网络与通讯安全教程

中国权利在行动 开发制作

2014年4月

关于网络与通讯安全教程

现在，人们已经习以为常的使用电脑、手机、平板与外界进行沟通、协作或交易了，但在具体操作过程中往往隐藏着不同来源、不同种类、不同程度的风险。对此，大多数用户或是未觉察，或是未足够重视，或是不知道如何应对，而使风险控制处于停滞、被动的状态。

在本教程中，我们试图告诉人们，在网络活动过程中会面临什么样的风险，风险程度如何，应该如何应对。不仅使人们了解哪些应用、场景、操作方法中存在风险，也使人们了解如何使用更安全的操作方式，从而提高防范风险的能力。

课程目录

第一章

BT Sync 的使用

前.言

BT Sync 是一款文件同步工具，它支持传输各种文件，支持各种系统平台。在本教程中我们不仅介绍 BT Sync 的使用，同时也会把 BT Sync 做为传输教程的载体。

一、BT Sync 概述

介绍 BT Sync 的定义、特性，应用场景, 运行原理。

（一）定义

BT Sync （BitTorrent Sync）是一款支持现代设备的文件同步工具。

（二）特性

BT Sync 具有以下特性：

1、支持多种网络：互联网、局域网、WIFI；

2、支持多平台多设备： 可支持 Windows 、 Linux 、 Mac OSX 、 Android系统；可运行在PC机、苹果电脑、智能手机、平板等设备上；

3、点到点（P2P）传输，也就是说，不需要有专门的服务器，只要使用个人电脑或手机或平板，就可以把需要发布的文件传递到世界的任何角落；如果你传输的文件越受欢迎，下载速度就越快；

4、它是安全的，文件在传递过程中是加密的，在接收端又会自动解密。也就是说，即使在舆过程中被截取，截取者也无法得到原文件；

5、它很方便：1. BT Sync 支持任何格式的文件，不限制文件的大小，也不限制传递文件的数量；2. 使用 BT Sync 不需要用户名和密码； 3. BT Sync 通过分享码或二维码标示一个分享文件夹，方便而简洁。

（三）应用场景

BT Sync 在什么情况下所用呢？下面我们介绍两个应用场景：

1、（配个一对多传文件的图片）比如你有一些文件，这些文件可能很多，可能很大，也可能需要经常更新，而你需要把这些文件分享出去，让任何人都可以得到，或者让你指定的人可以得到；你希望文件在传递过程中是安全的，不会被非法截获；也许 你还希望限定时间，比如这些文件你只希望公开分享一个小时。

这样的任务，BT Sync 可以帮你实现。

2、（配个多台设备同步的图片）又比如，随着智能电子设备的丰富，也许你已经有了很多不同的设备，并且它们分布在不同的场所，比如你书房有台式机、卧室有笔记本，客厅有智能电视、出门还携带平板电脑或智能手机，而在办公间还有工作用的电脑。经常你会有这样的需要，比如一些程序、电子书、视频、照片等，你希望他们在所有这些设备上保持同步。 另外，办公室的场景也还可以稍微延伸一下，可能你在单位的同事或远方的协作者之间，大家还需要随时同步一些文档。

以上需求，BT Sync 可以帮你做到。

（四）运行原理

BT Sync 是如何便捷而有效率的运行？现在我们对 BT Sync 的运行原理做一个简要的介绍 。

如果用户A 要与别人分享一些文件，A要在电脑上建立一个文件夹，把要分享的文件放进去，并通过 BT Sync 生成文件分享码（一段密文或者是一个二维码），然后，再把文件分享码公布出去，或者只发送给他信任的人，就完成了一个文件分享的操作过程。

网络中的 用户B得到这个文件分享码后，只需要在他的电脑（或手机或平板）的 BT Sync 软件中，为这个分享码建立一个文件夹，就可以把A分享出来的文件夹内容同步到自己的设备上。

在只有一个接收者的情况下，文件是从A传到B，如果又有C加入，因为使用同一个分享码，C 可以从 A 和 B 处分享到文件。这样，加入的传递者越多，下载的速度越快。

前面是对 BT Sync 的综合介绍，接下来，我们就以电脑 Windows 系统和手机安卓系统为基础，具体介绍 BT Sync 的下载、安装、使用、配置等操作方法。

先以 Win7 为例介绍 Windows 系统下的使用。

二、下载与安装（以 Win7为例）

（一） BT Sync 的下载

运行 BT Sync 需要先下载安装，这个程序很小，目前最新的 1.1.48 版只有 870 K 。 BT Sync 的开发者会根据程序的运行状况不断做出改善，并把稳定的版本发布在 BT Sync 官方网站，因此，建议使用者去 BT Sync 官方网站下载最新的程序。

官方下载地址： http://www.bittorrent.com/sync/downloads

进入下载页面后，根据你使用的操作系统版本选择载载，选择文件存储的位置 ..... 就放在桌面好了。然后，点“保存”，就开始下载了。

（二）下载软件后，安装过程

1、去桌面找到你下载的程序，双击安装；

2、出现安装界面，有四个勾选的页面，在这里点“下一步”；

3、出现“选择 BitTorrent Sync 配置”页面，有两个勾选页面，在这里点“安装”；

4、安装完成后，桌面已经创建了 BT Sync 启动的快捷图标；

5、出现 “BT Sync 安装”界面，是让你建立一个分享文件夹，或为已经得到的分享码。建立一个文件夹。勾选 “我已阅读并同意隐私政策和条款”后，可以点击“跳过”；

6、这时，BT Sync 已经正确启动。

然后，我们进行下面的操作。

三、了解 BT Sync 在状态栏选项以及BT Sync程序主界面

（一）了解状态栏功能

- BT Sync 安装完成后，或启动后，会驻留在系统的状态栏（电脑右下角）；
- 鼠标指向 BT Sync 程序的图标，点击鼠标右键，就会出现一个操作选项卡；
- 最后一个选项最容易识别，就是退出BT Sync ；
- 倒数第二个选项是一个反馈表单，如果在BT Sync 使用中，发现什么问题，或者提出什么建议，都可以填写并提交该表单。也许开发者能对问题给予解决，或者采纳你的建议；
- 如果你要填写反馈表单，在最上面一行填写你的邮件地址，往下是选择你对于 BTSync 的喜欢程度，从最好到最不好；
- 再往下，是一个大文本框，用来填写你的反馈意见，文本框下面有一个勾选 框，如果你提交的反馈需要附带 BT Sync 的系统日志，那么你可以勾选这个框。但是，使用 BT Sync 的系统日志，可能会泄露一些你的私人信息；

- 最后，点发送就提交出去了；
- 注意：在这个反馈表单中，只有反馈文本是必须填写的，其它部分都是可选项，也就是说，你只要填写了反馈文本，就可以提交出去。
- 倒数第三个选项用于暂停或恢复 BT Sync 的工作，选择“暂停”将断开你的 BT Sync 与其它用户的分享通道；
- 倒数第四个选项用于禁止或启动 BT Sync 工作日志，也就是设置是否启用BT Sync 的工作记录；
- 最上面一个选项，单击它就可以进入了BT Sync 程序主界面；
- 另外一个进入BT Sync 程序主界面的方式是：在你系统状态栏的 BT Sync 图标上面，直接双击左键。

现在，我们先关闭 BT Sync 主界面，用双击的方式进入。

（二）BT Sync 主界面

BT Sync 程序的主界面里有五个选项卡，分别是：文件夹、设备、传输、历史和首选项。现在，我们先简要介绍一下 BT Sync 主界面各选项卡的功能。

- 在文件夹选项卡，在上面这一列，可以显示本地正在接收或发布的文件夹名，以及该文件夹下文件的字节数。下面两个大按钮，一个用于创建文件夹的发布与接收，一个用于断开文件夹的发布与接收。BT Sync 的关键操作都在这两个按钮，但现在，我们先主要介绍界面的布局，具体的操作方法，会在后面介绍。
- 在设备选项卡中，可以查看当前设备连接的其它设备。具体包括连接的设备名，连接的文件夹，传输的状态。
- 在传输选项卡中，会显示连接本地设备的其它设备正在传输文件的状态。会显示

传输中文件名，设备名，上传下载的速率；并且会在右下角显示与所有连接设备传输的总速率。

- 在传输选项卡中，会显示连接本地设备的其它设备正在传输文件的状态。会显示传输中文件名，设备名，上传下载的速率；并且会在右下角显示与所有连接设备传输的总速率。
- 在历史选项卡，会记录文件添加、删除、重命名、同步结果的日志。还包括是什么设备？在什么时间？做的什么动作。
- 在首选项，可以设置 BT Sync 程序在运行中的一些参数，包括一些基本的属性。
- 如：修改你设备的名称，在这里，你可以定义一个个性的名字，以便你或其它人更容易识别；也可以定义一个没有任何含义的名字，让它人无从猜测你是谁；或者还可以直接使用一个短语，借机张扬你的主张，总之在这里，你想玩的话，可以娱乐一下。
- 这里是勾选下载完成后是否要提示；
- 这里是勾选开机后是否自动运行 BT Sync；
- 这里是勾选有新版 BT Sync 时是否自动升级，或者你现在可以直接点击，让立即升级。；
- 这里可以分别限制上传下载的速率，默认为0 ，也就是不做限制。

在这个界面，你可以根据你的需要做适宜的设置。

- 最后，这里还有更高级的选项，但基本上不需要做调整。
- 总体上看，BT Sync 的五个选项卡中，在文件夹选项卡，可以通过操作，定义接收与发布什么样的文件；在参数选项卡，通过操作，可以设定程序的工作参数。

- 而设备名，传输、历史这三个选项卡，只能查看软件运行的状态，而不能做更多操作。，也就是不做限制。

好，关于 BT Sync 的界面，就介绍到这里。

下面介绍文件夹的发布与接收，这也是使用 BT Sync 的最常用的操作。

四、发布同步文件夹与接收同步文件夹的方法

（一）下面介绍发布一个文件夹的过程

1、先建立一个文件夹，把需要发布的文件放进去；

操作：在 D盘建立一个文件夹起名 BT Sync ，这个做为 BT Sync 程序使用的根目录，本身不做为接收与发布的文件夹； 然后，在这个文件夹下在建立一个 ”寻找 1949”的文件夹，移入几个文件，好，发布的需要的文件夹就建立好了，现在进入 BT Sync；

2、进入 BT Sync 发布文件选项卡；

3、点击“添加文件同步”；

4、点击上面一个空格右侧的按钮，生成一个密码；

5、然后点击下面一个空格右侧的按钮，选择需要发布的文件夹，在这里，也就是找到 D:\BT Sync\寻找1949 ，点击确定；

- 这时候可以看到，在发布文件夹界面，已经多了一列 ”寻找1949”的文件夹，这表明，一个新的分享文件夹已经创建。

- 然后，会需要把这个文件夹分享出去，也就是把这个文件夹的分享码或者是二维码发布出去。
- 那么，怎么再次找到刚才的分享码呢？ 还是在这个分享文件列表中，现在介绍一下分享文件夹列表的操作方法：
    - 双击分享文件夹，可以打开这个文件夹的原始位置
    - 点击右键，会显示右键选项卡，其中：
        - 在第一个选项（Copy secret），点左键或右键都可以，会把这个文件夹的读写分享码复制出来，当然，如果这个文件是你同步其它设备的，并且你的到的分享码是只读权限的，那么，你复制到的就是只读分享码。
        - 在第二个选项（Connect mobile），点左键或右键，会弹出这个分享文件夹的 QR 码（QR码也是一种二维码，1994年由日本人发明），二维码有两个，一个是读写访问权限的，一个是只读访问权限的。移动智能设备扫描这个二维码就可以获得相应的分享权限。
        - 在第三个选项（Open SyncArchive），点左键或右键，可以打开分享文件下面记录同步信息的一个文件夹
        - 在第四个选项（显示文件夹首选项），点击左键或右键，可以打开一个选项卡，这个选项包括两个选项页面，默认的是专门用来处理分享码和二维码的界面。
            - 这个界面分三部分，上面两个输入框用来生成分享文件夹的读写分享码只读分享码鈥
            - 中间一个用来生成24小时有效的读写分享码与只读分享码

- 下面按钮与刚才右键第二个选项功能相同，点击后会显示分享文件夹的二维码，与刚才的一样，也是有读写与只读两个权限的。
- 在第四个选项卡中的属性第二个选项界面，是对这个文件夹分享参数的一些配置，一般情况不需要做更改。

6、这里，我们就在第一个界面中，复制只读分享码，然后把这个分享码告诉你希望得到此文件的人，或是公开发布出去，供任何知道此分享码的人使用。

（二）接收一个分享包的过程

1、先取得一个分享码：朋友给的，或者是从可信任渠道得到的，包括官方网站或社交媒体好友的分享。这里，我们就使用一个视频教程的分享码：BIY3W3VTH47XIZEVNA2G4AZCEVTZFOP4X；

2、建立一个文件夹，如：D:\BT Sync\Gephi；

3、进入BT Sync 文件夹选项卡；

4、点击”添加文件同步” 填写分享码；

5、选择 D:\BT Sync\Gephi 文件夹

6、点确定，在分享文件夹看到添加的文件夹后，就表示获取同步已经建立，然后等待同步就可以了。

（三）删除一个分享任务的方法

当发布的一个文件夹，已经被需要的A好友收到，或公开分享的文件，打算停止分享。或者是，你得到一个分享码，已经下载完成后，并且你也不打算继续接收新的文件或接力传播这个文件夹。那么，这时候，你就可以把这个文件夹从分享的状态释放出来，具体方法是，选中一个分享文件夹，然后点击下面的 “移除分享文件夹“，这

样就可以释放出来不在接收各种同步。做这个操作，不会丢失你原本发布的文件或你接收过来的文件，这个操作只是从 BT Sync 中断开这个文件夹与远程文件夹的连接。

（三）删除一个分享任务的方法

当发布的一个文件夹，已经被需要的A好友收到，或公开分享的文件，打算停止分享。或者是，你得到一个分享码，已经下载完成后，并且你也不打算继续接收新的文件或接力传播这个文件夹。那么，这时候，你就可以把这个文件夹从分享的状态释放出来，具体方法是，选中一个分享文件夹，然后点击下面的 “移除分享文件夹” ，这样就可以释放出来不在接收各种同步。做这个操作，不会丢失你原本发布的文件或你接收过来的文件，这个操作只是从 BT Sync 中断开这个文件夹与远程文件夹的连接。

BT Sync 支持安卓手机与苹果手机的版本都已经发布，下面以安卓系统为例，介绍 BT Sync 在手机上的使用方法。

五、在手机上使用 BT Sync （以安卓系统为例）

（一）下载移动设备版 BT Sync

安卓版下载地址：https://play.google.com/store/apps/details?id=com.bittorrent.sync
苹果版下载地址：https://itunes.apple.com/us/app/bittorrent-sync/id665156116
国内安卓系统用户如果无法在 Google Play 下载安装的话，可以在豌豆荚下载。
下载地址：http://www.wandoujia.com/apps/com.bittorrent.sync

安卓版的 BT Sync ，针对移动设备的特性，在功能和界面上做了很多简化，具体功能包括同步、发送和备份：

1、同步，获得其它设备分享出的文件；

2、发送，手机间通过二维码快速分享；

3、备份，把手机中的文件同步到其它设备。

(二) 下面分别介绍这三个功能的操作方法

1、同步

这里同步所做的是：把其它设备中的文件存储到本地。

1) 所以，第一步是点击同步界面右上角的文件+按钮，选择一个存放其它设备中文件的本地文件夹;

2) 第二步是扫描远程分享出来文件夹的二维码，或输入远程分享文件夹的分享码；

3) 可以选择自动同步；

4) 点击完成。就会建立一个同步其它设备文件夹的任务。

2、发送

这里的发送，其应用场景是，两个或多个近距离移动设备之间快速同步文件的情 况，比如几个朋友见面时，互相间分享手机或平板中的文件。

1) 在发送界面，选择一个或一些要发送的文件，特别的 BT Sync 支持照片文件的浏览与选择，选好文件后，点完成，生成分享码；

2) 接收方，在发送界面，点“接收文件”会出现扫描二维码的界面，对准发送方的分享扫描，就会启动接收动作。

以上操作，可以实现两台或多台移动设备之间快速分享文档。

3、备份

这里的备份，指把移动设备的文件传输到其它设备。

1) 在备份界面，点击右上角的文件夹+;

2) 选择一个文件夹，点下一步;

3) 会生成一个同步代码，可以把这个代码复制下来，或者用邮件或蓝牙发送出去。

4) 其它设备，用此分享码创建文件夹后，就可以同步此文件的内容。

以上操作，可以实现把手机文件同步出去的操作。

六、相关技巧和需要注意的

(一) 技巧

1、如果你的一个文件夹已经分享出去，那么即使在你本地丢失文件也没有关系，你可以用分享码重新取回，并且，用有读写权限的分享码还可以取回编辑这个文件夹下面文件的权限;

2、建议在一个较大的磁盘，建立一个 BT Sync 的目录，然后，把需要分享的文件夹 建立在此文件夹下，这样便于你的管理。

(二) 需要注意的

1、发布或者接收的 BT Sync 文件夹，互相之间不可以嵌套否则会报错;

2、在一个多人都i可以编辑的文件夹中，在一些用户不在线时，删除的文件，在那些用户重新回到网络时，会把删除的文件在带进来。

(三) 拓展

基于以上了解，也许你已经可以拓展想象出一些 BT Sync 的新奇用法，比如，可以设想，能把BTS当成是一种发行工具来使用，比如你是一个出版社，或媒体，或是一个想办画展的艺术家，你只需要在你的电脑上面，建立一个文件夹，把相关文件放进去，再把分享码公布出去，得到分享码的人就可以下载到你发布的信息，并随意浏览。这里只是随意举一个例子，放开想象，你一定会想到其它更多的用途。

（四）BT Sync与BT Syncg种子的差异

BT Sync对BT**种子运行机制做了改进，主要包括两点**：

- BT Sync种子（分享码）对应的是一个文件夹，而BT种子对应的是一个文件；
- BT Sync文件夹可以自动同步发布者的文件，而 BTf无此特性。

七、提 问

对于电脑和所有一切智能设备来说，文件即一切，也就是说，文件是构成机器智能的基础，那么，BT Sync 这样的文件同步应用还能更多做些什么呢？

1、怎么设计一个方案，使 BT Sync可以成为应用软件升级与更新的一个解决方案？
2、怎么设计一个用BT Sync发布个人网站的方案？
3、尝试用 BT Sync创建一个类似微信的公众账户的应用？
4、如果你创建了一个用于面向公众分享的文件夹，你会用什么办法去推广它？
5、对于你已经分享出去的文件夹，为了保全你的数据，对于你设备可能出错，比如硬盘坏掉的风险，你有什么应对策略？
6、如果你使用过一些“网盘”之类的云存储服务，你能够谈谈与BT Snyc有什么不同吗？

7、应该实验一下，如果我保留了一个分享文件夹的读写分享码，然后，我在另外一台机器上，使用这个读写分享码创建一个分享文件夹，那么这个分享夹的只读分享码与原来的会一样吗？

本章视频教程：https://www.youtube.com/watch?v=a4B3LNEiCmk

第二章

简单个人信息安全模型

前　言

信息安全绝对不是单指某一件事，现代信息安全的边界随着现代信息技术的扩展而延伸。与此同时，入侵者与入侵手段也在增长，这使得安全防护无法仅仅依靠"木桶短板"模型找出最薄弱点进行加固就能保证安全。那么，我们就需要用一种系统的、全方位的模型去构思与安全有关的整个系统，并能够根据不同场景，动态的调整相应策略，才能有效应对不同的挑战。

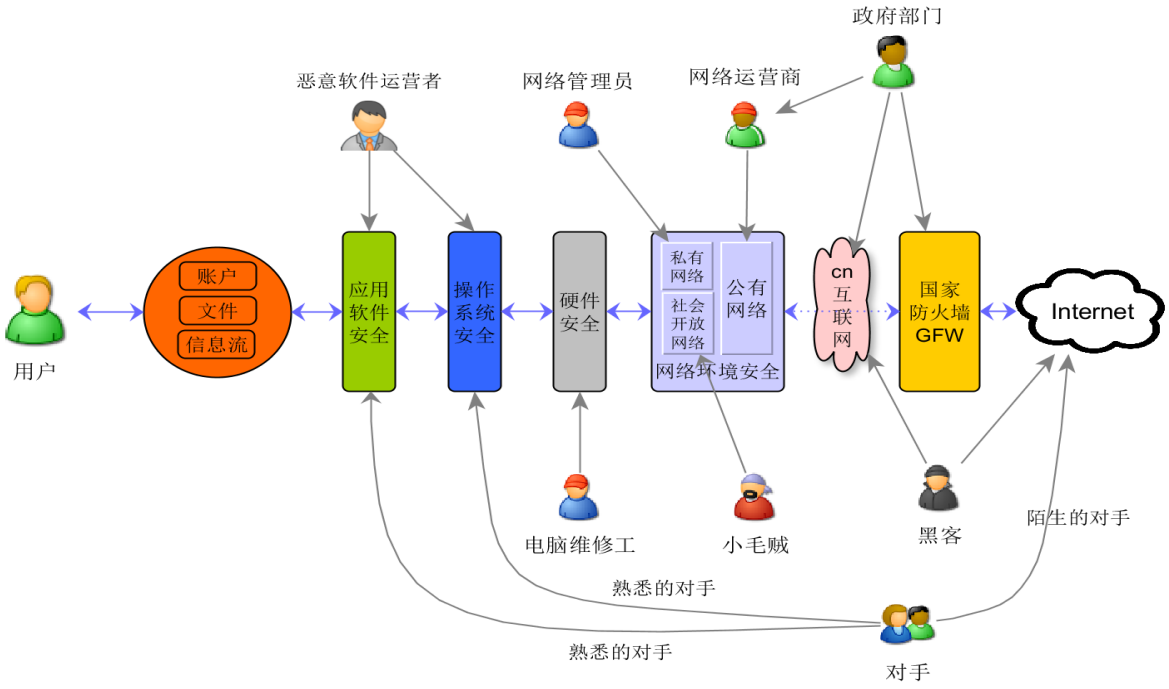
在这一节教程中，会围绕以下三个问题，力求全景式描述个人面对信息安全的整体状况，介绍与安全有关的各方面要素，以及要素之间的相互关系，为后面的知识建立一个基础。

1、什么需要保护？

2、需要保护的内容，在使用者与互联网之间的流通需要经过哪些环节？各环节有什么不同的特性？

3、谁是"敌人"？

网络与电脑安全防范模型图



一、什么需要保护？

要保证信息安全，首先应该明确哪些内容需要保护。这里根据不同的特性，我们把需要保护的内容分为账户、文件、信息流、用户行为习惯四种，以下分别介绍。

（一）各种账户

随着网络条件的改善，如果说将数据存储于网络（而不是本地硬盘），是一种数据存储更便利、更可靠的选择，那么，对于分享及协同作业来说，网络存储就是一种必然的选择。

在这种情况下，给用户行为带来的变化是：过去人们关注的是“我的文件存在C盘还是D盘 的什么目录下？” 现在变成“我的文件存储在什么网站？用户名和密码是什么？” 这样一种由数据存储位置的转移带来的操作行为的变化，也使得账户（包括用户名和密码），这个开启人们各种信息之门的钥匙成为更加重要的、不可或缺的、也需要认真保护的财产。

账户，既包括电脑本身的账户，也包括网络各种应用账户，比如：

1、电子邮件；
2、货币类：贝宝、支付宝等；
3、 社交类：推特、脸书等；
4、 各种在线类应用及工具；
5、 购买域名主机空间的账户等。

（二）文件

虽然所有文件都可以存储在网络上，这样，保护好账户的安全，也就保护了文件的安全。但现实中，可能因为网速的原因，可能因为操作习惯的原因，也可能一些工作（比如图形编辑、视频编辑等）需要，或必须将大量的文件存储在本地硬盘。那么，这里说

的文件安全，主要就是指存储在电脑上的，用户自己编辑或接收到的各种类型的文件。

这些文件可以分为如下几类：

1、文字编辑类：一般是扩展名为 DOC、PDF、PPT、TXT 的各类文本文件；
2、数据类，一般是扩展名为 XLS 的 Excel 表格文件，扩展名为 CSV 的文本表格等；
3、照片图片类，一般是扩展名为： JPG、PNG、GIF 的文件；
4、另外，如果安装过一些管理类软件，并往里面输入了数据，或者是在本地电脑建立过数据库，比如 MySQL 、MSSQL 等，它们虽然不是把数据保存在某一个文件中，但软件本身存储了用户的数据，因此，也是需要保护的一种文件类型。

（三）信息流

账户与文件是相对有形的信息，还有一种相对无形的信息流，比如用户通过文字、语音或视频与他人的交流，也可能被非法截获，这类实时信息同样能够泄露有价值的信息，因此在相应的操作中也需要进行安全防范。

（四）用户行为

除以上三类外，还有一种看上去与安全无关的用户浏览行为，会暴露用户网络及现实的个人信息，比如经常访问的网站、作息时间、社交关系、购物习惯等等。这些看似琐碎的信息，如果对其进行整体的关联分析，往往能透露出重要的信息。如果有心者检测到这些信息后，可以根据用户的行为习惯，做出不利于用户的安排与设计。因此，用户行为数据也变得越来越重要。

以上是在考虑信息安全的时候，首先需要明确的，也就是我们需要保护的内容。

接下来介绍这些需要保护的内容，在从用户与互联网传输的过程中，会有哪些环节涉及到安全问题。

二、不同安全环节的划分

如前面图形所示，信息从用户到互联网之间，要经过文件、应用软件、操作系统、电脑硬件、局域网络、GFW 等不同环节的连接与传递。在不同的环节，有不同的安全特性，也有不同的防护要点，以下分别介绍。

（一）网络环节

用户数据离开用户电脑后要经过不同的路径才能到达互联网，但这些路径对于大多数用户是不可见的。也为了简单表述，我们把离开用户电脑到互联网的中间环节全部称为网络环节，不同的网络环节可以归结为以下五个部分：

1、 GFW，防火长城；
2、 公有网络，包括：中国电信，中国联通，中国移动，中国铁通；
3、 私有网络，包括：公司网络、单位网络、网吧等；
4、 开放网络，包括：旅馆、咖啡屋、书店、候机/候车等公共 WIFI 网络；
5、 家庭网络，包括：家庭连接网络的各种设备。

上面列表中 3、4、5 是人们登录网络的一般方式，然后 3、4、5会接入2 ； 然后 2会接入 1 ，最后通过 1 接入国际互联网。

在网络连接过程中，不同环节会有不同的监听者：在私有网络和开放网络，网络管理员有可能监听；在家庭网络，因为直接连接公有网络，网络运营商有可能监听；在公有网络，可能会有来至政府的要求，也可能有运营商为自己的利益而监听；GFW 也是政府监听的环节。

来自网络环节的监控一般情况下用户是不可见的，也是无法干预的，所以用户可以使用的安全措施也相对简单。

（二）硬件设备

指直接与硬件有关的安全问题。包括电脑、平板、智能手机、移动存储设备、家中无线路由器等的安全问题。涉及硬件的风险，比如使用装有USB键盘记录器的电脑造成的泄密；电脑维修过程中的泄密；丢失、被盗以及淘汰的电脑转让、出售导致的信息泄露；移动存储设备泄密等。

硬件设备的安全泄露往往与用户在现实中接触的人有关，比如电脑维修工，购买、偷窃或抢劫你电脑的人。

（三）操作系统

操作系统安全是电脑所有功能的基础环境，安全问题主要来自系统没有及时修补的漏洞或被恶意软件破坏而造成的信息丢失或破坏。

（四）应用软件

应用软件是直接依附于操作系统，是电脑实现各种功能的提供者。应用软件包括：浏览器、 MSOffice、图形处理软件、一些工具软件（如压缩软件、视频播放器等）。应用软件的安全直接影响到操作系统的安全。

操作系统与应用软件的风险来源相同，包括以下几方面：

1、 安装盗版操作系统时携带的恶意软件；
2、 使用移动存储设备时染上了病毒；
3、 安装一些不良程序时带人恶意软件或病毒；
4、 在浏览恶意网站时下载了恶意软件或病毒；
5、 下载了邮件附件中的恶意软件或病毒。

以上介绍了信息流通各个环节的不同特性。那下面介绍这些环节中，有什么样的入侵者；他们会从什么位置、以什么手法入侵。

三、谁是“敌人”？

潜在的敌人来自多方面，他们有不同的目的和不同的信息窃取方法。只有对侵入者有充分的了解，才能更好的设计有针对性的防范措施。

（一）政府有关部门或个人

头号入侵者可能来自政府部门。政府的第一使命应该是为公民服务，但时常他们中有些人会做出超越法定权限，侵害公民权利的行为，信息窃取是其行为之一。因此，公民应该有防范政府非法窃取个人信息的意识和准备。

许多信息显示，政府可以通过 GFW 获取信息；政府有专门部门，比如国家安全局，公安系统的网警等，通过专门渠道获取用户信息；还有一些隐蔽的政府部门也介入信息的监控；政府还可以通过网络运营商，网吧、旅馆等公共场所进行信息监控。

（二）网络运营商

网络运营商主要指联通、移动、铁通等公司，他们管理着基础的 “公有网络”。网络运营商一方面会执行政府的监管指令，另一方面他们可以从窃取信息中获得私利。比如他们会在管理的设备中注入一些收集用户信息或添加广告的代码，这些谋私利的行为也会增添用户信息的风险。

（三）网络管理员

网络管理员指维护公司、机构、单位或网吧设备的网络管理员。他们窃取信息的动机也许是个人兴趣，也许是受其雇佣者或政府管理部门的安排。他们借助一些专门的软件，可以随时或定时截取用户屏幕，观察用户行为。在前面的“网络与电脑安全防范模型图”中，他们的作用主要发生在“私有网络 “。

（四）恶意黑客

指在互联网上以技术窃取信息的人。他们中有些人的目的就是破坏网络秩序，也有些人的目的是刺探政治或商业信息。这其中有些是个人行为，有一些组织行为，有些是政府支持的项目。他们一般会通过互联网寻找、发现系统漏洞或软件Bug窃取用户信息。

（五）小毛贼

指直接以偷窃信息谋利的新型小偷。他们可能会在一些人口密集的公共场所临时搭建免费Wifi ，当戒备心不强的用户使用时，他们可以获取使用者的私密信息，目的是窃取用户的网上财产或更多的有价信息，在前面的“网络与电脑安全防范模型图”中，他们的作用发生在”开放网络“。

（六）维修工

指从用户送去维修的电脑中窃取信息的人。典型的例子是：一个用户电脑出现故障送去维修，维修者顺便浏览用户电脑中的个人信息。他们这样做也许仅仅是猎奇心理，当发现足够有趣或有价值的信息时，也许会下载到本地或直接发布于网络。如果把电脑交给这样的维修工，无疑是非常危险的。

（七）潜在对手

潜在对手分为两种，一种是熟悉你的人，因为竞争或报复的目的，窃取你的信息。这类人因为熟悉你，所以有机会从你的硬件或软件下手；还有一种可能是你的商业竞争对手或敌对者，他们对你的个人信息不是很熟悉（或者知道一些），他们不一定能接触到你的电脑，但他们可以根据你的部分信息，通过网络或寻找黑客帮助窃取你的信息。

（八）恶意软件制作及运营者

国内有很多恶意软件的制作及运营者，他们会以不良的方式推广软件，并以不良的方式赢取利润，从而直接或间接的破坏用户系统的安全性。

以上基本包含了一个用户所面对的影响信息安全的各方面的因素。

本章视频教程：https://www.youtube.com/watch?v=lKSBqSckYMM

第三章

网络及电脑安全应对措施

前　言

上一篇介绍了与个人信息安全有关的各组成要素。在这一节中，我们将围绕五个安全环节，分别介绍它们的安全防护策略与措施。如上一篇中“网络与电脑安全防范模型图”所示，信息从用户到互联网之间，要经过文件、应用软件、操作系统、电脑、局域网络、GFW 等不同环节的连接与传递。在不同的环节，有不同的安全特性，也有不同的防备要点，以下将分别介绍。

一、网络安全

（一）基础情况

不同的网络环境有不同的安全特性，比如：

1、公有网络与GFW，是你连接互联网时必须通过而又无法做任何干预的部分；

2、在家庭网络，可能不会有网络管理员的监听，但网络运营商能够监控你，并可以直接对你定位；

3、在私有网络，比如你所在的公司或单位的局域网。你的信息和操作可能会被网络管理员监听，但如果你没有注册及登录操作，外部网络无法区分你与你同事的身份；

4、在开放网络，比如网吧或酒店，虽然可能被网络管理员监听，但如果同时有多人使用公共电脑上网，并且你没有提供身份证明的话，网络管理员并不知道你是、谁，外部运营商更不可能知道；

针对以上不同情况，应根据你所做的事情，来调整相应的对策。基本的原则是在安全性高的环境做重要的操作，在安全性低的环境做不重要的操作。

(二) 操作技能

1、Wifi，如果使用开放网络中的 Wifi 信号，要确定 Wifi 信号来自正式渠道 (比如是商家提供的) ，而不是来源不明的;

2、VPN，除了具有翻墙功能外，还可以在访问国内网站时隐匿你的 IP 地址;

3、https，使用 Https 可以保护你浏览网页的内容不被获悉，应尽量保持在任何环境下都使用 Https连接网络;

- https使用方法其实很简单，就是在你访问网址的前缀 http 后面加一个 s，比如在访问 http://www.v2ex.com/ 的时候，在 http 后面 加 s，让链接变成: https://www.v2ex.com/。在 http 后面 加 s，是使浏览的内容得到了一种安全协议的保护。但有以下几点需要注意:
    - 只有支持 https 的网站才能使用 https 加密协议;
    - Google 的很多服务，包括 Gmail，出于安全的考虑，现在已经强制用户使用https ;
- 使用谷歌浏览器搜索一些网站时， https:// 部分不会出现。比如: wikipedia.org，在这种情况下，可以手动在网址前面加入协议名称，如: https://wikipedia.org/ 。如果觉得这样不够方便的话，可以在谷歌浏览器地址栏输入chrome://netinternals/#hsts，在 Add domain 选项的 Domain 右侧输入 wikipedia.org，点选Include subdomains for STS 或 Include subdomains for PKP，然后点 Add 。就可以把wikipedia.org 定义为自动使用 https 访问。

4、一些公共场所的电脑，比如网吧，可能都安装了截屏软件。在这种情况下，即使用https 或 VPN 也无法保证安全，因为你眼睛能够看到的，截屏软件也同样会捕捉到。

二、硬件安全

（一）彻底删除硬盘及移动存储设备中的文件

防止你的移动存储设备，比如U盘、移动硬盘、存储卡等成为泄密渠道，重要文件使用后应该立即彻底删除。

彻底删除文件的方法分为两种：一种是全盘删除，也就是格式化；一种是只把重要文件删除。格式化分为两种：一种是高级格式化，一种是低级格式化。一般认为低级格式化比高级格式化删除文件更彻底，但实际上这两种方法都不能把文件彻底删除。也就是说，用这两种方法格式化磁盘后，其中的数据还有被恢复的可能。

要真正彻底删除全盘文件，需要把文件删除后，或者是格式化后，在用较大的文件重复复制多次，才能达到彻底删除的效果。这个过程手工操作有点繁琐，可以借助其它软件完成。

CCleaner 正是这样一款软件工具，它可以对一个磁盘的全盘或者删除文件后的部分空间做多次擦写操作，达到彻底删除的目的。下载地址: http://www.piriform.com/ccleaner/download 使用方法是，启动 CCleaner 后，选左侧的 “工具” ，再选 “驱动器擦除器”，然后在右侧“驱动器”位置选择你要擦除的磁盘盘符，在最上面选“擦除”整个驱动器，还是仅擦除剩余的空间，然后在“安全”位置选覆盖的次数，有1、3、7、35遍的选择，数字越大擦除次数越多越安全，也越需要时间。

CCleaner 针对的是整个磁盘或磁盘的剩余空间，还有另外一款软件 Eraser 用于彻底删除选定的文件或文件夹。下载地址: http://sourceforge.net/projects/eraser/files/Eraser%206/6.0.10/Eraser%206.0.10.2620.exe/download 安装后，会在鼠标右键自动增加一个选项。如果要删除一个文件，将鼠标移动到要删除的文件上面，点右键，选 Eraser ，这个文件就会被彻底删除。

也可以进入 Eraser 界面，选择一个文件、一个目录，或一个磁盘，做彻底删除。

（二）防范硬件丢失、被劫、被盗

1、 出行的时候也可以使用笔记本防盗锁；
2、 其它各种防止电脑被盗的方法。

（三）防范设备维修中的泄密

电脑送去检修，应防范硬盘中的信息泄密。拆除硬盘虽然安全，但也会给电脑维修带来不便。可行的办法是：

- 本人随电脑去维修处，先不拆除硬盘进行检测，看是什么故障。如果确认是硬盘故障，一般需要到专门的地方去维修或返厂维修。此时需要衡量，是否应该送去维修；或者找可信任的人或公司做硬盘维修；
- 如果确认不是硬盘故障，可以和维修处协商，告诉他们你的硬盘中有重要数据，不能放在维修处，请他们先把硬盘拆除下来。等其它故障维修好，下次来取电脑时，再把硬盘带来安装上。
- 你也可以自己动手先拆除硬盘再送去维修。如果是台式机，要打开机箱盖，找到硬盘，拔出硬盘上的两条线（一条电源线，一条数据线），用螺丝刀拧下硬盘上的螺丝，然后取出硬盘保存起来。等电脑修好后，再把硬盘安装回去。如果是笔记本，一般在底部会有一个活动的卡式开关，把开关拨到开启状态，就可以取出硬盘了。

（四）防范淘汰设备转让或出售后的泄密

淘汰不用的电脑在转让或出售前，用前面介绍的方法做彻底的数据删除；或把硬盘拆下，用锤子彻底砸烂再扔掉。

（五）防范窃密硬件

在使用电脑前，要注意检查是否有异常硬件设备，特别要提防USB键盘记录器。如果你使用公共电脑（比如网吧），它可能藏在主机箱后面，也可能直接连接在主机箱里面的主板上。即使在你自己熟悉的环境，也要提防有人偷偷插上USB键盘记录器获取你的信息。但目前USB记录器还不能自动把信息传输出去。也就是说，放置USB键盘记录器的人要把它取走，才能读取上面记录下来的数据。

三、操作系统安全

操作系统安全主要指电脑的操作系统未升级，或被恶意软件破坏而造成的信息丢失或泄密。

（一）操作系统的选择

操作系统有多种，根据安全的特性，优先使用顺序如下：

1、开源免费操作系统，比如 Ubunut http://www.ubuntu.org.cn/ 。它是一款对桌面程序支持丰富的 Linux 系统，操作容易，安全可靠；

2、付费系统，比如 Windows 或 MacOS 。使用付费软件不仅可以保证系统原本的安全性，还可以获得一定的服务支持，但及时升级补丁预防系统本身的漏洞仍然是必要的；

3、盗版 Windows系统，许多安全隐患往往来自盗版的 Windows系统。现在中国大陆大量电脑使用的是经过处理后的盗版 Windows系统，本着面向事实的态度，我们也将盗版操作系统的安全问题列入教程。

注意：无论任何操作系统，应该尽可能使用高版本。因为高版本的系统一般漏洞更少，对病毒或攻击的防御更好。

（二）操作系统常规技术管理

1、保持操作系统升级；

2、设置登机口令和屏幕保护口令；密码长度应达到8位数以上；；

更多密码安全问题，在《密码安全》一章会有专门介绍。

3、禁用来宾账户

Guest 是 Windows 系统默认的来宾账户，用于临时访问的用户，这会给一些用户窥探系统状态提供机会，一般应禁用 Guest 。方法： 在win7 中，打开 “控制面板” ，打开 “用户账户” ，如果能看见 “Guest来宾账户 ” 就单击它，然后点“关闭来宾账户” 。 如果在 “用户账户” 看不见 “Guest 来宾账户” 的话，说明它已经关闭了。

4、可选用的系统防护软件

1) 杀毒软件

- avast，下载地址：http://download.cnet.com/Avast-Free-Antivirus-2014/3000-2239_4-10019223.html
- AVG ，free.avg.com 下载地址：：http://download.cnet.com/AVG-AntiVirus-Free-2014/ 3001-2239_4-10320142.html

2) 卸载管理软件

- Uninstall Tool 是一款专门的卸载管理工具，完整的使用 Uninstall 的卸载功能，需要在安装软件前就启动它，并通过 Uninstall 安装程序， Uninstall 会监控整个安装过程，记录安装程序对系统的所有改动，并在卸载的时候，保证彻底卸载。如果你经常安装新程序，那么需要这样一款软件保驾护航。

（三）意外情况管理

如果发现电脑有未经授权的访问，应做如下处理：

1、检查文件是否有被非法打开、复制、删除的操作；
2、 检查是否有新安装的程序，以及是否植入了隐藏的程序；
3、 查杀病毒木马；
4、 极端情况下，应该重新安装操作系统。

四、应用软件安全

应用软件直接依附于操作系统，是电脑实现各种功能的提供者。包括：浏览器、 MS Office、图形处理软件、一些工具软件如压缩软件、视频播放器等，应用软件的安全会直接影响到操作系统的安全。

（一）需要知道的知识

1、优先考虑使用国外知名的应用软件，只有在没有替代品的情况下才使用国产软件；
2、优先使用开源软件；
3、从官方网站下载安装程序；
4、避免使用有恶意传统的软件，比如：360系列、腾讯软件、Skype 中文版、各类国产浏览器等。

更多国产软件的使用，在《国产软件安全》一章会有专门介绍。

推荐使用谷歌浏览器（Goolge Chrome），下面简要介绍谷歌浏览器的几个安全问题。

（二）谷歌浏览器

1、使用谷歌浏览器时，当浏览内容不希望在浏览器中留下痕迹时，打开“隐身窗口“，方法：点击右上角浏览器管理图标（三横杆），选“打开新的隐身窗口”，在这个窗口浏览网页不会在电脑上留下隐私信息；

2、移除不可信任的 CNNIC 证书。方法：：

1) 在windows 系统的 “开始” 下面的“搜索程序和文件” 框输入： certmgr.msc ，跳出一个程序界面，点上面的certmgr.msc；

2) 点其中“受信任的根证书颁发机构”，再点下面的“证书”，然后在右边找到 CNNIC 相关的证书；找都后，将鼠标放在上面点右键 “属性”，在第一个选项卡中的 “证书目的”下面选为 “禁用此证书的所有目的”；然后点“确定”。然后用谷歌浏览器访问该地址：

3、https://cnnic.net/，如果显示“服务器证书无效”，表示CNNIC证书已被移除。

4、使用最新版本的浏览器。访问浏览器版本检查网站：

http://www.whatbrowser.org/intl/zh-CN/，这个网站会显示你正使用的浏览器版本号，如果你使用的浏览器不是最新版本，会有一个 “更新您的浏览器” 链接，点击可以进入下载页面，并升级你的浏览器。

五、账户、文件、信息流，及用户行为的信息安全

以上几节主要介绍账户、文件、信息流，及用户行为信息在各个环节中流通时的安全，这四者本身也有一些相关的安全问题，以下分别介绍。

（一）保护电脑账户及网站账户的安全

设置安全级别高的密码，启用两步验证，做好密码管理；关于密码安全问题，在《密码安全》一章会有专门介绍。

（二）保护存储在电脑中的各种主要文件

1、 个人文件分级管理。比如分为：不重要，非关键，重要，关键；

2、重要文件删除后，清空一下垃圾箱，并彻底删除文件，方法见二、（二）；

3、 定期备份重要文件；

4、用加密工具AES Crypt，加密本地存储的重要文件。

1) 官方网站：http://www.aescrypt.com/

2) 下载地址：http://www.aescrypt.com/download/

3)下载安装后：

a. 用鼠标单击一个需要加密的文件，点鼠标右键，点 “AES Encrypt “；

b. 输入一个密码，并重复输入， 一个加密的文件就建好了；

c. 如果要打开这个文件，双击加密文件，输入密码。

注意：如果在一个目录中加密了一个文件，那么，在同一个文件夹中，必须删除（或者复制到其它文件夹）原来的文件。在这种情况下，这个加密的文件才能解密。

（三）用谷歌环聊代替其它聊天工具

（四）避免在网络上公开个人生活信息；避免填写不信任的表单

（五）不在陌生电脑上做重要操作

（六）在公共场所进行重要操作时，防备你的屏幕被窥视。

（七）更多链接

参考链接：

- http://www.williamlong.info/archives/3635.html
- http://news.sina.com.cn/c/2013-10-24/061928516914.shtml
- http://www.maiooo.com/goods.php?id=135

信息流窃听：

- Microsoft handed the NSA access to encrypted messages http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
- 美国安全局曾向国际通用加密技术植入后门 http://www.cnbeta.com/articles/253741.htm

运营商：

- 你们以为运营商只是HTTP插点广告而已么 http://zone.wooyun.org/content/2507

WIFI 安全：

- WIFI 安全：http://news.xmnn.cn/a/xmxw/201310/t20131002_3524258.htm

电脑防盗锁：

- http://www.pcpop.com/doc/0/683/683116_all.shtml

- http://www.kensington.com/kensington/zh/cn/p/1479/K64670/%E8%82%AF%E8%BE%9B%E9%80%9A(kensington)%E9%BB%84%E8%89%B2%E7%BA%A7%E4%BE%BF%E6%90%BA%E5%BC%8F%E5%AF%86%E7%A0%81%E7%94%B5%E8%84%91%E9%94%81%EF%BC%88%E9%BB%91%E8%89%B2%EF%BC%89.aspx

加密软件：

- http://www.truecrypt.org

防火墙：

- 一些工具：http://www.nirsoft.net
- 合理使用 hosts 文件：
    - 编辑 hosts，比如用 https://smarthosts.googlecode.com/svn/trunk/hosts 替换你系统的 hosts （Windows 中，在C:\Windows\System32\drivers\etc\hosts ）可以翻墙，但也有一定的风险，因为hosts 文件或文件中的 ip 地址往往是通过网络获得，如果这里面包含了错误的 ip 地址，也有可能把你引导到恶意的网站。因此，如果如果做重要的操作，也应该避免使用这种翻墙方法，除非你能确认里面的配置一定是准确的。
    - 安装 CurrPorts （这个软件其实挺 ”偏僻” 的，也在犹豫要不要介绍给用户）
        a. TCP/IP 和 UDP 类似电脑与外界网络连接的一个个小窗口，检测他们的状态，可以了解电脑目前运行的状态，CurrPorts是一款检查你电脑使用 TCP/IP 和 UDP 及他们运行端口情况的工具。
        b. 官网：http://www.nirsoft.net/utils/cports.html
        c. 2.10 版下载：http://download.pchome.net/internet/tools/down-19312-11.html
        d. 中文包：http://download.pchome.net/internet/tools/down-19316-11.html
        e. 基本使用方法：启动 CurrPorts 后就会显示电脑中运行软件及系统的状况。
- 避免浏览一些不可信的网站

  比如国内一些广告横飞，丝毫也不尊重用户使用体验的网站，尽量少在这些网站停留，并最好不要点击其间的链接。

推荐：谷歌浏览器有一款插件，可以查看什么网站是可信任的，并且可以自己为可信任或不可信任的网站打分，一个网站获得的好评越多越安全：https://chrome.google.com/webstore/detail/wot/bhmmomiinigofkjcapegjjndpbikblnp

使用方法：当安装了插件，打开一个网站后，点击浏览器地址栏右侧的 WOT 绿色圆圈按钮，会弹出一个评分窗口，先点评级，有信任度和儿童适合阅读度，然后需要在下面选择一个评价理由，还可以写要超过30个字符的评论，再然后，就可以点保存了。

本章视频教程：https://www.youtube.com/watch?v=RMcUCcGeWqo
https://www.youtube.com/watch?v=z8kpimfWMDc
https://www.youtube.com/watch?v=XG2mt0yBTh8

第四章

Gmail安全

前　言

Gmail 的安全介绍分三个部分：

1、账户安全。介绍Gmail 的两部验证，账户安全的五个要点，丢失密码与两步验证时如何找回。其中两步验证是这一章的重点；

2、内容安全，介绍如何检查未授权的访问，以及其它四个防护要点；

3、与 Gmail 相关的两个问题。

一、账户安全

以下介绍账户安全。包括：两步验证，账户安全注意事项，如何找回丢失的密码及两步验证码。

注意：谷歌所有应用账户都是 Gmail 账户。本章中，有的地方叫谷歌账户，有的地方叫Gmail账户，这样区别是为了与不同场景相适合，但它们本质上是一样的。

（一）两步验证

两步验证是保护账户安全的新方法（推特、苹果、雅虎、微软等大型网络服务商现在也都支持两步验证）。应该把两步验证做为保护Gmail安全的标准配置。鉴于很多用户对这种重要保护方法的运行原理还不够了解，我们在此做详细的介绍

所谓两步验证，就是登陆谷歌账户时，需要输入两个密码。这一改进对于账户保护具有很大帮助。但要熟悉它的运行原理，才能够更好的使用它。本章将介绍如何设置谷歌两步验证，获得两步验证码的方法，添加两步验证码后，在其它电脑和智能设备如何登录。

1、启动两步验证

使谷歌账户只在你的计算机登录，可获得更高的安全性。

1) 使用两步验证必须在Gmail账户中绑定一个手机号码，方法：点击邮箱右上角的小齿轮“设置”-“账户”-“更改账户设置”-“其他Google账户设置”-“安全性”-“恢复选项”，确认绑定的手机号码是正确的；

2) 到下面的”两步验证“位置启动两步验证流程；也可以在登入谷歌账户后，通过这个链接进入两步验证设置页面：https://accounts.google.com/SmsAuthConfig 如果通过这个链接进入两步验证设置页面，你还需要再次输入邮箱密码,才能开始设置；

3) 点“修改”进入设置两步验证的页面（如果从上面的链接进入，请点右边的”开始设置”）；

4) ①点“开始设置”，进入四步设置的第一步：填写手机号码。如果您填写过不正确的或已过时的手机号码，请改成正确的。并在“设置您的手机，您希望我们通过哪种方式向您发送验 证码？”下面选择短信或语音电话，然后点“发送验证码”；

5) ②转到“验证您的手机”页面。在收到短信或语音电话后（如果你选语音电话，谷歌真会把电 话打过来），把得到的验证码填写进去，然后点下一步；

6) ③转到“信任此计算机？”页面。会有提示：“受信任的计算机不会在您每次登录时都要求您输入验证码。 即使您丢了手机，无法获取验证码 …..” 注意，这里有一个“信任此计算机 “的选项，默认是选中的。如果这是你信任的电脑，并且你会经常使用它，那么就保持选 中状态，这样就不必每次进入邮箱都输入一次验证码；如果这不是你信任的电脑，请把勾选去掉。这种情况下，你每次进入邮箱都要输入手机上新获得的验证码，然后点下一步；

7) ④转到“确定”页面，会有提示：“启用两步验证 只有当您使用自己的 xxxxxxxx@gmail.com 账户从非可信任电脑或设备登录时，系统才会每次都要求您输入验 证码。如果您丢了手机，可以随时在账户设置中进行更改”，点

确认；

注意：如果你在上面一步，也就是③没有选择信任当前计算机，并且后来不幸丢失了 手机，登录谷歌账户的方法见本节（三）如何找回丢失的密码与两步验证码

8) 转到两步验证的管理页面。在这里可以做关于验证码的更多操作；

9) 这时，谷歌账户的两步验证就设置完成了，并且该账户的验证码也已存储在这台电脑上。也就是说，在这台电脑上30天之内登录 Gmail 账户不需要输入验证码（30天后需要使用新的验证码登录）。但如果你在其它电脑上登录的话，除需要输入密码外，还必须输入验证码。也就是说，从现在开始，即使有人知道你的Gmail 账户的密码，也不能在这台电脑之外的其它电脑登录，除非他人能同时得到你的两步验证码。

如果你只在一台信任的电脑上使用Gmail账户，那么两步验证设置已经完成，现在退出即可。30天后或你在其它电脑登陆时，谷歌将会给你的手机发短信或语音告诉你新的验证码。

接下来，如果谷歌检测到你使用过不支持两步验证的设备或程序（只能输入用户名和密码，不能同时输入两步验证码），比如：一些旧版的安卓智能手机或平板、苹果手机上的Google应用或者是接收 Gmail 邮件的邮件客户端软件。那么，它会显示一个请你创建这类应用设备专用密码的窗口。

2、为不支持两步验证的设备生成专用密码

1) 此时，你可以点击”以后再说“ 离开，也可以点击 “创建密码” ；
2) 当点击 “创建密码” 后，会进入登录账户的页面；
3) 到两步验证的位置，点“管理您的应用专用密码”；
4) 再次输入密码；
5) 在“应用专用密码”部分的“第一步”输入一个使用设备的名字，比如：“我

的安卓手机“，然后点”生成密码“；

6) 出现一个供你的应用设备使用的专用密码；

7) 把这个专用密码输入你的设备的密码框，就可以登录了。

以上是为老设备而设计的支持两步验证的办法。

如果没有检测到你有不支持两步验证的设备或程序，谷歌就会引导你进入“不让您的 Google 账户遭遇锁定”的页面。在这里，可以点击“立即更新” 来添加备用电话号码或打印备用验证码。当你的手机不在身边或丢失后，谷歌系统可以把验证码发送到备用电话号码上。备用电话号码可以是手机也可以是座机。

下面介绍设置两步验证后，在其它电脑上登录的方法。

3、打印备用验证码

备用验证码是一组预先打印下来的两步验证码。当你的手机不在身边或丢失后，备用验证码仍然可以使你登录 Gmail 账户。

1) 提示需要输入应用专用密码，点 “创建密码” ，会要求你重新登录；

2) 登录后，提示填写备用手机号码，提示打印备用验证码，点“立即更新”；

3) 进入添加备用号码和打印验证码的页面；

4) 添加备用手机号码，在“可打印的备用验证码” 右侧，点 “显示备份验证码” 并打印它们。

为了预防手机不在身边，并且你打印的备用验证码也用完或丢失了，你还可以启用移动智能设备 实时生成验证码。支持的设备有 ：安卓手机、 苹果手机、 黑莓手机 。下载地址： https://accounts.google.com/b/0/SmsAuthSettings ，下面以安卓系统为例，介绍使用谷歌身份验证器的方法。

4、安装安卓版谷歌身份验证器

1) 下载地址：

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

2) 安装完成，启动后，点击开始设置。可以手动添加账户，有条形码扫描器和手

动输入密匙两种方式；

3）如果智能设备没有安装条形码扫描器，程序会引导安装；

4）安装条形码扫描器后，点击扫描，扫描“设置谷歌身份验证器”页面的二维码（在 http:// g.co/authenticator页面）。正确识别后，会在智能设备上显示一个六位的数字。把这个六 位数字填入验证码输入框，点击 验证并保存。显示 “谷歌身份验证器设置成功，您的谷歌身份验证器应用已成功配置。”表示谷歌身份验证器与你的谷歌账户已成功建立联系；

5）然后，在登录谷歌需要验证码的时候，就可以用智能设备生成验证码了。

5、管理两步验证码的更多介绍

1）可以删除计算机上存储的验证码。当启用两步验证后，也可以在这个页面（https://accounts.google.com/b/0/SmsAuthSettings）删除存储在本地或其它电脑上的验证码；

比如你去亲戚家住几天，并使用了亲戚家的电脑。方便起见，你在电脑上保存了验证码，当你离开亲戚家时，你应该删除存储在这台电脑上的验证码。如果你离开时忘记删除了，你不必再回去做这件事情，也不必通知亲戚帮你删除，你可以回到自己家后，在自己的电脑上，选”不再记住所有其他受信任的计算机的状态“ 删除所有存储在其它电脑上的验证码。这样，存储在你亲戚家电脑上的验证码就被删除了。如果你在公司的电脑也存储了验证码，同时也会被删除。

2）接收验证码有四种方式：短信、语音、移动设备（智能手机或平板）、从谷歌账户打印下来的备用验证码；

3）如果你要在其它电脑上访问谷歌账户，就需要输入备用验证码。可根据情况考虑是否勾选“在此计算机上不再要求输入验证码” ；

4）关于两步验证的介绍：http://www.google.com/intl/zh-cn/landing/2step/

使用两步验证要点提示

一、启动两步验证;

二、在电脑上使用两步验证的方法:

（一）在启动两步验证的电脑上保存下来两步验证码可以使用30天;

（二）30天到期或者需要在其它电脑登录时得到验证码的三种方式:

1、使用打印下来的10个备用验证码;

2、用注册绑定的手机接收短信或语音发送的验证码;

3、安装谷歌身份验证器软件，实时生成两步验证码。

三、在智能手机或平板上，一些谷歌账户或Gmail客户端不支持两步验证，也不支持网页登录。遇到这种情况时的使用方法:

（一）在电脑上进入两步验证码管理页面，生成专用密码;

（二）把专用密码输入智能手机或平板的密码输入框登录。

两步验证码管理页面功能指示图

(二) 账户安全注意事项

1、定期修改密码

选择邮箱右上角的小齿轮，设置-账户-更改账户设置-“密码”-“更改密码”，输入正在使用的密码和将要使用的新密码，新密码需要输入两次，然后点“更改密码”。

2、设置 “更改密码恢复选项”

为了使你在忘记密码时能够自己恢复密码，可以设置“更改密码恢复选项”，具体方法是，接着上面的操作，“更改账户设置”-“更改密码恢复选项”-“账户恢复选项”，在这里可以设置：您的手机号码、辅助邮箱地址、辅助电子邮件地址、安全问题。

3、在一个账户中管理两个或多个账户

如果你有两个或两个以上的 Gmail 账户，并且经常使用它们，那么可以设置在一个账户中管理两个或多个账户。这样一是方便，另外也能避免因为登陆多个账户而增加的风险。方法是：

1) 在主账户（A）做一个“用这个地址发送邮件”的设置，使它能够以辅账户（B）的身份发邮件。具体步骤：
   a. 在A账户，点小齿轮，设置-账户-用这个地址发送邮件-添加您拥有的B账户；
   b. 在新的小窗口页面输入名称和你希望管理的电子邮件地址，点下一步；
   c. 显示 “确认您的电子邮件地址”，发送验证邮件，点发送验证码；
   d. 去B账户中，会收到“您已请求将 xx@gmail.com 添加到您的Gmail 账户，确认代码：293203937”。把其中的验证确认码293203937，输到A“输入和验证确认代码框” 中，点确认；

e. 小窗口页面关闭，但在“用这个地址发送邮件” 位置，已经多了一个邮箱账户。你就可以在 A 账户，代替 B 账户发邮件了。

2) 在辅账户做“转发”设置，使它把收到的邮件都转发到主账户：

a. 登录 B 账户，点小齿轮，设置 - 转发和 POP/IMAP；
b. 在转发位置点“添加转发地址”；
c. 在弹出的窗口输入 A 账户的地址，点下一步；
d. 在确认转发地址，点“继续”，会显示“添加转发地址，已发送确认码验证权限”；
e. 再登录 A 账户，从新接受到的邮件中复制确认码；
f. 将复制的确认码填写到 B 账户转发位置的验证 A 账户验证框中，点“验证”，A账户地址会进入 B 账户的转发列表；
g. 在 B 的转发列表中点选 A 账户前面的复选框。这样，B账户在收邮件时就会给 A 账户转发一份。

这样，就实现了在 Gmail 主账户A中，同时收发 B 账户的邮件。用这个方法添加更多账户，就可以在一个 Gmail 账户中，管理多个账户邮件了。

4、提防关联程序非法使用你的信息

修改关联程序的权限，选择 ”查看关联的应用和网站” 选项下的 ”查看权限”。具体步骤：

1) 点小齿轮，设置-账户-用这个地址发送邮件-添加您拥有的 B账户；
2) 点小齿轮，设置-账户-更改账户设置-其他谷歌账户设置；
3) 在新页面点安全性；
4) 点安全性页面最下面“账户所授权限”点“查看全部”；
5) 可能需要重新输入密码；
6) 进入“账户所授权限”页面，会显示你授权的外部服务或程序。这些程序或服务具有访问你的谷歌账户的权限，如果不是你授权或你长期不使用的权限，就点击它，并选择右边的“撤销访问权限”。

5、检查邮箱底部

1) 经常检查“上次账户活动时间”；

2) 经常查看“详细信息”，这里会显示你的账户近期登录的时间与IP地址。你可以核对它们与你的实际活动是否符合。如果发现在你未登录的时间，或者未使用的 IP 地址（比如你在北京，但IP地址显示为北京以外的地区），可以去这个网址检查 IP 地址的地理位置：http://www.ip.cn/，如果发现账户有异常活动的记录，应该立即选”退出其它所有会话”，并修改密码，以防范风险扩大，并检查所有可能的破坏，具体方法见下面的内容安全。当然，如果在你使用代理或其它翻墙工具时，IP 地址有变化是正常的。

（三）如何找回丢失的密码与两步验证码

在一些极端的情况下，比如密码或验证码确实丢失或被窃，甚至你绑定的手机号码与安全问题都被篡改了，在所有安全机制都失效的情况下，你还可以求助谷歌账户丢失申诉服务（幸好还有这样的渠道）。

1、找回丢失的密码：

回答多个账户问题来验证你的身份。到这个链接https://www.google.com/accounts/recovery/skt，选“我在登录时遇到其他问 题”。注意，这里的回答多个问题，并非指注册时提交的问题：

1) 输入一个电子邮件地址，以便我们在必要时能够与联你系（必填）；

2) 填写你最后一次使用的密码，最后登录的时间，以及注册的时间；

3) 填写你曾经设定的安全问题，如果已被更改，”跳过“此问题；

4) 经常联系人的电子邮件地址（最多五个），标签名称（最多四个），第一个辅助邮箱；

5) 您使用的其他 Google 产品；

6) 如果你提供的信息与账户中的信息不一致。你还可以尝试另提交一份更准确的申请表单；通常，找回密码是根据你对邮件内容的描述和其它注册信息结合起来进行核实。

2、找回丢失的两步验证码：

当你的谷歌账户设置了两步验证码后，可以通过电脑预存，手机短信或语音接收，打印备用验证码，谷歌身份验证器这四种方式获得两步验证码，用来登陆你的谷歌系统。这四种方式，只要其中一种有效的，就可以得到用于登录的两步验证码。但在一些极端情况下，你的这四种获得验证码的方式都失效了，你仍然可以通过申诉找回你的谷歌账户。具体方法：在输入验证码的下面选“无法使用电话？” 然后点击下一页中的 “我无法使用自己的手机或备用方式”，引导进入申诉流程。与上一个问题类似，如果他人知道或猜测出了你的邮箱信息，也可以用同样的办法得到你的验证码，虽然这并不容易，但总是一个缺口。

二、内容安全

内容安全一节，主要讲如何防止邮件内容丢失，以及来自邮件内容的恶意破坏。

（一）在设置中，检查是否有未授权的非法窃用

前面介绍账户安全，主要是防止入侵者进入你的账户做非授权操作，并检查是否已经有入侵者。那么，如果有入侵者进入你的账户，他们会做什么呢？一方面是获取或破坏邮件中有价值的信息，另一方面可能冒充你发送邮件给你的联系人，混淆视听或骗取更多的信息。还有一种可能，他们只是不动声色的设置一些后门，为今后获取更多信息留下路径。包括三种情况：1.“转发和POP/IMAP”；2.”过滤器”转发；3.”授权访问“，以下分别介绍：

- 检查”转发和 POP/IMAP”
  - 检查是否启用了 POP 或 IMAP，
  - 检查是否启用了转发；

如果有不是你设置的转发或 POP 或 IMAP ，立即停用或删除它们。

- 检查 ”过滤器”
  - 如果存在内容为“转发邮件”的任何过滤器，请检查以确保它们是你设置的地址。点击过滤器右侧的编辑或删除可进行更改；
  - 检查其它的过滤器，确保它们都是你自己设置的。
- 检查“授予访问您账户的权限（允许其他人代表您阅读并发送邮件）”
  - 如果此权限被非法开启，应立即删除，制止未经你授权的账户访问你的邮箱。

（二）内容安全的其它注意事项

1、启用辅助备份邮箱；

另外申请一个邮箱，用自动转发或过滤转发方式把主邮箱的所有往来邮件都往备份邮箱发一份。这样，当主邮箱受到破坏时辅助邮箱会有备份；

经常检查是否有人非法修改了你的辅助邮箱。

2、警惕恶意附件及链接

有些恶意程序会隐藏在邮件的附件里；有些恶意的链接会隐藏在邮件的正文中。在收到来源不明或朋友发来的异常邮件时，不要轻易下载附件或点击其中的链接。

3、重要的聊天内容选择 “不保存环聊记录

最近有关于 Skype 透露用户隐私的报道，Google Hangouts 是一个不错的替代聊天工具。Gmail 环聊的文本内容默认是保存的。如果你聊的是一些私密内容，可以启用“不保存环聊消息”。启用此功能时，聊天双方都不保存文本内容。已经保存下来的聊天记录，你也可以选择性删除。删除后要到”已删除邮件” 中再选择 ”永久删除”。

4、通讯录中的联系人被删除后，30天内可以恢复

通讯录中的联系人，如果被你不小心删除，或被入侵者恶意删除的话，可以选择还原通讯录，恢复被删除的联系人，最长保留时间是一个月。具体方法如下：

1) 在 Gmail 邮箱，左上角的谷歌图标下面，点 Gmail右边的小三角- 通讯录，进入通讯录界面；
2) 点右侧上方的“更多”-“还原通讯录”；
3) 在弹出的小窗口选择你要还原的时间，然后点”还原“，就完成了还原操作。

不安全的 Gmail 运行环境，包括电脑、智能手机、平板的系统环境，它们也会给 Gmail 带来风 险。因此，保护 Gmail 不只是保护账户及内容的安全，还需要注意 Gmail 运行设备及系统环境的 的安全。关于这方面的内容，在《安全使用国产软件》以及《网络及电脑安全》两章会有介绍。

三、两个问题

（一）邮件群发

比如，某机构在香港组织一个活动，邀请了30人参加，活动议程和邀请都是通过邮件中的（密送）功能群发的。但可能其中某一人的邮箱被盗，30人全部被阻止出境。我们的问题是：从密送邮件中能否查看到其它活动受邀者名单？有没有更安全的方法？

密送的邮件不包含密送收信人的信息，所以，密送的收信人，不可能知道发送者还给哪些人人密送了此邮件。

如果出现上例中的情况，有可能是香港发信者使用的邮件服务器丢失了信息，或者是从其它非邮 件渠道（比如其它社会关系或信息传输渠道）泄露的信息。

如果是从服务器丢失信息，那么一个更安全的方法是从不同的Gmail邮箱分别发出邮件，

这样即使消息泄露，也不至于全军覆没；如果是其它非邮件渠道泄密的话，就需要其它相应的安全防护办法。

（二）备用验证码问题

如果邮箱被盗，10个备用验证码被盗窃者打印，两步验证的安全措施如何保障？

下面假设的情景是：有人进入你的邮箱，打印走了备用验证码，但没有修改你的密码，所以你还可以进入自己的邮件，但你担心无法阻止他人再次进入。在这种情况下，是没有办法阻止得到备　用验证码的人再次进入你的邮箱。但是，你可以检查备用验证码是否被他人使用。因为谷歌验证码管理程序会记录你打印出的备用验证码已经使用了几个。

检查方法是，到两步验证管理页面 https:/ /accounts.google.com/b/0/SmsAuthSettings 在“如何接收验证码”-“可打印的备用验证码”右侧点击 ”显示备份验证码”，查看是否有你没有使用的验证码已经被他人使用。如果你的备用验证码已被使用，请点下面的“生成新的验证码”，让过去的备用验证码全部失效。

本章视频教程：https://www.youtube.com/watch?v=m7OGUNgnCA0
https://www.youtube.com/watch?v=FE3LwHz6U7o

第五章

密码安全

前　言

密码是人类的发明，且历史久远。随着互联网时代的到来，密码更被广泛使用，并与人们的生存状态紧密相关，作为从现实进入各种虚拟身份的关卡，密码安全知识也成为现代人必备的基本信息素养。

不知晓风险，也就无从应对风险；要了解密码安全知识，首先应该了解密码的风险来自何方。

一、密码风险的来源

潜在但会影响密码安全的人或群体，可以分为以下五类：

（一）你自己

有点奇怪吗？但想一想，或者你自己随意使用了一个简单的密码，被轻而易举的破解，造成信息损失；或者你设置了一个难记的密码，急需使用时却无法想起，这样的例子不胜枚举。所以，第一个需要防范的正是你自己不够严谨的密码设定习惯。

（二）你身边的人

包括你的同事、朋友、商业伙伴、家庭或亲戚。因为他们知道你的一些私人信息，如果你设置的密码是常用个人信息的组合，就很容易被他们猜中，并造成你的隐私或其它秘密的泄露。

（三）网络上的窃密者

网络上有许多出于各种目的窃取信息的人。他们使用大量设备，各类密码库，多种算法，长时间的测试、破解网络账户，如果你不幸被他们盯上，你的密码又不够安全，那你将没有任何秘密可言。

（四）提供服务的网站

你所使用的网络服务商是可信任的吗？其实，你无法确定他们会不会为了自己的利益而盗用你的密码或出售你的个人信息。即使他们不会主动这样做，他们是否有足够保管密码的能力。最近几年就有国内几个大型网站把用户密码泄露出去的报道，其中包括中国知名的技术社区 CSDN 和国内大型社区天涯论坛。另外，你还要防范这样一种可能：几个网站串通起来，从你的几个不同的账户密码，来推测你密码生成的规律，用于破解你其它账户的密码。

（五）电脑被抄、被盗

最后，你还要防范一种更恶劣的情况 ——你的电脑被抄、被窃。当你的电脑硬件被非法占有的时候，是否仍然能保证你的信息安全？类似的例子还有，如果你的电脑发生故障无法启动，在送去维修的过程中，是否能防范信息泄露？另外，现在有一些账户的安全性是与手机绑定在一起的，如果你的手机丢失或被监听，怎样保证你的账户安全？

以上五类风险，我们在讨论密码安全问题时需要有足够的了解，并在设置密码时，把这五类风险作 为考虑密码安全性的整体框架进行防范。

二、升级你的密码管理方法到密码算法

在互联网时代，不仅风险来源是多方面的，各种新应用也层出不穷，使得用户持有的各种账户数量不断增多，密码管理难度也不断增大，过去依靠记忆或记录来保存密码的方式已经不再适用。现在，需要升级密码管理方法，启用一种更科学的密码算法来管理密码，使你的网络生活更安全、更有效率。

采用密码算法，只需要记忆一套密码规则，就可以管理多个账户，并且在遵循密码设计规范的情况下，获得足够的安全性。

三、密码算法简介

所谓密码算法，就是设计一个方法（算法）把一些与账户及密码有关联的字串混合起来，生成一个密码。

首先，生成四个字串：一个自定义的种子字串，一个与账户域名直接有关的字串（显字串），一个与账户域名间接有关的字串（隐字串），一个与注册环境有关的字串；

其次，根据自己的设定，在这四个字串中有规律的包含字母大小写、数字和符号；

最后，用一种方法把这四个字串混淆起来，形成一个安全度较高的密码。

下面分别介绍这三个环节的具体算法。

四、三步法密码算法生成步骤

辅助生成一个完整密码算法的流程，共分为三步：

1、辅助生成四个字串；
2、伪装字串；
3、混淆字串。

以下分别介绍：

（一）辅助生成四个字串

下表是定义、方法及示例，你可以根据此表的示例做适合自己的扩展与扩充。

	种子字串	网站域名	网站域名	与注册环境关联的字串
		显字串	隐字串	
定义	一组你容易记忆的种子字串，用于所有密码	域名的部分字串，或从域名特定位置选取的字串	网站各种属性的数字表示字串	与这个账户有关联的表示一个外部事物的字串
生成方式	1. 你喜欢的一个短 语的首字符缩写，可以是　一句名言，一部电影名，一些事件的名称，你未来的一个目标，你的一个愿望等 2. 你自制的字符串	1. 前三个字串 2. 1和3和末尾字符 3. 前后两位，中间加后缀字符数量	1. 网站的类型 2. 网站的基色 3. 网站的喜爱度 4. 域名外观圆滑度 * 量化参照表见附表1	1. 注册网站时你关注社会事件的字串 2. 注册网站时你的情绪 3. 注册网站那几天你见过谁 4. 谁告诉你这个网站的 5. 你在什么地点注册的这个网站 6. 那段时间你正和谁恋爱 7. 那段时间你正看什么书
示例	1. 一部电影：The Man from Earth 提取为：TMFE 2. 我所在省份的首字符+我居住地的首字符+我出生年份的最后一位数字+我出生日的最后一位数字。比如：河北，石家庄，1983年9月16日 提取为：hs36	比如 Google.com.hk 1. 提取为：goo 2. 提取为：goe 3. 提取为：go5oe	比如 Google.com.hk 1. 提取为：14 2. 提取为：3 3. 提取为：10 4. 提取为：9	1. 北京时装周：bjszz 2. 失望：sw 3. 张强：zq 4. 刘勇：ly 5. 北京：bj 6. 陈青：cq 7. 小团圆：xty

附表1：网站域名隐字串模拟定义：

网站类型数值定义	网站基色数值定义	网站喜爱度定义	域名外观圆滑度值
邮件类：1 门户类：2 社交类：3 微博类：4 账务类：5 主机/域名服务商：6 博客：7 图片网站：8 视频网站：9 聊天软件：10 社区类：11 书签类：12 在线绘图：13 搜索引擎：14	蓝色：1，blue 白色：2，white 红色：3，red 绿色：4，green 黄色：5，yellow 棕色：6，brown 橙色：7，orange 黑色：8，black 粉色：9，pink 金色：10，gold 灰色：11，gray 桃紅色：12，Peach 棕色：13，Brown	最喜爱：10 比较喜爱：9 喜爱：8 不错：7 还行：6 无所谓：5 非常讨厌：0	字符外观越圆分值越高，越尖分值越低， 最圆：10 … 一般：5 最尖：0 例如： 最圆：O、Q、C、G 次圆：B、P、U、R. …… 最尖：V、Y、Z、T 次尖：N、L、I、 X ……

（二）伪装字串

为使密码字串不容易被识别和破解，可以对以上字串做伪装处理，包括以下三种方法：

1、 位移易识别字串：显字串和一些环境关联字串，如果容易识别，可以做位移操作，使它变得难以识别。比如 google 的前三位 goo ，可以位移两位，就是沿着英文26个字母的顺序分别向后读两位，g 就变成了 i ，o 变成了 q ，goo 位移两位就变成了：iqq ；

2、 设定字符串大小写：比如设定一组字串全部为大写字母，其它为小写字母；或者每个字串的首字母都是大写，其它字母是小写；

3、 嵌套隐藏字串：用一部分数值字串的值，做为另外一部分字串位移的数字，比如，用隐字串决定种子字串的位移，如果种子字串是 TMFE ，显字串是数字 10 ，那么就把 TMFE 按26个英文字母循环位移 10 位，变成：DWPO 。

（三）混淆字串

得到前面四种字串后，就可以做混淆操作了。也可以设计不同的混淆方式。

原始字串：

	种子字串	网站域名 显字串	网站域名 隐字串	与注册环境有关联 的字串
字符	**1234**	**123**	**12**	**123**

示例混淆方法：

1、混乱种子字串、显字串、隐字串、关联字串四者的顺序

2、可以把四个字串的首字母放在最前面，其它依次排列，比如：**1111234232323**

3、可以后三个字串夹在前面一个字串中，比如：**1123212312344**

五、示例步骤：模拟生成一个推特（Twitter）账户密码

练习题：用三步法给 twitter.com 生成一个密码

（一）生成四个字串

	种子字串	网站域名 显字串	网站域名 隐字串	与注册环境有关联 的字串
所用方法	2	2	1	1
结果字串	hs36	tir	3	bjszz

（二）伪装字串

1、种子字串 hs36 大写为：HS36

2、关联字串bjszz位移1步，变为：cktaa

（三）混淆字串

其它字串倒序插入种子字串，HcktaaS33tir6

这样，就生成了 twitter.com 的密码 HchtkaS33tir6

六、结束语

掌握密码生成算法的原理和步骤仅仅是开始，一方面需要反复练习，做到熟能生巧、运用自如；另一方面，还需要不断探寻改进流程的方法，使它更趋完美。

密码算法还需善加使用，对于国内一些本身就不安全的网络应用，配置再强的密码意义也不大，密码只要方便使用就可以了。

要养成定期更换密码的习惯，比如一月换一次。

本章视频教程：https://www.youtube.com/watch?v=yw0S6AfWrSw

第六章

安全使用国产软件

前　言

国产软件纷繁复杂，良莠不齐，在本章里，我们将围绕安全的目的，介绍使用国产软件的原则及边界；介绍一些恶意软件的手法；讲解使用不良软件可能造成的后果及必要的防护措施。在具体的操作环境里，使用者还需要通过自己的观察和体会，持续改善、提高自我安全防范意识。

一、关于国产软件

（一）好软件的特征及国产软件的现状

一个好软件，除提供专有的功能外，还应该提供良好的用户体验，提供对用户信息和隐私的必要保护，并符合以下特性：

1、干净安装。指在安装的过程中，不会携带其它软件，也不会试图修改用户已有的一些配置，比如修改用户浏览器首页等；
2、容易卸载。首先是能够卸载，并且在卸载的时候不会提一些繁琐的问题并试图误导用户做一些无益的操作；
3、不会收集用户隐私；
4、不会与其它程序发生冲突；
5、不携带炫耀醒目的广告。

互联网发展到今天，各种软件/网站已逐渐变得扁平化、国际化，例如许多国际上流行的软件/网站都支持多语言版本。但大多数中国人，或许受使用习惯的影响，往往喜欢选择国产应用软件。

人们在现实的环境中，既需要与各种背景、各种目的的人打交道，又需要防范来自互联网的各种风险。那么，有一些知识就需要学习，比如中国软件生态环境，应用软件受污染的应对措施等。

国产软件也分很多种情况，有些虽然有广泛的用户，也运行久远，但大多没有很好的顾全用户体验，甚至误导用户进行各种不必要、不适当的操作，在给用户使用带来困惑之外，还埋藏了种种安全隐患。

因此，在使用国产软件的时候，应该遵循一些原则并设定必要的边界。

（二）使用国产软件的原则与边界

1、 在没有国外替代软件的时候才使用国产软件；
2、 尽可能从官方网站下载；
3、 使用前要确认这个软件是可信任且没有不良记录的；
4、 在安装的时候，不要一路“下一步”点下去，要注意安装过程中一些默认选项是否引导你安装其它软件，取消不必要的选项；
5、 知道如何卸载；
6、 尽可能在不做重要操作的电脑中运行可能有风险的软件；
7、 如果必须在有风险的情况下使用软件，要清楚的了解可能存在的风险。

（三）如何找到好的国产软件

要避免去国内一些专门下载网站下载软件；去下面这类信誉好的网站找到符合要求的软件：

- 善用佳软 http://xbeta.info/
- 心海e站 http://hrtsea.com
- 小众软件 http://www.appinn.com/

二、部分国产软件的安全性

（一）盗版微软视窗（Windows）系统的安全问题

操作系统是人们首先需要使用的软件，严格来说不应该把Windows 列入国产软件，但现在大量电脑使用的是经中国人自己处理过的盗版 Windows，本着实事求是的态度，我们也把操作系统的安全问题列入本章。

盗版 Windows 分为两种情况，一种是直接使用正版的复制品；一种是正版系统经过所谓“易用性”、“方便性” 的改造后的集成品。

第一种是正版的复制品，在大多数情况下，它与付费的正版软件没有太大区别。安装过程也是全程Windows界面。

现在更广泛使用的是第二种盗版Windows ，就是在正版软件的基础上做了很多外在的改动，比如更容易安装，集成了更多补丁，去掉了不常用的系统部件等。更重要的是，提供了所谓的 “方便性” ，也就是在服务用户的口号下，实际上为了商业目的而夹带了很多用户不需要的垃圾，甚至隐藏着安全隐患的软件。安装时基本都是通过一个 Ghost（克隆软件）实现；并且安装完成后会携带各种国产软件。

现在市面上很难找到干净的第二种盗版 Windows 系统。如果一定要用的话，就选一个比较有名的。也许更有名意味着获得更多的使用者监督而更安全？反正是盗版，又有谁能为这种 “品牌” 提供担保呢？好在盗版的种类繁多，比如去这个网站 http://www.xpghost.com/ 选一个操作系统。

在安装的时候要注意，一般盗版 Windows 系统都有以下操作：

1、锁定浏览器的默认首页；
2、修改默认搜索引擎；
3、预装媒体播放、IM、文字编辑以及一些小系统工具软件等；
4、暗藏木马或病毒。

针对以上问题，在安装完成后应做相应处理：

1) 更换浏览器默认首页，或直接安装新版的 谷歌浏览器；
2) 修改浏览器默认搜索引擎为，比如谷歌；
3) 删除全部预装的应用软件，更新为你熟悉的安全软件；
4) 如果安装的新系统是以前没有使用过的，应该用杀毒软件做一次全面的病毒检测。

一般情况下，高版本的操作系统比低版本的操作系统漏洞更少，对病毒或攻击的防御更好，也更安全，但高版本的操作系统对硬件的要求也更高。因此，在硬件配置足够的情况下，应该尽可能安装高版本的操作系统。

（二）聊天软件

建议使用谷歌环聊，不要使用有泄露用户聊天信息前科的 QQ，和中国版 Skype 。如果不得已必须使用时，请使用在线版QQ （ http://web.qq.com ），避除安装过程中夹带不必要的软件。

注意：使用语音聊天的在线版 QQ 仍然会在浏览器中安装一些插件。因此，使用完毕后尽量卸载或禁用这些插件。方法是：在谷歌浏览器地址栏输入：chrome://plugins/ ，然后停用QQ开头的插件。如果你只是一次性使用在线版 QQ ，请彻底删除这些插件。方法是：在 chrome://plugins/ 页面点“详细信息”，在你要删除的插件“位置”中，找到插件文件的实际路径，然后删除此文件。

应该从Skype 国际官方网站 （http://www.skype.com/）下载原版，不要使用为中国用户定制的中文版。但目前 Skype国际官方网站被 其中国代理光明方正网站劫持，会自动转到 http://skype.gmw.cn ，发生这种情况时，需要翻墙，去Skype 国际官方网站下载。

此外，在使用微信、易信等软件时，要避免谈论敏感内容。

（三）输入法

输入法本来是安静的小工具，但在个性化需要以及云方向的驱动下，输入法成为一种在线应用，既会下载常用词汇方便输入，也会上传用户词汇方便移动使用。在国产软件普遍缺乏规范引导的现状下，输入法也可能被恶意使用，比如有可能上传用户输入的文本内容到开发者网站，造成用户信息泄露。这是关于搜狗输入法泄密的披露：
http://www.wooyun.org/bugs/wooyun-2010-024626 因此，在使用国产中文输入法的时候，应关闭输入法与服务器同步用户词汇的功能。比如使用搜狗输入法时，应在“设置”中关闭搜狗用户账户或关闭 “自动同步用户” 。这有可能影响你的输入习惯，但这绝对是一个安全的办法。

搜狗输入法检查办法：把鼠标移到搜狗输入条上方，点右键，选“设置属性“ - ”账户“ ，查看右上方“账户登陆” 。如果显示“当前账户” 为公共账户，并且右侧显示”登陆输入法账户“ ，就说明用户没有登陆，是相对安全的状态。 如果“当前账户”有电子邮箱地址或用户名，就是已经登陆。这种情况下，可以点搜狗输入法输入条上面中间的小人图标，在新出现的小窗口点”注销“ 退出账户； 如果只是要禁止上传数据，可以在 “账户” -“用户词库” ，把“自动同步用户词库” 前面的对勾去掉。这样，就在程序中关闭了同步用户数据的功能。

（四）国产电子邮箱

电子邮箱是重要的信息沟通工具。但国产电子邮箱，不仅可能被服务商用来获取信息，还可能会被有关部门非法利用。除非你使用的国产电子邮箱要收、发的邮件内容不重要性，或不介意被破坏，否则建议不要使用国产电子邮箱。

安全使用国产电子邮件的方法就是不使用它们。

（五）云存储

推议不要使用百度云盘等服务。有用户曝光百度云盘除了存储空间受到监视和删除，还有个人信息被泄漏。如果要使用国产的云存储，推荐使用云诺硬盘 https://www.yunio.com/ ，他们的服务团队背景比较国际化，相对比较可靠，目前也有一些跨国公司使用他们的服务。

但是无论如何，使用国内的云存储服务应当尽量小心，根据目前的网络环境，我们认为所有的国产服务端都内容审查（虽然各个服务的审查状况不同）。 如果你要与其他人分享大文件，应该把文件名修改为双方都理解的，但又不明显的英文或拼音。最好先把文件做加密或压缩处理，以减少在服务端被“盯上”的机会。

（六）其它推荐或建议

1、浏览器，尽可能使用谷歌浏览器或火狐浏览器；不建议使用国产浏览器；

2、 下载软件，可以用 QQ 旋风代替迅雷。迅雷曾有携带病毒的报道，迅雷软件还会造成用户数据泄密；

3、 尽可能不在重要的电脑上使用国产软件。如果有些国产软件必须使用，请在一台不重要的电脑上使用。

本章视频教程：https://www.youtube.com/watch?v=WIW04dIIFDc

第七章

手机安全

前　言

本章介绍在智能手机被广泛运用的现代社会，如何保护手机的安全，怎样为手机建立一个安全的通信环境。

在几乎每人一部智能手机的今天，手机应用也从最初仅仅是通讯功能，扩展到娱乐、购物、金融、交友等多个领域，甚至用移动小型电脑来形容手机也不为过。手机正为人们的生活提供多种多样的便利，也在现代生活中占有越来越重要的地位。

随着手机应用的范围不断扩大，通过手机泄露、窃取个人隐私、盗窃电子银行账户的事件不断发生，越来越多的人开始关注个人的手机安全。

通常情况下，手机生产商会为手机设置防火墙和杀毒软件，比如安卓系统手机会有短信防火墙、来电防火墙（也就是人们常说的防打扰功能，或称短信或来电拦截功能）。但是，一方面单纯的防火墙和杀毒软件并不能满足用户对手机安全保障的要求 。另一方面，大部分手机用户对于手机安全防范的的认识并不清晰，想要保护自己的手机安全却不知道从哪里下手。

本章我们讲述的手机安全问题，主要是分析手机安全隐患造成的原因；阐述针对这些安全隐患如何保护手机中个人信息的安全；减少手机因丢失、被盗、窃听等造成的信息泄露对人们生活造成的困扰。

本章虽然以安卓系统手机为基础，但鉴于不同手机系统之间的相通性，希望学习者能够举一反三对自己的手机进行安全管理。

一、造成手机安全隐患的原因

通过对各种资料的搜集整理和分析，我们列出以下造成手机安全隐患的原因。

（一）使用不明来源或公共wifi

2012年2月，一篇名为《有图有真相，你还敢用UC上网吗？》的文章在网络上流传

（http://bbs.tianya.cn/post-itinfo-167066-1.shtml），讲述作案者如何针对喜欢使用免费WI-FI的用户

设置陷阱。作案过程分四步完成，速度从最初的2小时提升到最后的15分钟，窃取使用设陷网络用户的账户信息。此消息一出，其震荡不亚于各大网站的“泄露门”事件。

（二）用户随意下载来源不明的软件或访问不安全的网址

随着智能手机市场占有率的迅速扩大，与之相应的手机移动应用程序也呈现爆发式增长。手机用户在享受方便、有趣的各种手机应用功能的同时，由于短信、照片、视频、手机银行账户、支付账户等私密信息大量保存在手机上，手机也成为盗窃者的目标。而为智能手机设计的各类开放的手机应用平台，网络无缝对接等功能，让用户信息与外界有了零距离接触的机会，也为盗窃者提供了窃取的通道。

另一方面，随着手机移动应用的丰富，针对手机的恶意程序、病毒、木马也随之而来。

几乎所有手机用户都有接收到不明来历信息的经历。这种信息往往包含一个网址，一旦访问该网址，手机会自动安装病毒程序，使用户信息在毫无防备的情况下被盗取。

2013年9月，新华网报道了一起手机访问不明网址后，被安装病毒程序，造成用户手机上所有联系人和其它敏感信息的泄露。

还有许多用户喜欢的“免费”软件，也会对手机安全造成威胁。目前，国内大部分用户习惯使用网络上的付费软件，包括游戏、阅读、广播等娱乐软件。寻找免费软件成为人们的一大乐趣。这也给了黑客们可乘之机，“免费”成为许多身份不明软件的诱饵，一旦被上勾的鱼儿吞下，手机病毒会迅速蔓延。

（三）互联网企业不良行为

个人信息如何保护才算得当，这个问题让很多手机用户相当苦恼。他们并没有主动或者是有意向外人透露自己信息，为什么这些信息会丢失呢？

一般情况下，用户安装手机应用软件只注重使用效果，不会或者不懂该软件在安装使用后会获得用户的哪些信息；另一方面，手机应用开发商也不向用户提供涉及用户隐私的说明，或者是将此项说明隐晦的放置在某个选项下，并且默认为同意。

2013年，新浪、百度、腾讯都有不当获取用户隐私的报道。首先，手机客户端缺少隐私条款，而且在版本更新后，针对新增的可能涉及用户隐私的功能，也不及时通知用户；其次，涉嫌对用户数据库进行商业利用。在手机应用“百度搜索”中，相关的隐私权保护条款难以找到；苹果APPSTORE中下载的应用，没有任何隐私条款提示；安卓系统的隐私条款藏在“用户体验”选项

下面，并且在安装时主动替用户在“是否接受隐私保护条款”一项上打勾，这意味着用户在不知不觉中“被同意”了（http://business.sohu.com/20130820/n384592051.shtml）。在这些互联网不良行为的情况下，手机用户信息保护成为难题。

（四）手机破解越狱

造成用户为手机越狱的最主要原因，是用户希望摆脱手机的限制，使用更多的免费软件和破解程序。但是，越狱除了让手机失去手机生产商的保护之外，还会引起手机频繁崩溃、掉线，速度慢，不可靠的数据连接，或不准确定位数据等问题。

手机越狱后，也给了黑客更多窃取个人资料的可乘之机，进行无线网络攻击，用户被恶意软件或病毒侵害而导致账户信息丢失；甚至造成手机设备损坏等等。

（五）对手机安全认识不足

对手机安全认识不足有两种类型：一是了解手机安全的重要性，因此拒绝使用手机第三方程序，比如手机银行。以为只要不使用，手机的安全就得以保障；二是明白手机安全的重要性，但因为缺乏相关的知识，无法对自己的手机进行安全设置。

这两种类型的用户存在于各年龄层次的手机用户当中。手机黑客无处不在，无缝不钻，拒绝使用手机功能，并不能保证手机安全；不能正确为手机添加安全设置，使用户面临同样的手机安全隐患。

（六）手机丢失

如果事先没有对手机进行安全设置，手机丢失后个人信息完全落入他人之手，无任何安全可言。

（七）手机被窃听

有时候我们会接到广告短信，推销窃听服务。这个问题之所以引起人们的重视，是因为手机通信是一个开放的电子系统，只要有相应的接收设备，就能够截获任何时间、任何地点、任何人的通话信息，在用户毫不知情的情况下，个人资料，联系人，短信，往来电话录音，甚至手机用户的地理位置等被窃听。

从目前搜集到的资料来看，实现手机窃听非常简便，常用的手段有：

- 复制手机卡；
- 在手机上安装窃听软件；
- 在手机上安装微型手机窃听器；
- 利用较为专业的窃听设备。

窃听设备和软件在电子市场、网上商城可以轻松购买。复制一张SIM卡用不了30分钟；软件安装只要发条彩信就可以完成；专业窃听器只要直接输入需要窃听的号码就行了；微型手机窃听器的安装麻烦一点，但对于别有用心的人来讲，借用一下手机，或者是在手机维修的时候在手机上安装一个小晶片，就能达到窃听的目的。

二、手机安全隐患解决方案

（一）数据备份

手机数据是用户最宝贵的财富，包括联系人、短信、聊天记录、账户信息、照片、视频、录音、文档，甚至辛辛苦苦搜集的歌曲等。

让手机数据在手机之外保存备份，目前有两种方法：一是定期将手机数据备份到电脑上，这项工作目前主要是通过手机管理程序完成，如豌豆夹；二是将手机数据上传到网络存储空间，如谷歌云端硬盘。

手机用户可以通过数据备份保存信息，万一手机数据丢失，手机管理程序，或才网络存储空间可以帮助手机用户迅速恢复数据。

（二）手机加锁及密码保护

目前，智能手机加锁和密码保护功能已经普及。以安卓系统手机为例，系统设计当中已经加入了密码保护功能和隐私保护功能，基本可以满足用户实现手机安全的初级保护需求。

根据手机生产商对安卓系统的二次开发，以上截图中显示的功能在手机中的位置有可能不同。一般情况，密码保护和隐私保护是在手机的“设置-->安全和隐私”下，或者在手机中有独立的模块“系统与安全”。

提示：随着系统的更新，名称或位置会有所改变，需要用户熟悉自己的手机或阅读手机使用指南。

（三）手机软件授权管理

与手机加锁及密码保护类似，手机软件授权管理程序让用户有了深入了解和接触手机内部管理的机会。用户应该经常查看软件授权状态，建议关闭“自动启动（允许程序后台自动启动）”这项功能。其他权限，可根据具体要求进行调整。

根据手机生产商对安卓系统的二次开发，以上截图中显示的功能在手机中的位置有可能不同。一般情况，手机软件授权管理是在手机的“设置-->应用程序”下，或者在手机中有独立的模块“授权管理”，分别对软件授权、Root授权进行管理。

提示：随着系统的更新，名称或位置会有所改变，需要用户熟悉自己的手机或阅读手机使用指南。

安卓系统手机会为手机用户提供软件授权管理功能。一般用户对手机这一功能的关心程度远远不如手机的其他功能。但我们在前面提到，互联网服务商的不良行为会导致个人信息在不知不觉中被盗取。因此，重视软件授权管理功能，会对手机隐私保护起到一定作用。

（四）手机找回或远程清除数据

如果我们的手机丢失，并且再也无法找回时，清除手机上的个人数据，将个人信息泄露的危害降到最低点，应该是最好的选择。

目前谷歌、诺顿提供了一项手机数据远程清除服务。这项服务要求用户预先在手机里安装相关软件并且启用该服务。

1、谷歌远程擦除移动设备

谷歌提供名为“远程擦除移动设备”的管理程序（https://support.google.com/a/answer/173390?hl=zh-Hans）。要求：“用户在某个受支持的移动设备上，或者安装了 Google Apps 设备规范应用的安卓设备上配置 Google Sync”，“当设备丢失或被盗时，可以使用此功能擦除设备上的所有数据并重置该设备。”，但同时谷歌也提示：“远程擦除操作会从设备上删除所有基于设备的数据（例如邮件、日历和联系人），但不会删除存储在SD 卡上的数据。”。

“远程擦除移动设备”服务目前支持的版本：Google Apps for Business、Google Apps for Education 、 Google Apps for Government。如果您对Google Apps还不了解，建议阅读: <Google Apps Administrator>: https://support.google.com/a/?hl=zh-Hans#topic=24642

谷歌提供了“远程擦除移动设备”功能的操作教程，具体如下：

1) 远程擦除移动设备

如果用户在某个受支持的移动设备上，或者安装了 Google Apps 设备规范应用的安卓设备上配置了 Google Sync”，可以使用 Google Apps 控制台对该设备进行远程擦除。

当设备丢失或被盗时，可以使用此功能擦除设备上的所有数据并重置该设备。用户的设备必须已经配置了 Google Sync 或设备规范。而不能补装 Google Sync 或设备规范，也不能事后再去运行远程擦除。

重要信息：远程擦除操作会从设备上删除所有基于设备的数据（例如邮件、日历和联系人），但不会删除存储在SD 卡上的数据。用户的 Google Apps 数据仍然可以通过网络浏览器或其他授权的移动设备访问。
要对已丢失或被盗的设备执行远程擦除，请执行以下操作：

a. 登录 Google Apps 控制台；
b. 点击"设置 "> 移动版；
c. 在“设备”标签中，将光标悬停在要擦除其设备的用户上方；
d. 点击显示框中的"远程擦除"；
e. 此时会出现第二个框，要求确认是否要对设备执行远程擦除。如果确认要对设备执行擦除，请点击"擦除设备"。

Google Apps 会显示一条讯息，表明该设备已成功擦除。在下次同步时，该设备上的所有内容都会被删除，并且会重置为默认状态。有关远程擦除过程的信息，请参阅相关设备的文档。

关于安卓设备上的远程擦除：通常情况下，设备会在几秒钟内收到远程擦除命令。不过，有时该命令不会立刻到达设备。设备规范应用会每隔3小时检查一次服务器，确定是否有发出的擦除命令。因此，最多等待3小时便可擦除设备，或者等到该设备重新连接到网络时执行擦除。

2) 用户远程擦除其设备

远程擦除可以让用户从"我的设备"页远程擦除其设备。该功能默认情况下是关

闭的，并且，目前只提供给在设备上安装了设备规范应用的安卓2.2 以上版本的用户。请按照以下步骤为用户启用该设置：

a. 登录 Google Apps 控制台；
b. 点击"设置" > 移动版；
c. 启用"允许用户远程擦除设备"；
d. 点击屏幕底部的“保存更改”。

您可以将该设置应用于整个单位，也可以按单位部门为特定用户群组启用远程擦除。在启用该设置后，用户可以按照以下步骤远程擦除其设备：

a. 到"我的设备"页，即使用户已经登录其账户，也需要输入密码才能访问该页；
b. 点击“擦除设备”；
c. 显示包含以下警告内容的窗口：这会从您的设备擦除所有应用和个人数据。任何没有同步的内容都会丢失。确定要继续吗？(This will wipe all application and personal data from your device. Anything that hasn't been synced will be lost. Are you sure you want to proceed?)
d. 点击“确认”，即会擦除该设备。

3）启用擦除设备的优缺点

优点：启用该设置可以为用户带来更大的灵活性。如果设备丢失，安卓用户可以远程擦除该设备，而不必再麻烦Google Apps 管理员；如果用户在周末或节假日丢失了设备，可以立即对设备进行擦除；可以按单位部门启用该设置，从而允许和阻止单位中的特定用户和群组使用该功能。

缺点：启用了该设置的安卓用户可以擦除其设备。如果用户担心自己在没有

意识到操作后果的情况下从“我的设备”页意外擦除其设备，则请不要启用该设置。

2、诺顿手机安全软件

1) 基本功能介绍：http://cn.norton.com/norton-mobile-security/

通过一个基于网络的应用服务为多个移动设备提供保护

- 使用一个便捷的网站，控制对所有移动设备的保护；
- 保护安卓智能手机和平板电脑；
- 使用苹果移动设备远程定位和备份联系人。

帮助找回丢失或被盗的设备

- 在地图上显示丢失设备所在的位置，帮您迅速找到它。此功能也可用于苹果移动设备；
- 可使用内置的网络摄像头来拍摄任何使用该设备（需启用网络摄像头的设备）的人的照片；
- 如果您将手机或平板电脑错放在某处，可以通过发出“尖叫”警报迅速找到它；
- 能够向捡到你丢失设备的人显示可定制的消息，使你可以方便找回设备。

阻止访问隐私信息

- 通过我们提供的安全网站远程锁定丢失或被盗的智能手机和平板电脑，以免他人使用或访问的你信息；
- 可以根据需要擦除设备中的信息，确保你的个人资料安然无恙；
- 阻止企图诱骗你泄露个人信息以此窃取你的身份信息和金钱的虚假（网页仿冒网站；
- 在手机 SIM 卡被取出时立即锁定手机，使手机不能使用其他 SIM 卡。

还原丢失的信息

- 备份安卓移动设备、苹果移动设备中的联系人，并且可在意外删除联系人或有新设备时轻松恢复；

- 允许苹果移动设备和 安卓移动设备之间共享联系人信息。

防御数字威胁

- 消除恶意软件、灰色软件和其他移动威胁;
- 识别可能造成隐私风险的应用程序（如泄露设备上的个人信息），并帮助删除这些应用程序;
- 允许通过拦截不受欢迎的电话和短信消除手机垃圾信息;
- 自动扫描下载的应用程序及其更新程序，查看其中是否存在威胁并清除威胁。
- 提供了在将安全数字 (SD) 内存卡插入移动设备时自动扫描其中威胁的选项。

2) 诺顿手机安全防盗用功能

诺顿移动安全软件中的防盗用功能可以在手机被盗时将其远程锁定并远程擦除手 机上的信息；还可以获取手机坐标，以便在手机遗失或者被盗时找到它。

初次使用防盗用功能需要进行一些设置：在主界面上点击设置防盗用，然后按照提示进行设置。其中，信任的朋友是指当你忘记密码时，哪些朋友可以帮助你解锁手机，在功能简介的朋友列表中会有详细介绍。

诺顿手机安全**防盗用功能可以执行以下操作：**

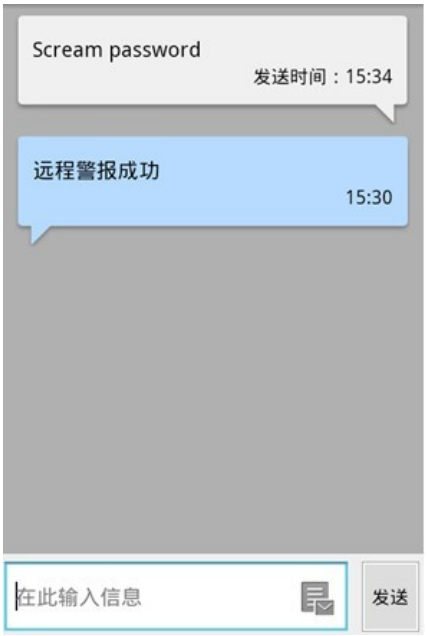
名称	作用	命令格式 （以短信形式发送）
远程警报	将防盗窃命令以短信的形式发送给目标手机，使其发出警报声，从而定位您的手机	Scream [password]
远程定位	将防盗窃命令以短信的形式发送给目标手机，可以返回当前手机所在位置。	Locate [password]
远程锁定	将防盗窃命令以短信的形式发送给目标手机，可以远程锁定目标手机，阻止陌生人访问手机上的信息。	Lock [password]
远程擦除	将防盗窃命令以短信的形式发送给目标手机，可以远程擦除手机上的私密信息，包括联系人列表，短信，通讯记录，浏览器浏览历史，书签以及内存卡上存储的数据。	Wipe [password]
SIM 卡锁定	一旦 SIM 卡被拔出，立即锁定手机，这样即使手机落到其他人手中，也不会被其使用。	无
安全擦除	在手机锁定的情况下，10 次输入错误防盗窃密码，NMS 将自动擦除手机上的信息。	无

远程报警：

通过任意手机发送短信Scream [password]到目标手机；

目标手机收到短信后将会发出持续15秒钟的警报，你可以根据声音的位置找到手机；（即使手机被设置成震动或者静音，也会触发警报）

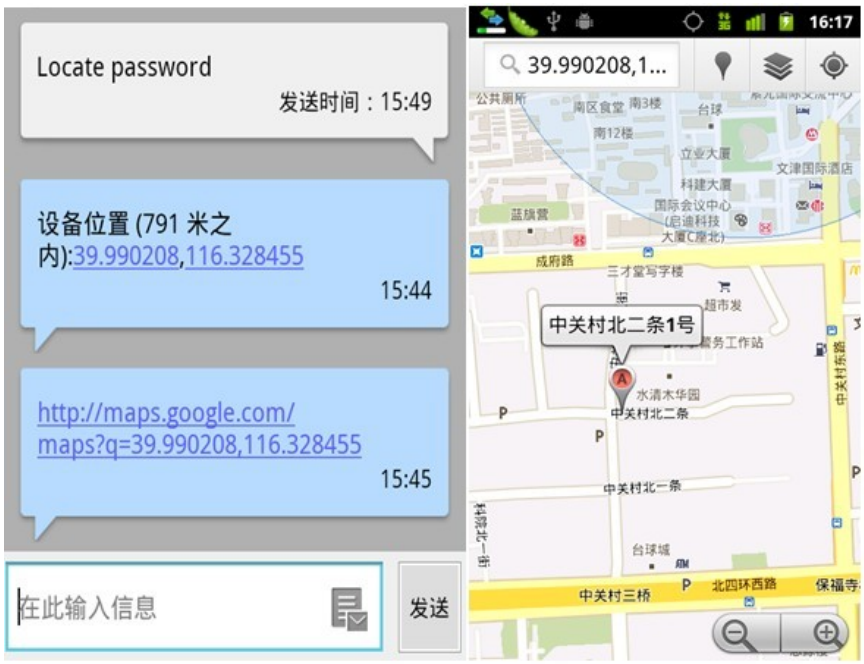
如果仍未找到手机，可以重复发送命令使手机发出警报，直到找到为止。



远程定位：

使用任意手机向丢失设备发送短信：Locate [password]

你将会收到两条短信，第一条是GPS定位坐标，第二条是地图链接，打开链接后，丢失设备当前所在的地点就会显示在地图上。

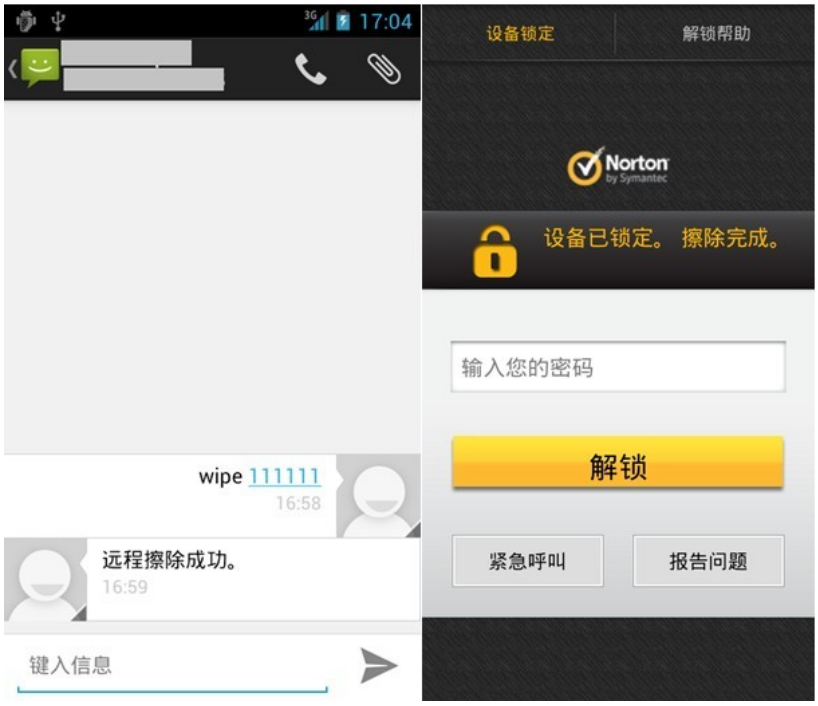


远程锁定：

通过任意手机发送短信：Lock [password]到目标手机，目标手机收到短信后将马上被锁定；当手机被找回时，你可以在锁定界面上输入防盗用密码进行解锁。

远程擦除:

通过任意手机发送短信：Wipe [password]到目标手机，目标手机收到短信后将自动擦除手机上的信息，并将主屏锁定。

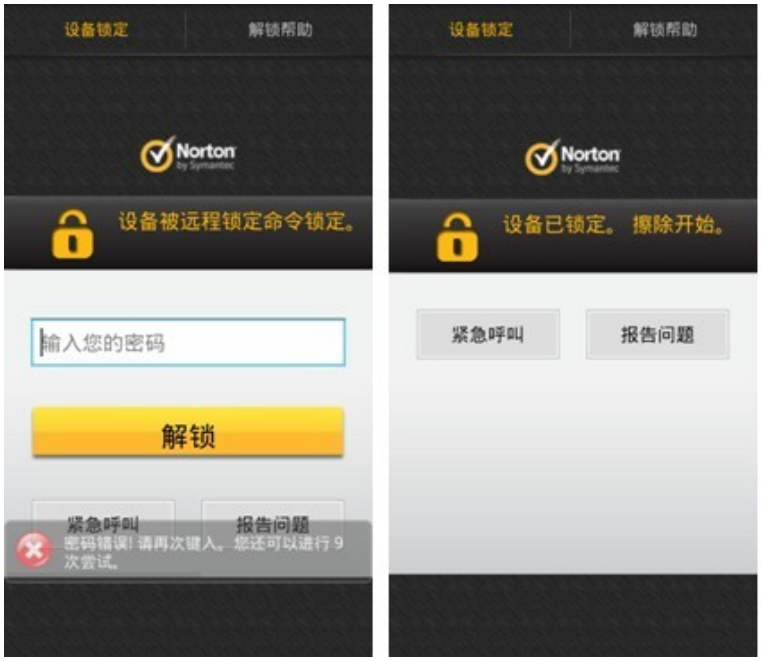


SIM卡锁定：

如果有人将SIM卡拔出或者试图更换SIM卡，诺顿手机安全防盗用功能将自动锁定手机。你可以输入防盗窃密码给手机解锁。

安全擦除：

开启此功能后，当手机被锁时，如果连续10次密码输入错误，将自动擦除手机上信息，并将主屏锁屏。



朋友列表：（用于远程解锁及重置密码而不是联系人列表）

当您初次使用防盗用功能的时候，诺顿手机安全防盗用功能将要求你设置朋友列表。你可以从你的联系人列表中选择信任的人加入朋友列表。朋友列表中的联系人可以在你忘记防盗用密码时帮助你解锁手机或重新设置密码。

当你第一次安装诺顿手机安全防盗用功能并激活该功能时，诺顿手机安全防盗用功能将引导你设置朋友列表。你也可以按照以下步骤在任何时候更改、编辑或者添加朋友。最多可以添加3个联系人到朋友列表中。一旦你忘记了设置的防盗用密码，只需要请朋友列表中的任何一个朋友给的你手机发送一条内容为“Unlock”的短信，即可解锁。解锁后你将被要求立即设置新的防盗用密码。

在NSM主界面选择“防盗用”-“SMS Anti-Theft状态”，输入你设置的密码，选择更改朋友。

单击绿色的“+”按钮添加朋友，联系人列表会自动弹出，可以你从中选择想添加的朋友。

如果要删除朋友列表中的某个人，只需要在朋友列表的主界面上单击该朋友后边的“-”按钮即可。

当你的手机被锁定且忘记密码时，可以点击锁定界面右上角的“解锁帮助”来查看朋友列表，给其中一位朋友打电话，请他给你发送一条内容为Unlock 的信息，就可以解锁手机，解锁后要立即重新设置防盗用密码。

（五）手机窃听

本章的一、（七）部分，已经对手机窃听做了简要介绍。这里再回顾一下常用的窃听手段：

复制手机卡：在得到手机的原装SIM卡后进行复制；

在手机上安装窃软件：也叫卧底软件或间谍软件，类似于电脑上的病毒程序。一旦它被安装在手机里，就能在后台自动运行，保存用户的通话或短信记录，甚至通过远程遥控进行窃听；

在手机上安装微型手机窃听器：这类产品价格比专业窃听工具便宜很多，体积小，内置锂电池，具备完整的手机通话功能，用麦克风收音，但没有扩音器，因此运作时不会发出声音。只要在窃听器上插入SIM卡，就可以借助通信网络传输语音。这类窃听器待机时间较短，要求事先安装，对环境要求较高，而且近距离窃听。因为成本较低，使用方便，而被广泛使用；

专业窃听设备：利用专业窃听设备进行窃听。成本非常高而，不可能公开销售。例如一

种叫做GSM阻截器的设备，它是一种网络信号屏蔽工具，利用无线通信的开放性，每个环节都能成为窃听接口。只要知道对方电话号码，发出窃听程序信号，即使对方手机关机，也会自动执行程序。但这种窃听效果会受到距离限制，当窃听者与窃听目标处于不同通信基站时，不能拦截到目标信号。

特别需要注意的是，如果你的手机处于被窃听状态，在以下三种情况下都会泄密：

通话状态下：

这点一般人都能够理解，专业人士的解释是：手机的通信过程就是使用手机把语言信号传输到移动通信网络中，再由移动通信网络将语言信号变成电磁频谱，通过通信卫星辐射漫游传送到接听者的电信网络中，接听者的通信设备将接收到的无线电磁波转换成语言信号接通通信网络。因此，手机通信是一个开放的电子通信系统，只要有相应的接收设备，就能够在任何时间、任何地点，截获任何人的通话信息。这些设备包括专业的窃听设备、可植入手机的窃听晶片以及窃听软件。

待机状态下：

即使手机在待机状态，也要与通信网络保持不间断的信号交换，监控者很容易利用侦察监视技术发现、识别、监视和跟踪目标，并且能对目标进行定位，从中获得有价值的情报。一些手机还具有隐蔽通话功能，可以在不响铃，也没有任何显示的情况下由待机状态转变为通话状态，从而将周围的声音发射出去。

关机状态下：

手机在关机状态下泄密的情况有两种：一是通过特殊仪器遥控打开手机话筒，继续窃听话筒有效范围内的任何谈话；另一种是在手机制造过程中就在芯片中植入接收和发送功能。因此手机只要有电池，手机上的接收装置就能将其有效范围内的谈话信息接收到，并可随时发送出去。

那么如何防止手机被窃听呢？

1、不要把手机随便借给别人，以防被植入窃听木马；维修时一定要拔出SIM卡，防止他人复制；一旦发现SIM卡被复制，应立即到运营商营业厅更换新的SIM卡；

2、要随时备份数据，记录在本子上，备份到个人电脑里，或者保存到网络存储空间；

3、不要下载来路不明的软件，以免病毒植入；不随便查看来路不明的彩信或邮件，删掉是最好的处理方法；

4、关闭蓝牙、USB等无线接收器的自动开启功能，设置为手动开启，使用完及时关闭；

5、定期为手机杀毒；

6、将手机关闭后，放在密闭的金属盒中，这是一种有效的防窃听手段；

7、重要保密场合，关闭手机后取出电池，让手机完全至于无电状态；

8、如果怀疑有窃听，在通话时可制造噪音，使窃听效果大受影响。

（六）手机定期杀毒

通过以上的阐述，手机可从多个途径感染病毒，而手机病毒对手机用户造成的危害是较为巨大的。因此，手机病毒的防御和定期检测尤其重要。

手机病毒的传播途径有：短信、彩信、电子邮件、网页、下载、蓝牙、不明WIFI等方式。手机中毒后的主要表现有：

- 手机无故自动下载并且安装应用程序；
- 手机预存话费无故减少，甚至欠费停机；
- 手机无法正常接收运营商发送的短信；
- 不知情订购业务；
- 不知情向其他手机发送短信；
- 手机上网数据流量异常增加；
- 个人账户信息盗；
- 其他异常状况。

手机病毒的传播并不是很强，这与手机管理设计有关。许多功能必须得到手机用户的许可才可以使用。但是一旦手机中毒，首先可能出现巨额话费的消费，这是真金白银的财产损失，还有信息丢失或泄密的损失。因此，一下要定期杀毒。

跟电脑的情况类似，如果发现手机有不正常表现，第一时间应请出手机杀毒软件来帮忙。目前可以推荐使用的杀毒软件有：

免费：

AVG Mobilation（AVG手机安全软件永久免费版） http://www.wandoujia.com/apps/oem.antivirus

付费：

诺顿手机安全软件 http://www.wandoujia.com/apps/com.symantec.mobilesecurity.base
McAfee安全软件 http://www.wandoujia.com/apps/com.wsandroid.suite
McAfee安全创新 http://www.wandoujia.com/apps/com.mcafee.mmi
卡巴斯基平板安全软件 http://www.wandoujia.com/apps/com.kaspersky.kts

（七）使用安全的网络

在对手机安全隐患进行原因分析时，第一条我们就提到了手机使用不安全网络造成的后果。在第一条所罗列的安全原因中，盗窃者利用手机使用的UC浏览器上的安全漏洞，以免费WIFI为诱饵，从而盗取用户信息。因此使用WIFI时一定要保持警惕。建议如下：

1、对于陌生的、不需要密钥的Wi-fi网络，在不清楚提供者的情况下不要使用。目前机场、休闲场所、餐饮场所会向客户提供免费网络，在看到有Wi-fi提示标准时，应咨询确认正确名称后再使用；

2、使用安全度高的浏览器。
比如：谷歌浏览器
https://play.google.com/store/apps/details?id=com.android.chrome&hl=zh-CN//

火狐浏览器
http://www.wandoujia.com/apps/org.mozilla.firefox Opera http://www.opera.com/zh-cn/mobile

3、在来路不明的网络环境下，尽可能不进行上网操作；在手机授权管理中，停用各软件的“自动启动”功能；以火狐浏览器的下载为例：首先，确定网络环境是否

安全；其次，选择官网或通过可信度较高的手机应用商店下载，比如Google Play、豌豆荚；最后，安装浏览器后，可在浏览器设置中查看浏览器隐私等选项，根据自己的需要对浏览器进行重新设置。

注意：非专业技术人士直接通过无线网络获取客户信息的可能性非常低，他们往往是借助手机上的各种应用软件来完成窃密。关键是用户要克服贪求免费的心理，以及为手机进行安全设置。

（八）手机丢失的信息保护措施

之前的介绍都是基于手机在用户可操控范围内而言的，如果手机丢失、被窃等情况发生，我们应该做什么呢？

1、 申请手机卡挂失；

2、 报案；

3、 **启动“寻找我的手机”程序，定位跟踪手机，为手机加锁，甚至为手机打上被盗标志（应保证你的手机已经开启此项功能）**；

4、 启动“远程清除个人信息”功能；

5、 购买新手机后，启用“恢复备份数据”功能。

各项功能的启用，请参考二、(四）。

（九）其他

大多数手机出现的安全问题，与手机生产商有关。现在国内销售的安卓系统手机，包括国产品牌和国外品牌中国版手机，比如三星，大都是安卓原版系统 (http://www.android.com/) + 手机厂家自己开发的应用 + 第三方应用 ，形成的一个大系统。这与电脑上作用的盗版 Windows 系统很相似。

如果手机生产商不能为用户提供安全、清洁、可靠的系统，那么购买手机的用户在开始使用手机的那一刻起，已经陷入了风险之中。

三、介绍几类重要的手机软件的安全情况

有相当一部分手机用户因为习惯的原因，或者担心安全问题而不愿意了解，甚至排斥使用手机上的新功能。然而，智能手机从产生到广泛运用，不仅为用户提供了生活、工作、娱乐的便捷，而且也不可阻挡地进入了我们的生活。虽然伴随而来的安全问题确实困扰着我们。

下面我们选择用户普通关心的三个问题进行讨论，希望人们能够正确认识手机应用的现状。

（一）手机银行

手机银行在近几年兴起，而且使用越来越广泛。它将我们从电脑前解放出来，解决了在移动中使用的问题，但是它的安全问题也时常困扰着用户。从各银行系统发布的手机银行安全策略来看，安全性能是开发手机银行优先考虑的因素之一。目前手机银行的安全措施与网上银行基本一致，并配合手机短信使用，同时运行手机安全软件，手机安全基本可以得以保障。但作为一种便捷的移动应用终端，手机银行的安全问题与网上银行有很大区别。手机银行是否安全与用户个人的使用行为有很大关系，例如手机丢失，使用不明来源的公共wifi造成用户信息丢失，刷机越狱等，都会造成手机银行的安全事故发生。因此，对于用户而言，保证账户和密码的安全，保证手机使用网络的安全，手机银行的安全才能得以保障。对于银行而言，最重要的是如何保护用户信息在传输过程中的安全。

（二）应用分发平台

应用分发平台，对于大部分手机用户是陌生的，但是提到 Google Play 商店，大家是不是就明白了呢？这些助手们为手机提供了应有尽有的功能，比如音乐、视频、游戏、阅读、广播，只要你能想到的，网络助手都可以提供。只要点击就可以安装下载，十分便捷。提供这些服务的助手就是应用分发平台。各分发平台之间的剧烈竞争，使手机在销售给用户之前已经打包安装了不少应用，且无法删除。这种打包服务虽然为手机用户提供了便利。但也存在一些安全隐患。

（三）手机杀毒软件

手机杀毒软件在二、(六) 中有详细介绍。手机杀毒软件也是应用分发平台所分发的重要应用之一。手机系统中往往有预装的杀毒软件，它为手机提供了重要的安全保障。手机杀毒软件在二、(六) 中有详细介绍。手机杀毒软件也是应用分发平台所分发的重要应用之一。手机系统中往往有预装的杀毒软件，它为手机提供了重要的安全保障。

手机预置的杀毒软件作为手机自带的“关键软件”是无法卸载的。是否选用所推荐的杀毒软件，需要手机用户根据自己的具体情况来决定。

四、总　结

结合上面的所有内容，我们可以发现，手机软件本身的安全性用户个人是难以控制的；而手机信号的安全性在当下的环境中也难以控制。我们所做的所有努力，就是希望用户在使用手机的时，能够自觉、自主、自如的保护好个人信息安全。

本章视频教程：https://www.youtube.com/watch?v=G0Z3KjLfifk