账号安全

1、小O：经理，我在公司业务系统的权限较低，我可以使用你的账号权限来进行操作吗？

经理：借用账号密码我是拒绝的，这个“锅”我不背！。

这属于哪项安全？ B

A. 杜绝弱口令。

B. 杜绝账号共享。

C. 杜绝信息泄露。

D. 杜绝泄密。

2、如果您接触到单位的外包/第三方人员，您是否会因为工作需要把密码告知为您服务的第三方人员？ B

A． 会告诉

B． 不会，自己输入。

C． 会告诉，第三方使用后自己会更换。

D． 会告诉，自己会定期修改。

3、与朋友共享账号，将有可能导致账号被盗，下列哪种属于不正确的做法？D

A．切勿与他人共用同一账号。

B．如有某次被他人登录过账号，应及时更换密码。

C．并不是只有自己的账号共享有害，参与共享他人账号也容易导致被盗。

D．账号共享，方便你我他。

人员安全

上网行为规范

4、在日常工作和生活中，经常需要从互联网上下载文件，此时必须要关注下载内容的安全性，谨慎使用下载完成的文件，以避免造成不必要的损害。以下关于互联网下载、使用等行为的说法，错误的是 D

A. 不随意下载使用来路不明的文件或程序。

B. 应进入软件的官方下载主页，或那些规模大、知名的网站进行下载。

C. 后缀名为 \*.exe、\*.rar、\*.zip、\*.doc等文件，下载后一定要先杀毒。

D. 在浏览网页过程中弹出的插件，都可以直接安装。

社会工程学

5、以下哪项不属于社会工程学？ D

A． 骗取他人的信任，从而获取有用的信息

B． 搜集他人的信息，尝试破解他人的账号密码

C． 冒充某公司的员工或来访人员，混入该公司内部

D． 通过技术手段拦截他人的电子邮件

社交网络安全

6、社交网站中个人隐私泄露的形式一般有？ D

A． 引导用户填写隐私信息

B． 诱骗用户填写隐私信息

C． 数据挖掘

D． 以上都是

7、我们的信息是怎么丢失的？D

1. 不及时打补丁浏览被挂马网站、随意点开可执行文件、电脑裸奔。
2. 复制后不小心粘贴到QQ聊天或群里会直接上传或传给对方、借用U盘拷重要文件最后忘记删除。
3. 维护时不在旁陪同信息被拷走。随意填写问卷调查。
4. 以上均是。

数据安全

8、关于数据保存，可能不妥当的行为是（ADE）

A．将重要数据文件保存到C盘或者桌面。

B．定期对重要数据文件用光盘进行备份（遵循各单位内部操作规程基础上）。

C．将重要数据文件保存到C盘外的其他硬盘分区。

D. 将外网PC和内网PC的数据随便交互拷贝。

E．将重要文件存放于网络共享区域。

无线安全

9、第三方公司人员到公司洽谈业务，期间向您要公司无线网络的账号密码，您应该怎么做？ C

A. 给他一个公用的账号密码

B. 将自己的账号密码告诉他

C. 礼貌的告诉他，公司的无线网络使用需要相应审批申请

D. 让他使用公共电脑上网

10、小李：我最近装了一个WiFi万能钥匙，几乎到哪里都不用问WiFi密码，自动连接上WiFi。

小明：那么神奇，为什么呢？

小李：都是热心网友连接那里的WiFi后贡献出来的密码啊。

小明：团结就是力量啊，我也装个试试。

小黑：嘿嘿嘿，手机自动连接Tal公司WiFi。这些小白，都不知道WiFi万能钥匙默认会上传自己连接WiFiI的密码。哈哈哈，让我进他们内网逛一圈。

万能钥匙不仅可以窃取WiFi密码，还可以通过这个软件看到这个WiFi网络后面所有的隐私（如：银行卡密码、身份证号、手机号等等）对于以上出现的问题，有什么安全建议？ABCDE

1. 不要使用WiFi万能钥匙类的APP。
2. 如果使用必须关闭自动上传密码功能。
3. WiFi网络提供者应谨慎共享自己的WiFi网络，并定期更换WiFi网络密码。
4. WiFi网络使用者应增强安全上网意识，谨慎使用WiFi“蹭网”类移动应用程序。
5. 警惕重名WiFi。

便携电脑使用安全

11、在旅行中或出差时等办公室之外的地方使用便携电脑，以下哪些使用方式不符合安全规定：DF

A．乘飞机旅行时，将便携电脑放在托运的行李中。

B．外出时将便携电脑锁在酒店保险柜里。

C．如果便携带闹闹被偷或丢失，报告给公司当地的安全部门和你的上级主管。

D．在候机室或者飞机上看影片。

E．出差前做个数据备份及加密

F．在机场候机室，笔记本放在身边的座椅上自己睡着了。

弱口令：

12、小黑：哈哈哈，终于进入了Tal公司内网了，我来破解一下ERP用户的口令。

……

ERP系统破解成功

账 号：小明

破解时间：1秒

破解结果：123456

小黑：这也太弱了吧，试一下其他用户。

账 号：小红

破解时间：30秒

破解结果：abc1234

关于口令安全的说法正确的是（）？ABEF

1. 一般情况下，设置口令时，应保证口令位数在8位以上。
2. 口令应至少包含大小写字母、数字及特殊符号中的任意两种字符。
3. 为避免口令丢失，将口令记录在笔记本中，或者贴在计算机机箱或终端屏幕上，或者上传到Github上。
4. 为避免遗忘，应将口令设置为生日、电话号码等容易记忆的内容。
5. 定期修改各种口令，如三个月或半年。
6. 最好不要包含自己的名字、生日、手机号或车牌号。

安全意识

13、小王是Tal公司的员工，正当他在忙于一个紧急工作时，接到一个陌生的电话：“小王您好，我是系统管理员，咱们的系统发现严重漏洞，需要进行紧急升级，请提供您的账户信息”，他应该\_\_\_\_\_  **C**

1. 配合升级工作，立即提供正确的账户信息。
2. 先忙手头工作，再提供账户信息。
3. 身份不明确，电话号码认识，直接拒绝。
4. 事不关己，直接拒绝。

14、以下哪种行为最可能会导致敏感信息泄露？ A

A. 打印的敏感文件未及时取走

B. 及时清除使用过的移动介质中的数据

C. 硬盘维修或报废前进行安全清除

D. 企密信息作废时通过碎纸机碎掉

个人应当加强信息安全意识的原因不包括（）。D

A. 人的信息安全意识薄弱具有普遍性且容易被渗透，攻击者更喜欢选择这条路径发起攻击。

B. 认识信息安全防护体系中最薄弱的一个环节。

C. 研究实验已表明，增强个人信息安全意识能有效减少由人为因素造成安全威胁发生的概率。

D. 基于技术的防御手段已经无法成为安全防护体系的重要组成部分。

物理环境安全

15、小a加班到很晚，期间外出去吃夜宵，回公司时发现自己的门禁卡落在工位上了，于是，便尝试利用其他办法，触发动作探测器，结果门就开了。

物理环境的安全是信息安全的重要环节，一定要引起充分重视！所以哪些建议是正确的？ACDE

1. 将敏感设备和信息放置在受控的安全区域。
2. 打印的敏感文件不再使用了，就直接丢到垃圾桶中。
3. 所有到受控区域的入口都应该加锁、设置门卫，或者以某种方式进行监视，并做好进出登记。
4. 使用公共区域的打印机、传真机、复印机时，一定不要遗留敏感文件。
5. 应主动防止陌生人尾随进入办公区。

16、小秦是刚入职的实习生，这天，小秦接到一电话，就离开工位了。回来后，发现办公桌上的学生报名信息表不见了。里面有学生的家庭住址，父母联系方式等等。正着急呐，再一看，邻桌的小a拿的就是小秦的学生报名信息表。马上要了回来，小秦心想，幸亏不是外人看到，要不然小秦丢了学生报名表，对公司不好交代，学生的信息也都泄露了。

所以，离开电脑，切记锁屏。以下不属于办公区安全做法？D

A. 桌面不要遗留门禁卡、密钥、钥匙、手机等重要物品

B.下班或者长时间离开工位后，建议电脑关机

C.敏感文件一定要锁到柜子里

D. 短时间离开工位，可使用Win+P锁屏

17、您本身想使用“安全打印”功能，可是不小心点击了“立即打印”，于是您锁住了电脑屏幕，起身前去打印机前，您要取走机密文件。这时，您的经理正好要找您，要谈一项重要工作。以下做法不正确的是？B

1. 先让经理稍等，取回机密文件再谈工作。
2. 先谈工作，再取打印出来的文件不迟。

C．临时让值得信任的同事帮忙代取。

D．先确保清除机密文件的打印队列。

防病毒

18、下面哪几种情况可能预示着电脑中病毒了？ABCDE

A．可用内存空间减少，使原来可运行的程序不能运行。

B．计算机运行速度明显变慢，系统死机现象增多。

C．文件无故丢失、无法打开。

D．在屏幕上出现莫名奇妙的提示信息，发出不正常的声音。

E．防病毒软件无法正常运行。

19、糟糕，中招了

描述：老师您好，这是咱们公司新开发的pc端教学系统（xxx.exe），请查收，若有什么问题请及时联系。

老师不加思索的运行了xxx.exe……之后什么都打不开了，而且还弹出来要交费之后才能查看自己的文件。糟糕，老师的电脑中毒了。

邮件安全

20、又是钓鱼，又是病毒，看来邮件是个多事之地啊，那我们怎么做才能安全的收发邮件呢， 以下选项中不安全的做法是？ D

A. 要对收发邮件使用SSL或TLS进行加密，以免通信过程被窃听。

B. 陌生链接勿点击。

C. 有一个复杂的定期更改的密码，用一次性口令更加安全。

D．以上均是。

办公区域安全

21、开会啦开会啦，这个项目是咱们公司的重要项目之一，然后在白板上写下项目的策划方案……，下面来讨论一下，ok，会议结束各自去准备吧。现在会议室里已空无一人，但是项目策划方案还在，请问有关会议安全的安全建议包括哪些？ D

A．注意选择隔音的会议室。开会期间拉上窗帘。

B．会后整理会场，不遗留文件，注意檫白板

C．会前叮嘱参与人员，不许拍照录音。

D．以上均是。

22、XYZ公司遭遇重大数据失窃，一名不愿透露姓名的报料者向记者透露……，怎么会发生这种事情呢？节目刚一播出，客户服务部门便收到大批客户的投诉，明天肯定会更多。这次事故肯定会让公司损失不少，甚至会对公司的信誉带来不良影响。如何有效防范这类攻击事件发生呢？ABCDE

A．不要让他人尾随您进入公司区域。

B．在公司区域内全程陪伴访客。

C．离开位置钱锁住电脑屏幕和敏感文档。

D．随身携带如智能手机、平叛电脑、U盘等移动设备。

E．及时取走打印出的文件和擦除白板上的敏感内容，保持桌面和办公区域的清洁。

23、密码通常是较为脆弱的安全防线。A

1. 错误
2. 正确

24、公司应用系统都在内网，人员离职不需要回收其访问权限，反正他也访问不到内网 A

1. 错误
2. 正确

25、在公共场所应使用VPN连接办公网络，在自己家里是不需要的 A

1. 错误
2. 正确

26、定义资产责任人的目的是使信息资产的管理具体落实到人，并且通过具体职责的界定，使信息资产的价值得到有效保证 B

1. 错误
2. 正确

27、打印错的合同或协议应该及时扔进垃圾桶处理 A

1. 错误
2. 正确

28、使用了VPN，就不会因为远程连接服务器而导致服务器感染病毒 A

1. 错误
2. 正确

29、无线网络是需要频繁使用的，定期更换密码不方便大家的使用，所以不用定期更换 A

1. 错误
2. 正确

30、每个产品都有安全漏洞，就连微软的windows系统都有，我们的产品有些小漏洞不用放在心上，只要事后能够补救就行。 A

1. 错误
2. 正确