SANGFOR
深信服科技

让每个用户的数字化更简单、更安全

深信服官方微信

深信服移动官网

深圳市南山区学苑大道1001号南山智园A1栋
售前咨询：400-806-6868　售后服务：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn

SANGFOR
深信服科技

深信服智安全
SANGFOR SECURITY

网络安全100个小知识

网络安全风险无处不在，深信服为大家梳理了100个网络安全相关的小知识，希望能提升大家的安全意识，帮助大家建立更加安全的网络环境。

目录 CONTENTS

01

账户密码安全

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

08 工作中用到的专业术语、职业特征避免设置为密码

09 密码字典中不应包含单词，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 防止网页自动记住用户名与密码

12 上网注册帐号时，用户名密码不要与公司内部用户名密码相同或有关联

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

02

病毒风险防范

15 安装病毒防护程序并及时更新病毒特征库

16 下载电子邮件附件时注意文件名的后缀，陌生发件人附件不要打开

17 网络下载的文件需要验证文件数字签名有效性，并用杀毒软件手动扫描文件

18 使用移动存储介质时，进行查杀病毒后打开

19 安装不明来源的软件时，手动查杀病毒

20 浏览网页时，若发现电脑工作异常，建议断开网络并进行全盘杀毒

03

上网安全注意

21 使用知名的安全浏览器

22 收藏经常访问的网站，不要轻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 通过社交网站的安全与隐私设置功能，隐藏不必要的敏感信息展示

27 避免将工作信息、文件上传至互联网存储空间，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

04

网上交易安全

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HTTPS协议，保证数据传输中不被监听篡改

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 遇到填写个人详细信息可获得优惠券，更要谨慎填写

40 注意保护个人隐私，使用个人的银行账户、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，应按要求安装支付环境的安全防范程序

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

05

电子邮件安全

44 不打开、回复可疑邮件、垃圾邮件、不明来源邮件

45 收发公司业务的邮件时，应使用公司企业邮箱处理，私人邮件应使用个人邮箱处理

46 员工应对自己的邮箱用户名及密码安全负责，不得将其借与他人

47 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

48 应警惕邮件的内容、网址链接、图片等

49 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

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用户名密码验证

51 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

52 定期检查邮件自动转发功能是否关闭

53 不转发来历不明的电子邮件及附件

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

06

主机电脑安全

55 操作系统应及时更新最新安全补丁

56 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

57 针对中间件、数据库、平台组件等程序进行安全补丁升级

58 关闭办公电脑的远程访问

59 定期备份重要数据

60 关闭系统中不需要的服务

61 计算机系统更换操作人员时，交接重要资料的同时，更改该系统的密码

62 及时清理回收站

63 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

07

办公环境安全

64 禁止随意放置或丢弃含有敏感信息的纸质文件，废弃文件需用碎纸机粉碎

65 废弃或待消磁介质转交他人时应经管理部门消磁处理

66 离开座位时，应将贵重物品、含有敏感信息的资料锁入柜中

67 应将复印或打印的资料及时取走

68 废弃的光盘、U盘、电脑等要消磁或彻底破坏

69 禁止在便签纸上留存用户名、密码等信息

70 UKey不使用时应及时拔出并妥善保管

71 办公中重要内容电话找到安全安静的地方接听，避免信息泄露

72 U盘、移动硬盘，随时存放在安全地方，勿随意借用、放置

08

移动手机安全

73 手机设置自动锁屏功能，建议锁屏时间设置为1-5分钟，避免手机被其他人恶意使用

74 手机系统升级应通过自带的版本检查功能联网更新，避免通过第三方网站下载到如篡改后的系统更新包等，从而导致信息泄露

75 尽可能通过手机自带的应用市场下载手机应用程序

76 为手机安装杀毒软件

77 经常为手机做数据同步备份

78 手机中访问Web站点应提高警惕

79 为手机设置访问密码是保护手机安全的第一道防线，防止手机丢失导致信息泄露

80 蓝牙功能不用时，应处于关闭状态

81 手机废弃前应对数据进行完全备份，恢复出厂设置清除残余信息

82 经常查看手机正在运行的程序，检查是否有恶意程序在后台运行，并定期使用手机安全管理软件扫描手机系统

83 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

84 不要试图破解自己的手机，以保证应用程序的安全性

09

无线网络安全

85 在办公环境中禁止私自通过办公网开放Wi-Fi热点

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

87 部门需要单独增设Wi-Fi网络时，应到IT部门报备，禁止自行开热点

88 禁止使用Wi-Fi共享类APP，避免导致无线网络用户名及密码泄露

89 无线网络设备及时更新到最新固件

90 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

91 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

敏感信息安全

92 敏感及内网计算机不允许连接互联网或其它公共网络

93 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

94 严禁维修人员读取或复制敏感信息，确定需送外维修的，应当拆除敏感信息存储部件

95 敏感信息设备改作普通设备使用或淘汰时，应当将敏感信息存储部件拆除

96 敏感及内网计算机不得使用无线键盘、无线鼠标、无线网卡

97 敏感文件不允许在普通计算机上进行处理

98 内外网数据交换需使用专用的加密U盘或刻录光盘

99 工作环境外避免透露工作内容

100 重要文件存储应先进行加密处理

网络安全风险层出不穷，需要注意的地方还有很多，这里只为大家梳理了常见的100个网络安全小知识，如需更多网络安全保障措施可扫码咨询。