1. 安全的安装是保障 Windows 终端安全的基础，对于特定的计算机系统或者由于故障等原因需要进行系统重新安装时，可以考虑从安装做起，打造一个安全的 Windows 终端系统，下列关于安全安装说法错误的是（ ）

A.在选择安装的操作系统时应安装企业版以获取更多功能，无需考虑计算机的应用场景

B.系统安装完成后，应首先进行系统的安全更新，确保系统不存在已知的安全漏洞

C.安全更新可通过互联网直接连接到微软服务器进行

D.安装过程中用户自建的账户应设置安全的密码

参考答案：A
难易程度：一级

解析：目前 Windows10 官方提供家庭版、专业版、专业工作站版和企业版，在软件功能上根据不同的应用有功能上的区别，因此在选择安装的操作系统时，应根据计算机终端的应用场景，选择合适的系统版本。

所属知识子域：windows 终端安全

2. Windows 系统安装完成后，除了安装过程中用户自建的账户外，默认会生成在两个内置的账户，下列哪个账户是内置账户（ ）

A. MyAccount

B. Root

C. Guest

D. admin

参考答案：C
难易程度：一级
解析：Windows 系统安装完成后，除了安装过程中用户自建的账户外，默认会生成在两个内置的账户，分别是管理员账户 administrator 和来宾账户 guest。

所属知识子域：windows 终端安全

3. 下列关于 Windows 系统账户安全说法错误的是（ ）

A. Administrator 账户可以更名

B. 设置密码策略可以对登录错误达到一定次数的账户进行锁定从而抑制口令暴力破解攻击

C. 在实际使用过程中，需要根据业务和自身需要选择账户的验证方式

D. 如果确认不需要 Guest 账户，可设置安全的口令、对其进行更名并禁用以提高安全性

参考答案：B
难易程度：一级

解析：密码策略是避免系统中出现弱密码，而账户锁定策略通过设置对登录错误达到一定次数的账户进行锁定从而抑制口令暴力破解攻击。

所属知识子域：windows 终端安全

4. Windows 系统的安全设置中，账户策略用于保护账户的安全性，避免弱口令以应对口令暴力破解，而本地安全策略也提供了审核策略、用户权限分配和安全选项对系统安全进行管控，下列选项错误的是（ ）

A. 审核策略的作用是通过策略设置，实现对用户操作进行审核从而形成安全日志

B. 安全选项通过对系统安全机制、安全功能进行设置调整，实现有效的提高整体安全性。

C. 用户权限分配对一些敏感或者风险操作的用户权限进行了限制

D. 默认情况下，审核策略全部都是开启的

参考答案：D
难易程度：一级
解析：默认情况下，审核策略并不是全部都开启的，需要根据相关安全设置指导文档进行设置
所属知识子域：windows 终端安全

5. 关于 windows 内置的防病毒软件，说法错误的是（ ）

A. 系统内置，提供对系统进行实时监控、计算机病毒的检测和查杀、文件夹的访问限制等多种功能

B. 系统内置，可以卸载

C. 默认情况下，除了勒索软件防护功能为不启用外，其他都是启用

D. 实时防护功能关闭一段时间后，被关闭的实时保护功能会被系统自动开启

参考答案：B
难易程度：一级
解析：Microsofe Defender 内置在 Windows 系统中，不可从系统中卸载或删除
所属知识子域：windows 终端安全

6. Windows Defender 防火墙是内置在 Windows 系统中的系统防护软件，下列关于 Windows Defender 防火墙说法错误的是（ ）

A. 默认状态下，Windows Defender 防火墙为开启状态，包括域网络、专用网络和公用网络

B. Windows defender 的防火墙可阻挡或者允许特定程序或者端口进行连接，对出入站和连接基于规则进行防护。

C. 入站规则是设置允许哪些程序接受外部连接进入的数据，出站规则设置允许那些程序向外发起连接

D. Windows Defender 防火墙是谷歌研发的系统防护软件

参考答案：D

难易程度：一级
解析：Windows Defender 防火墙是微软自主研发的系统防护软件，内置在 Windows 系统中。
所属知识子域：windows 终端安全

7. 下列哪个选项不属于 Windows 系统的服务启动策略（ ）

A. 自动
B. 手动
C. 禁用
D. 重启
参考答案：D
难易程度：一级
解析：Windows 系统的服务为操作系统提供许多重要功能，服务的启动策略有所不同，分别是自动(系统开机自动启动)、手动(按需由管理员启动)和禁用(禁止启动)。
所属知识子域：windows 终端安全

8. 下列选项中对 Windows 系统安全没有帮助的是（ ）

A. 关闭管理共享
B. 关闭自动播放
C. 禁用 Guest 账户
D. 关闭账户锁定策略
参考答案：D
难易程度：一级
解析:账户锁定策略通过设置对登录错误达到一定次数的账户进行锁定从而抑制口令暴力破解攻击。
所属知识子域：windows 终端安全

9. 在 Windows 系统中，通常删除文件有两种方式，使用 CMD 命令控制台中的“delete”命令删除文件，或者使用鼠标右键点击菜单中删除，下列有关两种方式说法正确的是（ ）

A. 两种方式删除的文件都会被放入回收站
B. 两种方式都会直接删除
C. 鼠标右键点击删除的文件会进入回收站，而命令行删除的文件不会进入回收站
D. 鼠标右键点击删除的文件不会进入回收站，而命令行删除的文件会进入回收站
参考答案：C
难易程度：一级
解析：在 Windows 系统中，通常删除文件有两种方式，使用 CMD 命令控制台中的“delete”命令删除文件，或者使用图形的交互界面删除并清空回收站。
所属知识子域：windows 终端数据安全

10. 数据加密是保护数据安全的主要措施。通过对数据进行加密，可以避免存储在计算机终端上的数据被攻击者窃取。下列关于数据加密的说法错误的是（ ）

A. 加密文件系统（EFS）是 Windows 提供的一个对 NTFS 卷上的文件、文件夹进行加密的软件，内置在 Windows 系统中

B. EFS 的加密是基于公钥体系

C. 在首次使用 EFS 时系统会自动进入证书导出的操作界面引导用户备份密钥

D. 由于 EFS 的密钥是不会存储在系统中的的，因此即使计算机终端发生盗窃时，也可以有效的保证数据的安全。

参考答案：D
难易程度：一级
解析：使用 EFS 可以对文件和文件夹进行加密，由于密钥是存储在系统中的，因此对于计算机终端发生盗窃等方式时，是无法有效的保证数据的安全。

所属知识子域：windows 终端数据安全

11. 以下关于 BitLocker 说法错误的是（ ）

A. BitLocker 是从 Windows Vista 开始在系统中内置的数据加密保护机制
B. 如果计算机系统上没有 TPM，BitLocker 就不可用于加密 Windows 操作系统驱动器
C. BitLocker 可以对 Windows 系统中的驱动器进行加密，并且支持可信计算
D. 计算机系统安装了可信平台模块 （TPM）时，BitLocker 可以与 TPM 进行协作，保护用户数据并且避免计算机在系统离线时被篡改
参考答案：B
难易程度：一级
解析：如果计算机系统上没有 TPM，BitLocker 仍然可以用于加密 Windows 操作系统驱动器，只是此时密钥是存储在 USB 中，用户在启动计算机或从休眠状态中恢复都需要插入 USB key。

所属知识子域：windows 终端数据安全

12. 下列哪个选项是错误的（ ）

A. 移动智能终端的硬件信息属于用户个人数据
B. 移动智能终端不是用户身份验证的主要方式
C. 伪基站是移动智能终端面临的安全威胁之一
D. 移动智能终端中安装的应用软件的操作记录属于需要保护的移动智能终端数据
参考答案：B
难易程度：一级
解析：智能手机是起到支付通道和鉴别作用的设备，是整个应用场景中信息安全的关键因素。

所属知识子域：移动智能终端安全

13. 下列哪个选项不属于移动智能终端面临的主要威胁（ ）

A. 伪基站
B. 设备丢失、被盗
C. 系统漏洞
D. DLL 注入
参考答案：D

难易程度：一级
解析：目前，移动智能终端面临的安全威胁主要有：伪基站、设备丢失和损坏、系统漏洞、恶意 APP 等。
所属知识子域：移动智能终端安全

14. 理论上对数据进行反复（ ）的覆写就基本无法进行恢复，因此我国对涉及国家秘密的计算机中的数据删除，要求使用专用的数据粉碎软件进行删除，这个删除操作就会对需要删除的文件所在的硬盘数据区块进行反复的覆写。

A. 七次
B. 六次
C. 五次
D. 四次
参考答案：A
难易程度：一级
解析：理论上对数据进行反复七次的覆写就基本无法进行恢复
所属知识子域：windows 终端数据安全

15. 自动播放功能是 Windows 系统为了方便用户而设置，这项为方便用户而提供的功能为系统带来了较大的安全风险，一些病毒的传播就是依托于该功能，因此出于安全性的考虑，应禁止使用设备的自动播放功能，彻底解决这一安全风险。关闭自动播放功能需要通过 Windows 系统的（ ）实现

A. 系统配置
B. 组策略设置
C. 系统组件服务
D. 本地安全策略
参考答案：B
难易程度：一级
解析：关闭自动播放功能需要通过 Windows 系统的组策略设置实现。组策略设置可执行 gpedit.msc 打开组策略编辑器，在组策略编辑器中进行编辑。
所属知识子域：windows 终端安全

16. 在 cmd 中哪个命令可以查看共享文件（ ）

A. net share
B. net localgroup
C. net send
D. net session
参考答案：A
难易程度：二级
解析：net send 作用是向网络的其他用户、计算机或通信名发送消息，net localgroup 作用是添加、显示或更改本地组，net session 作用是列出或断开本地计算机和与之连接的客

户端的会话

所属知识子域：windows 终端安全

17. Win+R 打开运行后输入下列哪个选项可以打开注册表编辑器（ ）

A. mstsc

B. nslookup

C. regedit

D. regedit.msc

参考答案：C

难易程度：二级

解析：mstsc 打开远程连接，nslookup 打开 IP 地址侦测器，regedit.msc 不存在，干扰项

所属知识子域：windows 终端安全

18. 柯克霍夫原则是（ ）

A. 密码系统的运作步骤泄露，该密码不可用

B. 密码系统的运作步骤泄露，该密码仍可用

C. 密码系统的运作步骤泄露，密钥未泄露，该密码仍可用

D. 密码系统的运作步骤泄露，密钥泄露，该密码仍可用

参考答案：C

难易程度：二级

解析：柯克霍夫原则

所属知识子域：windows 终端数据安全

19. 以下关于管理共享的说法那个是错误的（ ）

A. 默认情况下，Windows 会自动创建特殊隐藏的共享资源

B. IPC$共享资源是进程间通信的命名管道，用于传递通信信息，无法被删除

C. 管理共享是系统设置的，无法取消

D. net share 命令用来管理共享资源

参考答案：C

难易程度：二级

解析：如果对共享资源没有使用的需求，可以通过编辑注册表来阻止系统自动创建

所属知识子域：windows 终端安全

20. 以下哪个管理共享是不存在的（ ）

A. C$

B. D$

C. ADMIN$

D. 1$

参考答案：D

难易程度：二级

解析：系统的每个根分区或卷，共享名称为驱动器号名称附加“$”符号。例如当 Windows 系统上有 C、D 两个分区时，管理共享为 C$和 D$。ADMIN$：Windows 系统的安装目录被共享为该名称，用于远程管理计算机时使用。

所属知识子域：windows 终端安全

21. 某 windows 系统用户名为 Admin，该系统开启了账户策略中的口令符合复杂性的策略，并限制密码长度最小值为 6 个字符，以下哪个口令是符合策略要求会被系统接受的（ ）

A. Admin246!
B. a135!
C. AdlLN153!
D. 2w3e4dfg
参考答案：C
难易程度：二级
解析：如果密码必须符合复杂性要求，密码必须符合下列最低要求:不能包含用户的帐户名，不能包含用户姓名中超过两个连续字符的部分；至少有六个字符长；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 !、$、#、%)；
所属知识子域：windows 终端安全

22. Win+R 打开运行后输入下列哪个选项可以打开组策略编辑器（ ）

A. services.msc
B. regedit
C. gpedit.msc
D. magnify
参考答案：C
难易程度：三级
解析：services.msc 为打开本地服务设置 regedit 为打开注册表编辑器 magnify 为打开放大镜
所属知识子域：windows 终端安全

23. Windows 共享目录的中的“更改”和“完全控制”有什么区别（ ）

A. 删除文件
B. 修改文件
C. 新建文件
D. 修改权限
参考答案：D
难易程度：三级
解析：“更改”权限没有修改权限的能力，“完全控制”有修改权限能力
所属知识子域：windows 终端安全

24. 下列方法哪个适用于防御 U 盘病毒（ ）

A. 关闭自动播放
B. 关闭 Security Center 服务
C. 关闭管理共享
D. 开启审核策略
参考答案：A
难易程度：一级
解析：自动播放功能是 Windows 系统为了方便用户而设置，U 盘病毒的传播就是依托于该功能。

所属知识子域：windows 终端安全

25. 下列关于 windows 系统备份的说法哪个是错误的（ ）

A. 需要在确保系统稳定可靠的情况下对系统进行备份

B. 需要专业的第三方软件才能进行

C. 可以在系统刚配置好时进行备份

D. 如果硬盘空间较为宽松，可以设置定期产生一个备份

参考答案：B

难易程度：一级

解析：Windows 系统还原点创建方式：右键点击“此电脑”，弹出菜单中选择属性，在弹出的对话框中选中“系统保护”。

所属知识子域：Windows 终端数据安全

26. （ ）是保障 windows 终端安全的基础

A. 安全的安装

B. 应用程序

C. 硬件

D. 杀毒软件

参考答案：A

难易程度：一级

解析：安全的安装是保障 Windows 终端安全的基础，可以考虑从安装做起，打造一个安全的 Windows 终端系统。

所属知识子域：windows 终端安全

27. 下列关于数据备份的说法错误的是（ ）

A. 使用专用备份软件进行备份

B. 可通过云盘或者存储系统进行远程备份

C. 数据最好在自有的存储系统或私有云进行备份

D. 数据备份无法防止由于操作失误导致的数据丢失风险

参考答案：D

难易程度：一级

解析：通过数据备份，能防止由于操作失误或硬件损坏等原因导致的数据丢失风险

所属知识子域：Windows 终端数据安全

28. 为 windows 系统内置的管理员账户更名可以防御什么攻击（ ）

A. 针对 administrator 的口令暴力破解

B. 针对 guest 的口令暴力破解

C. DLL 注入

D. 拒绝服务攻击

参考答案：A

难易程度：一级

解析：对内置管理员账户 administrator 设置安全的口令并进行更名是针对该账户进行口令暴力破解防御的有效手段

所属知识子域：windows 终端安全

29. 数据粉碎的原理是（ ）

A. 反复覆盖

B. 加密存储区域

C. 物理销毁

D. 破坏存储区域
参考答案：A
难易程度：一级
解析：文件粉碎方式，是通过反复的对文件存储的硬盘区块进行覆盖写入垃圾数据，使得原来的数据彻底被破坏，无法恢复，从而实现对数据的保护
所属知识子域：Windows 终端数据安全

30. 下列哪个选项不属于 EFS 加密的优点（ ）

A. 内置在 Windows 系统中
B. 对用户透明
C. 对于 NTFS 卷上的文件和数据，都可以直接作加密保存
D. 解密无需依赖密钥
参考答案：D
难易程度：一级
解析：用 EFS 对数据加密保护，虽然对用户透明，但用户需要明白的一点，EFS 解密时依赖密钥。
所属知识子域：windows 终端数据安全

31. 需要进行 windows 系统备份的原因是（ ）

A. 防止系统崩溃
B. 防止数据丢失
C. 系统崩溃时可以还原到可用状态
D. 以上都对
参考答案：C
难易程度：一级
解析：系统备份并不能防止系统崩溃和数据丢失，只是当系统发生故障时，可以配合系统还原来将系统恢复到一个可用的状态
所属知识子域：windows 终端数据安全

32. 下列说法错误的是（ ）

A. 在 Windows 系统中，通常删除文件有两种方式，使用 CMD 命令控制台中的“delete”命令删除文件，或者使用图形的交互界面删除
B. 使用“delete”命令删除后数据无法恢复
C. 目前对于重要数据的安全删除（也称为文件粉碎）方式，是通过反复的对文件存储的硬盘区块进行覆盖写入垃圾数据
D. 一些机密性要求较高的计算机系统需要考虑硬销毁
参考答案：B
难易程度：一级
解析：Windows 系统为提高文件操作的效率，只是从文件系统中将此文件标记为删除，告诉系统这个文件所占用的硬盘空间已经被释放，可以使用。文件实际上还存储在硬盘上，没有任何改变，只有当系统需要向硬盘中写入数据时才有可能将此数据区覆盖
所属知识子域：windows 终端数据安全

33. 下列有关 windows 系统服务说法错误的是（ ）

A. 服务的启动策略分为自动、手动、禁用
B. 所有的服务项都需要用户登录系统后才会启动
C. 运行权限较高
D. 部分为默认“启动”

参考答案：B
难易程度：一级
解析：无需用户登录即可自动运行
所属知识子域：windows 终端安全

34. 移动终端对于信息安全的重要意义在于（ ）

A. 移动终端中存储着大量的用户个人信息
B. 移动终端已经成为用户身份验证的一种物品
C. 移动终端已经成为大量的业务办理渠道，例如手机银行
D. 其他三个选项的说法都对
参考答案：D
难易程度：一级
解析：移动智能终端作为移动业务的综合承载平台，传递着各类内容资讯，存储着大量数据。移动智能终端已经成为用户身份验证的主要方式或者主要通道。
所属知识子域：移动终端安全

35. 移动智能终端出现下列哪种情况时可能正在遭受伪基站攻击（ ）

A. 手机信号很弱或者突然回落到 2G 信号，接到可疑短信
B. 自动下载 APP
C. 设备卡顿
D. 某款 APP 申请多项不需要的权限
参考答案：A
难易程度：一级
解析：伪基站诈骗短信欺骗性很强，但也并非不可识别。如果用户手机信号很弱或者突然回落到 2G 信号，但还能接到可疑短信时，就需要提高警惕。
所属知识子域：移动终端安全

36. 下列哪种安全措施适用于移动设备丢失、被盗（ ）

A. 设置 SIM 卡锁
B. 启用过滤未知发件人功能
C. 数据粉碎
D. 取消 APP 不需要的权限
参考答案：A
难易程度：一级
解析：除了设置手机屏幕密码之外，手机卡同样需要设置 PIN 密码，被设置 PIN 密码的 SIM 卡，换了手机需要输入 PIN 码，否则无法正常使用。
所属知识子域：移动终端安全

37. 对于 WiFi 的安全使用下列哪种说法是正确的（ ）

A. 如果 WiFi 接入时需要密码那么该 WiFi 一定是安全可信的
B. 可以通过 WiFi 名称判断是否可信
C. 在进行敏感数据传输时一定要确保 WiFi 可靠，必要时可使用流量传输
D. 所有 WiFi 都是可信的
参考答案：C
难易程度：一级
解析：识别接入点的标识（SSID）可以由接入设备（无线路由器）进行随意设置
所属知识子域：移动终端安全

38. 下列关于 windows 账户说法正确的是（ ）

A. guest 不是 windows 系统内置账户
B. administrator 可以删除 system 账户
C. system 账户可以从交互界面登录
D. system 账户拥有系统最高权限
参考答案：D
难易程度：一级
解析：system 账户账户拥有系统最高权限且无法从交互界面登录
所属知识子域：移动终端安全

39. Windows 的第一个版本于（ ）年问世

A. 1984
B. 1985
C. 1986
D. 1987
参考答案：B
难易程度：一级
解析：Windows 的第一个版本于 1985 年问世
所属知识子域：windows 终端安全

40. 默认情况下操作系统安装在哪个分区（ ）

A. C 盘
B. D 盘
C. E 盘
D. F 盘
参考答案：A
难易程度：一级
解析：windows 系统基础知识
所属知识子域：windows 终端安全

41. 在 windows 系统中，如果想要限制用户登录尝试失败的次数，应该如何设置（ ）

A. 在本地组策略编辑器中对密码策略进行设置
B. 在本地组策略编辑器中对审核策略进行设置
C. 在本地组策略编辑器中对账户锁定策略进行设置
D. 在本地组策略编辑器中对用户权限分配进行设置
参考答案：C
难易程度：一级
解析：在在本地组策略编辑器中对账户锁定策略的账号锁定阈值进行设置
所属知识子域：windows 终端安全

42. 在你为一台新的电脑安装 windows 操作系统时,以下哪一种做法最可能导致安全问题（ ）

A. 安装完毕后进行系统的安全更新
B. 启用防火墙
C. 关闭管理共享
D. 启用自动播放功能
参考答案：D
难易程度：一级
解析：出于安全性的考虑，应禁止使用设备的自动播放功能

所属知识子域：windows 终端安全

43. 关于软件安全获取，下列做法错误的是（ ）

A. 从微软官方的应用商店进行软件下载

B. 去软件开发商的官网下载

C. 去可靠的第三方网站进行下载

D. 在百度随意找一个下载

参考答案：D

难易程度：一级

解析：Windows 软件安全防护可以采取类似 MAC OS 的策略，尽量只从微软官方的应用商店进行软件下载和安装，这些软件都经过微软的官方检测，具有较高的安全性，并且对系统的兼容性也较好。应用商店没有的软件，也尽量去软件开发商的官网或相对可靠的第三方网站进行下载。

所属知识子域：windows 终端安全

44. 以下对 Windows 服务的说法正确的是（ ）

A. 为了提升系统的稳定性管理员应尽量不关闭服务

B. 不能作为独立的进程运行或以 DLL 的形式依附在 Svchost.exe

C. windows 服务可以以 system 的身份运行

D. windows 服务通常是以 guest 的身份运行的

参考答案：C

难易程度：一级

解析：系统服务会以 system 身份运行

所属知识子域：windows 终端安全

45. 在对一台 windows 进行扫描时发现该设备开放了 445 端口，那么该电脑可能开启了什么功能（ ）

A. FTP

B. 远程桌面

C. 共享文件夹或共享打印机

D. SMTP

参考答案：C

难易程度：二级

解析：FTP 端口号 21、远程桌面端口号 3389、SMTP 端口号 25

46. 在 NTFS 文件系统中，如果共享权限和 NTFS 权限发生了冲突，那么以下说法正确的是（ ）

A. 共享权限高于 NTFS 权限

B. NTFS 权限高于共享权限

C. 系统会认定最少的权限

D. 系统会认定最多的权限

参考答案：C

难易程度：二级

解析：在权限冲突的情况下，系统会按照最少的权限给与

所属知识子域：windows 终端安全

47. 如果想禁止旧密码连续重新使用应该开启哪个策略（ ）

A. 重置账户锁定计数器

B. 审核策略更改

C. 审核账户管理
D. 强制密码历史
参考答案：D
难易程度：二级
解析：强制密码历史可以使管理员能够通过确保旧密码不被连续重新使用来增强安全性。
所属知识子域：windows 终端安全
48. 关于防火墙作用的说法中，下列选项错误的是（ ）
A. 防火墙可以抵挡外部攻击
B. 防火墙占用一定的系统资源
C. 防火墙能够隐蔽个人计算机的 IP 地址等信息
D. 防火墙可以阻止病毒文件
参考答案：D
难易程度：二级
解析：防火墙无法阻止病毒文件
所属知识子域：windows 终端安全
49. Windows10 中设置注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWKS 子项的值为 0，可以（ ）
A. 关闭管理共享
B. 关闭自动播放
C. 关闭实时防护
D. 禁用内置账户
参考答案：A
难易程度：三级
解析：Windows10 阻止创建共享资源的注册表子项为：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWKS
注册表子项 AutoShareWKS 必须设置为 REG_DWORD，值为 0。
所属知识子域：windows 终端安全
50. 常用的数据备份方式包括完全备份、增量备份、差异备份，这三种备份方式的备份速度从快到慢为（ ）
A. 完全备份、增量备份、差异备份
B. 完全备份、差异备份、增量备份
C. 增量备份、差异备份、完全备份
D. 增量备份、完全备份、差异备份
参考答案：C
难易程度：三级
解析：完全备份方式的备份速度最慢，但恢复速度最快。增量备份的备份速度最快，但恢复速度最慢。
所属知识子域：windows 终端数据安全
51. 加密技术不能提供下列哪种服务（ ）
A. 身份认证
B. 完整性
C. 保密性

D. 可用性
参考答案：D
难易程度：三级
解析：保密性——加密算法、完整性和身份验证——签名
所属知识子域：windows 终端数据安全

52. 下列关于 EFS 的说法错误的是（ ）

A. 是 Windows 提供的一个对 NTFS 卷上的文件、文件夹进行加密的软件
B. EFS 加密系统对用户是透明的
C. 当系统被删除，重新安装后，原加密的文件可直接打开
D. 可以对文件和文件夹进行加密
参考答案：C
难易程度：一级
解析：解密时依赖密钥的，为了防止系统崩溃或重装系统导致密钥丢失从而无法解密数据，在使用 EFS 时应将密钥备份出来并保存在安全的地方
所属知识子域：windows 终端数据安全

53. 在对 windows 系统进行安全配置时，下面不可采用的安全措施是（ ）

A. 关闭注册表远程访问
B. 为系统内置账户更名
C. 设置账户锁定阈值为 0
D. 设置密码长度最小值
参考答案：C
难易程度：一级
解析：如果将账户锁定阈值值设置为 0，则永远不会锁定帐户。
所属知识子域：windows 终端安全

54. （ ）是 Windows NT5.0 之后所特有的一个实用功能，对于 NTFS 卷上的文件和数据，都可以直接被操作系统加密保存，在很大程度上提高了数据的安全性。

A. EFS
B. SAM
C. Bitlocker
D. NFS
参考答案：A
难易程度：一级
解析：SAM 是安全账号管理器，用于管理用户账号，BitLocker 是从 Windows Vista 开始在系统中内置的数据加密保护机制，NFS 是网络文件系统能让使用者访问网络上别处的文件就像在使用自己的计算机一样
所属知识子域：windows 终端数据安全

55. 下列哪个是 windows 系统开放的默认共享（ ）

A. 1$
B. IPC$
C. CD$
D. 6!$
参考答案：B
难易程度：一级
解析：系统默认开放的共享有 DriveLetter$、ADMIN$、IPC$

所属知识子域：windows 终端安全

56. 一个安全的口令应该具有足够的复杂度，下列选项中（ ）具有最好的复杂度

A. Morrison

B. zhangsan1999

C. 12785563

D. Wm.S*F2m5@

参考答案：D

难易程度：一级

解析：安全的口令要有足够的长度，以及大写字母、小写字母、数字、特殊字符组合

所属知识子域：windows 终端安全

57. 物理销毁的方式不包括（）

A. 消磁

B. 焚化炉烧毁

C. 反复覆写数据

D. 机器研磨粉碎

参考答案：C

难易程度：一级

解析：物理销毁的方式包括消磁、焚化炉烧毁、机器研磨粉碎等方式

所属知识子域：windows 终端安全

58. 计算机上存储数据的介质主要是（ ）

A. 硬盘

B. 内存

C. U 盘

D. 光盘

参考答案：A

难易程度：一级

解析：计算机上存储数据的介质主要是硬盘

所属知识子域：windows 终端数据安全

59. 某用户把系统登录密码设置为“147258”该密码属于（ ）

A. 弱口令密码

B. 强口令密码

C. 强安全性密码

D. 以上都不对

参考答案：A

难易程度：一级

解析：147258、123456 之类的密码都属于典型的弱口令

所属知识子域：windows 终端安全

60. 弱口令一直是威胁网络安全的一个重大问题，以下对弱口令的描述正确的是（ ）

A. 容易被破解从而威胁用户计算机安全

B. 仅包含简单数字和字母的口令

C. 连续的某个字符或重复某些字符的组合

D. 以上都对

参考答案：D

难易程度：一级

解析：弱口令，通常认为容易被别人猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险
所属知识子域：windows 终端安全

61. 当 windows 系统因恶意代码、系统升级等原因导致系统不稳定时，可以通过（ ）来恢复

A. 更新驱动
B. 之前创建的系统还原点
C. 卸载程序
D. 系统服务
参考答案：B
难易程度：一级
解析：如果系统设置了备份，通过使用系统自带的还原功能可将系统还原到某个系统不存在缺陷的状态
所属知识子域：windows 终端数据安全

62. BitLocker 是从（ ）开始在系统中内置的数据加密保护机制，主要用来解决由于计算机设备丢失、被盗或者维修等物理接触方式导致的数据失窃或恶意泄露的威胁。

A. Windows Vista
B. Windows 7
C. Windows XP
D. Windows NT 5.0
参考答案：A
难易程度：一级
解析：BitLocker 是从 Windows Vista 开始在系统中内置的数据加密保护机制
所属知识子域：windows 终端数据安全

63. 依据中华人民共和国国家标准《GB/T 34977-2017 信息安全技术 移动智能终端数据存储安全技术要求与测试评价方法》，用户个人数据主要有（ ）方面

A. 五个
B. 六个
C. 七个
D. 八个
参考答案：C
难易程度：一级
解析：通信信息、使用记录信息、账户信息、金融支付信息、传感采集信息、用户设备信息和文件信息七个方面
所属知识子域：移动终端安全

64. 下列说法错误的是（ ）

A. 本地组策略的安全选项中可启用管理员账户
B. 本地组策略的安全选项中可重命名管理员账户
C. 开启强制密码历史是为了防止频繁更换密码
D. 可在本地组策略的安全选项启用不允许 SAM 账户的匿名枚举
参考答案：C
难易程度：一级
解析：开启强制密码历史是为了确保旧密码不被连续重新使用来增强安全性

所属知识子域：windows 终端安全

65. 下列针对 windows 主机安全说法最准确的是（ ）

A. 系统刚安装后最安全

B. 系统开启防火墙就安全了

C. 禁用系统内置的账户就安全了

D. 经过专业的安服人员评估后根据评估结果进行加固较为安全

参考答案：D

难易程度：一级

解析：专业的安服人员评估比较全面，可以发现更多的安全隐患。ABC 选项都比较片面

所属知识子域：windows 终端安全

66. 下列哪个选项不能防止智能移动终端信息泄露（ ）

A. 经常备份数据

B. 不随意连接不明无线网络

C. 开启丢失找回

D. 不访问不明网站

参考答案：A

难易程度：一级

解析：经常备份数据可以防止数据丢失，但不能防止信息泄露

所属知识子域：移动终端安全

67. EFS（加密文件系统）可以用在下列哪种文件系统下（ ）

A. Ext4

B. NTFS

C. FAT32

D. HFS+

参考答案：B

难易程度：一级

解析：加密文件系统（EFS）是 Windows 提供的一个对 NTFS 卷上的文件、文件夹进行加密的软件

所属知识子域：windows 终端数据安全

68. 在 windows 系统中，为了显示隐藏文件应该首先选用的菜单是（ ）

A. 查看

B. 编辑

C. 文件

D. 属性

参考答案：A

难易程度：一级

解析：点击查看后在隐藏的项目前打钩

所属知识子域：windows 终端安全

69. 下列关于 system 账户描述错误的是（ ）

A. 是本地系统账户

B. 权限高于用户自建账户

C. 不可用于从交互界面进行登录

D. 权限和 administrator 相同

参考答案：D

难易程度：一级
解析：system 拥有系统最高权限，高于 administrator
所属知识子域：windows 终端安全

70. 在 windows 系统中设置账户锁定阈值可以防止下列哪种攻击（ ）

A. 暴力破解
B. 钓鱼攻击
C. 缓存区溢出攻击
D. 会话劫持
参考答案：A
难易程度：一级
解析：设置账户锁定阈值可以使账户在几次无效登录后被锁定一段时间，即使密码正确也无法登陆
所属知识子域：windows 终端安全

71. 下列说法错误的是（ ）

A. Web（World Wide Web）也称为万维网
B. Web 应用广泛使用的是客户端/服务器架构(C/S)
C. Web 应用在互联网上占据了及其重要的地位
D. 浏览器是检索、展示以及传递 Web 中信息资源的应用程序
参考答案：B
难易程度：一级
解析：Web 应用广泛使用的是浏览器/服务器架构(B/S)
所属知识子域：web 浏览安全

72. Web（World Wide Web）也称为（ ），是一种基于（ ）和 HTTP 的互联网上的网络服务，为用户信息浏览提供（ ）、易于访问的交互界面，通过超级链接将互联网上的资源组织成相互关联的（ ）。

A. 超文本、图形化、万维网、网状结构
B. 万维网、超文本、图形化、网状结构
C. 万维网、图形化、超文本、网状结构
D. 超文本、万维网、图形化、网状结构
参考答案：B
难易程度：一级
解析：Web（World Wide Web）也称为万维网，是一种基于超文本和 HTTP 的互联网上的网络服务，为用户信息浏览提供图形化、易于访问的交互界面，通过超级链接将互联网上的资源组织成相互关联的网状结构。
所属知识子域：web 浏览安全

73. 下列关于 xss（跨站脚本攻击）的说法错误的是（ ）

A. 跨站脚本攻击英文为 Cross Site Scripting
B. 跨站脚本攻击开发人员对用户提交的数据没有进行严格的控制，使得用户可以提交脚本到网页上
C. xss 可以提交的脚本只有 JavaScript
D. 跨站脚本攻击是目前互联网常见的的面向浏览器的攻击方式
参考答案：C
难易程度：一级
解析：跨站脚本攻击开发人员对用户提交的数据没有进行严格的控制，使得用户可以提交脚

本到网页上，这些脚本脚本包括 JavaScript、Java、VBScript、ActiveX、Flash，甚至是普通的 HTML 语句。
所属知识子域：web 浏览安全

74. 下列关于 xss（跨站脚本攻击）的描述正确的是

A. xss 攻击就是 DDOS 攻击的一种
B. xss 攻击无法获得 cookie
C. xss 攻击可以劫持用户会话
D. xss 攻击危害很小
参考答案：C
难易程度：一级
解析：攻击者可以在受害者的计算机执行命令、劫持用户会话、插入恶意内容、重定向用户访问、窃取用户会话信息、隐私信息、下载蠕虫木马到受害者计算机上等威胁行为
所属知识子域：web 浏览安全

75. 下列关于 window 的 SAM 的说法错误的是（ ）

A. SAM 文件即账号密码数据库文件
B. 安全账号管理器的具体表现就是%SystemRoot%\system32\config\sam 文件
C. 当我们登录系统的时候，系统会自动地和 Config 中的 SAM 自动校对
D. SAM 中存储的账号信息 administrator 是可读和可写的
参考答案：D
难易程度：二级
解析：SAM 文件在系统运行中无法打开
所属知识子域：windows 终端安全

76. 如果在安全设置中开启账户锁定策略并设置账户锁定阈值为 5，账户锁定时间为 0，重置账户锁定计数器为 30，那么在进行五次无效登录后账户会被（ ）

A. 一直被锁定，直到管理员明确解除对它的锁定
B. 永久锁定，无法解锁
C. 不会被锁定
D. 30 分钟
参考答案：A
难易程度：二级
解析：windows 系统账户锁定时间官方说明：如果将帐户锁定时间设置为 0，帐户将一直被锁定直到管理员明确解除对它的锁定。
所属知识子域：windows 终端安全

77. 对于 windows 的系统服务，应采取最小化原则：关闭不用的服务、关闭危险性大的服务等。在无需远程管理和共享打印机的情况下，下列哪个服务最好不要关闭（ ）

A. Remote Registry
B. Security Center
C. Remote Desktop Services
D. Server
参考答案：B
难易程度：二级
解析：Security Center 是 windows 的安全中心
所属知识子域：windows 终端安全

78. 下列哪个选项可以设置禁止某些用户和组作为远程桌面服务客户端登录（ ）

A. 管理共享
B. 系统服务
C. 本地组策略
D. 系统组件服务
参考答案：C
难易程度：二级
解析：用户权限分配对一些敏感或者风险操作的用户权限进行了限制，用户权限设置位于本组策略设置
所属知识子域：windows 终端安全

79. 下列关于 windows 注册表的说法错误的是（ ）

A. 使用 Win+R 打开运行后输入 gpedit.msc 即可打开注册表编辑器
B. 注册表如果受到破坏会影响系统正常运行
C. 配置注册表的某些键值可以关闭管理共享
D. 注册表中有系统启动时自动加载相关的信息
参考答案：A
难易程度：二级
解析：regedit 打开注册表编辑器
所属知识子域：windows 终端安全

80. Windows10 系统的安全日志存放路径在哪里修改（ ）

A. 注册表编辑器
B. 组策略编辑器
C. 文件资源管理器
D. 本地服务
参考答案：A
难易程度：二级
解析：在 win10 系统中打开“注册表编辑器”窗口，展开并定位到如下分支：HKEY_LoCAL_MACHinE/system/CurrentControlset/semces/EventLog/security 双击并修改右侧窗格中的“file”值即可修改
所属知识子域：windows 终端安全

81. 在 windows 系统中设置账号锁定策略为：账号锁定阈值为 5 次、账号锁定时间为 20 分钟、重置账号锁定计数器为 20 分钟，下列说法正确的是（ ）

A. 账号锁定阈值与发生时间段长短（比如一天内）无关，只要该账户登录失败超过五次就会被自动锁定
B. 账户被锁定后要等待二十分钟才可以进行正常登录
C. 重置账户锁定计数器的时间应大于或等于账号锁定时间
D. 以上都对
参考答案：B
难易程度：二级
解析：重置账号锁定计数器为 20 分钟，所以 A 选项错误。重置账户锁定计数器的时间应小于或等于账号锁定时间，所以 C 选项错误
所属知识子域：windows 终端安全

82. 可远程访问的注册表路径可在下列哪个选项修改（ ）

E. 在本地组策略编辑器中对审核策略进行设置
F. 在本地组策略编辑器中对用户权限分配进行设置

G. 在本地组策略编辑器中对账户策略进行设置
H. 在本地组策略编辑器中对安全选项进行设置
参考答案：D
难易程度：三级
解析：对本地组策略编辑器——安全选项——网络访问：可远程访问的注册表路径进行修改
所属知识子域：windows 终端安全

83. windows 系统组策略编辑器的账户锁定策略中有账户锁定阈值、账户锁定时间、重置账户锁定计数器三项，如果将账户锁定阈值设置为 0，那么下列说法正确的是（ ）

A. 账户锁定时间与重置账户锁定计数器都无法设置
B. 账户锁定时间可设置，重置账户锁定计数器无法设置
C. 账户锁定时间无法设置，重置账户锁定计数器可设置
D. 账户锁定时间与重置账户锁定计数器都可以设置
参考答案：A
难易程度：三级
解析：因为只有在指定了帐户锁定阈值时，重置账户锁定计数器与账户锁定时间才可用。
所属知识子域：windows 终端安全

84. 在 cmd 中输入下列哪个命令可以查看所有账户（ ）

A. net user
B. net share
C. net localgroup
D. net config
参考答案：A
难易程度：三级
解析：B 选项作用：创建、删除或显示共享资源、C 选项作用：添加、显示或更改本地组、D 选项作用：显示当前运行的可配置服务，或显示并更改某项服务的设置。
所属知识子域：windows 终端安全

85. Windows 新建一个名为 abc 密码为 123 的用户命令是（ ）

A. net user abc 123 /add
B. net user “abc 123” /add
C. net user 123 abc /add
D. net user 123 “abc” /add
参考答案：A
难易程度：三级
解析：在 cmd 里面输入：net user /? 来查看 net user 命令参数的用法
所属知识子域：windows 终端安全

86. 下列选项中哪个是 windows 系统内置的文件加密方式（ ）

A. MD5
B. RC4
C. SM7
D. EFS
参考答案：D
难易程度：一级
解析：加密文件系统（EFS）是 Windows 提供的一个对 NTFS 卷上的文件、文件夹进行加密的软件，内置在 Windows 系统中。

所属知识子域：web 浏览安全

87. Web1.0 的概念是在哪一年出现的（ ）

A. 1990

B. 1995

C. 2005

D. 2018

参考答案：A

难易程度：一级

解析：1990——web、2005——web2.0、2018——web3.0

所属知识子域：web 浏览安全

88. 下列哪个选项不属于常见的 web 应用服务器（ ）

A. IIS

B. Apache

C. Nginx

D. SQL Server

参考答案：D

难易程度：一级

解析：SQL Server 是由 Microsoft 开发和推广的关系数据库管理系统

所属知识子域：web 浏览安全

89. 下列关于跨站脚本攻击的描述正确的是（ ）

A. 跨站脚本攻击英文为 Cross Site Scripting

B. 反射型跨站脚本攻击是持久性的

C. 跨站脚本攻击是一种利用客户端漏洞实施的攻击

D. 跨站脚本攻击无法重定向用户访问

参考答案：A

难易程度：一级

解析：反射型跨站脚本攻击是非持久性的、跨站脚本攻击是一种利用网站漏洞实施的攻击，可用于重定向用户访问

所属知识子域：web 浏览安全

90. 关于 XSS 分类说法错误的是（ ）

A. 反射型 XSS

B. 存储型 XSS

C. 字符型 XSS

D. DOM 型 XSS

参考答案：C

难易程度：一级

解析：XSS 分类可分为反射型、存储型、DOM 型三类

所属知识子域：web 浏览安全

91. 关于跨站请求伪造下列说法错误的是（ ）

A. 是一种以用户身份在当前已经登录的 Web 应用程序上执行非用户本意操作的攻击方法

B. 获取受害者 cookie

C. 不攻击网站服务器

D. CSRF 利用的是网站对用户网页浏览器的信任

参考答案：B
难易程度：一级
解析：CSRF 是借用用户 cookie 而不是获取 cookie
所属知识子域：web 浏览安全

92. 下列选项中属于 CSRF 的危害的是（ ）

A. 修改受害者个人信息
B. 以受害者名义购买商品
C. 修改受害者的收件地址
D. 以上都是
参考答案：D
难易程度：一级
解析：服务器认为这个请求是正常用户的合法请求，从而导致攻击者的非法操作被执行，例如窃取用户账户信息、添加系统管理员、购买商品，虚拟货币转账等
所属知识子域：web 浏览安全

93. 下列关于 CSRF 描述最准确的是（ ）

A. 是一种以用户身份在当前已经登录的 Web 应用程序上执行非用户本意操作的攻击方法
B. 攻击者嵌入恶意脚本代码到正常用户会访问到的页面中，当用户访问该页面时，则可导致嵌入的恶意脚本代码的执行，从而达到恶意攻击用户的目的
C. 攻击者构造携带木马程序的网页，利用系统漏洞、浏览器漏洞或用户缺乏安全意识等问题将木马下载到用户的系统中并执行
D. 攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式
参考答案：A
难易程度：一级
解析：B 选项是 XSS 攻击、C 选项是网页挂马、D 选项是网络钓鱼
所属知识子域：web 浏览安全

94. 下列防御 CSRF 攻击不正确的是（ ）

A. 检查 Referer 报头
B. 添加验证码
C. 添加 token
D. 更换浏览器
参考答案：D
难易程度：一级
解析：CSRF 是服务端没有对请求头做严格过滤引起的，更换浏览器并不能解决问题
所属知识子域：web 浏览安全

95. （ ）是一种以用户身份在当前已经登录的 Web 应用程序上执行非用户本意操作的攻击方法。

A. 网页挂马
B. CSRF
C. 网络钓鱼
D. XSS
参考答案：B
难易程度：一级
解析：跨站请求伪造是一种以用户身份在当前已经登录的 Web 应用程序上执行非用户本意操

作的攻击方法。
所属知识子域：web 浏览安全

96. 以下对跨站脚本攻击的解释最准确的一项是（ ）

A. 通过将精心构造的代码注入到网页中，并由浏览器解释运行这段代码，以达到恶意攻击的效果
B. 构造精巧的数据库查询语句对数据库进行非法访问
C. 以用户身份在当前已经登录的 Web 应用程序上执行非用户本意操作的攻击方法
D. 一种 DDOS 攻击
参考答案：A
难易程度：一级
解析：XSS 攻击就是将一段精心构造的代码代码注入到网页中，并由浏览器解释运行这段代码，以达到恶意攻击的效果
所属知识子域：web 浏览安全

97. 常见的网页挂马方式不包括（ ）

A. 利用操作系统、浏览器或者浏览器组件的漏洞
B. 伪装成页面的正常元素
C. 利用浏览器脚本运行的漏洞自动下载网页上的木马
D. 通过邮件发送链接
参考答案：D
难易程度：一级
解析：邮件发送链接属于钓鱼攻击
所属知识子域：web 浏览安全

98. 下列关于网页挂马的说法错误的是（ ）

A. 可能会盗取个人信息
B. 可能会对计算机系统进行破坏
C. 网页挂马不会自动下载
D. 尽量访问官方网站能降低感染木马的概率
参考答案：C
难易程度：一级
解析：如果浏览器的脚本权限设置为全部无需用户确认执行时，攻击者可构造特定的网页，当用户访问时，通过脚本将木马自动释放到用户的系统中。
所属知识子域：web 浏览安全

99. 关于预防网页挂马的措施，以下哪个选项最合适（ ）

A. 尽量访问可靠的官方网站
B. 及时安装微软官方发布的系统补丁
C. 使用安全防护软件
D. 以上选项的综合使用
参考答案：D
难易程度：一级
解析：ABC 三项综合使用效果最好
所属知识子域：web 浏览安全

100. （ ）是攻击者构造携带木马程序的网页，该网页在被浏览器访问时，利用系统漏洞、浏览器漏洞或用户缺乏安全意识等问题，将木马下载到用户的系统中并执行，从而实现对用户的系统进行攻击。

A. 网页挂马
B. 跨站脚本攻击
C. 跨站请求伪造
D. 网络钓鱼
参考答案：A
难易程度：一级
解析：网页挂马是攻击者构造携带木马程序的网页，利用系统漏洞、浏览器漏洞或用户缺乏安全意识等问题，将木马下载到用户的系统中并执行，实现对用户的系统进行攻击。
所属知识子域：web 浏览安全

101. （ ）是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式。

A. 网页挂马
B. 跨站脚本攻击
C. 跨站请求伪造
D. 网络钓鱼
参考答案：D
难易程度：一级
解析：网络钓鱼是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式。
所属知识子域：web 浏览安全

102. 下列哪种攻击方式属于网络钓鱼（ ）

A. 通过电子邮件向用户发送伪造银行邮件
B. 以受害者身份在当前已经登录的 Web 应用程序上执行修改密码的操作
C. 向网站插入 JavaScript 代码获取受害者 cookie
D. 攻击者构造携带木马程序的网页，利用操作系统漏洞将木马下载到目标计算机系统
参考答案：A
难易程度：一级
解析：网络钓鱼(Phishing)是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式
所属知识子域：web 浏览安全

103. 下列有关养成 web 浏览安全意识说法错误的是（ ）

A. 安全意识是 Web 浏览的时候安全攻防的关键所在
B. 应关注 Web 浏览过程的隐私保护
C. 尽量使用密码自动保存功能
D. 在 Web 浏览的时候，应遵循信息安全中通用的“最小特权原则”
参考答案：C
难易程度：一级
解析：在浏览器使用过程中，对于浏览器弹出的自动保存网站密码、自动登录等设置，应在确保系统可控的情况下再进行确定。特别是在多人公用的计算机系统中，更应禁止使用密码保存和自动登录，避免由此造成的个人隐私信息泄露。
所属知识子域：web 浏览安全

104. 网络钓鱼的主要手法包括（ ）

A. 发送包含虚假信息的电子邮件引诱用户提供个人信息
B. 建立假冒网站骗取用户账号密码

C. 通过短信平台群发大量包含“退税”字眼的短信诱骗受害者点击链接套取金钱
D. 以上都是
参考答案：D
难易程度：一级
解析：网络钓鱼方式
所属知识子域：web 浏览安全

105. 下列选项不属于网络钓鱼的是（ ）

A. 发送带有中奖信息的邮件，诱导被攻击者输入银行账号和密码等信息
B. 注册和百度非常相似的域名，制作和百度相同的页面后引诱受害者访问
C. 通过跑字典得到了被攻击者的密码
D. 以银行升级为诱饵，欺骗客户点击伪造的银行网站进行升级
参考答案：C
难易程度：一级
解析：C 选项属于暴力破解
所属知识子域：web 浏览安全

106. 下列关不属于良好的 web 浏览安全意识的是（ ）

A. 不明链接访问要先确认
B. 关注网站备案信息
C. 慎用密码自动保存功能
D. 所有的网站设置相同的登录口令
参考答案：D
难易程度：一级
解析：应该确保登录口令安全，补同网站应设置不同的密码
所属知识子域：web 浏览安全

107. 关于 Web 浏览中最小特权原则说法错误的是（ ）

A. 不需要的页面不要随便访问
B. 无需明确需要访问的资源
C. 不需要下载的文件不要下载
D. 不熟悉的联网方式不要随便连接
参考答案：B
难易程度：一级
解析：Web 浏览中最小特权原则是明确需要访问的资源，对于不需要的页面不要随便访问，不明确的链接不随意去点击，不需要下载的文件不要下载，不熟悉的联网方式不要随便连接等
所属知识子域：web 浏览安全

108. 在 Web 应用中需要设置口令时，无需遵循以下哪个要求（ ）

A. 口令应具有足够的复杂性
B. 多个网站共用一个口令避免遗忘
C. 养成定期更改口令的好习惯
D. 口令的相关信息包括验证信息应避免告诉其他人
参考答案：B
难易程度：一级
解析：应遵循以下要求：口令应具有足够的复杂性，口令的相关信息包括验证信息应避免告诉其他人；口令分类分级，避免多个网站共用一个口令导致的撞库攻击；养成定期更改口令

的好习惯；登录时应注意防“偷窥”。

所属知识子域：web 浏览安全

109. 下列哪个选项不是防范网络钓鱼的方法（ ）

A. 不轻易在网站中输入自己的个人账户信息

B. 不在不可信的电子商务网站进行在线交易

C. 不随意点击不明电子邮件中的网址

D. 短信收到链接后直接复制到浏览器打开

参考答案：D

难易程度：二级

解析：短信中收到的链接应谨慎打开

所属知识子域：web 浏览安全

110. 以下属于 2017 年 OWASP 十大安全漏洞的是（ ）

A. SQL 注入

B. 不安全的反序列化

C. 敏感信息泄露

D. 以上都是

参考答案：D

难易程度：二级

解析：查看 OWASP Top 10

所属知识子域：web 浏览安全

111. 以下关于网络钓鱼的说法中,不正确的是（）

A. 网络钓鱼属于社会工程学攻击

B. 网络钓鱼融合了伪装、欺骗等多种攻击方式

C. 网络钓鱼攻击和 web 服务没有关系

D. 将被攻击者引诱到一个钓鱼网站是典型的网络钓鱼

参考答案：C

难易程度：二级

解析:网络钓鱼(Phishing)是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式

所属知识子域：web 浏览安全

112. 下列说法错误的是（ ）

A. 攻击者构建的网络钓鱼网站通常情况下无法进行备案

B. 如果备案信息与网站不一致，该网站的安全性就存疑

C. 我国对于网站上线要求具备 ICP 备案号

D. 没有进行备案的网站允许临时接入互联网一年时间

参考答案：D

难易程度：一级

解析:我国对于网站上线要求具备 ICP 备案号，没有进行备案的网站是不允许接入互联网并提供服务的

所属知识子域：web 浏览安全

113. Cross Site Scripting 的中文名称是（ ）

A. 跨站脚本攻击

B. 跨站请求伪造

C. 网络钓鱼
D. 网页挂马
参考答案：A
难易程度：一级
解析：跨站脚本攻击英文为 Cross Site Scripting，由于采用常用的缩写方式写成 CSS，会与层叠样式表（Cascading Style Sheets，CSS）的缩写混淆，因此通常习惯将跨站脚本攻击缩写为 XSS
所属知识子域：web 浏览安全

114. 要安全浏览网站的话下列哪个哪个操作是错误的（ ）

A. 定期清理浏览器 cookie 数据
B. 定期清理浏览器缓存
C. 尽量使用记住密码功能，防止遗忘密码
D. 访问之前没浏览过的网站时，禁用浏览器 JavaScript
参考答案：C
难易程度：一级
解析：记住密码功能应在确保系统可控的情况下再进行确定。特别是在多人公用的计算机系统中，更应禁止使用密码保存和自动登录，避免由此造成的个人隐私信息泄露。
所属知识子域：web 浏览安全

115. 下列描述错误的是（ ）

A. Cookie 是浏览器使用的文本格式的小文件，用于存储用户信息和用户偏好等信息
B. 设置浏览器的“不跟踪”请求，浏览器在访问网站时告诉网站不希望被跟踪，这个“不跟踪”请求是否执行的决定权在浏览器
C. 如果不是必须，网站使用位置信息、操纵摄像头、弹出式窗口等权限应尽量避免允许网站使用
D. 对于保存的口令信息，不建议同步到云端保存
参考答案：B
难易程度：一级
解析：可以设置浏览器的“不跟踪”请求，浏览器在访问网站时告诉网站不希望被跟踪，虽然这个“不跟踪”请求是否执行的决定权在网站，但规范设计的网站会遵守浏览器的要求。
所属知识子域：web 浏览安全

116. CSRF 攻击的中文名称是（ ）

A. 服务端请求伪造
B. 跨站请求伪造
C. 网络钓鱼
D. 网页挂马
参考答案：B
难易程度：一级
解析：跨站请求伪造（英语：Cross-site request forgery），也被称为 one-click attack 或者 session riding，通常缩写为 CSRF
所属知识子域：web 浏览安全

117. 网页浏览的好习惯不包括（ ）

A. 选择火狐等大牌浏览器
B. 打开网站之前仔细核对网站域名是否正确
C. 不在所有网站使用相同的用户名和密码

D. 重要网站密码使用姓名简拼加出生年月日
参考答案：D
难易程度：一级
解析：姓名简拼加出生年月日是典型的的弱口令
所属知识子域：web 浏览安全

118. 在注册和浏览社交网站时下列哪个做法是错误的（ ）

A. 尽可能少输入个人信息
B. 充分利用网站的安全机制
C. 好友发送的链接等信息随意访问
D. 在社交网站发照片时要谨慎，不要暴露照片拍摄地址和时间
参考答案：C
难易程度：一级
解析：不要随意访问网站，访问前应判断该链接是否安全
所属知识子域：web 浏览安全

119. 攻击者通过邮箱和短信群发大量包含“中奖”、“退税”、“兑换积分”等字眼的消息诱骗受害者点击链接后输入个人信息的攻击方式属于（ ）

A. XSS 攻击
B. CSRF 攻击
C. 网络钓鱼
D. 网页挂马
参考答案：C
难易程度：一级
解析:网络钓鱼(Phishing)是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式。
所属知识子域：web 浏览安全

120. 小白在某购物网站下单一部手机后没有退出该购物网站，此时收到一条短信说您近期购买的商品降价了，点击链接可申请退差价，小白点击短信附带的链接后回到购物网站发现自己刚下单的手机收货地址变成了一个陌生的地址，请问小白可能收到了什么攻击（ ）

A. 网络钓鱼和 XSS
B. 网络钓鱼和 CSRF
C. 网页挂马和 XSS
D. 网页挂马和 CSRF
参考答案：B
难易程度：一级
解析：退差价的短信是网络钓鱼，点击链接后收货地址被修改是 CSRF
所属知识子域：web 浏览安全

121. Phishing 攻击的中文名字是（ ）

A. 网络钓鱼
B. 网页挂马
C. 跨站脚本攻击
D. 外部实体注入攻击
参考答案：A
难易程度：一级

解析：网络钓鱼（Phishing，与钓鱼的英语 fishing 发音相近，又名钓鱼法或钓鱼式攻击）
所属知识子域：web 浏览安全

122.　　关于安全使用浏览器，下列说法错误的是（ ）

A. 清除浏览器缓存
B. 防止跟踪
C. 避免自动口令填充
D. 多使用代理服务器
参考答案：D
难易程度：一级
解析：在代理模式下，用户的访问信息都需要通过代理服务器进行处理，如果对代理服务器的安全性无法保证，应尽量避免使用。
所属知识子域：web 浏览安全

123.　　下列说法错误的是（ ）

A. 应养成定期清除浏览器记录的习惯
B. 为了解决 Cookie 的安全问题，应在浏览器的 Cookie 管理相关设置处开启允许所有 Cookie
C. 重要的网站的账号和口令不要设置自动填充
D. 代理服务器访问模式下浏览器不直接向网站服务器请求数据
参考答案：B
难易程度：一级
解析：如果没有特别的必要，不建议选择允许所有 Cookie 开启，所有 Cookie 开启会导致相应的安全风险
所属知识子域：web 浏览安全

124.　　下列哪个选项不属于常用的浏览器安全措施（ ）

A. 定期清除浏览记录
B. 管理和清除 Cookie
C. 设置浏览器的“不跟踪”请求
D. 禁止访问国外的网站
参考答案：D
难易程度：一级
解析：不访问国外网站并不能加强浏览器的安全性
所属知识子域：web 浏览安全

125.　　下列说法错误的是（ ）

A. CSRF 利用的是网站对用户网页浏览器的信任
B. XSS 是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序
C. 网络钓鱼是指在网络上组织的钓鱼活动
D. 网页挂马是攻击者构造携带木马程序的网页，该网页在被浏览器访问时
参考答案：C
难易程度：一级
解析：网络钓鱼是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式
所属知识子域：web 浏览安全

126.　　下列关于 Cookie 的描述错误的是（ ）

A. 浏览器使用的文本格式的小文件

B. 用于存储用户信息和用户偏好等信息
C. Cookie 通常是加密的
D. 由于 Cookie 包含较隐私的信息，所以设计的 Cookie 非常安全，没有安全隐患
参考答案：D
难易程度：一级
解析：Cookie 使用文本文件格式，而其中又包含较隐私的信息，攻击者可以通过获取 Cookie 来收集用户信息或获得其他权限
所属知识子域：web 浏览安全

127. 下列选项中不属于 cookie 作用的是（ ）

A. Cookie 为 Web 应用程序保存用户相关信息提供了一种有用的方法
B. 解决 http 协议无连接无状态问题
C. 美化网页
D. 辨别用户身份，进行 Session 跟踪
参考答案：C
难易程度：一级
解析：cookie 是某些网站为了辨别用户身份，进行 Session 跟踪而储存在用户本地终端上的数据，根本作用是为了解决 http 协议无连接无状态问题
所属知识子域：web 浏览安全

128. 下列有关代理服务器说法错误的是（ ）

A. 代理服务器访问模式是浏览器不直接向网站服务器请求数据，而是将请求先发送给代理服务器
B. Exchange Server 是代理服务器软件
C. 如果对代理服务器的安全性无法保证，应尽量避免使用
D. 在代理模式下，用户的访问信息都需要通过代理服务器进行处理
参考答案：B
难易程度：一级
解析：Exchange Server 是微软公司的一套电子邮件服务组件，是个消息与协作系统
所属知识子域：web 浏览安全

129. 下列哪个选项不属于 XSS 漏洞危害（ ）

A. 窃取管理员帐号或 Cookie
B. 网站挂马
C. 记录按键
D. SQL 数据泄露
参考答案：D
难易程度：一级
解析：跨站脚本攻击可以在受害者的计算机执行命令、劫持用户会话、插入恶意内容、重定向用户访问、窃取用户会话信息、隐私信息、下载蠕虫木马到受害者计算机上等威胁
所属知识子域：web 浏览安全

130. 下列哪个选项属于 XSS 攻击类型（ ）

A. 延时型 XSS
B. DOM 型 XSS
C. 字符型 XSS
D. 布尔型 XSS
参考答案：B

难易程度：一级
解析：XSS 分类可分为反射型、存储型、DOM 型三类
所属知识子域：web 浏览安全

131. 防御 XSS 跨站脚本攻击，不可取的是（）

A. 对用户数据进行严格检查过滤
B. 可能情况下避免提交 HTML 代码
C. 禁止用户向 Web 页面提交数据
D. 移除用户上传的 DOM 属性
参考答案：C
难易程度：二级
解析：禁止用户向 Web 页面提交数据不合理
所属知识子域：web 浏览安全

132. 在某网站的留言板处存在 XSS 漏洞，攻击者提交恶意 JavaScript 脚本后被存在了数据库当中，每当有用户浏览留言板页面时就会受到该恶意脚本的攻击，本案例所描述的 XSS 攻击属于（ ）

A. 反射型
B. 存储型
C. 字符型
D. 搜索型
参考答案：B
难易程度：二级
解析：反射型 XSS 攻击是一次性的，仅对当次的页面访问产生影响。存储型 XSS，会把攻击者的数据存储在服务器端，攻击行为将伴随着攻击数据一直存在。
所属知识子域：web 浏览安全

133. 下列防御 XSS 攻击的方式可取的是（ ）

A. 设置安全的密码
B. 更换浏览器
C. 对用户输入的内容进行严格过滤
D. 为网站添加验证码
参考答案：C
难易程度：二级
解析：XSS 防御的总体思路是：对输入(和 URL 参数)进行过滤，对输出进行编码
所属知识子域：web 浏览安全

134. 下列关于电子邮件说法错误的是（ ）

A. 电子邮件是一种信息交换的服务方式
B. 用户代理是用户与电子邮件系统的接口
C. 用户使用电子邮件客户端软件收发和处理邮件，用户代理就是邮件客户端软件
D. 接收方通过用户代理，使用邮件传输协议(SMTP)将邮件从接收方邮件服务器下载到客户端进行阅读
参考答案：D
难易程度：一级
解析：接收方通过用户代理，使用邮局协议(POP3)将邮件从接收方邮件服务器下载到客户端进行阅读。
所属知识子域：互联网通信安全

135.　　下列选项中用于发送电子邮件的协议是（ ）

A. SNMP

B. POP3

C. SMTP

D. FTP

参考答案：C

难易程度：一级

解析：当发送方给接收方发送电子邮件时，发送方使用用户代理撰写邮件后发送，邮件会通过简单邮件传输协议(SMTP)与发送方邮件服务器通信，将邮件上传到发送方邮件服务器，发送方邮件服务器会进一步使用 SMTP 协议将邮件发送到接收方邮件服务器

所属知识子域：互联网通信安全

136.　　下列选项中用于接收电子邮件的协议是（ ）

A. SMTP

B. SFTP

C. POP3

D. ICMP

参考答案：C

难易程度：一级

解析：接收方通过用户代理，使用邮局协议(POP3)将邮件从接收方邮件服务器下载到客户端进行阅读。

所属知识子域：互联网通信安全

137.　　下列关于系统工作过程描述错误的是（ ）

A. 发送方使用用户代理撰写邮件并发送

B. 邮件会通过邮件传输协议(SMTP)与发送方邮件服务器通信，将邮件发送到接收方邮件服务器

C. 发送方邮件服务器进一步使用 SMTP 协议将邮件发送到接收方邮件服务器

D. 接收方通过用户代理，使用邮局协议(POP3)将邮件从接收方邮件服务器下载到客户端进行阅读

参考答案：B

难易程度：一级

解析：邮件会通过简单邮件传输协议(SMTP)与发送方邮件服务器通信，将邮件上传到发送方邮件服务器

所属知识子域：互联网通信安全

138.　　电子邮件面临的威胁包括（ ）

A. 邮件地址欺骗

B. 邮件病毒

C. 邮件炸弹

D. 以上都是

参考答案：D

难易程度：一级

解析：随着电子邮件的广泛应用，电子邮件面临的安全威胁越来越多。这些威胁包括邮件地址欺骗、垃圾邮件、邮件病毒、邮件炸弹、邮箱用户信息泄露等。

所属知识子域：互联网通信安全

139.　　常见邮件仿冒方式有哪些（ ）

A. 仿冒发送地址
B. 仿冒发件人
C. 仿冒显示名称
D. 以上都是
参考答案：D
难易程度：一级
解析：早期的电子邮件发送协议（SMTP）缺乏对发送者的身份验证机制，发送者可以随意构造发送电子邮件的发送地址、显示名称等信息，这些信息对于接收者是无法进行验证的。
所属知识子域：互联网通信安全

140. 下面哪些不属于电子邮件安全使用常识 （ ）

A. 电子邮件账号使用安全的口令
B. 使用易于记忆的口令避免忘记，例如 123456
C. 邮箱密码和其他应用的密码不同
D. 不在陌生终端上登录自己的邮箱
参考答案：B
难易程度：一级
解析：应该使用自己容易记别人不好猜的口令，123456 这种是典型的弱口令不应该使用
所属知识子域：互联网通信安全

141. 向接收者的邮件地址发送大量的电子邮件，消耗接收者的邮箱空间，最终因空间不足而无法接收新的邮件，导致其他用户发送的电子邮件被丢失或退回，这种攻击方式是（ ）

A. 邮件地址欺骗
B. 口令爆破
C. 邮件病毒
D. 邮件炸弹
参考答案：D
难易程度：一级
解析：邮件炸弹是垃圾邮件的一种，通过向接收者的邮件地址发送大量的电子邮件，消耗接收者的邮箱空间，最终因空间不足而无法接收新的邮件，导致其他用户发送的电子邮件被丢失或退回。
所属知识子域：互联网通信安全

142. 下列关于垃圾邮件过滤技术描述错误的是（ ）

A. 垃圾邮件过滤是应对垃圾邮件威胁的有效措施之一
B. 内容过滤是垃圾邮件过滤技术中广泛应用的技术
C. 垃圾邮件过滤技术是一种主动防御
D. 是目前应用最广泛的反垃圾邮件技术
参考答案：C
难易程度：一级
解析：垃圾邮件过滤技术是一种被动防御，也是目前应用最广泛的反垃圾邮件技术。
所属知识子域：互联网通信安全

143. 通过对邮件标题、附件文件名、邮件附件大小等信息进行分析，由系统将识别为垃圾邮件的其他电子邮件进行删除，这种过滤方法是（ ）

A. 内容过滤
B. 黑名单过滤

C. 白名单过滤
D. 发件人过滤
参考答案：A
难易程度：一级
解析：内容过滤是垃圾邮件过滤技术中广泛应用的技术，通过对邮件标题、附件文件名、邮件附件大小等信息进行分析，由系统将识别为垃圾邮件的其他电子邮件进行删除。
所属知识子域：互联网通信安全

144. 下列不属于电子邮件防护技术的是（ ）

A. 邮件过滤
B. 邮件加密
C. 邮件炸弹
D. 邮件签名
参考答案：C
难易程度：一级
解析：邮件炸弹是电子邮件威胁的一种
所属知识子域：互联网通信安全

145. 下列关于邮件加密与签名说法错误的是（ ）

A. SMTP、POP3 协议在设计上没有对安全有足够的考虑
B. 对邮件进行加密和签名最常用的方式是使用 MD5 对会话进行保护
C. 使用 SMTP、POP3 进行邮件收发的会话缺乏加密机制
D. PGP（Pretty Good Privacy）是一个用于消息加密和验证应用程序
参考答案：B
难易程度：一级
解析：对邮件进行加密和签名最常用的方式是使用 SSL 对会话进行保护
所属知识子域：互联网通信安全

146. 下列关于即时通信应用安全说法错误的是（ ）

A. 经过多年的发展，即时通信应用信息系统自身已经不存在安全风险
B. 即时通信有庞大的用户数量，并且每个用户都有大量的联系人清单，这些都为蠕虫病毒传播提供了很好的基础
C. 攻击者可能利用即时通信破坏防御系统
D. 可能利用即时通信进行网络欺诈
参考答案：A
难易程度：一级
解析：即时通信应用系统所面临的安全问题包括：即时通信应用信息系统自身安全风险、利用即时通信传播恶意代码传播、利用即时通信破坏防御系统、网络欺诈及非法信息
所属知识子域：互联网通信安全

147. 关于电子邮件安全威胁与防护，下列描述错误的是（ ）

A. SMTP 协议的升级增加了发送方身份验证的功能，彻底抑制了邮件地址欺骗的泛滥
B. 攻击者可能通过自建 SMTP 服务器来实现发送伪造地址的邮件
C. 邮件服务器如果具备反向认证机制，可通过对邮件来源 IP 地址进行检查、反向 DNS 查询等方式，验证邮件发送方的真伪
D. 早期的 SMTP 协议缺乏对发送者的身份验证机制，发送者可以随意构造发送电子邮件的发送地址、显示名称等信息
参考答案：A

难易程度：一级
解析：随着 SMTP 协议的升级增加了发送方身份验证的功能，在一定程度上抑制邮件地址欺骗的泛滥
所属知识子域：互联网通信安全
148.　　下列关于安全使用即时通信说法错误的是（ ）
A. 安全的使用即时通信，是构建安全可靠的应用环境最重要的环节
B. 即时通信账户登录口令可与其他系统、平台账户一致
C. 通过学习网络安全知识，提高安全意识，具备基本的安全意识，就能避免大部分的安全风险
D. 应具备良好的安全意识，不随意添加不了解的人员成为好友
参考答案：B
难易程度：一级
解析：即时通信账户登录口令应具备足够安全性，并且不与其他系统、平台账户一致
所属知识子域：互联网通信安全
149.　　对邮件进行加密和签名最常用的方式是使用（ ）对会话进行保护
A. MD5
B. SSL
C. SMTP
D. POP3
参考答案：B
难易程度：一级
解析：对邮件进行加密和签名最常用的方式是使用 SSL 对会话进行保护，目前主流的邮件服务系统基本都已经支持 SSL 连接，利用 VPN 技术确保会话过程的安全可靠。
所属知识子域：互联网通信安全
150.　　下列说法错误的是（ ）
A. 数据是信息化而产生的结果，也是信息化的核心要素
B. 不同类型的企业对数据安全的重视程度相同
C. 网络安全法在第四章网络信息安全中对个人的信息保护提出了明确的要求
D. 数据的价值已经得到高度的认可
参考答案：B
难易程度：一级
解析：不同类型的企业对数据安全的重视程度不同，对数据依赖程度越高的组织机构，对数据安全的重视程度越高
所属知识子域：个人隐私保护
151.　　（ ）是目前信息泄露的主要途径
A. 公开收集
B. 非法窃取
C. 合法收集
D. 无意泄露
参考答案：B
难易程度：一级
解析：非法窃取是目前信息泄露的主要途径
所属知识子域：个人隐私保护
152.　　下列关于个人隐私保护做法错误的是（ ）

A. 注册如 QQ、微博等大厂的社交软件时可放心的详细填写个人信息
B. 快递盒、车票、发票等不要随意丢弃
C. 不要在各种调查问卷、测试程序、抽奖等网站填入个人信息
D. 不要在微博、微信朋友圈等发布的与自身密切相关的信息
参考答案：A
难易程度：一级
解析：在注册各类网站账户时应尽量避免填写个人信息
所属知识子域：个人隐私保护

153. 下列在日常生活避免个人信息泄露的做法错误的是（ ）

A. 尽量不要注册不知名的网站
B. 包含个人信息的资料不要随意丢弃，进行敏感信息销毁后再处置
C. 不随意使用公共场所中的 Wifi，特别未经加密的 Wifi
D. 废旧电子设备直接卖给二手设备回收商
参考答案：D
难易程度：一级
解析：废旧电子设备不要随意丢弃或卖给二手设备回收商，应进行数据粉碎再处置
所属知识子域：个人隐私保护

154. （ ）是由于组织机构或个人没有意识到数据的重要性，或者对攻击者进行数据收集的实现方式缺乏了解，在数据发布上缺乏足够的安全防护及安全意识，从而导致数据泄露。

A. 公开收集
B. 非法窃取
C. 合法收集
D. 无意泄露
参考答案：D
难易程度：一级
解析：无意泄露是由于组织机构或个人没有意识到数据的重要性，或者对攻击者进行数据收集的实现方式缺乏了解，在数据发布上缺乏足够的安全防护及安全意识，从而导致数据泄露。
所属知识子域：个人隐私保护

155. 下列关于组织机构敏感信息保护描述错误的是（ ）

A. 组织机构的敏感信息泄露防护是一个体系化的工作
B. 组织机构加强信息安全泄露防护通过技术措施即可实现，无需制定和落实各类管理措施
C. 敏感信息泄露防护措施包括数据加密、信息拦截、访问控制等具体实现
D. 在实际应用中需要综合利用各类防护技术的优点才能更好地保护隐私信息的安全性
参考答案：B
难易程度：一级
解析：加强信息安全泄露防护不仅仅通过技术实现，还应结合各类管理措施并进行落实
所属知识子域：个人隐私保护

156. （ ）是在在网络出口和主机上部署安全产品，对进出网络主机的数据进行过滤，发现数据被违规转移时，进行阻止和警报

A. 数据加密
B. 访问控制
C. 信息拦截
D. 权限分离

参考答案：C
难易程度：一级
解析：信息拦截是在在网络出口和主机上部署安全产品，对进出网络主机的数据进行过滤，发现数据被违规转移时，进行拦截和警报
所属知识子域：个人隐私保护

157. Windows 如何在删除文件时不经过回收站直接删除（ ）

A. 选中文件后按 delete
B. 选中文件后按 shift + delete
C. 选中文件后 Ctrl + delete
D. 选中文件后按回车加 delete
参考答案：B
难易程度：一级
解析：A 选项删除文件时文件会被放入回收站，C、D 选项是无用的组合键
所属知识子域：windows 终端安全

158. Windows10 各版本中，功能最少的是（ ）

A. 家庭版
B. 专业版
C. 企业版
D. 教育版
参考答案：A
难易程度：一级
解析：功能从少到多：家庭版——专业版——教育版——企业版（教育版和企业版功能基本相同）
所属知识子域：windows 终端安全

159. 为什么要对数据进行加密（ ）

A. 保护数据安全
B. 避免存储在计算机终端上的数据被攻击者窃取
C. 防止未授权用户读取计算机中的数据
D. 以上都对
参考答案：D
难易程度：一级
解析：数据加密是保护数据安全的主要措施。通过对数据进行加密，可以避免存储在计算机终端上的数据被攻击者窃取，防止未授权用户读取计算机中的数据。
所属知识子域：windows 终端数据安全

160. 当我们离开电脑出于安全考虑应锁定计算机，锁定计算机的快捷键是（ ）

A. Win 键+Q
B. Win 键+E
C. Win 键+L
D. Win 键+M
参考答案：C
难易程度：一级
解析：Win 键 + Q 搜索应用、Win 键 + E 打开文件资源管理器、Win 键 + M 最小化所有窗口
所属知识子域：windows 终端安全

161.　　把一个文件移动到回收站后发现删除错误，想撤回该文件可使用哪个快捷键（ ）

A. Ctrl+A

B. Ctrl+Y

C. Ctrl+X

D. Ctrl+Z

参考答案：D

难易程度：一级

解析：Ctrl+A 全选、Ctrl+Y 重新执行某项操作、Ctrl+X 剪切选择的项目

所属知识子域：windows 终端安全

162.　　当我们想测试本机是否能与服务器连接,应该使用下列哪个命令（ ）

A. ping

B. type

C. shutdown

D. whoami

参考答案：A

难易程度：一级

解析：type 显示文本文件内容、whoami　显示当前用户的名称、shutdown　关闭、重启、注销、休眠计算机

所属知识子域：windows 终端安全

163.　　从保护数据的角度来看，下列哪种分区方式最不合理（ ）

A. 分 C、D 两个分区，操作系统安装在 C 盘，软件和数据在 D 盘

B. 分 C、D、E 三个分区，操作系统安装在 C 盘，软件在 D 盘、工作资料在 E 盘

C. 分 C、D、E、F 四个分区，操作系统安装在 C 盘，其他盘分别用来存储 软件、工作资料、系统备份

D. 只分一个 C 盘，操作系统和数据都存放在 C 盘当中

参考答案：D

难易程度：一级

解析：操作系统和数据都存放在 C 盘当中的话，如果系统崩溃需要重装系统时可能导致数据丢失

所属知识子域：windows 终端安全

164.　　小明想要把自己从旧电脑拆下来的二手硬盘卖掉，但害怕硬盘中的一些隐私数据删除后会被买家恢复，下列哪个选项可以最大程度的避免这种问题（ ）

A. 在命令提示符界面下用 del 命令删除掉隐私数据

B. 在图形交互界面右键鼠标点击删除掉隐私数据

C. 选中文件后使用 shift + delete 组合键删除掉隐私数据

D. 使用专用的数据粉碎软件删除掉隐私数据

参考答案：D

难易程度：一级

解析：理论上对数据进行反复七次的覆写就基本无法进行恢复，使用专用的数据粉碎软件进行删除，这个删除操作就会对需要删除的文件所在的硬盘数据区块进行反复的覆写

所属知识子域：windows 终端数据安全

165.　　一些机密性要求极高的计算机系统，使用普通的删除方式并不能真正保护系统安全，下列哪种方式最适合用于此种系统（ ）

A. 使用专用的数据粉碎软件删除数据

B. 格式化整个硬盘
C. 对硬盘进行硬销毁
D. 格式化包含机密性文件的分区
参考答案：C
难易程度：一级
解析：一些机密性要求较高的计算机系统，使用软件进行删除并不能真正保护系统安全，此时需要考虑硬销毁
所属知识子域：windows 终端数据安全

166. 关闭 windows 系统的自动播放可以预防下列哪种安全威胁（ ）

A. 跨站脚本攻击
B. 网络钓鱼攻击
C. U 盘病毒
D. 网页挂马
参考答案：C
难易程度：一级
解析：U 盘病毒的传播就是依托于自动播放功能
所属知识子域：windows 终端安全

167. 系统的日常使用中需要安装各种不同类型的软件以实现不同的功能，这些软件毫无疑问是攻击者入侵系统的一个渠道，所以软件的安全获取对于计算机终端安全是非常重要的，下列哪个选项获取的软件可靠性是最差的（）

A. 微软官方的应用商店
B. 软件开发商官网
C. XX 软件下载站
D. 可靠的第三方下载工具（如腾讯软件管理中心）
参考答案：C
难易程度：一级
解析：尽量只从微软官方的应用商店进行软件下载和安装，应用商店没有的软件，也尽量去软件开发商的官网或相对可靠的第三方网站进行下载。
所属知识子域：windows 终端安全

168. Windows 系统账户的安全是计算机终端安全的核心，下列哪种账户密码的安全性最高（ ）

A. 连续的数字（如 123456）
B. 重复的数字（如 111222）
C. 出生年月日（如 970823）
D. 随机的六位数字（如 153829）
参考答案：D
难易程度：一级
解析：使用连续或重复的数字以及出生年月日设置的密码都是典型的弱口令，非常容易被暴力破解
所属知识子域：windows 终端安全

169. 小敏由于电脑磁盘空间不足想卸载一些软件，下列卸载方式无效的是（ ）

A. 找到应用程序安装目录，通过软件自带的卸载程序进行卸载
B. 到 windows 设置中的应用中卸载
C. 删除掉桌面的图标

D. 使用第三方工具进行卸载（如 360 软件管家）
参考答案：C
难易程度：一级
解析：删除掉桌面的图标只是删除掉了快捷方式，并没有卸载掉程序
所属知识子域：windows 终端安全

170. 在 windows 系统的命令提示符界面下用来删除文件的命令是（ ）

A. replace
B. del
C. dir
D. cd
参考答案：B
难易程度：一级
解析：replace 替换文件、dir 显示目录中的内容、cd 切换目录
所属知识子域：windows 终端安全

171. 在 windows 系统的命令提示符界面下用来复制文件的命令是（ ）

A. copy
B. move
C. exit
D. date
参考答案：A
难易程度：一级
解析：move 移动文件、exit 退出当前 cmd 窗口实例、date 显示或设置当前日期
所属知识子域：windows 终端安全

172. 关于 Windows 系统的安全设置，下列描述错误的是（ ）

A. 账户策略用于保护账户的安全性，避免弱口令以应对口令暴力破解
B. 审核策略的作用是通过策略设置，实现对用户操作进行审核从而形成安全日志
C. 安全选项在实际的使用中，无需根据业务需要进行相应设置，直接采用默认设置即可
D. 用户权限分配对一些敏感或者风险操作的用户权限进行了限制
参考答案：C
难易程度：一级
解析： 默认情况下，为了确保系统的易用性，很多安全选项中的设置并不是基于安全考虑，因此在实际的使用中，需要根据业务需要进行相应设置，确保在不影响业务的前提下提高安全能力。
所属知识子域：windows 终端安全

173. 关于 windows 系统补丁，下列说法最合理的是（ ）

A. 安装 windows 系统补丁会影响系统稳定性，应尽量避免安装
B. 安装 windows 系统补丁会影响电脑性能，所以无需安装
C. 应该安装最新的操作系统补丁。安装补丁时，尽量先对系统进行兼容性测试
D. windows 系统补丁修复了漏洞，只要看到补丁就应该立即安装
参考答案：C
难易程度：二级
解析：安装最新的操作系统补丁。安装补丁时，应先对服务器系统进行兼容性测试
所属知识子域：windows 终端安全

174. 下列的设置中应对 windows 口令暴力破解无效的设置是（ ）

A. 为系统内置账户更名
B. 开启审核策略中的审核登录事件
C. 开启密码必须符合复杂性要求
D. 设置账户锁定策略
参考答案：B
难易程度：二级
解析：开启审核登录事件后系统会记录用户账号登录、注销等事件，无法应对口令暴力破解
所属知识子域：windows 终端安全

175. 下列关于 Windows 操作系统安全加固做法错误的是（ ）

A. 禁用或删除无用账户
B. 开启账户锁定策略
C. 从远程系统强制关机的权限只分配给 Administrators 组
D. 从网络访问此计算机的权限分配给所有用户
参考答案：D
难易程度：二级
解析：从网络访问此计算机的权限应该给指定授权用户
所属知识子域：windows 终端安全

176. 在 windows10 中下列哪个版本不支持远程桌面（ ）

A. 家庭版
B. 专业版
C. 企业版
D. 教育版
参考答案：A
难易程度：二级
解析：家庭版支持的功能是最少的
所属知识子域：windows 终端安全

177. 小敏安装了一款 APP，该 APP 在小敏不知情的情况下读取了小敏的通讯录并通过网络发送出去，小敏的通讯录是被下列哪种途径泄露的（ ）

A. 公开收集
B. 非法窃取
C. 合法收集
D. 无意泄露
参考答案：B
难易程度：二级
解析：该 APP 在小敏不知情的情况下采集了小敏的通讯录，属于非法窃取
所属知识子域：个人隐私保护

178. 某 windows 系统管理员通过安全日志看到了用户的登录和注销事件，那么他可能是开启了审核策略中的（ ）

A. 审核登录事件
B. 审核进程跟踪
C. 审核目录服务访问
D. 审核特权使用
参考答案：A
难易程度：三级

解析：开启审核登录事件后系统会记录登录、注销等事件
所属知识子域：windows 终端安全

179. 对 windows 系统内置防火墙自定义规则描述错误的是（ ）

A. 可分别设置出站规则、入站规则和连接安全规则
B. 仅可设置出站规则和入站规则
C. 仅可设置入站规则和连接安全规则
D. 仅可设置出站规则和连接安全规则
参考答案：A
难易程度：一级
解析：自定义规则的创建在“高级设置”中，可分别设置出站规则、入站规则和连接安全规则
所属知识子域：windows 终端安全

180. 伪基站隐蔽性强的原因是（ ）

A. 伪基站能够将自己伪装成运营商的基站，任意冒用他人手机号码
B. 伪基站采用的技术高于正常真实的基站
C. 5G 技术让伪基站更容易实现
D. 伪基站可以入侵真实的运营商基站
参考答案：A
难易程度：一级
解析：伪基站能够将自己伪装成运营商的基站，任意冒用他人手机号码
，且伪基站运行时，信号强度高于正常的基站信号，用户手机自动选择信号较强的设备，因此被连接到伪基站上
所属知识子域：移动终端安全

181. 下列哪个选项可以通过设置对用户操作进行审核从而形成安全日志（ ）

A. 账户策略
B. 审核策略
C. 用户权限分配
D. 公钥策略
参考答案：B
难易程度：一级
解析：审核策略的作用是通过策略设置，实现对用户操作进行审核从而形成安全日志
所属知识子域：windows 终端安全

182. 下列哪个选项无法防止智能手机信息泄露（ ）

A. 不连接不明 WIFI
B. 不点击垃圾短信中附带的网址
C. 从手机自带的应用商店下载软件，避免安装到恶意 APP
D. 为了使用便捷取消掉手机的锁屏密码
参考答案：D
难易程度：一级
解析：安全意识常识
所属知识子域：移动终端安全

183. 开启手机的丢失找回功能能做到（ ）

A. 增加手机续航
B. 对手机进行定位，必要时可远程对手机数据进行擦除，保护个人隐私安全

C. 提高手机性能
D. 防止手机被盗
参考答案：B
难易程度：一级
解析：手机丢失找回功能除了可以定位、最重要是开启了手机找回功能的同时，可以在手机丢失后，设置对数据的擦除，这样当手机连接到互联网时候，其中的数据就会自动被抹除，保障我们的重要数据和个人隐私安全。
所属知识子域：移动终端安全

184. Windows 内置的防火墙不能提供下列哪个功能（ ）

A. 对系统中的传入和传出数据进行实时监测
B. 阻挡或者允许特定程序或者端口进行连接
C. 清理系统垃圾
D. 自定义规则对出入站进行访问控制
参考答案：C
难易程度：一级
解析：Windows Defender 防火墙是微软自主研发的系统防护软件，内置在 Windows 系统中，对系统中的传入和传出数据进行实时监测，可阻挡或者允许特定程序或者端口进行连接，如果对防火墙有较好的了解，可通过设置自定义规则对出入站进行访问控制。
所属知识子域：windows 终端安全

185. 根据密码学中著名的柯克霍夫准则，目前广泛使用的密码体系安全性依赖于（ ）

A. 密钥的安全
B. 算法的复杂度
C. 对加密系统的保密
D. 对密码算法的保密
参考答案：A
难易程度：一级
解析：根据密码学中著名的柯克霍夫准则，目前广泛使用的密码体系安全性依赖于密钥的安全
所属知识子域：windows 终端数据安全

186. 为了确保计算机终端的物理安全，我们养成远离计算机就锁屏的好习惯，这个好习惯主要解决以下哪个问题？（ ）

A. 避免离开时电脑被其他人操作
B. 避免其他人搬走电脑
C. 避免其他人对电脑主机打砸损毁
D. 以上都是
参考答案：A
难易程度：一级
解析：给电脑锁屏并不能防止其他人对电脑硬件设备的操作和损毁
所属知识子域：windows 终端安全

187. windows 内置的安全中心不能提供以下那个安全功能？（ ）

A. 对系统进行实时监控
B. 数据备份
C. 计算机病毒的检测和查杀
D. 文件夹的访问限制

参考答案：B
难易程度：一级
解析：Windows 系统中的病毒防护软件，提供了对系统进行实时监控、计算机病毒的检测和查杀、文件夹的访问限制等多种功能
所属知识子域：windows 终端安全

188. 为什么需要进行数据备份（ ）

A. 确保数据的安全性
B. 防止由于操作失误或硬件损坏等原因导致数据丢失
C. 发生问题后可及时恢复
D. 以上都对
参考答案：D
难易程度：一级
解析：为了确保数据的安全性，在日常系统使用的过程中需定期进行数据备份。通过数据备份，能防止由于操作失误或硬件损坏等原因导致的数据丢失风险，可以在发生问题后立即进行恢复。
所属知识子域：windows 终端数据安全

189. 小李收到一条短信说同城的某某公司在做市场调研，点开下方的链接填写调查问卷即可获得一个礼品，小李此刻最应该做的是（ ）

A. 点开链接查看需要填写什么信息，在考虑是否填写
B. 无法确定链接是否安全，不予理会
C. 打电话询问朋友是否收到信息，如果收到即可放心填写
D. 有免费礼品拿，立即填写资料
参考答案：B
难易程度：一级
解析：在收到一些广告、推销等消息时，其中的链接不要随意打开，可能会跳转到各种钓鱼网站，挂马网页等
所属知识子域：移动终端安全

190. 自动播放功能是 Windows 系统为了方便用户而设置，默认为启动状态，当系统检测到移动设备接入时，会弹出操作提示或自动播放其中音、视频程序、运行安装软件等，U 盘病毒的传播就是依托于该功能，下列选项中对防御 U 盘病毒没有帮助的是（ ）

A. 启用 windows 系统内置的防病毒软件，并及时更新病毒库
B. 在组策略中关闭自动播放功能
C. 安装第三方的杀毒软件
D. 设置可靠的管理员账户密码
参考答案：D
难易程度：一级
解析：设置可靠的管理员账户密码可以预防暴力破解，无法抵御 U 盘病毒
所属知识子域：windows 终端安全

191. 浏览某些网站时，网站使用会话 ID 来辨别用户身份，这个会话 ID 会存储在计算机本地，用于存储的是下面选项的哪个（ ）

A. 书签
B. 收藏夹
C. 历史记录
D. Cookie

参考答案：D
难易程度：一级
解析：Cookie 是浏览器使用的文本格式的小文件，用于存储用户信息和用户偏好等信息。部分浏览器还使用 Cookie 记录用户访问某个网站的账户和密码，方便用户下次访问该网站时可直接登录而无需输入用户名和密码。
所属知识子域：web 浏览安全

192. 为了确保数据的安全性，在日常系统使用的过程中需定期进行数据备份。通过数据备份，能防止由于操作失误或硬件损坏等原因导致的数据丢失风险。但备份出来的数据也需要妥善的处理，否则会有数据泄露的风险，下列处理方式不正确的是（ ）

A. 将数据备份到 U 盘，再把 U 盘存放在安全的地方
B. 数据备份到移动硬盘，备份完毕后把硬盘锁在柜子里
C. 将备份的数据存储在自有的存储系统或私有云
D. 将敏感数据备份在公有云
参考答案：D
难易程度：一级
解析：对于数据较敏感的组织机构，数据建议在自有的存储系统或私有云进行备份，尽量不在公有云上进行备份，避免由此导致的数据泄露。
所属知识子域：windows 终端数据安全

193. 小李使用的电脑是 windows 系统，朋友建议他不要把重要文件放在 C 盘，下列观点最合理的是（ ）

A. 这种说法是错误的，重要的文件应该放在 C 盘才对
B. C 盘是用来安装操作系统的，不能存放其他的东西
C. C 盘会定期清空清空，会导致数据丢失
D. 如果系统崩溃重装电脑时需要清空 C 盘，如果没有及时备份会导致数据丢失
参考答案：D
难易程度：一级
解析：重装系统需要清空 C 盘，没有备份的话会导致数据丢失
所属知识子域：windows 终端数据安全

194. 怀疑电脑感染病毒后最合理的解决办法是（ ）

A. 格式化硬盘
B. 卸载所有软件
C. 关闭电脑永不开机，防止数据被窃取
D. 使用杀毒软件进行查杀
参考答案：D
难易程度：一级
解析：ABC 三项都不是很合理
所属知识子域：windows 终端安全

195. 在 windows 系统中，使用 win+r 快捷键打开运行后输入下列哪个选项可以打开命令提示符窗口（ ）

A. cmd
B. gpedit.msc
C. services.msc
D. notepad
参考答案：A

难易程度：一级
解析：windows 的命令提示符窗口就是 cmd
所属知识子域：windows 终端安全

196. 下列不属于 windows 系统安全加固常用方法的是（ ）

A. 启用无用的服务
B. 配置安全策略
C. 启用防火墙和系统内置的防病毒软件
D. 为系统打补丁
参考答案：A
难易程度：一级
解析：启用无用的服务会扩大攻击面
所属知识子域：windows 终端安全

197. 很多应用在做重要操作时都需要给手机发一个短信验证码，关于短信验证，以下说法哪个是正确的（ ）

A. 手机号具有唯一性，是证明实体的一个鉴别依据
B. 除短信验证码外没有其他可用的验证方式
C. 短信验证码没有泄露的分险
D. 以上都对
参考答案：A
难易程度：一级
解析：口令、二维码、短信验证码、指纹、虹膜等生物特征则是实体身份的标识，是证明实体的一个鉴别依据，而智能手机是将实体身份与互联网身份建立关联的通道。
所属知识子域:移动终端安全

198. 移动智能终端作为移动业务的综合承载平台，存储着大量应用软件数据和用户数据，这些数据都涉及到用户的商业密码或个人隐私，如果去维修设备，或者把旧手机卖给维修中心，这有可能会导致重要数据丢失和泄露，下列哪个方式无法防止设备在维修或出售时泄露数据（ ）

A. 手机需要维修时开启手机自带的维修模式
B. 维修之前，和维修商签署保密协议
C. 经常备份手机数据
D. 出售前借助安全管家类的软件进行彻底删除
参考答案：C
难易程度：一级
解析：数据备份只是保障我们的重要数据不会丢失，无法防范数据泄露
所属知识子域：移动终端安全

199. 恶意 app 对个人隐私信息及资金安全等方面所造成的威胁逐年增加，下列哪个选项可能是恶意 APP（ ）

A. 政务类 APP
B. 各大行的手机银行 APP
C. 网上下载的盗版 APP
D. 从手机自带的应用商店下载的微信、支付宝等知名 APP
参考答案：C
难易程度：一级
解析：网上下载的盗版 APP 可能被恶意篡改过，可能有安全威胁

所属知识子域：移动终端安全

200.　　下列哪个选项可能存在安全风险（ ）

A. 街头电线杆上贴的二维码

B. 垃圾短信中的网址

C. 公共场所中不需要密码的 WIFI

D. 以上都是

参考答案：D

难易程度：一级

解析：二维码实际访问的地址对用户并不直观可见，有较大的安全风险，垃圾短信中的这些网站有可能是山寨的、被恶意篡改的、带有木马及病毒的网站，用户随意接入 Wifi，可能导致接入到攻击者控制的无线接入点中，其中传输的数据会被攻击者获取。

所属知识子域：移动终端安全

201.　　某公司在对公司的电脑进行安全检查时发现很多员工的电脑密码设置的都是 123456、aaabbb 之类的弱口令，如果想让员工设置的密码必须包含大小写字母、数字、特殊字符、中的三项，可设置下列哪项（ ）

A. 开启安全设置中的密码必须符合复杂性要求

B. 开启安全设置中的账户锁定阈值

C. 在安全设置中设置密码长度最小值为 6

D. 设置密码最长使用期限

参考答案：A

难易程度：一级

解析：如果启用此策略，密码必须符合下列最低要求:不能包含用户的帐户名，不能包含用户姓名中超过两个连续字符的部分，至少有六个字符长，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 !、$、#、%)

所属知识子域：windows 终端安全

202.　　小李从二手网站买了一个 U 盘，收到货后准备使用，但由于担心 U 盘有病毒，就对电脑进行了以下操作进行防范：（1）关闭电脑自动播放功能（2）开启 windows 内置防病毒软件（3）更新病毒库（4）开启本地策略中的审核策略。这些操作中无法起到防范作用的是（）

A. 操作（1）

B. 操作（2）

C. 操作（4）

D. 操作（3）

参考答案：C

难易程度：一级

解析：审核策略的作用是通过策略设置，实现对用户操作进行审核从而形成安全日志。

所属知识子域：windows 终端安全

203.　　小李查看系统的安全日志时发现自己的账户在凌晨三点登录了系统，于是小李怀疑自己的账户密码被黑客暴力破解了，如果想预防这种情况的发生小李可开启下列哪项设置（ ）

A. 账户锁定阈值设置为 5

B. 密码必须符合复杂性要求

C. 密码长度最小值设置为 8

D. 以上都可开启
参考答案：D
难易程度：一级
解析：开启这些设置可以很好的防止暴力破解
所属知识子域：windows 终端安全

204. windows10 提供了绑定蓝牙设备来实现计算机自动锁屏的功能，当蓝牙设备离开笔记本电脑蓝牙的覆盖范围时，计算机就自动锁屏。小李有四个蓝牙设备，请问哪个最不适合用来进行绑定（ ）

A. 手机
B. 蓝牙手环
C. 蓝牙耳机
D. 蓝牙键盘
参考答案：D
难易程度：一级
解析：蓝牙键盘一般都是配合电脑使用，不会离开电脑太远距离，所以无法自动锁屏
所属知识子域：windows 终端安全

205. 网络环境的安全也是 windows 移动办公的安全威胁之一，下列哪种接入互联网的安全分险是最小的（ ）

A. 使用咖啡厅的免费 WIFI
B. 使用名为 CMCC 的免费 WIFI
C. 使用无需密码可连接的 WIFI
D. 使用自己手机开的热点
参考答案：D
难易程度：一级
解析：在公共场所，如公交车上、酒店、商场、火车站等地方的不明免费 wifi，特别是不需要密码的不要轻易连接，用于识别接入点的标识（SSID）是可以由接入设备（无线路由器）进行随意设置的，无法通过名字辨别是否安全
所属知识子域：windows 终端安全

206. 对于数据较敏感的组织机构，不应该使用下列哪种方式进行数据备份（ ）

A. 使用移动硬盘将数据完整复制一份进行保存
B. 使用专用备份软件自动比对移动硬盘上已经备份的数据与计算机终端上的数据差异，并将有变动部分备份到移动硬盘上
C. 在公有云进行数据备份
D. 在自有的存储系统进行数据备份
参考答案：C
难易程度：一级
解析：对于数据较敏感的组织机构，尽量不在公有云上进行备份，避免由此导致的数据泄露。
所属知识子域：windows 终端数据安全

207. 在 windows 系统的安全设置——密码策略设置中，一般不建议开启的设置是（ ）

A. 密码必须符合复杂性要求
B. 密码长度最小值
C. 强制密码历史
D. 用可还原的加密来储存密码
参考答案：D

难易程度：一级
解析：使用可还原的加密储存密码与储存纯文本密码在本质上是相同的，所以一般不建议启用
所属知识子域：windows 终端安全

208. 某公司在进行安全检查时发现，虽然员工会定期修改电脑密码，但大多数员工都是两个密码轮换，效果并不理想，如果想避免这种情况出现可对下列哪个选项进行设置（ ）

A. 密码策略中的强制密码历史
B. 账户锁定策略中的账户锁定阈值
C. 审核策略中的审核策略更改
D. 用户权限分配中的允许本地登录
参考答案：A
难易程度：一级
解析：开启密码策略中的强制密码历史可避免可用于轮换的密码数量太少带来的安全风险
所属知识子域：windows 终端安全

209. 对下列选项中的哪项进行配置可避免密码永不更换带来的安全风险 （ ）

A. 密码最短使用期限
B. 密码最长使用期限
C. 审核账户管理
D. 重置账户锁定计数器
参考答案：B
难易程度：一级
解析:密码最长使用期限安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间(以天为单位)。
所属知识子域：windows 终端安全

210. 如果想在 windows 安全日志中记录下创建、更改或删除帐户或组等操作，应配置下列哪个审核策略（ ）

A. 审核帐户管理
B. 审核策略更改
C. 审核系统事件
D. 审核权限使用
参考答案：A
难易程度：一级
解析：此安全设置确定是否审核计算机上的每个帐户管理事件。帐户管理事件示例包括:创建、更改或删除用户帐户或组。重命名、禁用或启用用户帐户。设置或更改密码。
所属知识子域：windows 终端安全

211. 小李在使用电脑时有以下习惯，（1）电脑密码由字母、数字、特殊字符组成（2）安装防病毒软件（3）定期为电脑中重要的数据做备份（4）离开电脑时不锁定屏幕，在这些习惯中可能存在安全风险的是（ ）

A. 习惯（1）
B. 习惯（4）
C. 习惯（3）
D. 习惯（2）
参考答案：B
难易程度：一级

解析：离开电脑时不锁定屏幕可能会被其他人操作电脑造成信息泄露等风险
所属知识子域：windows 终端安全

212. 某公司出于安全考虑对员工电脑密码设置策略做了下列要求，这些要求中不合理的是（ ）

A. 密码必须包含字母、数字、特殊字符这三项
B. 密码长度不能低于六个字符
C. 密码当中必须包含姓名简拼
D. 每三个月必须更换一次密码
参考答案：C
难易程度：一级
解析：一个安全的密码中不应该包含姓名简拼、手机号等信息
所属知识子域：windows 终端安全

213. 为防止手机丢失后，被他人取出 SIM 卡，利用其它手机启动 SIM 卡，使用短信验证，登录你的微信、支付宝等 APP，可进行下列哪项设置（ ）

A. 设置手机锁屏密码
B. 设置 PIN 密码
C. 开启垃圾短信过滤功能
D. 开启手机的自动备用功能
参考答案：B
难易程度：一级
解析：被设置 PIN 密码的 SIM 卡，换了手机需要输入 PIN 码，否则无法正常使用
所属知识子域：移动终端安全

214. 定期修改计算机密码的作用是（ ）

A. 提高系统运行速度
B. 避免密码遗忘
C. 确保密码安全性
D. 满足法律规定
参考答案：C
难易程度：一级
解析：定期更换密码可降低密码被爆破的风险
所属知识子域：windows 终端安全

215. 下列哪种方式删除的文件最彻底，最难以恢复（ ）

A. 按 shift + delete 组合键删除的文件
B. 按 delete 删除的文件
C. 在 CMD 中用 del 命令删除的文件
D. 使用文件粉碎工具删除的文件
参考答案：D
难易程度：一级
解析：文件粉碎方式，是通过反复的对文件存储的硬盘区块进行覆盖写入垃圾数据，使得原来的数据彻底被破坏，无法恢复
所属知识子域：windows 终端数据安全

216. 以下哪种行为能有效防止计算机感染病毒（ ）

A. 公司门口捡到的 U 盘直接插电脑上打开看看有什么东西
B. 随意查看不明邮件和附件

C. 安装防病毒软件，并经常更新病毒库
D. 浏览网站的过程中随意点击弹出的领奖链接
参考答案：C
难易程度：一级
解析：病毒防护软件，一般都提供了对系统进行实时监控、计算机病毒的检测和查杀
所属知识子域：windows 终端安全

217. 小李的笔记本电脑中存储着大量的隐私数据，为防止电脑丢失、被盗等物理接触方式导致数据泄露，小李想采用内置在 windows 系统中的数据加密保护机制对驱动器进行加密，下列选项中最适合小李的加密方式是（ ）

A. EFS
B. BitLocker
C. SM7
D. MD5
参考答案：B
难易程度：一级
解析：BitLocker 是从 Windows Vista 开始在系统中内置的数据加密保护机制，主要用来解决由于计算机设备丢失、被盗或者维修等物理接触方式导致的数据失窃或恶意泄露的威胁。BitLocker 可以对 Windows 系统中的驱动器进行加密，并且支持可信计算
所属知识子域：windows 终端数据安全

218. 从安全方面考虑，下列做法不正确的是（ ）

A. 为操作系统设置密码
B. 每天的工作结束后，将笔记本电脑妥善保管，如锁入文件柜
C. 设置电脑在接通电源的情况下永不锁屏
D. 离开电脑时锁定屏幕
参考答案：C
难易程度：一级
解析：接通电源的情况下永不锁屏可能会导致用户离开电脑时电脑被其他人操作导致信息泄露
所属知识子域：windows 终端安全

219. 什么是系统补丁？（ ）

A. 操作系统安全性修复程序
B. 操作系统备份数据
C. 操作系统功能升级
D. 操作系统配置文件
参考答案：A
难易程度：一级
解析：系统补丁就是用来修复操作系统漏洞的程序
所属知识子域：windows 终端安全

220. 下列关于下载安全的建议中正确的是（ ）

A. 哪个网站的资源丰富就在哪个网站下载
B. 下载时关闭杀毒软件，提高下载速度
C. 尽量下载破解版的软件
D. 只通过可信的渠道下载软件，如软件开发商官网
参考答案：D

难易程度：一级
解析：开发商官网下载的软件都是正版软件，有安全风险的可能性较低
所属知识子域：windows 终端安全

221. 下列操作中可能为 windows 系统终端带来安全威胁的是（ ）

A. 启用安全设置中的用可还原的加密来储存密码
B. 为系统更新的补丁
C. 启用 Microsofe Defender
D. 关闭不需要的服务
参考答案：A
难易程度：一级
解析：使用可还原的加密储存密码与储存纯文本密码在本质上是相同的，所以启用后可能带来安全分险
所属知识子域：windows 终端安全

222. 关于数据备份说法错误的是（ ）

A. 数据备份能恢复由于人为操作失误删除的文件
B. 备份的数据必须和源文件在同一分区中
C. 通过数据备份，能防止硬件损坏原因导致的数据丢失风险
D. 可以使用专用备份软件进行数据备份
参考答案：B
难易程度：一级
解析：备份的数据的源文件无需在同一分区，甚至无需在同一磁盘
所属知识子域：windows 终端数据安全

223. 关于 windows 系统的安全性的说法，以下哪个是正确的？（ ）

A. Windows 系统存在安全设计缺陷，所以才会总感染病毒
B. Windows 系统基本没考虑过安全问题，因此才会容易被病毒感染
C. Windows 系统的安全机制设计完善，感染病毒都是因为用户使用不当
D. Windows 系统安全机制设计完善，只是为了方便用户使用，很多安全机制默认没有启用
参考答案：D
难易程度：一级
解析：易用性和安全可以说是一对矛盾体，两者性往往不能兼顾，windows 系统为了方便用户使用默认关闭了一部分安全机制
所属知识子域：windows 终端安全

224. 我们经常从网站上下载软件，为了确保系统安全，以下哪个处理措施最正确（ ）

A. 下载完成自动安装
B. 先做系统备份，安装后有异常直接恢复系统
C. 下载后直接安装使用
D. 下载后先使用杀毒软件进行病毒查杀再安装使用
参考答案：D
难易程度：一级
解析：安装前先使用杀毒软件进行病毒查杀可降低安全风险
所属知识子域：windows 终端安全

225. 以下应对恶意ＡＰＰ安全问题正确的是（）

A. 只安装通过安全认证的 APP
B. 安装通过官网下载的 APP

C. 通过正规第三方应用商店下载 APP
D. 以上都对
参考答案：D
难易程度：一级
解析：为了防范恶意 APP，建议正规渠道下载 APP，如官方网站、正规应用商店，
所属知识子域：移动终端安全

226. 小王收到了一个发件人显示为中国银行的电子邮件，点开邮件中的链接后要求小王提供银行账户和密码，这是属于何种攻击手段（ ）

A. DDOS 攻击
B. 网页挂马
C. 网络钓鱼
D. SQL 注入
参考答案：C
难易程度：一级
解析：网络钓鱼(Phishing)是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式
所属知识子域：web 浏览安全

227. 网络钓鱼攻击主要采用的手段不包括（ ）

A. 邮件地址欺骗
B. 伪造一些知名网站的 web 页面
C. 社会工程学
D. 蜜罐技术
参考答案：D
难易程度：一级
解析：蜜罐技术是一种主动防御技术，对攻击方进行欺骗
所属知识子域：web 浏览安全

228. 你的 U 盘中有重要数据，同学临时借用，下列哪个做法最安全（ ）

A. 把 U 盘中的资料拷贝到电脑中，然后使用文件粉碎工具对 U 盘中的文件进行粉碎，再格式化 U 盘，才借给同学
B. 把资料删除后借给同学
C. 和该同学关系较好，直接借用
D. 为文件设置隐藏属性，把资料隐藏起来
参考答案：A
难易程度：一级
解析：使用文件粉碎功能删除的文件很难在恢复，所以该选项最安全
所属知识子域：windows 终端安全

229. 从安全角度来看，使用下列哪种方式接入互联网使用银行 APP 进行转账安全性最高（ ）

A. 星巴克的 WIFI
B. 自己的手机 5G 网络
C. 机场的免费 WIFI
D. 以上都对
参考答案：B
难易程度：一级

解析：不要随意连接公共网络，更不要连接后操作网银和微信转账等功能
所属知识子域：移动终端安全

230. 小王浏览网页时弹出“全网最热网游，注册即送一千元大礼包”的广告，点击广告后该网页游戏提示“您的浏览器缺少插件，请安装插件”，这种情况下如何处理最合适（ ）

A. 立即安装插件，有免费的游戏大礼包，不要白不要
B. 安装杀毒软件后再打开该页面
C. 先做系统备份，如果打开网页后有异常大不了恢复系统
D. 网页游戏一般是不需要安装插件的，这种情况骗局的可能性非常大，不安装
参考答案：D
难易程度：一级
解析：无法确定该网站是否可靠，安装插件分险太大
所属知识子域：web 浏览安全

231. 从安全的角度考虑，下列哪个上网习惯是不好的（ ）

A. 安装知名度和评价高的杀毒软件
B. 不更新软件和操作系统
C. 浏览完网页后及时清理浏览记录和 cookie
D. 只下载和安装经过签名、安全的 ActiveX 控件
参考答案：B
难易程度：一级
解析：不更新软件和操作系统可能会使一些漏洞一直存在得不到修复
所属知识子域：web 浏览安全

232. 关于如何防范钓鱼网站的做法，以下哪个选项最合适（ ）

A. 仔细核对域名
B. 查询网站备案信息
C. 查看网页有没有使用 Https 进行保护
D. 以上选项的综合使用
参考答案：D
难易程度：一级
解析：攻击者在设置钓鱼网站的地址时，选择的往往都是与仿冒网站非常相似的域名。查询网站的备案信息可以确定网站是否合规网站，没有备案信息，或备案信息与网站不一致，那么该网站的安全性就存疑了。很多网络钓鱼网站出于成本或其他原因，通常会选择 Http 这类没有加密的协议。
所属知识子域：web 浏览安全

233. 小李访问一个网站时，页面还没显示，杀毒软件就提示检测到木马病毒，小李访问的这种网站的专业名称是（ ）

A. 门户网站
B. 个人网站
C. 挂马网站
D. 购物网站
参考答案：C
难易程度：一级
解析：打开一个网站，结果页面还没显示，杀毒软件就开始报警，提示检测到木马病毒。这是网页恶意代码，这就是典型的网页挂马现象。

所属知识子域：web 浏览安全

234. 养成良好的上网习惯，有助于避免泄露重要的个人信息，以下行为中容易造成隐私泄露的是（ ）

A. 注册无法完全信任的网站时，账号密码不应该与重要网站使用的账号和密码相同

B. 为电脑设置自动锁屏

C. 定期清理网页浏览记录

D. 上网时直接关闭网页，不退出账号

参考答案：D

难易程度：一级

解析：直接关闭网页，cookies 不会被自动删除，有泄露的风险

所属知识子域：个人隐私保护

235. 下列选项中最有可能存在木马的是（ ）

A. 政务网站

B. 知名网站官网

C. 盗版软件下载网站

D. 朋友的微信二维码名片

参考答案：C

难易程度：一级

解析：盗版软件下载网站可能会存在一些木马程序

所属知识子域：web 浏览安全

236. 小张收到短信说有快递没有及时领取，请致电 XXXXX 核对，小张拨打电话后对方让小张提供了个人信息进行核对，核对完成后对方告诉小张并没有他的快递，一段时间后小张发现自己多个网站的账号提示异地登录，请问在这个事件中小张最可能遇到了下列哪种情况（ ）

A. 快递信息错误，小张账号异常的情况和此事无关

B. 小张遇到了电话诈骗，对方想欺骗小张财产

C. 对方以核对快递信息为由要到小张的一些个人信息并推断出了小张的账号密码

D. 小张的账号都使用了弱口令，所以被盗

参考答案：C

难易程度：一级

解析：对方使用社工手段骗取了小张的个人信息并推断出了密码

所属知识子域：个人隐私保护

237. 小李购买了一台液晶电视，并留了姓名、手机号、电子邮箱地址等信息方便售后，第二天他收到了一封显示发件人为电视机品牌商的中奖邮件，他按照邮件提示打开了邮件当中的链接缴纳中奖税款后并没有得到中奖奖金，再打电话询问品牌商才得知并没有举办中奖活动。根据上面的描述，由此可以推断的是（ ）

A. 品牌商把小李预留的个人信息经过了加密存储

B. 小李收到的邮件是钓鱼邮件，钱被骗了

C. 小李购买的电视可以联网

D. 小李的电脑中了木马，已经被黑客控制

参考答案：B

难易程度：一级

解析：网络钓鱼是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式。

所属知识子域：web 浏览安全

238.　　下列关于电子邮件说法错误的是（ ）

A.　电子邮件是一种信息交换的服务方式，是互联网上最古老也是应用最为广泛的服务之一。

B. 发送电子邮件时使用的协议是 SMTP 协议

C. 电子邮件不会被用来传播病毒

D. 支持多种文件格式的发送

参考答案：C

难易程度：一级

解析：邮件病毒是依托电子邮件进行传播的蠕虫病毒

所属知识子域：互联网通信安全

239.　　下列关于垃圾邮件的说法正确的是（ ）

A. 垃圾邮件是未经用户许可而发送到用户邮件地址的电子邮件

B. 邮件内容中包含垃圾字眼的就是垃圾邮件

C. 收件人事先预定的广告、电子刊物等具有宣传性质的电子邮件属于垃圾邮件

D. 和工作无关的邮件就是垃圾邮件

参考答案：A

难易程度：一级

解析：　垃圾邮件是未经用户许可而发送到用户邮件地址的电子邮件，通常情况下是各类广告、欺骗信息如赚钱、色情、赌博等。

所属知识子域：互联网通信安全

240.　　下列选项中存在安全风险的是（ ）

A. 下载软件时从开发商官网下载

B. 在不同的网站使用相同的账号密码

C. 设置密码时密码中不包含个人名字简拼等信息

D. 不随意点击浏览网页时弹出的广告

参考答案：B

难易程度：一级

解析：使用相同的密码的话一个网站的密码泄露会导致所有网站账号都不安全

所属知识子域：web 浏览安全

241.　　以下对防范网络钓鱼无效的做法是（　）

A. 不要响应要求个人金融信息的邮件

B. 经常修改社交网站的密码

C. 谨慎对待邮件和个人数据

D. 访问站点时核实网址和网站备案信息

参考答案：B

难易程度：一级

解析：网络钓鱼是攻击者利用欺骗性的电子邮件或其他方式将用户引导到伪造的 Web 页面来实施网络诈骗的一种攻击方式，修改社交网站的密码对防范网络钓鱼作用不大

所属知识子域：web 浏览安全

242.　　下列防范钓鱼网站的做法哪个是错误的（ ）

A. 浏览网站时通过网站备案信息查询网站真伪

B. 对包含中奖、退税等字眼的邮件和短信提高警惕，不随意点击附带的链接

C. 打开网站前仔细核对网址

D. 为提高系统性能上网时退出杀毒软件等消耗资源的网站
参考答案：D
难易程度：一级
解析：关闭杀毒软件上网时得不到相应的保护，会造成安全风险
所属知识子域：web 浏览安全

243. 为保证安全，在使用浏览器浏览网页时，以下那条是正确的（ ）

A. 所有网站都可以浏览
B. 只浏览证实为安全，合法的网站
C. 只要不是有反动言论的网站都可以浏览
D. 只要不是盗版软件下载网站都可以浏览
参考答案：B
难易程度：一级
解析：并不是只有盗版软件下载网站和拥有反动言论的网站会有安全风险
所属知识子域：web 浏览安全

244. 电子邮件的安全威胁不包括（ ）

A. 邮件地址欺骗
C. 使用公共 WIFI 收发电子邮件
D. 垃圾邮件
E. FTP 协议的相关漏洞
参考答案：D
难易程度：一级
解析：常用的电子邮件协议有 SMTP、POP3、IMAP4，FTP 协议是文件传输协议和电子邮件关系不大
所属知识子域：互联网通信安全

245. 常见的邮件欺骗方式有（ ）

A. 相似域名仿冒
B. 仿冒企业邮件
C. 仿冒发件人别名
D. 以上都是
参考答案：D
难易程度：一级
解析：常见的邮件欺诈方式有：仿冒发件人别名、相似域名仿冒、商业邮件诈骗、仿冒企业邮件等等
所属知识子域：互联网通信安全

246. 下列选项中对防止垃圾邮件没有作用的是（ ）

A. 不随意公开邮箱地址
B. 使用好邮件管理、黑白名单功能
C. 定期备份邮件
D. 使用专业的反垃圾邮件软件
参考答案：C
难易程度：一级
解析：定期备份邮件能防止重要邮件丢失但不能防止垃圾邮件
所属知识子域：互联网通信安全

247. 电子邮箱密码应该设置成下列哪种安全性最高（ ）

A. 姓名简拼+手机号
B. 取一段歌词或者诗歌，再把每个字的拼音首字母取出来，加上大小写和标点符号组成的密码
C. 姓名简拼+出生年月日
D. 键盘上相邻的按键
参考答案：B
难易程度：一级
解析：这种密码很好记，但是却极难猜测和破解，是安全性较高的密码
所属知识子域：互联网通信安全

248. 以下选项关于电子邮件存在的安全隐患说法不准确的是（ ）
A. 电子邮件传输协议不加密
B. 攻击者可能通过自建 SMTP 服务器来实现发送伪造地址的邮件
C. 电子邮件缺乏对发送者严格的身份验证机制
D. 电子邮件的使用者都缺乏安全意识
参考答案：D
难易程度：一级
解析：D 选项说法过于绝对
所属知识子域：互联网通信安全

249. 小张在某网站上找到了一篇他需要的资料，可以免费下载，但是下载要求在网站上使用邮箱进行注册，以下哪个做法是最正确的（ ）
A. 使用自己常用的邮箱进行注册，并把密码设置为和自己邮箱相同，便于记忆
B. 使用自己常用的邮箱进行注册，把网站密码设置和邮箱不同的密码
C. 单独申请一个邮箱用来注册不常用的网站，密码单独设置
D. 不注册，不下载了
参考答案：C
难易程度：一级
解析：C 选项安全性最高
所属知识子域：互联网通信安全

250. 下列是小张在使用电子邮件时的一些做法，这些做法中不正确的是（ ）
A. 使用垃圾邮件过滤功能
B. 使用最新版本的电子邮件客户端
C. 直接打开邮件中的附件
D. 为邮箱设置安全的密码
参考答案：C
难易程度：一级
解析：邮件中的附件可能含有病毒，应该先用杀毒软件等查杀后再打开
所属知识子域：互联网通信安全

251. 我们在配置电子邮件客户端时，从安全的角度来看，哪种说法最合适（ ）
A. 启用电子邮件客户端软件对 SSL 的支持选项，可以对邮件进行加密和签名
B. 不启用电子邮件客户端软件对 SSL 的支持选项，影响性能
C. 不启用电子邮件客户端软件对 SSL 的支持选项，因为启用后没有区别，浪费时间
D. 看情况，一般不需要启用 SSL 支持选项
参考答案：A
难易程度：一级

解析：未经加密的邮件很容易被攻击者获取，应该启用电子邮件客户端软件对 SSL 的支持选项
所属知识子域：互联网通信安全

252.　　下列哪个选项不属于即时通信应用（ ）

A. QQ
B. 网易新闻
C. 微信
D. 钉钉
参考答案：B
难易程度：一级
解析：即时通信软件是通过即时通信技术来实现在线聊天、交流的软件
所属知识子域：互联网通信安全

253.　　邮件炸弹攻击原理是（ ）

A. 对受害者服务器发起拒绝服务攻击，使受害者无法接收邮件
B. 窃取受害者邮箱密码
C. 消耗受害者的邮箱空间
D. 攻击受害者电脑，向电脑内植入木马
参考答案：C
难易程度：一级
解析：邮件炸弹是通过向接收者的邮件地址发送大量的电子邮件，消耗接收者的邮箱空间，最终因空间不足而无法接收新的邮件，导致其他用户发送的电子邮件被丢失或退回。
所属知识子域：互联网通信安全

254.　　下面哪些不属于即时通信存在的安全风险（ ）

A. 恶意代码传播
B. 网络欺诈
C. 即时通信系统自身安全问题
D. 操作系统漏洞利用
参考答案：D
难易程度：一级
解析：即时通信应用系统所面临的安全问题包括：即时通信应用信息系统自身安全风险、利用即时通信传播恶意代码、利用即时通信破坏防御系统、网络欺诈及非法信息
所属知识子域：互联网通信安全

255.　　以下哪种关系，更容易被即时通信中的安全威胁利用（ ）

A. 自己的领导
B. 陌生人
C. 不熟悉的朋友
D. 拉黑的联系人
参考答案：A
难易程度：一级
解析：大多数人对于自己的领导都有较高信任度，所以更容易被利用
所属知识子域：互联网通信安全

256.　　当你收到一份邮件时，比较安全的处理办法是（ ）

A. 确定发件人是否可信，然后使用杀毒软件对附件进行查杀后在查看
B. 直接打开附件

C. 只要邮件是认识的人发来的，那它就是安全的
D. 按照邮件中的要求填写个人详细信息
参考答案：A
难易程度：一级
解析：确定发件人是否可信后使用杀毒软件对附件进行查杀后在查看可有效的降低安全风险
所属知识子域：互联网通信安全

257. 随着电子邮件的广泛应用，电子邮件面临的安全威胁越来越多，攻击者可能通过恶意邮件来控制主机，下列设置中不安全的是（ ）

A. 以超文本格式读取所有邮件
B. 禁止自动下载附件
C. 禁止使用不信任的宏
D. 启用垃圾邮件过滤
参考答案：A
难易程度：一级
解析：应该设置为以纯文本形式约定邮件
所属知识子域：互联网通信安全

258. 钓鱼邮件是电子邮件的常见风险之一，针对钓鱼邮件，应采取下列哪种安全措施（ ）

A. 设置安全性高的密码
B. 使用邮件客户端接收邮件
C. 不轻易打开包含中奖等字眼的邮件
D. 使用自建的 SMTP 服务器
参考答案：C
难易程度：一级
解析：A、B、D 三项均无法对钓鱼邮件产生防御效果，防范钓鱼邮件应提高自身安全意识，不要轻易点击不明邮件
所属知识子域：互联网通信安全

259. 小张的邮箱突然收到了大量的垃圾邮件，占满了邮箱空间导致无法接受新的邮件，小张受到的这种攻击方式叫做（ ）

A. 邮件炸弹
B. 邮件病毒
C. 邮件地址欺骗
D. 暴力破解
参考答案：A
难易程度：一级
解析：邮件炸弹是垃圾邮件的一种，通过向接收者的邮件地址发送大量的电子邮件，消耗接收者的邮箱空间，最终因空间不足而无法接收新的邮件，导致其他用户发送的电子邮件被丢失或退回。
所属知识子域：互联网通信安全

260. 小李收到一封电子邮件，自称是某银行，提示说小李在该银行的账户出现问题已被冻结，让小李回信提供账户信息，核对完成后解冻，这种攻击方式叫做（ ）

A. 拒绝服务攻击
B. 钓鱼邮件
C. 邮件病毒

D. 缓存区溢出
参考答案：B
难易程度：一级
解析：钓鱼邮件指利用伪装的电邮，欺骗收件人将账号、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，如银行或理财的网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等而被盗取。
所属知识子域：互联网通信安全

261. 收到垃圾邮件后下列哪种处理方式最合适（ ）

A. 回信将发件人骂一顿
B. 点开看看有没有感兴趣的东西
C. 删除该邮件，并将该邮件的发件人拉入黑名单
D. 转发该邮件给其他人
参考答案：C
难易程度：一级
解析：通过设置黑白名单对垃圾邮件进行过滤，这是防范垃圾最直接也是最简单有效的方式
所属知识子域：互联网通信安全

262. 收到一封来自陌生人且含有附件的邮件，应该怎么处理（ ）

A. 转发给朋友，让朋友打开
B. 直接打开附件查看
C. 回复该邮件，询问是否有病毒
D. 直接删除该邮件
参考答案：D
难易程度：一级
解析：D 选项最合适
所属知识子域：互联网通信安全

263. 邮件炸弹攻击是（ ）

A. 破坏受害者的邮箱服务器
B. 消耗受害者的邮箱空间
C. 破坏受害者的邮件客户端
D. 破坏受害者的电脑
参考答案：B
难易程度：一级
解析：邮件炸弹是通过向接收者的邮件地址发送大量的电子邮件，消耗接收者的邮箱空间，最终因空间不足而无法接收新的邮件，导致其他用户发送的电子邮件被丢失或退回。
所属知识子域：互联网通信安全

264. 以下防范即时通信安全威胁做法错误的是（ ）

A. 聊天时不发送个人敏感信息
B. 进行转账等操作时通过电话等可靠渠道二次确认
C. 不随意点击群里的链接
D. 在朋友圈发布自己在工作单位的自拍照
参考答案：D
难易程度：一级
解析：随意发布自己在工作单位的自拍照会有敏感信息泄露等风险
所属知识子域：互联网通信安全

265. 邮箱中收到了一封广告邮件，新款 iphone12 开启预售，只要在链接中的页面中留下手机号码和身份证信息，在 iphone12 发布时就能比发行价格便宜 1000 元购买 iphone12，关于这样的广告邮件，以下哪个做法是最合适的（ ）

A. 不予理会，直接删除

B. 把手机号和身份证号提交了，能便宜 1000 呢

C. 点开链接查看一下，又不会损失什么

D. 以上做法都可以

参考答案：A

难易程度：一级

解析：很有可能是钓鱼邮件，直接删除最安全

所属知识子域：互联网通信安全

266. 下列哪项是正确使用邮箱的方式（ ）

A. 为工作邮箱和个人邮箱设置不同的密码

B. 为工作邮箱设置易于记忆的密码，例如 123456

C. 使用工作邮箱发送和工作无关的邮件给同事

D. 关闭邮箱的 SSL 支持选项

参考答案：A

难易程度：一级

解析：设置不同的密码可以防止一个密码泄露影响两个邮箱安全

所属知识子域：互联网通信安全

267. 即时通信是目前使用最为普遍的网络应用之一，下列关于及时通信安全防范错误的是（ ）

A. 重要的文件资料等不要通过即时通信传输

B. 在其他人的电脑上登录时不要启用自动登录功能

C. 即时通信应用中的好友都认识，可以传输和讨论一些敏感信息

D. 即时通信软件的加密措施很安全，可以用来传输敏感信息

参考答案：A

难易程度：一级

解析：如果使用即时通信传输敏感信息，攻击者通过攻击即时通信用户获得登录身份后，会收集到大量用户的敏感信息，甚至伪装成用户实施其他类型的攻击

所属知识子域：互联网通信安全

268. 下列哪个选项不是即时通信应用系统所面临的安全问题（ ）

A. 传播恶意代码

B. 伪造人设取得好感后实施诈骗

C. 损坏手机硬件

D. 散播非法信息

参考答案：C

难易程度：一级

解析:即时通信应用系统所面临的安全问题包括：即时通信应用信息系统自身安全风险、利用即时通信传播恶意代码、利用即时通信破坏防御系统、网络欺诈及非法信息

所属知识子域：互联网通信安全

269. 微信突然收到好友发来的一个网络投票链接，最合理的处理方式是（ ）

A. 打电话和朋友确认不是被盗号，并确认投票原因和内容后，再酌情考虑是否投票

B. 不投票，假装没有看到

C. 把好友拉黑
D. 和朋友关系很好，直接打开投票链接
参考答案：A
难易程度：一级
解析：因为有安全风险，所以要和好友确认后再决定是否投票
所属知识子域：互联网通信安全

270. 如果将未经处理的信息发布在朋友圈、微博、论坛等社交媒体中可能造成（ ）

A. 信息泄露
B. 信息丢失
C. 信息篡改
D. 信息拦截
参考答案：A
难易程度：一级
解析：攻击者可能通过搜索引擎，报纸、杂志、文库等各类媒体，微博、论坛、社交网站等各类社交媒体收集到你的信息，造成信息泄露
所属知识子域：个人隐私保护

271. 下列关于保护个人信息做法错误的是（ ）

A. 在朋友圈微博等社交媒体发布火车票、飞机票、护照、日程、行踪等
B. 只从手机自带的应用商店和软件开发商官网下载应用
C. 填写调查问卷时尽量不使用真实的个人信息
D. 在打印店等公众场合登录账号时不使用自动保存密码功能，且在离开时手动退出账号
参考答案：A
难易程度：一级
解析：在朋友圈微博等社交媒体发布火车票、飞机票、护照、日程、行踪等可能会导致个人信息泄露
所属知识子域：个人隐私保护

272. 下列预防个人信息泄露的做法错误的是（ ）

A. 增强个人信息安全意识，不要轻易将个人信息提供给无关人员
B. 及时撕毁快递单等包含个人信息的单据
C. 经常参加发起方不明但赠送小礼品的调查活动
D. 尽量不注册不知名的网站
参考答案：C
难易程度：一级
解析：经常参加发起方不明但赠送小礼品的调查活动有信息泄露的风险
所属知识子域：个人隐私保护

273. 在日常生活中，下列哪个做法可以降低我们信息泄露的风险（ ）

A. 定期更换各类平台的密码
B. 离开电脑时不锁屏
C. 在朋友圈晒各类纪念日
D. 拆过的快递盒随意丢弃
参考答案：A
难易程度：一级
解析：定期更换密码可以降低密码被攻击者猜到的可能性
所属知识子域：个人隐私保护

274. 养成良好的 APP 使用习惯可以降低个人信息泄露的风险，下列 APP 使用习惯中不正确的是（）

A. 不使用强制收集个人信息的 APP

B. 不使用破解版 APP

C. 为了多获取积分，填写真实姓名、出生日期、所从事的行业等各种详细的个人信息

D. 不被赚钱等噱头迷惑，安装不可信的 APP

参考答案：C

难易程度：二级

解析：填写太过细致的个人信息可能会导致个人信息泄露

所属知识子域：个人隐私保护

275. 下列哪种做法可能会造成个人隐私泄露（ ）

A. 为手机设置锁屏密码

B. 不使用公共场所中的 wifi

C. 为防止遗忘密码把账号密码写在便利贴并贴在办公桌上

D. 不在朋友圈发布生日纪念日等信息

参考答案：C

难易程度：二级

解析：把账号密码写在便利贴并贴在办公桌上容易被路过的人看到

所属知识子域：个人隐私保护

276. 以下可能会造成信息泄露的是（ ）

A. 将含有机密信息的文件锁在柜中

B. 复制和打印的资料及时拿走

C. 在微博等社交媒体谈论公司信息

D. 离开时，锁定电脑屏幕

参考答案：C

难易程度：二级

解析：在社交媒体谈论公司信息可能会被别有用心的人看到，造成信息泄露

所属知识子域：个人隐私保护

277. 二维码是现在生活中非常重要的一部分，但随意二维码可能带来信息泄露等安全风险，下列选项中相对安全的是（ ）

A. 朋友圈中微商发布的二维码

B. 小道消息得来的信用卡提额二维码

C. 街头扫描送礼品的二维码

D. 在官网下载的 APP 时扫描的官方公众号二维码

参考答案：D

难易程度：二级

解析：官网的公众号二维码一般都是安全的

所属知识子域：个人隐私保护

278. 邮件病毒是电子邮件的安全威胁之一，为防止邮件中恶意代码的攻击，应该使用下列哪种方式阅读电子邮件（ ）

A. 纯文本

B. 网页

C. 程序

D. 会话

参考答案：A
难易程度：二级
解析：以纯文本文件形式阅读一般可避免邮件中恶意代码的攻击
所属知识子域：互联网通信安全

279. SMTP/POP3 两个协议在传输数据时是明文传输，下列最可能产生的安全风险是（）

A. 信息泄露
B. 信息伪造
C. 信息丢失
D. 信息篡改
参考答案：A
难易程度：二级
解析：相较于其他选项，信息被截获泄露是最容易发生的
所属知识子域：互联网通信安全

280. https 是很多网站采用的网页访问协议，以下关于 https 与 http 相比的优势说法正确的是（ ）

A. https 访问速度比 http 快
B. https 安全性比 http 高
C. https 对服务器资源的占用小于 http
D. https 性能比 http 要好
参考答案：B
难易程度：二级
解析：https 是基于 HTTP 协议，通过 SSL 或 TLS 提供加密处理数据、验证对方身份以及数据完整性保护，安全性方面要优于 http
所属知识子域：web 浏览安全

281. 在 windows 系统中隐藏文件和系统文件默认是不可见的，在 cmd.exe 中，以下哪个命令可以列举出隐藏文件和系统文件？

A. dir /a
B. dir /q
C. dir /s
D. dir /l
参考答案：A
难易程度：二级
解析： /q 显示文件所有者、/s 显示指定目录和所有子目录中的文件、/l 用小写显示
所属知识子域：windows 终端安全

282. Windows 系统默认隐藏扩展名，在 Windows 的“资源管理器”窗口中，为了改变扩展名的显示情况，应首先选用的菜单是（ ）

A. 文件
B. 编辑
C. 查看
D. 工具
参考答案：C
难易程度：二级
解析：点击查看后勾选文件扩展名选项即可
所属知识子域：windows 终端安全

283. 通过扫描发现系统漏洞后，可通过以下哪种方式来弥补漏洞（ ）

A. 安装系统补丁

B. 重装系统

C. 卸载所有软件

D. 利用杀毒软件进行杀毒

参考答案：A

难易程度：二级

解析：安装系统补丁，就是通过安装相应的补丁软件，补上系统中的漏洞

所属知识子域：windows 终端安全

284. 在 windows 系统中，我们对安全配置进行设置，关闭一些不必要的服务等安全配置称之为安全加固，那么 Windows 安全加固的作用不包括（ ）

A. 增强系统安全性

B. 消除不合理的配置

C. 防止硬件损坏

D. 以上都是

参考答案：C

难易程度：二级

解析：windows 安全加固是针对系统及软件层面的一些安全配置

所属知识子域：windows 终端安全

285. 下列关于计算机木马的说法错误的是（ ）

A. 尽量访问知名网站能减少感染木马的概率

B. 随意安装不可靠的软件可能会感染木马程序

C. 只要不访问互联网，就能避免受到木马侵害

D. 杀毒软件对防止木马病毒具有重要作用

参考答案：C

难易程度：二级

解析：不访问互联网也可能受到木马的侵害

所属知识子域：windows 终端安全

286. 发送电子邮件时通常需要使用的协议是（ ）

A. 只用 SMTP

B. 只用 POP3

C. SMTP 和 POP3 都需要

D. 以上都不对

参考答案：A

难易程度：二级

解析：SMTP 协议是发送电子邮件时用的协议，POP3 是接收邮件时用的协议

所属知识子域：互联网通信安全

287. 为了防止系统崩溃或重装系统导致密钥丢失从而无法解密数据，在使用 EFS 时应进入证书管理器将密钥备份出来并保存在安全的地方。下列哪个操作可打开证书管理器（ ）

A. win+r 组合键打开运行后执行 certmgr.msc

B. win+r 组合键打开运行后执行 compmgmt.msc

C. win+r 组合键打开运行后执行 services.msc

D. win+r 组合键打开运行后执行 regedit

参考答案：A
难易程度：二级
解析：具体操作方式为执行 certmgr.msc 打开证书管理器，在个人的证书下可以找到一个以当前用户名命名的证书，执行证书的“导出”操作，按照引导进行操作就能将证书导出
所属知识子域：windows 终端数据安全

288. 为了保证 windows 系统的安全，我们可以设置账户密码的最长使用期限来强制用户定期修改密码，如果我们在安全设置中将密码最长使用期限设置为了 0，那么（ ）

A. 该账户密码永不过期
B. 该账户每次注销时都需要修改密码作为下次登陆时的凭据
C. 该账户被锁定，无法登陆
D. 该账户被立即禁用
参考答案：A
难易程度：二级
解析：此安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间(以天为单位)。可以将密码设置为在某些天数(介于 1 到 999 之间)后到期，或者将天数设置为 0，指定密码永不过期
所属知识子域：windows 终端安全

289. 在 windows 系统中如果想禁止外网访问自己的某个端口可以（ ）

A. 设置防火墙的出站规则
B. 设置防火墙的入站规则
C. 无须设置
D. 以上都不对
参考答案：B
难易程度：二级
解析：出站规则就是本机访问外网、入站规则就是外网访问本机
所属知识子域：windows 终端安全

290. 在安全设置的账户策略中开启密码必须符合复杂性要求，设置密码长度最小值为 2，那么在实际使用中，用户可设置的密码最小长度是（ ）

A. 6
B. 3
C. 2
D. 8
参考答案：C
难易程度：三级
解析：密码长度最小值为 2，所以密码长度设置范围为 2 到 14 个字符，但因为开启了密码必须符合复杂性要求所以密码必须包含大小写字母、数字、特殊字符其中的三项
所属知识子域：windows 终端安全

291. 关闭 windows 系统的 445 端口后无法使用下列哪个功能（ ）

A. 共享文件夹
B. 远程桌面
C. Telnet
D. FTP
参考答案：A
难易程度：三级

解析：远程桌面端口 3389、Telnet 端口 23、FTP 端口 21
所属知识子域：windows 终端安全

292. 在安全检查时我们有时需要查看计算机有没有开放可疑的端口号，在 windows 系统中用来查看端口情况的命令是（ ）

A. netstat
B. ping
C. ipconfig
D. cls
参考答案：A
难易程度：三级
解析：ping 用于检测网络是否通畅、ipconfig 查看电脑的 ip 地址信息、cls 清除当前屏幕内容
所属知识子域：windows 终端安全

293. 以下关于盗版软件的说法，错误的是（）

A. 可能会包含不健康的内容
B. 若出现问题可以找开发商负责赔偿损失
C. 使用盗版软件就是违法的
D. 成为计算机病毒的重要来源与传播途径之一
参考答案：B
难易程度：三级
解析：使用盗版软件本身就是违法行为，出现问题不会得到法律的支持，所以选 B
所属知识子域：windows 终端安全

294. 以下哪个不是做好软件安全测试的必要条件？ （）

A. 充分了解软件安全漏洞
B. 拥有软件的全部开发过程文档和源代码
C. 评估软件安全风险
D. 高效的软件安全测试技术和工具
参考答案：B
难易程度：三级
解析：
所属知识子域：windows 终端安全

295. 传输层协议允许应用程序同其他应用程序通信。以下属于传输层协议的是（）

A. TCP
B. ipconfig
C. ping
D. register
参考答案：A
难易程度：三级
解析：
所属知识子域：windows 终端安全

296. 公钥算法中，（）用来解密和签名

A. 公钥
B. 私钥
C. 数字证书

D. 注册中心
参考答案：B
难易程度：三级
解析：
所属知识子域：windows 终端安全

297. 计算机操作系统是管理和控制计算机软硬件资源的计算机程序。以下不属于操作系统基本特征是（）

A. 共享性
B. 并发性
C. 封闭性
D. 异步性
参考答案：C
难易程度：三级
解析：操作系统的基本特征有并发性、共享性、随机性、异步性、虚拟（virtual）
所属知识子域：windows 终端安全

298. 现已产生多种方法可用于鉴别病毒，下列选项中，利用病毒的特有行为特征来监测病毒的方法被称为（）

A. 代码测试法
B. 校验和法
C. 行为监测法
D. 软件模拟法
参考答案：C
难易程度：三级
解析：
所属知识子域：windows 终端安全

299. 容灾系统可用性与指标 RPO、RTO 的关系是（ ）

A. RPO 和 RTO 越大，可用性越大
B. RPO 和 RTO 越小，可用性越大
C. RPO 越大，RTO 越小，可用性越大
D. RPO 越小，RTO 越大，可用性越大
参考答案：B
难易程度：三级
解析：理论上 RPO 和 RTO 可以为 0，越大则代表效果差，损失越大
所属知识子域：windows 终端安全

300.( )游戏是计算机病毒的第一个雏形，体现了病毒自我复制的基本思想

A. 星际大战
B. 群雄争霸
C. 磁芯大战
D. 以上都不正确
参考答案：C
难易程度：三级
解析：磁芯大战(core war or core wars)就是汇编程序间的大战，程序在虚拟机中运行，并试图破坏其他程序，生存到最后即为胜者。会自我繁殖的程序
所属知识子域：windows 终端安全