个人信息安全管理

几个基本安全概念

管理重于技术

总体而言，就是做好系统、信息和账户的分级管理和备份工作，即使技术能力比较低的人，也能通过管理手段，保障自己的信息安全。

有限度的防护

对安全的要求及所付出的成本是密切相关的，甚至呈几何级数放大。要评估自己的信息重要程度如何，或是说，被窃取或公开后对事业对自己造成的损失如何，再决定自己投入的技术和资金。

鸡蛋不装到一个篮子里

不要把所有的用户账号与同一个邮箱关联，不要把所有的密码记在一个文档里或放在一个地方。避免这个账号或记录密码的地方被入侵，会让所有的账号失控。

避免雪崩效应

如果一个邮箱丢失，别的邮箱或账号都以这个邮箱作备份，那丢一个就丢了其他的，也不要把所有的密码设成一样或同样的规律。

按最坏的情况做准备

经常问自己，如果电脑丢失、系统崩溃、硬盘崩溃或账号失控的情况出现，自己正在进行的工作会不会无法进行？自己的社交关系会不会无法恢复？信息安全管理，要以最坏的情况出现作预案。

把自己当成透明，他们什么都知道

不管什么人，不管做什么样的安全防护，除非不把秘密记录下来及完全不告诉任何人，否则都有泄密的可能。进行信息安全管理，是为行动争取时间，减少自己的恐惧与损失。

安全的几个层面

系统的安全

主要指的是自己使用的电脑的安全性，包括有无足够强度的登录密码，登录密码是否定期更换，有没有及时升级补丁修复漏洞，有没有安装杀毒和防火墙的软件等。当系统安全出现问题时，一

则影响 工作效率，二则影响资料的安全，后果不仅仅是白辛苦，也会造成不可挽回原损失。

账户的安全

主要指包括邮箱社交平台等网络应用或服务的安全，一旦失控，轻则导致情况上的恐惧，重则导致资料的丢失，还有一项容易被忽略的，就是人际关系损失。想想看，大家如果主邮箱丢失，有多少人的联系方式就没有了？

虚拟资产的安全

针对虚拟财产是网络钓鱼及木马的主要目的，反而针对民运人士、媒体人及不同信仰人士往往是少数。大家都使用贝宝支付宝，虚拟资产的安全就变得很重要。

人际网络的安全

很多人把人际网络依赖于网上的某个社交应用，如脸书微博等，如果账号被封杀或失控，在此平台上建立的人际网络也会丢失。人际网络不安全，有往往是因沟通不畅引起，让有心之人搅混水有了可乘之机，他们往往是通过单方面提供不对称信息来达到目的的，如，私下告诉你某人如何如何。

影响安全的几个因素

使用习惯及人为失误

最大的影响因素来自于使用习惯及人为失误，例如，写东西时没有定时保存文档的习惯，脚一不小心踢到电脑的开关，一天的工作就不见了。误操作也会占很大的比例，例如把有资料备份的优盘给格式化了，把文档删了还顺手把回收站给清空了，操作完才发现弄错了。另外一个人为失误就是遗忘，设置或更改密码的时候觉得这个密码肯定不会忘记，但要用的时候却想不起来。

不可抗力

不可抗力包括很多因素，最常见的就是丢失电脑资料存储介质，国内的朋友还会碰到被查抄扣押电脑或存储介质的。在国内的服务账号被封杀也很常见，封杀之后，相关的资料就找不回来了。还有种不常见的情况是全部服务中止，例如Yahoo mail 在中国的服务停止了，没有及时备份资料下来，停止后资料就永久丢失了。

病毒木马

有时被病毒木马入侵，也可能导致资料的挂失，一是病毒本身的破坏，二是入侵者人为的操作。

远程操作软件

很多远程操作软件不会被杀毒软件报告为病毒，如果你的电脑被别人接触过，别人在里面安装远程监控软件，就可以实行全面的控制。

账户的攻击方式

穷举

也叫暴力拆解，就是用庞大的密码库对特定的账户进行逐一验证，从而找出弱口令的密码，如仅由几个数字或常见单词组成的密码。不过现在一般网络服务会在几次尝试后要求使用验证码，提高了攻击的难度。

钓鱼

这种方式最常见，便如，在一封Gmail中，说你的系统账号检测到异常，要求你再次输入账号密码验证，如果你在这里输入账号密码，账号密码就会被发送到一个服务器或邮箱存储起来，别人很可以获取。另外，也经常会有人假冒银行或购物网站，诱人上当。国内常见的就是在支付宝买东西，支付的时候给你另一个链接，钱支付到别的网站了。这很有效，我监测过有司的一个钓鱼后台，攻击对象有144个邮箱，获得到12个邮箱的密码，其中就包括了赵连海。无论如何，任何时候要求再输入密码，都要万分警惕。

木马

木马非常常见，主要寄身于一些非法软件下载网站的软件中，这一类木马，杀毒软件会有报告，不易得逞。针对特定人士的，现在主要通过邮箱附件的方式，主要有PPT和DOC等格式，有时针对特定对象还拟定特定文本的邮件，例如像是熟人或朋友所寄送。这类木马针对性较强，且杀毒软件有时候并不报警。这些木马通过系统的漏洞起作用，不下载附件只用线上服务浏览附件，经常升级安装补丁，安装杀毒软件，可以防御。

远程控制

一般是被熟悉的人或冒充熟悉的人接触你的电脑后安装，要避免这种情况的出现。有些国内的朋友有时突然发现上不去网，只好找来宽带的服务商解决问题，这时，有司就能假冒服务商的工作人员，接触到你的电脑，置入木马、远程控制软件，或直接扫瞄电脑的敏感资料。

系统漏洞

这种情况不大常见，但极难防备，例如Adobe Flash在去年就曾经出现漏洞，装有这个插件的浏览器，访问Gmail时会导致Gmail自动授权给特定账号，这个漏洞还是我发现的。出现这种情况，只能听天由命了。

几个传说

电脑被入侵了，被控制了

对于顶尖高手，入侵一台电脑也不是太容易的事情，就当局可以动员的技术力量而言，要入侵一台电脑并非易事，电脑一蓝屏就怀疑被入侵是不必要的恐慌。

手机被监听了，被定位了

基本上，国内的手机全部被录音，短信全部被过滤和记录，特定人士在特定事件时可能被实时监听。当局随时可以定位一部手机的位置，精度在数十米至数百米的误差之内。如果手机被监听，被监听方是不会感觉回声空洞之类的情况发生，但会有轻微的断点，人能觉察出来，其他与正常无异。

身边都是线人

这或许是真的，我们只凭公开的作为及表现来判断就可以了，台下的言行不应作为公开评判的依据。

应对措施

一般安全指引

- 不要让别人接触自己的电脑或移动终端
- 不在陌生的电脑上登陆重要账号
- 不打开未经确认的附件
- 重要文档及信息要多渠道确认
- 其他渠道约定密码
- 不点击邮件中陌生网站的链接
- 不安装未经确认来源的软件
- 使用加密链接的网站服务、产品及手机应用
- 不要开放手机通讯录及相册权限给不熟悉的应用程序
- 只换手机卡不能防追踪，要同时换手机
- 尽量不使用国内的服务
- 尽量不使用国内的服务或工具说敏感的事
- 不保存聊天记录
- 两步验证（Gmail、Dropbox、Facebook）
- 不直接接入公网

账户及文档分级管理

由高到低，按以下序列设置密码：本地系统> 密码管理器> 主要邮箱> 网银应用> 一般应用> 国内

服务。密码需要定期更换。

资料及账号信息多重备份

分不同介质，如光盘刻录、移动硬盘及优盘等；不同时空，备份的东西要放在不同的地方；线下线下，同时做互联网的云端备份和线下介质的备份。

分级分时备份，就是要把资料和信息按重要程序与否进行分级，越重要的备份时间周期越短，备份要求越高，例如线下线下多介质不同地点每隔一天备份一次；比较不重要的，可单一介质较长时间备份一次。自己进行分级分时的备份管理。

及时安装系统补丁

正版的操作系统，开启系统自动更新即可，自动更新间隔时间不要太长，一般应少于一周。非正版软件，可以考虑用QQ管家进行补丁更新，但这种软件也不大安全，甚至有副作用，可在每一次更新补丁后删除。

防毒防木马

一是优选是购买或安装没有（罕见）病毒木马的操作系统，如苹果的iOS系统，或是基于于linux的操作系统，如Ubuntu。二是安装杀毒软件防火墙，杀毒软件可以用Avast，免费注册可用一年，基本够用。三是不要直接接入公网，例如把网络服务商的电缆先接到一个路由，通过路由再接到自己的电脑里，可大大降低被攻击的可能。

信息及人际网络的矩阵化

不要把人际网络建立在单一的社交平台上，尽可能矩阵化，例如脸书与推特相结合，尽可能线上线下结合，万一某个平台失控，还可以保证人际关系的维持。

我的 GMAIL 安全 吗？

至少需要检查以下几项，确认自己的Gmail是否安全：

- 访问来源，有无异常来源？
- 转发设置，有无被转发至其他邮箱？
- POP/IMAP设置，自己没有开启的情况下，是否被开启？
- 过滤设置，是否被设置了过滤条件并将部分邮件转发至其他邮箱？
- 授权设置，是否将账号授权给其他邮箱？

紧急措施

丢失电脑

更改所有在此电脑上使用过的账号密码，通知此电脑保存资料可能涉及到的特别是有可能造成损失的相关人士。

丢失资料

更改所有在此资料中涉及的账号密码，通知此资料可能涉及到的特别是有可能造成损失的相关人士。

丢失账户

更改与此账户关联的其他账户密码及信息，例如：用这个邮箱注册的所有服务的联系邮箱及密码；争取一切办法联系服务商取回账户，通知此账户联系人及保存资料可能涉及到的特别是有可能造成损失的相关人士。

推荐一些工具及服务

- Gmail 及谷歌的系列产品
- Gtalk（SSL连接）>Skype（国际版，慎用TOM版）>QQ
- Whatsapp>微信
- Dropbox、BitTorrent Sync、Wuala（有穿墙能力的网盘）、Emule（电驴，http://www.emule-project.net，穿墙下载或发布）
- Firefox 或Chrome 浏览器
- Recuva 或Final Data（恢复误删数据）
- Ccleaner（安全删除）
- Twitter 、Facebook、Google Plus

国内朋友可参考的几个问答

做传唤笔录怎么办？

拒绝口头传唤，只接受书面传唤；不做证人笔录，至少不在证人笔录上签名；做嫌疑人笔录开始时一定要让对方写清楚案由及写清楚有没有挨打挨骂；尽量少提供信息，不回答与案由无关的问题。

被喝茶怎么办？

自己的事不记得；别人的事不清楚；特定事件不了解没看法。

他们问你密码怎么办？

我刚告诉境外朋友把我密码改掉了，我现在还不知道新密码。

一点建议

- 至少掌握一种电脑系统恢复办法
- 国内的朋友掌握两种或以上的翻墙方式
- 每天花上几分钟留意最新的翻墙及安全信息
- 多留意这个网站：https://security.ngoinabox.org/zh

有问题写信问我：wenyunchao@gmail.com

北风，2013 年5月11 日