

中共泉州师范学院委员会 网络安全与信息化领导小组办公室文件

泉师委网信办〔2020〕3号

中共泉州师范学院委员会网信办 中共泉州师范学院学生工作部 关于开展2020年网络安全知识答题学习活动的通知

各二级党委（党总支）：

为深入学习贯彻习近平总书记关于网络强国的重要思想，贯彻落实中央、省、市网络安全工作部署，进一步提升学生网络安全意识和管理水平，校网信办、学工部决定联合开展2020年网络安全知识答题学习活动。有关事项通知如下：

一、活动主题

网络安全为人民，网络安全靠人民。

二、活动时间

2020年9月15-30日

三、参加对象

全校学生

四、活动内容

组织全校学生认真学习习近平总书记关于网络强国的重要

思想和《中华人民共和国网络安全法》，以及个人网络安全防护技能、风险识别能力、公共基础设施检查等网络安全应知应会知识等。

五、参与方式

（一）组织学习。各二级党委（党总支）组织学生认真学习《网络安全知识学习材料》（附件1），学习网络安全相关知识。

（二）组织答题。各二级党委（党总支）将《网络安全宣传周“百问百答”试题题库》（附件2）分发给学生，组织学生登录易班平台答题。易班平台从题库中随机抽取题目生成试卷。

学习材料和试题也可以登录校园网进行下载。

六、有关要求

（一）要加强组织领导。答题学习活动是落实国家网络安全宣传周活动的主要载体，是普及网络安全管理知识的有效措施。各二级党委（党总支）要高度重视，切实履行网络意识形态工作责任制，精心组织学生认真开展答题学习活动。

（二）要增强学习实效。全校学生要自觉加强习近平总书记关于网络强国的重要思想和网络安全知识的学习，通过答题学习活动，切实树立正确的网络安全观，提高自身网络安全意识和防护技能，营造浓厚学习氛围。

（三）要认真做好总结。答题学习活动结束后，各二级党委（党总支）应及时将相关情况报校网信办（邮箱：

xw@qztc.edu.cn)。

附件：

1. 《网络安全知识学习材料》
2. 《网络安全宣传周“百问百答”试题题库》

中共泉州师范学院委员会网络安全与信息化领导小组办公室

中共泉州师范学院学生工作部

2020年9月15日

网络安全知识学习材料

一、习近平关于网络强国的讲话

1、没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。要依法严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，切断网络犯罪利益链条，持续形成高压态势，维护人民群众合法权益。要深入开展网络安全知识技能宣传普及，提高广大人民群众网络安全意识和防护技能。

2、核心技术是国之重器。要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。要抓产业体系建设，在技术、产业、政策上共同发力。要遵循技术发展规律，做好体系化技术布局，优中选优、重点突破。要加强集中统一领导，完善金融、财税、国际贸易、人才、知识产权保护等制度环境，优化市场环境，更好释放各类创新主体创新活力。要培育公平的市场环境，强化知识产权保护，反对垄断和不正当竞争。要打通基础研究和技术创新衔接的绿色通道，力争以基础研究带动应用技术群体突破。

3、网信事业代表着新的生产力和新的发展方向，应该在践行新发展理念上先行一步，围绕建设现代化经济体系、实现高质量发展，加快信息化发展，整体带动和提升新型工业化、城镇化、农业现代化发展。要发展数字经济，加快推动数字产业化，依靠信息技术创新驱动，不断催生新产业新业态新模式，用新动能推动新发展。要推动产业数字化，利用互联网新技术新应用对传统产业进行全方位、全角度、全链条的改造，提高全要素生产率，释放数字对经济发展的放大、叠加、倍增作用。要推动互联网、大数据、人工智能和实体经济深度融合，加快制造业、农业、服务业数字化、网络化、智能化。要坚定不移支持网信企业做大做强，加强规范引导，促进其健康有序发展。企业发展要坚持经济效益和社会效益相统一，更好承担起社会责任和道德责任。要运用信息化手段推进政务公开、党务公开，加快推进电子政务，构建全流程一体化在线服务平台，更好解决企业和群众反映强烈的办事难、办事慢、办事繁的问题。网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点，让人民群众在信息化发展中有更多获得感、幸福感、安全感。

4、网信军民融合是军民融合的重点领域和前沿领域，也是军民融合最具活力和潜力的领域。要抓住当前信息技术变革和新军事变革的历史机遇，深刻理解生产力和战斗力、市场和战场的内在关系，把握网信军民融合的工作机理和规律，推动形成全要素、多领域、高效益的军民深度融合发展的格局。

5、推进全球互联网治理体系变革是大势所趋、人心所向。国际网络空间治理应该坚持多边参与、多方参与，发挥政府、

国际组织、互联网企业、技术社群、民间机构、公民个人等各种主体作用。既要推动联合国框架内的网络治理，也要更好发挥各类非国家行为体的积极作用。要以“一带一路”建设等为契机，加强同沿线国家特别是发展中国家在网络基础设施建设、数字经济、网络安全等方面的合作，建设 21 世纪数字丝绸之路。

6、要加强党中央对网信工作的集中统一领导，确保网信事业始终沿着正确方向前进。各地区各部门要高度重视网信工作，将其纳入重点工作计划和重要议事日程，及时解决新情况新问题。要充分发挥工青妇等群团组织优势，发挥好企业、科研院所、智库等作用，汇聚全社会力量齐心协力推动网信工作。各级领导干部特别是高级干部要主动适应信息化要求、强化互联网思维，不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力。各级党政机关和领导干部要提高通过互联网组织群众、宣传群众、引导群众、服务群众的本领。要推动依法管网、依法办网、依法上网，确保互联网在法治轨道上健康运行。要研究制定网信领域人才发展整体规划，推动人才发展体制机制改革，让人才的创造活力竞相迸发、聪明才智充分涌流。要不断增强“四个意识”，坚持把党的政治建设摆在首位，加大力度建好队伍、全面从严管好队伍，选好配好各级网信领导干部，为网信事业发展提供坚强的组织和队伍保障。

二、网络安全法相关法律法规

1、《中华人民共和国网络安全法》开始实施的时间为 2017 年 6 月 1 日。

2、《中华人民共和国网络安全法》规定网络运营者应当制定网络安全应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络入侵等安全风险。

3、违反《中华人民共和国网络安全法》第 27 条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他们从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处 5 日以下拘留，可以并处五万元以上五十万元罚款。

4、网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

5、国家网信部门负责统筹协调网络安全工作和相关监督管理工作。

6、关键信息基础设施的运营者应当自行或者委托网络安全服务机构至少每年一次对其网络的安全性和可能存在的风险检测评估。

7、因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

8、国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、风险评估、监测等安全服务。

三、网络安全基础知识学习

1、当您准备登录电脑系统时，有人在您的旁边看着您，应该友好的提示对方避让一下，不要看您的机密。

2、社会工程学主要是通过对人的研究，利用人们的心理弱点实施的一中欺骗的手段。社会工程学的主要目的不是破坏。

3、社会工程学常被黑客用于口令获取。

4、1-3 个月更换一次计算机的密码较为安全。

5、通过限制密码错误次数，定期更换密码方式可以有效防止暴力破解。

6、为了有效保证操作系统或邮箱密码安全可将密码记录在隐秘的地方，保证密码口令一定的复杂度，需使用大写字母、小写字母、数字、特殊字符等；避免使用少于 8 位的短密码，同时密码应该定期更换，避免使用生日或者 ID 号码作为密码使用。

7、严格限定从一个给定的终端进行非法认证的次数、防止用户使用太短的口令、使用机器产生的口令属于防止口令猜测的措施。

8、不同重要程度的账号设置不同的密码，用以减少密码泄露带来的影响。

9、让浏览器记住访问某网站的用户名和口令，安全性会有大问题。

10、邮件在内部和外部网络上传输的过程中如果不加明文传输，可能会被人通过网络中串联或旁路监听的设备抓取并还原内容，造成邮件中信息泄密。

11、通过浏览网页、收发邮件、使用 U 盘或移动存储介质等方式都可能导致感染恶意代码。

12、关于安全计算机更新应该及时更新最新的补丁程序并及时重启计算机。尽可能规避第三方网站下载更新。

13、计算机被感染病毒的特征为出现不知名文件、后台未知程序运行等特征。

14、信息安全的威胁有木马病毒、蠕虫病毒等恶意代码；信息安全部门不作为；人员普遍缺乏安全意识；信息安全产品和设备不够先进。其中最大的威胁来源于人员普遍缺乏安全意识。

15、在大多数情况下，病毒侵入计算机系统以后一般并不立即发作，等到满足某种条件的时候，才会出来活动捣乱、破坏。

16、对防病毒工作的检查包括防病毒的安装情况、防病毒制度的执行情况、病毒事件的处理情况。

17、属于计算机病毒感染的特征文件长度增加、软件运行速度减慢、端口异常。

18、我们经常从网站上下载文件、软件，为了确保系统安全，应当先进性查杀病毒后再使用。

19、应用软件最好在官方网站下载，防止恶意软件捆绑在安装程序中。

20、在某电子商务网站购物时，卖家突然说交易出现异常，并推荐处理异常的客服人员。最恰当的做法是通过电子商务官网上寻找正规的客服电话或联系方式，并进行核实。

21、信息安全的基本属性保密性、完整性、可用性。

22、在公共电脑中不存放个人资料和账号信息。

23、小王是某公司的员工，正当他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”，如身份不明确，电话号码不认识，应直接拒绝。

24、许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是给系统安装最新的补丁。

25、及时安装系统补丁、定期进行漏洞扫描、加强安全设备的监控和管理能提高防病毒工作的实施效果。

26、系统已打了最新的补丁，防病毒软件也更新了最新的规则库，当我们安装来源不明的软件时，仍可能感染病毒。

27、社交网站安全防护建议的是尽量不要填写过于详细的个人资料、不要轻易加社交网站好友、充分利用社交网站的安全机制。

28、“肉鸡”的正确解释是被黑客控制的电脑。

29、什么是流氓软件？是指通过诱骗或和其他程序绑定的方式偷偷安装在你计算机上的危险程序。

30、浏览器存在的安全风险主要包含网络钓鱼，隐私跟踪，数据劫持，浏览器安全漏洞。

31、没有绝对安全的网络，使用者要时刻提高警惕，谨慎操作。

32、你收到一条 10086 发来的短信，短信内容是这样的：

“尊敬的用户，您好。您的手机号码实名认证不通过，请到 XXXX 网站进行实名制验证，否则您的手机号码将会在 24 小时之内被停机”，这可能是遇到了伪基站诈骗。

33、为了防止邮箱邮件爆满而无法正常使用邮箱，应定期备份邮件并删除

34、用户收到了一封可疑的电子邮件，要求用户提供银行账号及密码，这是属于钓鱼攻击手段。

35、信息安全领域内最关键和最薄弱的环节是人。

36、造成系统不安全的外部因素包含黑客攻击、间谍的渗透入侵、DDOS 攻击。

37、在网络规划和设计中，可以通过防火墙划分网络结构，将网络划分成不同的安全域。

38、小强接到电话，对方称他的快递没有及时领取，请联系 XXXX 电话，小强拨打该电话后提供自己的私人信息后，对方告知小强并没有快递。过了一个月之后，小强的多个账号都无法登陆。在这个事件当中，小强遭遇了社会工程学诈骗，得到小强的信息从而反推出各种网站的账号密码。

39、互联网世界中有一个著名的说法：“你永远不知道网络的对面是一个人还是一条狗！”，这段话表明，网络安全中身份认证的重要性和迫切性。

40、为了防御网络监听，最常用的方法是信息加密。

41、加密技术能提供身份认证、数据完整性服务。

42、防止用户被冒名所欺骗的方法是对信息源发放进行身份验证。

43、属于系统安全的技术是防火墙、认证、防病毒。

44、使用个人电脑设置操作系统登录密码，并开启系统防火墙、安装杀毒软件并及时更新病毒特征库、尽量不转借个人电脑。

45、关于防火墙的描述正确的是防火墙不能防止内部攻击、如果一个公司信息安全制度不明确，拥有再好的防火墙也没有用、防火墙可以防止伪装成内部信任主机的 IP 地址欺骗。

46、关于 U 盘的使用，建议安装杀毒软件，防止 U 盘携带病毒侵入计算机、个人 U 盘传输资料前可先进行格式化，防止 U 盘中有遗留病毒、不随意使用捡拾的 U 盘。

47、为了更好地防范病毒的发生，我们应该做定期对操作系统补丁进行升级、安装公司指定的防病毒系统，定期进行升级、使用注册过的可信的 U 盘。

48、普通移动存储介质和扫描仪、打印机等计算机外设严禁在信息内网和信息外网上交叉使用。

49、组织制定信息安全方针的主要意图是阐明管理层的承诺。

50、数据采集、数据检测、数据分析属于入侵的过程，数据存储不属于入侵的过程。

51、当你感觉到你的服务器系统运行速度明显减慢，当你打开任务管理器后发现 CPU 的使用率达到了百分之百，你最有可能收到了拒绝服务攻击。

52、发送和接收大量数据阻塞网络、发动拒绝服务攻击登录未经授权的网络、主机或网络设备属于干扰网络正常运行的活动。

53、为了简化管理，通常对访问者分类组织成组，以避免访问控制表过于庞大。

54、不可以将用户信息、计算机密码、近期工作计划的便签纸贴在办公桌上。

55、对于出差期间的信息安全，在公共交通工具上与同伴沟通或打电话时，应注意不要让陌生人听到无意间透露的敏感商业信息，比如投标报价、方案细节等；U 盘经常保持清空状态，以免借用客户或丢失造成泄密；同客户交流时不要直接展示其他项目的文档，一定要提前进行脱密处理后再展示给客户，也不要拷贝给客户。

56、关于手机使用安全，应开启二次验证；勤升级系统和应用，不要点击短信连接；为 SIM 卡设置 PIN 码。

57、关于 Wi-Fi 钓鱼，应该公共场合尽量使用手机网络，不随便连接 Wi-Fi；日常使用 Wi-Fi，最好关闭自动连接；选择 Wi-Fi 时，一定要选择官方的 Wi-Fi。

58、在使用支付 APP 时请使用运营商 4G 网络，不要使用公用 WIFI。

59、用手机或笔记本连接公共场所的 WIFI 时，收发外网邮件（通信未加密）可能会导致泄密。

60、小王收到一封邮件，自称是 OA 系统管理员，声称 OA 要升级迁移，要求小王提供用户名密码。小王可以利用打电话问单位 OA 管理员来准确判断这封邮件是否是钓鱼邮件。

61、手机丢失后若收到捡到手机的邮件，切勿点击任何链接、图片或附件。

62、打印时出错的合同付款申请单，应该用碎纸机碎掉。

63、日常请设置屏保程序，建议在 10 分钟以内自动启动，并勾选“恢复时显示登录屏幕”，以免离开电脑忘记锁屏。

64、使用 MAC 电脑办公也需要安装防病毒软件。

网络安全宣传周“百问百答”试题题库

一、单选题

- 1、没有网络安全就没有（ ），就没有经济社会稳定运行，广大人民群众利益也难以得到保障。（ ）
 - A. 社会稳定
 - B. 民族团结
 - C. 个人安全
 - D. 国家安全
- 2、要树立正确的（ ），加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。（ ）
 - A. 社会主义观
 - B. 共产主义观
 - C. 网络安全观
 - D. 国家安全观
- 3、（ ）是国之重器。要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。（ ）
 - A. 社会发展
 - B. 国家稳定
 - C. 人民安康
 - D. 核心技术
- 4、（ ）代表着新的生产力和新的发展方向，应该在践行新发展理念上先行一步，围绕建设现代化经济体系、实现高质量发展，加快信息化发展，整体带动和提升新型工业化、城镇化、农业现代化发展。（ ）

- A. 网信事业
 - B. 社会主义事业
 - C. 共产主义事业
 - D. 国家发展事业
- 5、企业发展要坚持经济效益和社会效益相统一，更好承担起社会责任和道德责任。要运用信息化手段推进政务公开、党务公开，加快推进（ ），构建全流程一体化在线服务平台，更好解决企业和群众反映强烈的办事难、办事慢、办事繁的问题。（ ）
- A. 电子政务
 - B. 流程化服务
 - C. 党政结合
 - D. 数据大集中
- 6、既要推动联合国框架内的网络治理，也要更好发挥各类非国家行为体的积极作用。要以“（ ）”建设等为契机，加强同沿线国家特别是发展中国家在网络基础设施建设、数字经济、网络安全等方面的合作，建设 21 世纪数字丝绸之路。（ ）
- A. G20 峰会
 - B. 一带一路
 - C. 金砖会晤
 - D. 十九大
- 7、《中华人民共和国网络安全法》开始实施的时间为（ ）。（ ）
- A. 2018 年 3 月 1 日
 - B. 2017 年 6 月 1 日
 - C. 2017 年 8 月 1 日
 - D. 2016 年 12 月 1 日
- 8、《中华人民共和国网络安全法》规定网络运营者应当（ ），及时处置系统漏洞、计算机病毒、网络攻击、网络入侵等安全风险。（ ）
- A. 采购安全设备

- B. 制定网络安全应急预案
 - C. 制定安全管理制度
 - D. 实施安全服务
- 9、违反《中华人民共和国网络安全法》第 27 条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他们从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处（ ）日以下拘留，可以并处五万元以上五十万元罚款。（ ）
- A. 五日
 - B. 七日
 - C. 十日
 - D. 十五日
- 10、网络运营者应当为（ ）、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。（ ）
- A. 国家网信部门
 - B. 公安机关
 - C. 数字办
 - D. 工信部
- 11、（ ）负责统筹协调网络安全工作和相关监督管理工作。（ ）
- A. 国家网信部门
 - B. 公安机关
 - C. 数字办
 - D. 工信部
- 12、关键信息基础设施的运营者应当自行或者委托网络安全服务机构（ ）对其网络的安全性和可能存在的风险检测评估。（ ）
- A. 至少一次
 - B. 至少每两年一次
 - C. 至少每半年一次

- D. 至少每年一次
- 13、因（ ）安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。（ ）
- A. 系统
 - B. 应用
 - C. 网络
 - D. 人为
- 14、当您准备登录电脑系统时，有人在您的旁边看着您，您将如何：（ ）
- A. 在键盘上故意假输入一些字符，以防止被偷看
 - B. 友好的提示对方避让一下，不要看您的机密
 - C. 不理睬对方，相信对方是友善和正直的
 - D. 凶狠地示意对方走开，并报告这人可疑
- 15、对于社会工程学，以下哪项描述是不正确的？（ ）
- A. 社会工程学是利用人们的心理弱点
 - B. 社会工程学也是一种欺骗的手段
 - C. 社会工程学的主要目的是破坏
 - D. 社会工程学是对人的研究
- 16、社会工程学常被黑客用于（ ）
- A. 口令获取
 - B. ARP 攻击
 - C. TCP 拦截
 - D. DDOS 攻击
- 17、多久更换一次计算机的密码较为安全（ ）
- A. 一个月或一个月以内
 - B. 1-3 个月
 - C. 3-6 个月
 - D. 半年以上或从不更新
- 18、通过以下哪两种方式可以有效防止暴力破解：（ ）

- A. 定期更新系统补丁，安装杀毒软件
 - B. 限制密码错误次数，定期更换密码
 - C. 开启系统防火墙，增加密码复杂程度
 - D. 使用加密后的密码存储，开启数据保护模块
- 19、以下哪项不属于防止口令猜测的措施？（ ）
- A. 严格限定从一个给定的终端进行非法认证的次数
 - B. 确保口令不在终端上再现
 - C. 防止用户使用太短的口令
 - D. 使用机器产生的口令
- 20、下面那种方式可能导致感染恶意代码？（ ）
- A. 浏览网页
 - B. 收发邮件
 - C. 使用移动存储设备
 - D. 以上都是
- 21、关于安全更新正确的是：（ ）
- A. 及时安装安全更新
 - B. 更新完毕后及时重启计算机
 - C. 可以从第三方网站下载更新
 - D. 可以关闭自动更新
- 22、下面那种方法能有效保证操作系统或邮箱密码安全？（ ）
- A. 使用生日或 ID 号码作为密码
 - B. 记录在某处
 - C. 复杂口令定期更换
 - D. 有规律的长口令
- 23、下列关于个人计算机的访问密码设置要求，描述错误的是（ ）
- A. 密码要求至少设置 8 位字符长
 - B. 为便于记忆，可将自己生日作为密码
 - C. 禁止使用前两次的密码
 - D. 如果需要访问不在公司控制下的计算机系统，禁止选择在

公司内部系统使用的密码作为外部系统的密码

- 24、以下哪种口令不属于弱口令（ ）
- A. 12345
 - B. abcdefg
 - C. AAAAAAAAA
 - D. QW!bydp009877e
- 25、加密技术不能提供下列哪种服务？（ ）
- A. 身份认证
 - B. 访问控制
 - C. 身份认证
 - D. 数据完整性
- 26、小张发现安全软件提醒自己的电脑有系统漏洞，小张应该（ ）
- A. 不予理睬，继续使用电脑
 - B. 立刻更新补丁，修复电脑
 - C. 重启电脑
 - D. 暂时搁置，一天之后在提醒修复漏洞
- 27、下列属于感染病毒的症状是：（ ）
- A. 系统访问速度很快
 - B. 网络访问速度很快
 - C. 出现不知名文件
 - D. C盘空间变小
- 28、私自安全下载的软件有多种危害，以下哪种不是私自安全软件而导致的危险？（ ）
- A. 感染病毒
 - B. 手机丢失
 - C. 可能涉及到版权，导致法律风
 - D. 可能被种下木马
- 29、信息安全最大的威胁是？（ ）
- A. 木马病毒、蠕虫病毒等恶意代码

- B. 信息安全部门不作为
 - C. 人员普遍缺乏安全意识
 - D. 信息安全产品和设备不够先进
- 30、在大多数情况下，病毒侵入计算机系统以后()。
- A. 病毒程序将立即破坏整个计算机软件系统
 - B. 计算机系统将立即不能执行我们的各项任务
 - C. 病毒程序将迅速损坏计算机的键盘、鼠标等操作部件
 - D. 一般并不立即发作，等到满足某种条件的时候，才会出来活动捣乱、破坏
- 31、对防病毒工作的检查不包括以下哪项？()
- A. 防病毒的安装情况
 - B. 防病毒制度的执行情况
 - C. 病毒事件的处理情况
 - D. 病毒数量增减情况
- 32、下列不属于计算机病毒感染的特征()
- A. 基本内存不变
 - B. 文件长度增加
 - C. 软件运行速度减慢
 - D. 端口异常
- 33、我们经常从网站上下载文件、软件，为了确保系统安全，以下哪个处理措施最正确()
- A. 直接打开或使用
 - B. 先查杀病毒，再使用
 - C. 习惯于下载完成自动安装
 - D. 下载之后先做操作系统备份，如有异常恢复系统
- 34、为了更好地防范病毒的发生，以下哪项不是我们应该做的？()
- A. 设置光驱的自动运行功能
 - B. 定期对操作系统补丁进行升级
 - C. 安装公司指定的防病毒系统，定期进行升级

- D. 使用注册过的可信的 U 盘
- 35、当你感觉到你的服务器系统运行速度明显减慢，当你打开任务管理器后发现 CPU 的使用率达到了百分之百，你最有可能认为你受到了哪一种攻击？（ ）
- A. 特洛伊木马
 - B. 拒绝服务
 - C. 欺骗
 - D. 中间人攻击
- 36、在某电子商务网站购物时，卖家突然说交易出现异常，并推荐处理异常的客服人员。以下最恰当的做法是（ ）
- A. 直接和推荐的客服人员联系
 - B. 如果对方是信用比较好的卖家，可以相信
 - C. 通过电子商务官网上寻找正规的客服电话或联系方式，并进行核实
 - D. 如果对方是经常交易的老卖家，可以相信
- 37、信息安全的基本属性是？（ ）
- A. 保密性
 - B. 完整性
 - C. 可用性
 - D. A,B,C 都是
- 38、下面关于使用公共电脑的叙述中错误的是（ ）
- A. 不在未安装杀毒软件的公共电脑上登录个人账户
 - B. 不在网吧等公共电脑上使用网上银行
 - C. 离开电脑前要注销已登录的账户
 - D. 在公共电脑中存放个人资料和账号信息
- 39、小王是某公司的员工，正当他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（ ）
- A. 配合升级工作，立即提供正确的账户信息

- B. 先忙手头工作，再提供账户信息
 - C. 身份不明确，电话号码认识，直接拒绝
 - D. 事不关己，直接拒绝
- 40、许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是什么？（ ）
- A. 安装防火墙
 - B. 安装入侵检测系统
 - C. 给系统安装最新的补丁
 - D. 安装防病毒软件
- 41、以下哪项工作不能提高防病毒工作的实施效果？（ ）
- A. 及时安装系统补丁
 - B. 定期进行漏洞扫描
 - C. 对数据加密保存
 - D. 加强安全设备的监控和管理
- 42、社交网站安全防护建议错误的选项是：（ ）
- A. 尽量不要填写过于详细的个人资料
 - B. 不要轻易加社交网站好友
 - C. 充分利用社交网站的安全机制
 - D. 信任他人转载的信息
- 43、“肉鸡”的正确解释是（ ）
- A. 比较慢的电脑
 - B. 被黑客控制的电脑
 - C. 肉食鸡
 - D. 烤鸡
- 44、什么是流氓软件？（ ）
- A. 那些通过诱骗或和其他程序绑定的方式偷偷安装在你计算机上的危险程序
 - B. 是蓄意设计的一种软件程序，它旨在干扰计算机操作、记录、毁坏或删除数据，或者自行传播到其他计算机和整个internet

- C. 是一种完全自包含的自复制程序。可以通过网络等方式快速传播，并且完全可以不依赖用户操作，不必通过“宿主”程序或文件
- D. 其名字来源于古希腊神话，它是非复制的程序，此程序看上去友好但实际上有其隐含的恶意的
- 45、浏览器存在的安全风险主要包含（ ）
- A. 网络钓鱼，隐私跟踪
 - B. 网络钓鱼，隐私跟踪，数据劫持
 - C. 隐私跟踪，数据劫持，浏览器安全漏洞
 - D. 网络钓鱼，隐私跟踪，数据劫持，浏览器安全漏洞
- 46、下面关于我们使用的网络是否安全的正确表述是（ ）
- A. 设置了复杂的密码，网络是安全的
 - B. 安装了防火墙，网络是安全的
 - C. 安装了防火墙和杀毒软件，网络是安全的
 - D. 没有绝对安全的网络，使用者要时刻提高警惕，谨慎操作
- 47、你收到一条 10086 发来的短信，短信内容是这样的：“尊敬的用户，您好。您的手机号码实名认证不通过，请到 XXXX 网站进行实名制验证，否则您的手机号码将会在 24 小时之内被停机”，请问，这可能是遇到了什么情况？（ ）
- A. 手机号码没有实名制认证
 - B. 实名制消息与本人信息不对称，没有被审核通过
 - C. 手机号码之前被其他人使用过
 - D. 伪基站诈骗
- 48、为了防止邮箱邮件爆满而无法正常使用邮箱，您认为该怎么做？（ ）
- A. 看完的邮件就立即删除
 - B. 定期删除邮箱的邮件
 - C. 定期备份邮件并删除
 - D. 发送附件时压缩附件
- 49、用户收到了一封可疑的电子邮件，要求用户提供银行账号

- 及密码，这是属于何种攻击手段？（ ）
- A. 缓存溢出攻击
 - B. 钓鱼攻击
 - C. 暗门攻击
 - D. DDOS 攻击
- 50、信息安全领域内最关键和最薄弱的环节是（ ）
- A. 技术
 - B. 策略
 - C. 管理制度
 - D. 人
- 51、造成系统不安全的外部因素不包含（ ）
- A. 黑客攻击
 - B. 没有及时升级系统
 - C. 间谍的渗透入侵
 - D. DDOS 攻击
- 52、在网络规划和设计中，可以通过（ ）划分网络结构，将网络划分成不同的安全域？（ ）
- A. IPS
 - B. IDS
 - C. 防火墙
 - D. 防病毒网关
- 53、小强接到电话，对方称他的快递没有及时领取，请联系 XXXX 电话，小强拨打该电话后提供自己的私人信息后，对方告知小强并没有快递。过了一个月之后，小强的多个账号都无法登陆。在这个事件当中，请问小强最有可能遇到了什么情况？（ ）
- A. 快递信息错误而已，小强网站账号丢失与快递这件事情无关
 - B. 小强遭遇了社会工程学诈骗，得到小强的信息从而反推出各种网站的账号密码
 - C. 小强遭到了电话诈骗，想欺骗小强财产

- D. 小强的多个网站账号使用了弱口令，所以被盗
- 54、互联网世界中有一个著名的说法：“你永远不知道网络的对面是一个人还是一条狗！”，这段话表明，网络安全中（ ）
- A. 身份认证的重要性和迫切性
 - B. 网络上所有的活动都是不可见的
 - C. 网络应用中存在不严肃性
 - D. 计算机网络中不存在真是信息
- 55、为了防御网络监听，最常用的方法是（ ）
- A. 采用物理传输（非网络）
 - B. 信息加密
 - C. 无线网
 - D. 使用专线传输
- 56、防止用户被冒名所欺骗的方法是（ ）。
- A. 对信息源发放进行身份验证
 - B. 进行数据加密
 - C. 对访问网络的流量进行过滤和保护
 - D. 采用防火墙
- 57、下列不属于系统安全的技术是（ ）
- A. 防火墙
 - B. 加密狗
 - C. 认证
 - D. 防病毒
- 58、哪项没有安全的使用个人电脑？（ ）
- A. 设置操作系统登录密码，并开启系统防火墙
 - B. 安装杀毒软件并及时更新病毒特征库
 - C. 尽量不转借个人电脑
 - D. 在未安装杀毒软件的电脑上登录个人账户
- 59、关于防火墙的描述不正确的是（ ）
- A. 防火墙不能防止内部攻击
 - B. 如果一个公司信息安全制度不明确，拥有再好的防火墙也

没有用

C. 防火墙可以防止伪装成外部信任主机的 IP 地址欺骗

D. 防火墙可以防止伪装成内部信任主机的 IP 地址欺骗

60、微信收到“微信团队”的安全提示：“您的微信账号在 16:45 尝试在另一个设备登录。登录设备：XX 品牌 XX 型号”。这时我们应该怎么做（ ）

A. 有可能是误报，不用理睬

B. 确认是否是自己的设备登录，如果不是，则尽快修改密码

C. 自己的密码足够复杂不可能被破解，坚决不修改密码

D. 拨打 110 报警，让警察来解决

61、以下哪种行为最可能会导致敏感信息泄露？（ ）

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. 信息作废时通过碎纸机碎掉

62、以下说法错误的是？（ ）

A. 需要定期更新 QQ 软件

B. 可以使用非官方提供的 QQ 软件

C. 不在合作网站轻易输入 QQ 号

D. 完善保密资料，使用保密工具

63、禁止从事与本职工作不相关的活动，以下哪项是与本职工作相关的活动？（ ）

A. 使用公司电子邮箱在工作时间从事私人活动

B. 在网上查找与工作相关的资料

C. 使用公司电子邮箱在工作时间从事私人活动

D. 使用私人邮箱发送私人邮件

64、普通移动存储介质和扫描仪、打印机等计算机外设（ ）在信息内网和信息外网上交叉使用。（ ）

A. 可以

B. 严禁

- C. 不确定
 - D. 看情况
- 65、注册或者浏览社交类网站时，不恰当的做法是（ ）
- A. 尽量不要填写过于详细的个人资料
 - B. 不要轻易加社交网站好友
 - C. 充分利用社交网站的安全机制
 - D. 信任他人转载的信息
- 66、关于U盘的使用，哪个是不安全的操作？（ ）
- A. 安装杀毒软件，防止U盘携带病毒侵入计算机
 - B. 使用陌生人的U盘进行重要文件传输
 - C. 个人U盘传输资料前可先进行格式化，防止U盘中有遗留病毒
 - D. 不随意使用捡拾的U盘
- 67、下面哪部分不属于入侵的过程？（ ）
- A. 数据采集
 - B. 数据存储
 - C. 数据检测
 - D. 数据分析
- 68、组织制定信息安全方针的主要意图是（ ）？
- A. 阐明管理层的承诺
 - B. 阐明信息安全管理人员的职责
 - C. 阐明信息安全体系的建设思路
 - D. 阐明每个员工应尽的义务
- 69、信息安全最大的威胁是？（ ）
- A. 木马病毒、蠕虫病毒等恶意代码
 - B. 信息安全部门不作为
 - C. 人员普遍缺乏安全意识
 - D. 信息安全产品和设备不够先进
- 70、为了简化管理，通常对访问者（ ），以避免访问控制表过于庞大。（ ）

- A. 分类组织成组
 - B. 严格限制数量
 - C. 按访问时间排序，删除长期没有访问的用户
 - D. 不作任何限制
- 71、可以将记录哪些信息的便签纸贴在办公桌上？（ ）
- A. 用户信息
 - B. 快递公司电话
 - C. 计算机密码
 - D. 近期工作计划
- 72、以下哪项不是干扰网络正常运行的活动？（ ）
- A. 发送和接收大量数据阻塞网络
 - B. 给客户发送工作电子邮件
 - C. 发动拒绝服务攻击
 - D. 登录未经授权的网络、主机或网络设备
- 73、如果员工小王问你要你手上的某个文档，之前没给他发过这类文档，哪个做法是不正确的？（ ）
- A. 查一下部门秘密保护细则，看这个文档的扩散范围是否包含小王，询问直接上级的意见
 - B. 不能确定这个文档的扩散范围，咨询信息安全经理
 - C. 你觉得应该没问题，就发给小王，并告知要保密
 - D. 如果你知道这个文档的编写部门，让小王直接找这个部门索要
- 74、对于出差期间的信息安全，以下说法中那一项是不合适的：（ ）
- A. 在公共交通工具上与同伴沟通或打电话时，应注意不要让陌生人听到无意间透露的敏感商业信息，比如投标报价、方案细节等
 - B. U 盘经常保持清空状态，以免借用客户或丢失造成泄密
 - C. 同客户日常交谈时也可以透露其他客户发生的安全事件及其细节等

- D. 同客户交流时不要直接展示其他项目的文档，一定要提前进行脱密处理后再展示给客户，也不要拷贝给客户
- 75、小王收到一封邮件，自称是 OA 系统管理员，声称 OA 要升级迁移，要求小王提供用户名密码。小王可以利用哪一条方法来准确判断这封邮件是否是钓鱼邮件？（ ）
- A. 看发件人邮箱是否是单位邮箱
 - B. 看发件人的签名是不是公司格式签名
 - C. 打电话问单位 OA 管理员
- 76、关于手机使用安全，以下说法错误的是：（ ）
- A. 开启二次验证
 - B. 勤升级系统和应用，不要点击短信连接
 - C. 出售手机前，恢复出厂设置即可，不用彻底删除数据
 - D. 为 SIM 卡设置 PIN 码
- 77、关于 Wi-Fi 钓鱼，下列说法错误的是：（ ）
- A. 公共场合尽量使用手机网络，不随便连接 Wi-Fi
 - B. 日常使用 Wi-Fi，最好关闭自动连接
 - C. 选择 Wi-Fi 时，一定要选择官方的 Wi-Fi
 - D. 为了方便，连接没有密码的 Wi-Fi
- 78、用手机或笔记本连接公共场所的 WIFI 时，哪个操作可能会导致泄密？（ ）
- A. 浏览新浪新闻
 - B. 收发外网邮件（通信未加密）
 - C. 用 word 编写技术文档
 - D. 用 qq 聊天
- 79、下列哪个物品在无人看管时摆放在办公桌上不会有泄密风险？（ ）
- A. 令牌 key
 - B. 重要文件
 - C. 计算机教材
 - D. u 盘

80、打印时出错的合同付款申请单，应该怎样处理？（ ）

- A. 丢在就近的垃圾桶
- B. 用碎纸机碎掉
- C. 拿回去当草稿纸，便于节约纸张
- D. 可放在原地，由保洁人员处理

二、判断题

1、习近平指出，网信军民融合是军民融合的重点领域和前沿领域，也是军民融合最具活力和潜力的领域。要抓住当前信息技术变革和新军事变革的历史机遇，深刻理解生产力和战斗力、市场和战场的内在关系，把握网信军民融合的工作机理和规律，推动形成全要素、多领域、高效益的军民深度融合发展的格局。（ ）

2、习近平指出，要加强党中央对网信工作的集中统一领导，确保网信事业始终沿着正确方向前进。各地区各部门要高度重视网信工作，将其纳入重点工作计划和重要议事日程，及时解决新情况新问题。（ ）

3、国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、风险评估、监测等安全服务。（ ）

4、系统已打了最新的补丁，防病毒软件也更新了最新的规则库，当我们安装来源不明的软件时，仍可能感染病毒。（ ）

5、应用软件最好在官方网站下载，防止恶意软件捆绑在安装程序中（ ）

6、经常联系的同事突然在 QQ 上发过了一个链接，还附带写了几句话，小明就立马就打开链接了。这样应该没什么风险。（ ）

7、好久不联系的同学突然在 QQ 上发过了一个链接，还附带写了几句话，小明就立马就打开链接了。这样应该没什么风险。（ ）

8、个人设定的密码，记不住的话可以记到本子上或者工位的某个地方（ ）

- 9、如果你手上有一个 A 部门发给你的文件，B 部门员工问你要这个文件，你直接发给 B 部门员工了。（ ）
- 10、当含有重要信息的纸张废弃时，要将其撕掉扔进垃圾桶。（ ）
- 11、不同重要程度的账号设置不同的密码，用以减少密码泄露带来的影响。（ ）
- 12、淘宝、京东、新浪这些网站有很高的安全性，我们存储在其中账号密码是不会被泄露的。（ ）
- 13、在你进入公司大门时有一个快递员在旁边说要找某同事，你可以把快递员放进去。（ ）
- 14、让浏览器记住访问某网站的用户名和口令，大大减少了后续的操作，同时安全性也不会有大问题。（ ）
- 15、邮件在内部和外部网络上传输的过程中如果不加密明文传输，可能会被人通过网络中串联或旁路监听的设备抓取并还原内容，造成邮件中信息泄密。（ ）
- 16、手机丢失后若收到捡到你手机的邮件，切勿点击任何链接、图片或附件。（ ）
- 17、在使用支付 APP 时请使用运营商 4G 网络，不要使用公用 WIFI（ ）
- 18、手机或 SD 卡上存储敏感信息，比如身份证照片、银行卡照片、工作文档，以备不时之需。（ ）
- 19、日常请设置屏保程序，建议在 10 分钟以内自动启动，并勾选“恢复时显示登录屏幕”，以免离开电脑忘记锁屏。（ ）
- 20、使用 MAC 电脑办公很安全，不需要安装防病毒软件。（ ）