



常见网络安全威胁与防范



不法分子通过各种手段，如虚假网站、中奖信息、网络兼职等，诱骗用户提供个人信息或转账汇款，从而达到骗取钱财的目的。还有的冒充公检法机关进行诈骗，声称您涉及某项重大案件，需要将资金转移到“安全账户”配合调查。

在网上注册账号、填写表单、使用公共WIFI等过程中，个人信息可能会被黑客窃取或非法收集，导致隐私泄露，甚至被用于非法活动。比如，一些不法分子获取个人信息后进行精准的电话推销或诈骗。

攻击者利用人性的弱点，如好奇心、同情心等，通过欺骗手段获取用户的信任，从而获取敏感信息。比如，伪装成熟人向您求助，借机询问密码等重要信息。

随着智能家居设备的普及，这些设备也可能成为被攻击的目标。黑客可能入侵智能摄像头，窃取家庭生活画面，或者控制智能门锁，威胁家庭安全。

01 网络诈骗

02 个人信息泄露

05 社交工程攻击

06 物联网安全威胁



03 恶意软件攻击

04 网络钓鱼

07 网络暴力

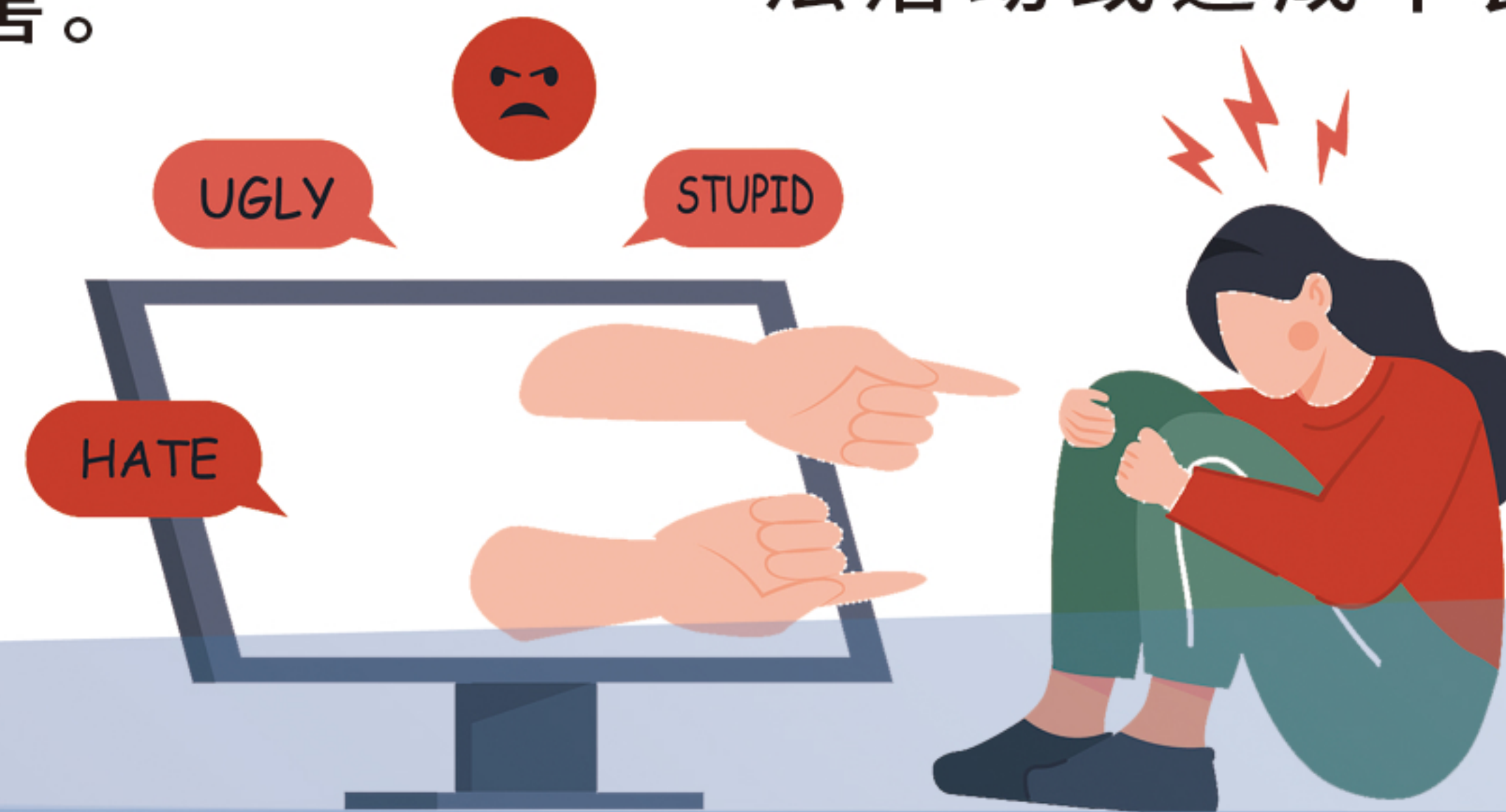
08 账号盗用

病毒、木马、蠕虫等恶意软件可能会潜伏在下载的软件、邮件附件或链接中，一旦运行，就会破坏计算机系统、窃取数据或控制设备。例如，勒索病毒会加密重要文件，然后要求支付赎金才能解锁。

攻击者通过发送看似来自合法机构的电子邮件或短信，引导用户点击链接并输入个人敏感信息，从而实施诈骗。此外，还有“伪基站”钓鱼，通过伪装成运营商基站，发送虚假短信，骗取用户信息。

在网络上，一些人可能会恶意攻击、诽谤他人，对受害者的身心健康造成极大的伤害。

黑客通过各种手段获取账号密码，盗用社交账号、游戏账号等，进行非法活动或造成不良影响。





一、账号密码

01

如果有初始密码，应尽快修改。

02

密码长度不少于8个字符。

03

不要使用单一的字符类型，例如只用小写字母，或只用数字。

04

用户名与密码不要使用相同字符。

05

常见的弱口令尽量避免设置为密码。

06

自己、家人、朋友、亲戚、宠物的名字避免设置为密码。

07

生日、结婚纪念日、电话号码等个人信息避免设置为密码。

100个网络安全知识 10个方面

08

工作中用到的专业术语、职业特征避免设置为密码。

09

密码中不应包含单词，或者在单词中插入其他字符。

10

所有系统尽可能使用不同的密码。

11

防止网页自动记住账号密码。

12

上网注册账户时，用户名密码不要与单位内部用户名密码相同或关联。

13

在通过密码管理软件保管好密码的同时，密码管理软件应设置高强度安全措施。

14

密码应定期更换。

10个方面 100个网络安全知识

二、病毒风险



10个方面 100个网络安全知识

三、上网安全

- 21 使用知名的安全浏览器（例如：EDGE、CHROME、FIREFOX、360安全浏览器、360急速浏览器）。
- 22 收藏经常访问的网站，不要輕易点击别人传给你的网址。
- 23 对超低价、超低折扣、中奖等诱惑要提高警惕。
- 24 避免访问色情、赌博、反动等非法网站。
- 25 重要文件通过网络、邮件等方式传输时进行加密处理。
- 26 利用社交网站的安全与隐私设置保护敏感信息。
- 27 避免将工作信息、文件上传至网上存储空间，如网盘、云共享文件夹等。
- 28 在社交网站谨慎发布个人信息。
- 29 根据自己对网站的需求进行注册，不要盲目填写信息。
- 30 上网的DNS应设置为运营商指定的或内部DNS服务的IP地址，避免使用不安全的DNS导致被劫持风险。



四、网上交易



31

所访问的网址与官方地址进行比对，确认准确性。

32

避免通过公用计算机使用网上交易系统。

33

不在网吧等多人共用的电脑上进行金融业务操作。

34

不通过搜索引擎上的网址或不明网站的链接进入交易。

35

在网络交易前，对交易网站和交易对方的资质全面了解。

36

可通过查询网站备案信息等方式核实网站资质真伪。

37

应注意查看交易网站是否为HTTP协议，保证数据传输中不被监听篡改。

100个网络安全知识 10个方面

38

在访问涉及资金交易类网站时，尽量使用官方网站提供的虚拟键盘输入登录和交易密码。

39

填写个人详细信息可获得优惠券，要谨慎填写。

40

注意保护个人隐私，使用个人的银行账号、密码和证件号码等敏感信息时要慎重。

41

使用手机支付服务前，按要求在手机上安装专门用于安全防范的插件。

42

无论以何种理由要求你把资金打入陌生人账户、安全账户的行为都是诈骗犯罪，切勿上当受骗。

43

当收到与个人信息和金钱相关（如中奖、集资等）的邮件时要提高警惕。



10个方面 100个网络安全知识

五、电子邮件

44

不打开、回复可疑邮件、垃圾邮件、不明来源邮件。

收发公司业务数据时，必须使用公司内部邮箱，公务处理和私人邮箱分开。

45

46

员工应对自己的邮箱账号和密码的安全负责，不得将邮箱账号借给他人。

若发现邮箱存在任何安全漏洞的情况，应及时通知公司邮件系统管理人员。

47

48

应警惕邮件的内容、网址链接、图片等。

机关工作人员工作邮件建议使用政府自建邮箱，严禁使用境外邮箱。

49

50

为电子邮箱设置高强度密码，并设置每次登录时必须进行账号密码验证。

开启防病毒软件实时监控，检测收发的电子邮件是否带有病毒。

51

52

检查邮件转发功能是否关闭。

不转发来历不明的电子邮件及附件。

53

54

收到涉及敏感信息邮件时，要对邮件内容和发件人反复确认，尽量进行线下沟通。

10个方面 100个网络安全知识

六、主机电脑

55

操作系统登录账户需要设置登录密码，且不为弱密码。

操作系统应及时更新最新安全补丁。

56

57

禁止开启无权限的文件共享服务，使用更安全的文件共享方式。

针对中间件、数据库、平台组件等程序进行安全补丁升级。

58

59

关闭办公电脑的远程访问。

定期备份重要数据。

60

61

关闭系统中不需要的服务。

计算机系统更换操作人员时，交接重要资料的同时，更改系统的密码。

62

63

及时清理垃圾邮箱。



员工离开座位时应设置电脑为退出状态或锁屏状态，建议设置自动锁屏。

64

10个方面 100个网络安全知识

七、办公环境

65

禁止随意放置或丢弃含有敏感信息的纸质文件，废弃文件需要用碎纸机粉碎。

66

废弃或待消磁介质转交他人时应经管理部门消磁处理。

67

离开座位时，应将贵重物品、含有机密信息的资料锁入柜中。



68

应将复印或打印机的资料及时取走。

69

废弃的光盘、U盘、电脑等要消磁或彻底破坏。

70

禁止在便签之上写有账号、密码等信息。

71

UKEY不使用时应及时拔出并妥善保管。

72

办公中重要内容电话应在安全安静的地方接听，避免信息泄露。

73

U盘、移动硬盘，随时存放在安全地方，勿随意借用、放置。



10个方面 100个网络安全知识

八、移动手机

74

手机设置自动锁屏功能，建议设置1-5分钟的，避免离开手机后被其他人恶意使用。

75

手机升级应通过自带的更新功能，避免通过网站下载更新。

76

尽可能通过手机自带的应用市场下载手机应用程序。

77

为手机安装杀毒软件。

78

经常为手机做数据同步备份。



79

手机访问WEB站点应提高警惕。

80

为手机设置访问密码是保护手机安全的第一道防线，防止手机丢失信息泄露。

81

蓝牙功能不用时，应处于关闭状态。

82

手机废弃前应对数据进行完全备份，恢复出场设置清除残余信息。

83

经常查看手机任务管理器，检查是否有恶意程序在后台运行，并定期使用手机安全系统软件扫描手机系统。

DOC

84

对程序执行权限加以限制，非必要程序禁止读取通讯录等敏感数据。

85

不要试图破解自己的手机，以保证应用程序的安全性。



10个方面 100个网络安全知识

九、无线网络

在办公环境中禁止私自通过办公网开发WIFI热点。

86



不访问任何非本单位的开放WIFI，发现单位附近的无密码、开放的WIFI应通知IT部门。

87

除测试、安全、移动端外，其他部门需求WIFI，需要报备IT部门，不许自行开热点。

88



无线网络设备及时更新到最新固件。

90

禁止使用WIFI共享类APP，避免导致无线网络账号密码泄露。

89

91

警惕公共场所免费的无线信号为不法分子设置的钓鱼陷阱。

92

设置高强度的无线密码，各单位的认证机制建议采取实名方式。



10个方面 100个网络安全知识

十、敏感信息

93

敏感及内网计算机不允许连接互联网或其它公共网络。



94

处理敏感信息的计算机、传真机、复印机等设备应当在单位内部进行维修，现场有专门人员监督。



95

严禁维修人员读取或复制泄密信息，确定需送外维修的，应当拆除涉密信息存储部件。



96

敏感信息设备改作非涉密信息设备使用或淘汰时，应当将涉密信息存储部件拆除。



97

敏感及内网计算机不得使用无线键盘、无线鼠标、无线网卡。



98

敏感文件不允许在非涉密计算机上进行处理。



99

内外网数据交换需使用专用的保密U盘或刻录光盘。



100

工作环境外避免透露工作内容。

