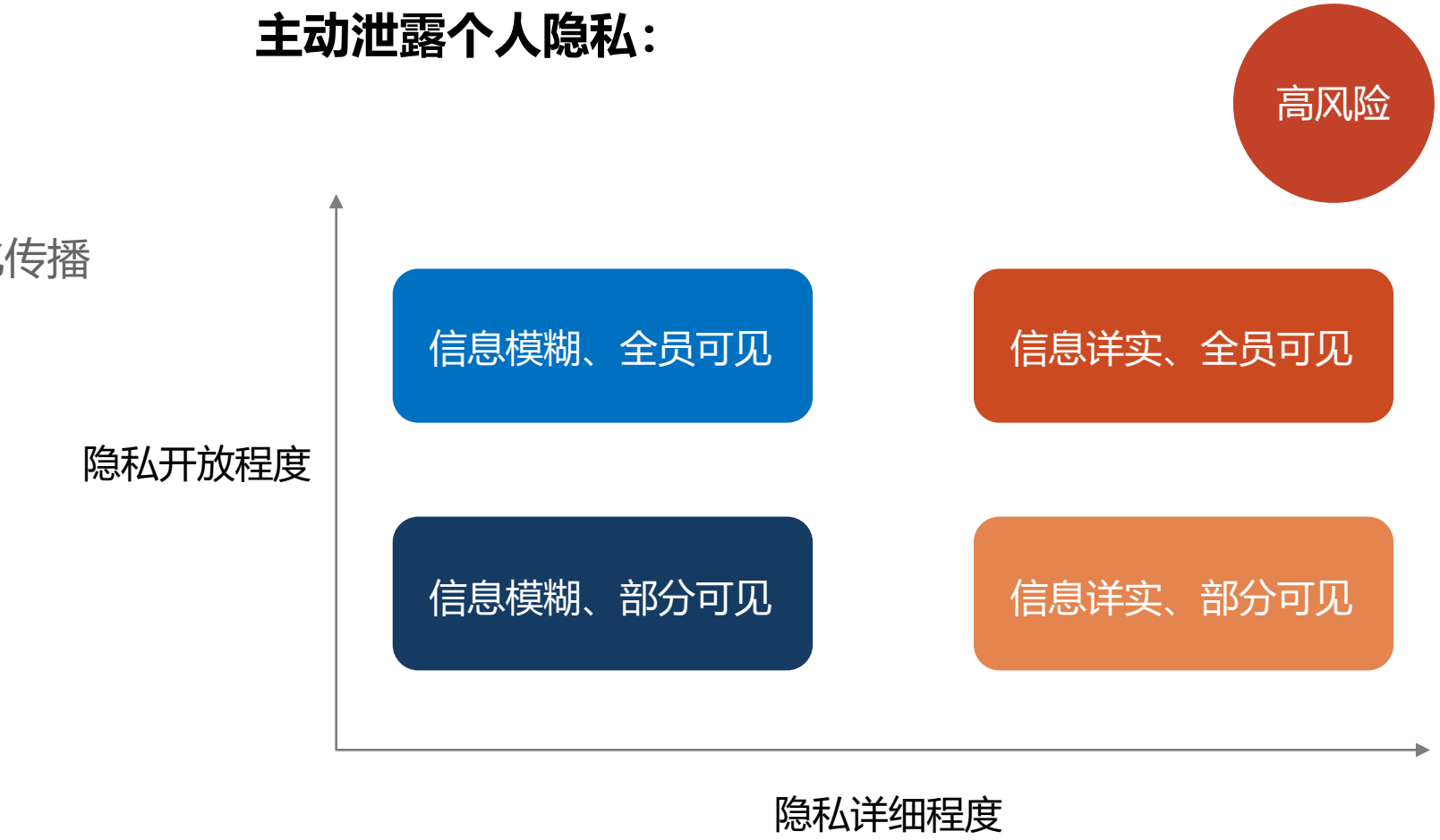
社交网络安全

社交网络威胁：

- 个人隐私泄露风险
- 网络谣言以及网络不良文化传播
- 影响社会稳定和国家安全



主动泄露个人隐私：



社交网络安全

恶意软件窃取个人信息

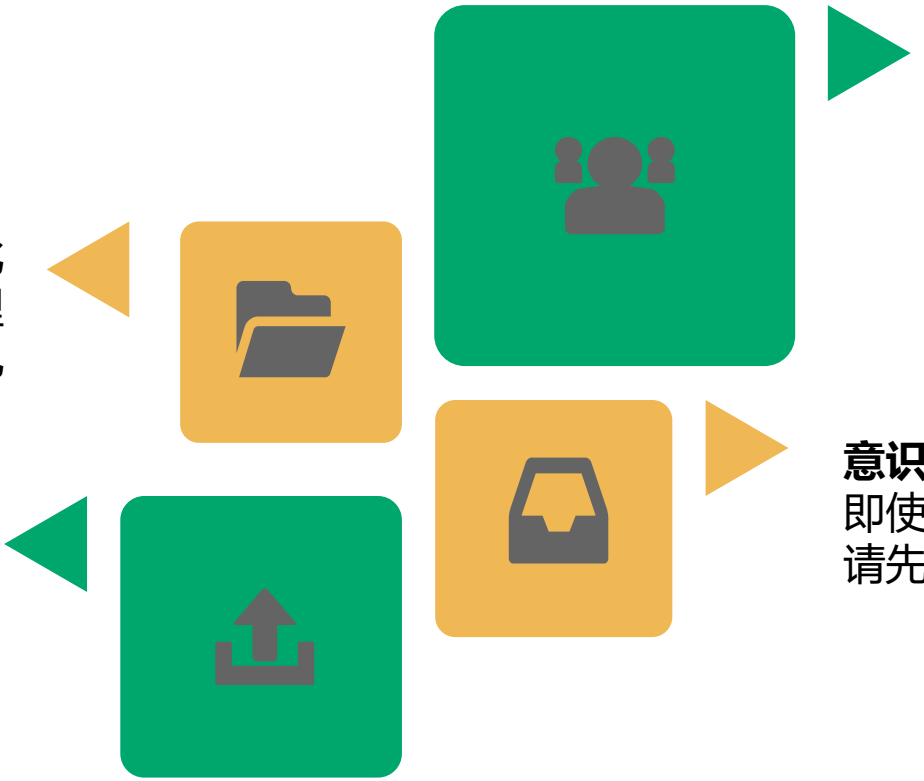
- **恶意插件**：用户无意中从非法网站下载安装了恶意的浏览器插件，从而社交网络的登录用户名和密码被监听，个人信息也会被抓取。
- **恶意链接**：通过社交网站的IM即时通讯工具，散播恶意软件下载链接。
- **第三方程序**：社交网站上的第三方应用程序可能会包含恶意软件。
- **恶意欺骗**：通过邮件或者社交网络发送欺骗信息，谎称某个软件有病毒，希望收到的人进一步大量转发。

恶意软件窃取个人信息

软件名称	所涉问题
今日头条	强行捆绑推广其他软件
经典连连看	
QQ同步管理助手	
YY影院	未经用户同意，使用用户个人信息
我的世界（我的海盗船世界）	未经用户同意，向外发短信
小猪佩奇的故事	APP内潜藏木马病毒，存恶意推广风险

社交网络安全

社交网站防护，个人要坚持以下原则：



信息最少化
当你在注册账号时，请仔细考虑你所提供的每一项信息是否都绝对必要，是否与该网站相关。

隐私最小化
隐私设置要合理
最好仅由朋友见

意识常态化
即使是你朋友发来的链接，也请先确认这个链接的真实性。

软件官方化
从官方应用商城下载软件