特定国家日常活动基本知识

电工

电工
特定国家日常活动基本知识
2012

zh.anarchistlibraries.net

2012

目录

说明：

- 斜体是在初期应当首先进行的检查，是更多后续活动的前置条件。
- 以下表述区分了“**应当**”“尽量”“可以”“**禁止**”等不同层次。

1 通用规范

1. **应当**知晓木桶原理，避免某一次活动成为一个方面的短板，避免某一方面成为个人的短板，避免某一个人成为团队的短板。
2. 能使用线下方式的，就不使用线上方式；能切割分开的，就不交叉共用；能使用电脑的，就不使用手机；能使用网页版的，就不使用客户端；能使用电子邮件的，就不使用即时通讯。
3. 可以换位思考攻防策略，认识到数据取舍过程必然只能抓主要矛盾并留下缝隙。
    - 涉及范围越大、集中程度越高的，统筹获取越容易：取国际全国，舍省内市域；取火车飞机，舍公共汽车；取街面监控，舍室内探头；取行业巨头，舍小型机构。
    - 占据空间越小、规整程度越高的，存储时间越长久：取电话账单，舍电话语音；取关系备注，舍互动详情；取邮件正文，舍附件内容；取快递运单，舍快递物品。
4. 在敏感时期尽量低调。

9. 在时间和路程允许的情况下，尽量选择火车和飞机以外的交通工具。在票价和剩余座位数允许的情况下，尽量不提前购票。

10. 通过**火车和飞机**会面的，尽量把到达时间、目的地、交通方式、车次或航班错开，**禁止**委托一人批量订票，**禁止**前后相邻排队购票或改签或退票，尽量不结伴检票或登机，可以买长乘短、换乘其他交通方式。匿名手机的开关机时间尽量远离火车和飞机的出发和到达时间，开关机地点尽量远离火车站和飞机场。

11. **在旅馆、饭店、宾馆、招待所等住宿的**，可以临时入住、不预订，**禁止**委托一人批量预订，**禁止**住在同一房间，**禁止**在相近时间在同一住宿场所结伴入住或退房。

12. 住宿期间，不在房间时尽量随身携带敏感物品；在房间时尽量不在房间内谈论敏感内容，有必要谈论时用电视机等噪音掩盖说话声。

13. 在餐饮场所预订座位用于会面的，尽量在抵达后临时要求更换座位。

2 电子设备

2.1 电脑和手机

1. 尽量少安装软件，尽量选用开源或外国的软件，尽量从官方网站下载安装包。**应当**卸载国产的防病毒、云输入法、管家、浏览器等软件，尤其是 360 杀毒/安全卫士、搜狗输入法、QQ 输入法、百度输入法、讯飞输入法、2345 输入法、360 手机管家、腾讯手机管家、360 安全浏览器、谋智网络的中国版火狐浏览器、学习强国、国家反诈中心和美图秀秀等。更换多种类型的软件时，可以按照功能的依赖关系合理计划卸载和安装顺序，先立后破，避免因为缺少输入法、浏览器等影响其他软件的更换。

2. 任何密码的五条设计原则：

   - 至少**应当**使用大写字母、小写字母、数字和特殊符号的复杂组合，尽量使用汉字；
   - 越长越好，汉字密码尽量在 10 位以上，其他密码**应当**在 20 位以上；
   - 含义隐晦，**禁止**使用常见弱密码，**禁止**直接使用自己或重要联系人的姓名、生日、手机号、地址门牌号等基本信息，尽量不使用现成的英语单词、中文词语、拼音或对于自身有特殊意义的人名、地名、日期等，如著名人物的姓名字号、著名组织的成立日期；
   - 匿名用途与实名用途**应当**不使用相同的密码，所有密码尽量各不相同，尽量定期更换密码；
   - **应当**便于记忆，能够不记混。

3. 任何密码的三条使用原则：
    - 尽量不在电脑上对密码进行复制和粘贴操作；
    - 在兼顾需要的情况下，**禁止**在手机上对密码进行复制和粘贴操作；
    - 密码和密文尽量从不同平台发送。
4. **禁止**在互联网（含社交平台的大型群组）**公开发布包含身份信息的内容**，不因迅速删除而抱有侥幸心理。
5. 不同平台的实名账号和匿名账号**禁止**使用相同的用户名，尤其是有个性的冷门用户名。匿名账号的用户名、昵称、头像、注册手机号、注册邮箱等**应当**与身份信息无关，个人页面**应当**设置为不公开账户资料，任何操作都不**应当**泄露真实身份信息，如生日、籍贯、住址、教育经历、工作经历、电话号码、金融账号、社交账号、语音以及证件、票据、人物、环境、截屏等照片。
6. **禁止**在**通讯录、好友列表或联系人列表**中对匿名手机号码、匿名电子邮箱地址、匿名账号等备注真实身份信息，尤其是特殊称谓、承担的任务、与自己的关系等。
7. 多用、善用翻墙软件，尽量多层嵌套。**禁止**使用中国背景的“蜜罐”型翻墙软件，其主要特征是免费、只有手机版而没有电脑版，如名称带有 Turbo、Snap、Thunder、Secure、Super、Freenet、Hotspot、Yunfan 等字样的部分 VPN。**禁止**使用可靠性存疑的翻墙软件，如自由门、蓝灯、老王等。使用 SOCKS5 协议时，**应当**设置 DNS 查询也经过翻墙软件。**应当**关闭智能判断 IP 地址归属地并直连国内 IP 地址的白名单功能。
8. 尽量用物理方式遮盖前置摄像头，**禁止**以视频方式召开敏感的线上会议，尽量不以音频方式召开敏感的线上会议。
9. 浏览器**应当**使用隐私/隐身/无痕模式，在使用后及时关闭整个浏览器。在忘记进入隐私/隐身/无痕模式时，**应当**删除过

3.2 金融

1. 与敏感人员之间**禁止**使用国内**邮政汇款服务**。
2. 与敏感人员之间**禁止**使用国内银行、大型第三方支付公司和贝宝（PayPal）的**电汇和转账服务**。

3.3 交通出行

1. 可以在早上 7 点前、晚上 9 点后外出活动。
2. 出行前可以把实名手机交给“他人”，使自己的轨迹和手机的轨迹完全不同。谨慎选择“他人”，自己的手机和他人的手机**应当**是可以发生关联的两个手机。
3. 尽量不直达往返目的地。到达目的地之前和之后，可以花费数小时在无关方向、无关区域、无关地点活动，跨越行政界限、地形界限，在没有视频探头的地方（如小路中间）更换交通方式、具体车辆和外貌服装等。
4. 可以自然地观察身后，如利用合理的动作或玻璃的反光，进入场所、道路、人群等，改变动静、速度、方向等。
5. 遇到路口带有人脸识别功能的视频探头时，尽量遮挡脸部或改变外貌。进入视频探头密集的场所时，可以遮挡脸部或改变外貌。
6. 可以预先考察沿途情况，可以在没有敏感任务时也多外出活动，都参照正式活动的做法。
7. 在敏感活动中乘坐地铁、公交车时**禁止**使用公共交通卡，**应当**购买单程票。
8. 尽量不使用大型网约车平台。

3 非电子设备

3.1 信件和快递

1. 尽量减少线上购物，尽量不使用淘宝、拼多多等购物平台的客户端。
2. 尽量选择国内小快递公司的高时效快递服务。
3. 在**填写快递发件人或收件人的联系方式**时，匿名手机号码、敏感地址**禁止**与真实身份信息发生关联，尤其**禁止**用于外卖。在兼顾需要的情况下，发件人或收件人的姓名尽量粗略甚至错误，发件人的电话号码尽量错误，发件人的地址尽量粗略甚至是实际存在的其他地点，收件人的地址尽量选择远离真实位置的代收点（驿站）。当发件人身份信息少于收件人身份信息时，两个手机号码之间**应当**避免因为双向收发快递导致互相泄露。与多方收发快递时，**应当**精心设计、严格控制，确保任何一方的任何一次快递都不泄露信息。
4. 负责转交物品的中间人尽量把收件时和发件时使用的姓名、电话号码、地址错开。
5. **禁止**通过第三方网站查询快递进度状态。
6. **禁止**夹带 X 光机能够发现的可疑物品。
7. 邮寄信件的注意事项参照快递，并且**应当**隐藏笔迹、指纹，粘贴邮资正确的邮票，投递到发件人地址附近的邮筒，**禁止**自发自收等可疑做法。

去所有时间里留下的历史访问记录、临时缓存、Cookie 文件、自动填充的用户名和密码等表单数据。尽量使用 Firefox、Chrome 等国际主流浏览器，尽量不使用 IE 和 Edge 浏览器。

10. **禁止**在国内搜索引擎搜索敏感词，尽量在翻墙后使用国外搜索引擎。
11. 转发、分享的处理原则：
    - 别人向我转发、分享——**禁止**在电子邮箱或社交类 APP 内直接点击各类链接地址。来源可靠且确有必要点击的链接地址，**应当**打开空白新标签，手动复制到浏览器的地址框内（较短的链接可以直接手动输入），检查域名是否仿冒，对链接地址净化后再访问。尽量不参加线上测试、抽奖、抢红包等活动。无法复制链接地址的，尽量请对方以文字形式发送链接地址。
    - 我向别人转发、分享——**禁止**直接使用社交类 APP 内的转发、分享功能。**应当**获取原始链接地址，把短网址还原为真实链接地址，把真实链接地址净化后，以文字形式发送。
    - 净化链接地址的方法：删除其中的账号 uid、IP 地址、访问时间、操作系统、浏览器版本、搜索关键词、令牌/凭据（token）等追踪参数。有困难时，可以用 URL/link 和 Clean/Cleaner/Clear 关键词寻找在线辅助工具。
12. **禁止**发送未清除 Exif 数据的照片，尽量不发送照片。
13. 尽量学习删除各类数据痕迹的方法。**应当**定期关闭设备，避免长时间运行，特别是电脑**应当**避免以休眠、待机、注销代替关机，手机**应当**避免以重启代替关机。
14. 已泄露信息的设备、手机号码、电子邮箱地址、账号等，尽量在评估风险、妥善设计后，一次性全部更换，确保切割干净，避免新更换的也被污染。新手机**应当**在调整 APP 和权限

后，再插入手机卡或导入文件。旧手机号码在淘汰前，**应当**完成关联账号的注销，**禁止**通过解绑、换绑操作把旧账号与新手机号码关联起来。完成更换并确认没有遗漏后，**应当**销毁旧设备。

2.2 电脑

1. **应当**及时安装系统补丁，更新杀毒软件的病毒库。
2. 尽量使用加密软件把所有敏感内容存储在电脑上。尽量不在手机上存储加密的或未加密的敏感内容。
3. 拥有足够内存并且拥有一定能力的情况下，把虚拟内存/Swap设置为无。

2.3 手机

1. **应当**卸载或强制停用手机自带/预装/推送的一切非必要 APP，**禁止**安装特定群体专用的小众 APP，**禁止**通过手机厂商的应用商店安装或更新敏感 APP，所安装的不同 APP 尽量避免构成个性鲜明的搭配组合方式。
2. **应当**检查手机对于每个 APP 授予的权限，关闭与必要功能无关的权限，果断放弃对非必要功能的需求。对某些 APP 没有特定权限就无法正常启动或使用的情况，通过反复尝试，尽量不授权、少授权，或以使用时每次询问的临时授权代替长期授权。**应当**从严收紧阿里（支付宝/淘宝）、腾讯（QQ/微信）、百度、字节跳动（今日头条/抖音）等公司 APP 的授权，以及涉及隐私的以下八方面授权：
   - 设备识别码（手机机身号码）
   - 通讯录
   - 通话记录

11. 可以通过别名功能，使同一个邮箱的登陆用户名、发件人用户名、收件人用户名互不相同，甚至与其他各个邮箱以不同的用户名单线联系。
12. 尽量发送定时自毁的邮件，尽量定期清理收件箱、发件箱、草稿箱、已删除邮件箱、垃圾邮件箱。

9. 在兼顾需要的情况下，尽量对主动搭讪的陌生人不予理会。

10. **应当**隔离不同用途的账号，尤其是对内和对外的账号。只有私下联系、没有公开联系的多个账号之间尽量减少公开互动行为，如点赞、评论、转发等。对外的账号尽量由多人共同维护、轮流发布，混淆终端时区、上线时刻、活跃时段、节假日、IP 地址等行为特征。

2.6 电子邮件

1. **禁止**使用实名手机号码**注册敏感邮箱账号或收取登陆验证码**。

2. **应当**使用国外邮箱，**应当**通过翻墙软件注册、登陆邮箱以及查阅、草拟、发送邮件（含抄送、密送）。即使无需翻墙能够直接访问的，也**禁止**使用国内 IP 地址直接访问。

3. 国外邮箱尤其是小众国外邮箱**禁止**与国内邮箱收发邮件，**禁止**与使用国内 IP 地址直接访问的国外邮箱**收发邮件**。

4. **禁止**使用邮箱客户端，**禁止**使用 POP3 协议把邮件存储到本地。

5. 多用、善用一次性邮箱。尽量及时注销不再使用的邮箱。

6. **应当**了解钓鱼邮件的一般特征，**禁止**点击来源不明的邮件或下载、打开其中的附件。

7. **应当**在设置中选择不自动加载显示邮件中嵌入的图片、视频等外部内容。

8. 邮件标题和附件名称尽量简单，不写称谓、事情等信息，这些信息尽量写在邮件正文里。

9. 回复时尽量写新邮件，不把原邮件内容附在回复的正文里。

10. 尽量加密附件。大附件可以分卷压缩并加密后，使用多封邮件分别发送。

- 短信
- 位置
- 相机
- 麦克风
- 应用列表

3. **禁止**不需要联网的 APP(如输入法等)使用移动流量和 WLAN（含 Wi-Fi）流量。**禁止**不需要后台运行的 APP 使用后台流量。

4. **应当**检查手机和每个 APP 的安全设置或隐私设置，仔细深入每一层菜单的每一个分支，关闭所有与广告标识符、匿名设备编号、个性化推荐、第三方信息收集与共享、用户体验改善等相关的选项。可以仔细阅读 APP 所接入的第三方软件开发工具包（SDK）清单，了解其收集的信息类型，进一步有针对性地收紧权限。

5. **应当**关闭 GPS 定位服务，关闭通过 WLAN（含 Wi-Fi）扫描、蓝牙扫描等方式获取精确位置的功能，**禁止**广告、支付、社交、购物等所有类别（地图除外）APP 申请位置信息。可以关闭地图类 APP 申请位置信息的权限，改用离线地图甚至纸质地图，或通过电脑访问地图网站。

6. 无法设置收紧剪切板权限时，**禁止**复制任何敏感内容。

7. **禁止**使用云同步与云备份功能，如 iCloud、网盘等。

8. 一个手机从启用到废弃的全生命周期**只能使用一个手机号码**，**禁止**混插不同号码甚至不同用途的手机卡。

9. 积极使用每个时代的新一代移动通信技术，如新推出四五年内的 4G、5G 服务。

10. 屏蔽手机信号的最佳方法是法拉第袋（不含日常生活中的金属罐、金属箔、塑料防静电袋等），其次是切换到飞行模式并

且避免因误操作发起紧急呼叫，再次是关机。开关机操作尽量在飞行模式下、在远离敏感位置的地方进行。处于开机状态且未处于飞行模式时，尽量不频繁刷手机。

11. **不应当发生关联**的两个手机（如一个人的匿名手机与实名手机，或多个人的实名手机）**禁止**共用同一个 Wi-Fi 或 WLAN 热点，**禁止**在未屏蔽手机信号的状态下沿相同轨迹移动，**禁止**在通讯录交叉存储号码，尽量不同时同地开关机，尽量不与相同的人拨打电话、收发短信和快递，尽量不在相邻时段以相同方式充值，尽量在使用的时间、地点、习惯等方面形成特征差异并且永不混淆，可以设置在连接 WLAN（含 Wi-Fi）时使用随机/私有 MAC 地址。
12. 匿名手机可以减少开机次数、缩短开机时间，开机地点尽量避开视频探头，尽量选在人群极其密集的公共场所或基站稀疏的夜间远郊、山区、水域等。
13. 拥有一定能力的情况下，可以把手机机身号码修改为克隆机常用的号码。
14. **应当**设置锁屏密码，但不要寄希望于锁屏密码。
15. 尽量不注册国内手机厂商的客服或会员账号。
16. 尽量减少手机的剩余空间，填充非敏感内容。

2.4 电话和短信

1. 固话/手机通话、短信**禁止**包含敏感内容。
2. 匿名手机尽量不用于拨打电话。如果不得不发生通话，那么**禁止**实际使用人成为参与通话的一方并留下语音。尽量不与某一个号码单线联系，可以设计合理的名义联系与身份信息无关的陌生人。

3. 分别位于境内和境外的两个固话/手机号码之间尽量不拨打国际/港澳台长途。漫游到境外的境内号码、漫游到境内的境外号码都尽量不与固话/手机号码**拨打电话**。
4. **禁止**使用公用电话。

2.5 线上社交和即时通讯

1. **禁止**使用实名手机号码、国内邮箱**注册敏感社交账号或收取敏感网站验证码**。**禁止**使用实名或匿名的境内手机号码注册推特（X）。
2. 社交类 APP **应当**关闭以下功能：上传我的通讯录并向我推荐已开通账号的通讯录成员，他人通过手机号码查找我的账号或查看我的账号资料（如用户名、昵称、头像、国家/地区、在线状态等），陌生人无需验证同意就直接添加我为好友，陌生人未成为好友就直接向我发送消息或拨打语音电话。
3. 能点对点逐个发送的，就不发送到群组；能发送到小群组的，就不发送到大群组；能发送到群组的，就不发送到公开页面。
4. 微信图片即使能够被顺利发出去，也**禁止**包含敏感词。各类敏感内容**禁止**通过电话、微信文字消息、微信图片消息、微信语音消息等方式传递，在极其紧急的情况下可以由微信语音通话极其隐晦地口头告知。
5. 在 Telegram 中，敏感内容**应当**使用私密聊天功能发送文字消息，尽量不包含图片、音频、视频和其他文件。
6. 即使在端对端加密的即时通讯平台上，也尽量使用暗语。
7. **应当**经常删除不需要保留的聊天记录，并清理本地存储空间。
8. **禁止**使用任何功能发布、发送位置。在兼顾需要的情况下，**禁止**使用基于位置的移动社交 APP 或邻近人员查找功能。