海外学员信息安全

注：本文是针对海外学员而发表。大陆学员可以参阅，但一些部分和大陆学员无关。

目录

通用原则

常见攻击方式

本培训教材旨在帮助您深入理解信息安全以建立最佳防范方法。请花时间学透本教材，并且尽力采取提及的防范措施。不能粗略地看一遍就完事。请多读几遍，以确保理解。

让我们先讲一个故事，以说明几种常见的安全隐患。相关的安全防范措施会显而易见。

大卫辗转逃离了中国，抵达了美国某机场。他查到了本市炼功点的联系方式，给约翰打电话寻求帮助。

约翰从机场接到了大卫。大卫在约翰家住了几天，随后租房搬了出去。此间约翰和大卫讨论了很多事情，其中包括大卫在国内遭受的迫害和在本地立足的打算。大卫的手机也使用了约翰家的上网服务。

大卫在手机通讯录里加上了约翰的联系方式，并加了更多细节。比如炼功点网站上只列出了约翰的电话和名，现在大卫在手机上也加入了约翰的姓和中文名。因为大卫还会到约翰家来，因此他在通讯录里也加上了约翰家的地址。为了申请居留，需要用电子邮件传送文件，于是大卫也将约翰的电子邮件加在了通讯录里。

约翰带大卫到了集体交流的地方，大卫见到了更多的学员。大卫的通讯录里加入了更多人的联系方式。

过了一段时间，大卫得到了一个安全电子邮箱。这个安全电邮被加入了当地学员的电子邮件群组。现在大卫开始看到参与不同项目的学员发的电子邮件。大卫开始了解各个学员承担的角色，也经常往通讯录里添加学员们的这些信息。例如，约翰经常组织集体交流。大卫断定约翰肯定是协调人甚至是佛学会辅导员。海伦在每次集体交流结束时都会谈到各种项目。大卫断定海伦大概是佛学会成员。他在通讯录里将约翰标为佛学会辅导员，海伦为佛学会成员。

后来，约翰在他的信箱里收到了一封电子邮件，提醒他用邮件里的链接修改密码。这个邮件看起来象是邮箱系统管理员发出的。他打开了链接，网页看起来挺熟悉。页面提示他输入现在的密码，然后再输入新密码两次。他照做了。他觉得有点奇怪，因为在手机上保存的旧密码仍然可以访问邮件。

后来，大卫收到了来自约翰的电子邮件，邮件的附件名字是“居留申请所需文件”。大卫觉得有点奇怪，因为他没有索取这个文件。不过，因为他们之前讨论过居留申请，这个邮件似乎也在情理之中。他信任约翰，因此打开了附件。大卫注意到文件打开的时候有点延迟，他想电脑或许太旧了，就没当回事。

后来，约翰收到了来自大卫的安全邮箱的邮件，附件名字是”我在中国遭受迫害的故事”。约翰觉得有点怪，因为他没有让大卫写这个。但是因为约翰和大卫之前谈到过他在中国遭受的迫害，而居留申请又需要这样的文件，因此这个邮件似乎也没有太出乎意料。约翰打开了附件文件。这的确是之前在明慧网上发表的关于大卫的故事。约翰觉得有点异样，因为文件打开的时候有短暂的延迟。

后来，约翰的家被人闯入。笔记本电脑、U 盘、外接式硬盘都被盗，里面有项目的源代码、服务器的密码和密钥，以及一个关于未来项目的计划。

这不是故事的结尾，但我们可以停下来数一数有多少安全漏洞，我们怎样做才能阻止针对这些漏洞的攻击。

从电子设备上删除微信、抖音及类似应用程序（App）

来自大陆的微信等应用收集很多个人信息，包括联络人的信息。邪恶从这些公司索取这些信息毫无障碍。因为邪恶可以很轻易的获取这些信息，这些应用对于我们就成为很大的安全威胁。

在第一次开启微信时，微信会索要授权以查看手机上的联络人的细节。如果不准许，微信会退出。如果您可以运行微信，说明您已经授权微信查看您的联络人信息，不管您理解与否。

如果大卫已经在邪恶的黑名单上而且手机上装有微信，从机场开始大卫辛勤加入的联络人细节都会被微信取走，从而落入邪恶手中。经由微信，大卫通讯录里所有本地学员的信息都被送到了邪恶那里，其中包括约翰的姓，中文名，家庭住址，电子邮件，承担的角色。微信使用家庭网络上网的时候，微信服务器也知道了这个家庭网络的 IP 地址。

于是邪恶可以向约翰发送网络钓鱼电子邮件。邪恶也可以直接攻击约翰的家庭网络和设备。当钓鱼邮件和网络攻击失败时邪恶可以闯入约翰的家进行物理攻击，偷走笔记本电脑和硬盘。邪恶还可以骚扰约翰在中国的家人。

如果约翰在机场向大卫解释了微信的危险性，大卫马上从手机上删除了微信，那么这一切都不会发生。

我们要求所有学员从主要电子设备（手机，平板和电脑）里删除微信、抖音和来自中国的类似应用程序（App）。如果非用不可，那么建议在一个没有学员通讯录的单独设备上使用。

谈论敏感话题时，请关闭设备并将设备从身边拿走

如果移动设备已经被侵入，那么就可能成为监听设备。当谈论敏感话题时，请关闭设备并将设备从身边拿走。这些谈话内容，如果被邪恶掌握，邪恶就可利用这些信息进行社交工程网络攻击。例如，故事中提到的邮件附件的文件名就与约翰和大卫以前讨论过的话题有关，这使得当事人很难避免堕入陷阱。

通过网络的直接攻击

通过微信等应用邪恶可以获取使用者的网络 IP。这个 IP 地址可能是家庭网络的 IP，也可以是媒体公司办公室的 IP，也可能是大组交流场所的 IP。装有微信的设备到哪里就会泄露那个地方的网路 IP。有了 IP 地址邪恶可以直接攻击该 IP 地址上的设备。

针对这种攻击的防护措施：启用防火墙，保持所有设备处于完全更新的状态。这里的设备包括路由器和所有内网的电脑和移动设备。

通过网络的欺诈攻击

欺诈攻击是通过精心设计的电子邮件或短信欺骗设备用户，让设备用户做一些不该做的操作从而导致设备中毒，比如诱骗用户用电邮中的链接去修改密码导致密码被盗取，比如诱骗用户打开电邮的病毒附件导致中毒，比如诱骗用户打开电邮中的链接打开恶意网页导致中毒，比如诱骗用户扫短信中的二维码打开恶意网页导致中毒，等等。如果邪恶知道目标用户的更多信息，比如目前关注的热点，人际关系，过去的谈话内容等等，邪恶就可以利用这些信息制造社交工程陷阱。信息越细致，陷阱就越有欺骗性。

就象故事中讲到的，当邪恶获取了约翰的电子邮件地址后，向他发送钓鱼邮件，让他通过电邮中的链接“修改密码”。这样的邮件为什么有欺骗性呢？是因为它利用了我们邮件系统的行为特征。

在您的电邮密码快过期时，我们的电子邮件系统会提醒您。邪恶利用了这一点。

避开这个陷阱的办法很简单。当您看到这个提醒后，直接到电邮网站页面登陆，在那里修改密码。

永远不要使用电子邮件中的任何链接修改密码。

作为一个更广的原则，永远不要打开电子邮件中的任何链接，除非您确信它们是安全的。

假设约翰没有遵守这个安全原则，点开了电子邮件中的链接修改了密码。因为这个链接里面的网页是被邪恶控制的，它就会拿到约翰在我们电邮服务器上的密码。邪恶就可以登录到约翰的电子邮箱，并设置一个邮件转发机制。从这时起，约翰收到的所有邮件就被邪恶所掌握，从而泄露大量信息。就算是约翰以后修改邮箱密码，只要转发机制还在，邪恶仍然会继续收到约翰的电子邮件。

查看电子邮件访问记录

一旦邪恶获得了约翰的电子邮件密码，它就会登录到约翰的电子邮件帐户并设置转发规则。对邪恶而言这可能是个一劳永逸的好办法。

针对邮件密码被盗我们的电子邮件系统有一种防护。我们的电子邮件系统每天都会告诉用户电子邮件的访问记录。如果约翰知道如何正确的检查访问记录，那么密码被盗的问题就会在一天之内被发现。之后约翰需要在干净的电脑上更改密码，查看并删除所有转发规则。

电子邮件访问记录包含过去 24 小时内对此电子邮件帐户访问的信息，包括访问者的 IP 地址，访问方式以及访问是否成功。正常情况下，通常显示的 IP 地址应该是您家庭电脑的 IP，工作单位电脑的 IP（如果您在工作的电脑中查看电子邮件），或手机的 IP（如果您从手机上查看电子邮件）。此外的任何 IP 都是可疑的，尤其是来自其他地区或国家的 IP。可以到 whatismyip.com 来查看您正在使用的电脑或手机的 IP。

如果约翰比较警觉，他会从电子邮件访问记录上注意到一个不熟悉的 IP。这足以提醒约翰，您 的电子邮件密码已泄露，并且电子邮件帐户设置可能已被更改。

假设约翰没有发觉，从此邪恶将能够收到约翰的所有电子邮件。邪恶将会监视电子邮件中的各种讨论和对话，以收集信息并寻找机会通过发带病毒软件的电子邮件和社交工程来破坏他人的电脑。

由于约翰和大卫讨论过居留申请，邪恶从约翰的电子邮件帐户向大卫发送了一封带有病毒软件附件的电子邮件。

保持电脑等设备更新到最新

作为一个准则：不要打开电子邮件中的附件，除非您确定附件是安全的。

但是如何知道附件是否安全？最简单有效的办法就是打电话给发件人确认。不要用电邮确认，因为此时发件人的电邮可能已经被邪恶控制。

大卫与约翰讨论过居留申请，现在接到了约翰的这封电子邮件，其中附有一份名为“居留申请所需文件清单”的附件。如果接到的邮件与附件和自己毫不相关，或是邮件来自陌生人，那么会比较容易不上当。但这时对

大卫来说，这封电子邮件是和自己相关的，而且发件人是自己信任的。这就是邪恶利用了受害者之间进行过的讨论，创造了一个完美的社交工程陷阱。

那么这就没有办法了吗？还不是。

这时正确的做法是在打开附件的文档之前打电话给发件人确认。这样约翰就会意识到自己的电子邮件帐户已被盗用。他需要在干净的计算机上更改密码，然后查看并删除转发规则。

让我们假设大卫没有打电话给约翰确认并落入了这个陷阱。他打开文档时触发了嵌入的病毒软件。接下来会发生什么将取决于附件里是什么样的病毒和我们电脑上有什么样的防护措施。

有一部分病毒针对的是操作系统或应用程序（Word，PDF 阅读器，Java 等）中公众已知的漏洞。对于这种情况，如果操作系统和应用程序已更新至最新，那么病毒就无法造成破坏。

这种防御的手段是很有效而且非常容易做到的，只要能保持操作系统和应用程序一直是更新到最新的状态即可。但很多人没有做到这一点。

当我们接到收到操作系统或应用程序的更新通知时，应该立即下载和安装更新，不要拖延。大多数应用程序（浏览器、PDF 阅读器、Java 等）都有自动更新机制。这很方便，所以务必要打开自动更新。

Windows 将自带的防御程序 Windows Defender 作为操作系统的一部分，这是一个很好的防御程序。用它就可以了，把电脑制造商捆绑的其它试用期的防病毒软件删除掉。Windows Defender 作为操作系统的一部分，在系统更新时会同时更新。

Mac（苹果）操作系统带有 Gatekeeper，XProtect 以及病毒删除工具，这些也都是非常棒的软件。除非您很在行，否则使用这些即可，无需为 Mac 使用其它防病毒软件。

另外，在电脑中把不使用的应用程序都删掉，以避免未来病毒通过攻击它而进入电脑。

如果大卫的电脑更新至最新，并且病毒针对的是已知漏洞，那么他的电脑就不会被攻入。

但如果病毒针对的是公众未知的漏洞怎么办？该漏洞尚未被修补，所有防病毒程序尚未能对其识别和防御。

那么就没有办法了吗？还不是。

在电脑上使用普通用户以完成绝大多数工作

电脑上至少有两种类型的账号：管理员用户（administrator) 和普通用户 (standard user)。

如果您以管理员身份登录，则可以在电脑上执行任何操作。这听起来不错，但如果您在使用管理员用户时触发了病毒，病毒会拥有相同的权限，也可以在电脑上执行任何操作。

如果您以普通用户身份登录则会安全很多，同时并不影响您完成绝大部分工作，只是有些限制比如无法写入系统文件夹。那么如果您触发了病毒，它将同样无法在系统文件夹中创建它的东西。这是一个很好的保护，而且通常情况下您也不需要写入系统文件夹的权限。

所以只要以普通用户身份登录，大多数病毒即使针对的是未知漏洞也无法造成损害。

好消息是，在现代操作系统（Windows 和 Mac）中，即使登录的用户是管理员，也是在普通用户的模式下操作。如果您要进行需要管理员权限的操作，Windows 会要求确认（请不要关闭这个提示），Mac 会要求输入密码。这就是您阻止病毒修改操作系统的机会。

在大卫的案例中，当他从电子邮件中打开附件时，系统会询问是否允许对系统进行更改。这时他应该警觉，因为打开一个文档不应该会引起对系统的更改。

为了避免在没有阅读和思考的情况下快速单击“是”，建议以普通用户身份登录，这时如果病毒要更改系统，系统将询问管理员密码，而不是简单的“是”与“否”。这个提示会让我们停下来思考一下。

如果您在 Windows 或 Mac 电脑上看到提示，让您输入密码或允许某种程序运行，请仔细阅读提示信息。如果不是由您引发的，不要输入密码，也不要让它运行。

如果您在手机上看到某种提示，让您做什么操作，请仔细读清楚。如果不是由您引发的，那就不要点击。这时，请强行关闭所有运行的 App，以去掉这个提示。

作为一个一般原则，当系统或邮件或短信提示您做某种操作时，请停下来想一想。如果不是您有意触发的，不要执行这个操作。

只运行信任的应用程序

只要使用普通用户身份登录，一部分病毒即使针对未知漏洞也不会造成损害。

“一部分”病毒，而不是所有病毒？是的，一些更高级的病毒能够自主的将普通用户提升为管理员，之后再对系统进行更改和破坏。

针对这些病毒，我们就没有办法了吗？还不是。

我们对此的防御方式是“应用程序白名单”：只运行自己信任的应用程序。

这些最先进的病毒虽然是针对未知漏洞并具有自主提升用户权限的能力，但如果它不在我们的受信任的应用程序列表中，它将不被允许运行，这样就无法对我们的电脑造成破坏。

在 Windows 系统上，可以使用 AppLocker 来创造和使用“应用程序白名单”。

在 Mac 系统中，针对应用程序有 3 个设置：仅允许 App Store 中的应用程序；允许 App Store 和已知公司的应用程序；允许运行任何应用程序。绝大多数情况下应该仅允许 App Store 中的应用程序。特殊情况下可以允许已知公司的应用程序。但公司的数字证书有被盗的可能性，所以允许已知公司的应用程序还是有风险。

只运行自己信任的应用程序的原则是终极防护。邪恶的病毒再高级也不会在我们信任的应用列表里。只要不执行病毒，病毒就不会造成破坏。同样的道理，如果不上当，病毒邮件或短信或二维码都不会对我们的设备造成破坏。

让我们假设大卫的电脑中没有这种防御，所以病毒成功的攻入他的电脑。该病毒将可以捕获他所有的在线帐户的密码，包括他的电子邮件帐户。邪恶会继而登录到他的账户并设置转发规则，而且向约翰发送病毒软件附件，标题为“我在中国被迫害的故事”。如果约翰打开此文档并落入了陷阱，他的电脑会被攻入。循环将继续，邪恶将重复使用这个办法来破坏更多人的电脑和盗取更多的信息。

在监视约翰的网上活动一段时间后，邪恶认为值得去一趟约翰的家。根据早些时候收集到的信息，邪恶闯入了约翰家中，并偷走了笔记本电脑，外接硬盘，USB 储存盘。

使用密码、加密和备份，保护设备上的数据

到了这一步，我们已经失去一切了吗？还不是。如果我们之前为我们的设备提供了保护，则不会。

对于移动设备，我们可以启用密码和自动数据删除。对于电脑，Windows 系统有对整个硬盘加密的 BitLocker，PGP 以及 Veracrypt；Mac 系统有 FileVault。使用这些在所有设备上开启加密，同时对外接硬盘和 USB 储存盘也进行加密。即使邪恶拿到了这些设备，它也无法获取任何信息。

但是如果我们没有了这些设备，我们的工作会受到严重影响，同样是损失。为了防止这种损失，我们需要在所有设备上设置自动加密的备份，将数据加密后，备份到远程站点或云。如果设备丢失，被盗或损坏，我们就可以将数据从备份恢复到替换设备中，得以迅速恢复工作。

我们这里谈到的攻击主要是邪恶针对我们的攻击。我们只谈到了最常见的几种方式。我们也谈到了一些重要防范措施的概念。实施的细节可以通过搜索找到。

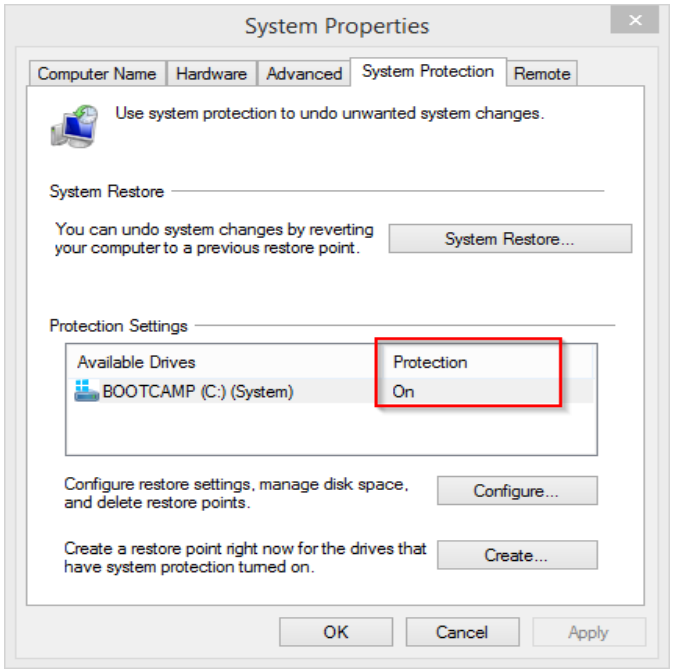
通用技术细节

数据备份

下面谈到的三种备份方式是针对不同情况的防范，都需要。

同盘备份

这个功能只在 Windows 上有，名称是系统保护 System Protection，也被称为系统还原点 System Restore Points。它使用磁碟区阴影复制（Volume Shadow Copy）将磁盘的快照保存在同一个磁盘上。启用系统保护，可以帮助恢复被误删除的文件或同一文件的早期版本。在 Windows 更新失败或因系统文件损坏而无法启动系统的情况下，有可能恢复文件并使系统再次可启动。按 Windows 键并输入 "system"，在搜索结果中点击 "System"，然后点击左侧的 "System Protection"，打开如下窗口。



案例：误删重要文件。操作员误删报纸模板文件，导致印刷厂无法印刷。技术人员找到前一次正常工作时的系统还原点，恢复模板文件，让印刷厂及时复工。

案例：软件安装导致系统无法正常启动。安装软件之后系统进入反复自动重启的状态。技术人员由 F8 让系统停在出错的地方以查看错误代码。从错误代码看出是系统注册表损坏。技术人员取出硬盘，接到另外一台电脑上从系统还原点中恢复出系统装软件之前的注册表文件。原机得以正常启动。

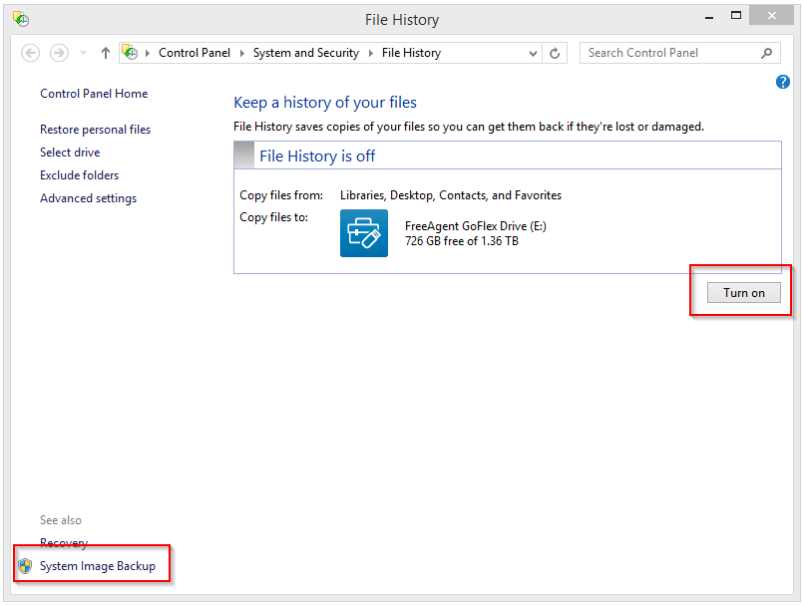
系统保护很有用。但在硬盘发生故障的情况下，数据和还原点会同时丢失。所以我们还需要异盘备份。

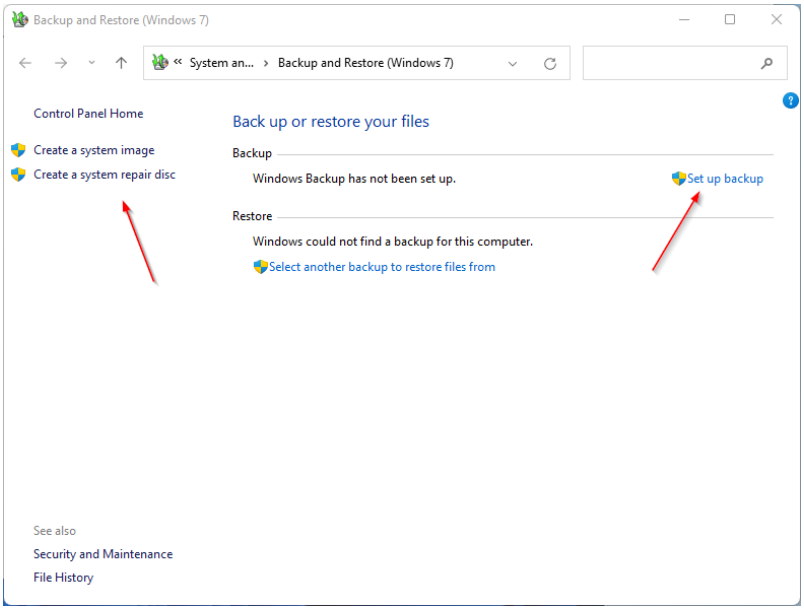
异盘同地备份

苹果操作系统有内置工具 Time Machine，Windows 有文件历史记录 File History，都是通过专用的外部磁盘备份数据。建议使用新的或空白磁盘，以避免在初始设置时丢失数据。

苹果：在 Spotlight 中搜索 Time Machine，找到后开始配置。Time Machine 备份可以用来恢复整个系统或者单个文件。

Windows：按 Windows 键，输入 "file history"，在搜索结果中点击 "File History "，找到后开始配置。File History 不包含系统镜像。请务必启用系统镜像备份，以便将来将操作系统恢复到早期的备份：





确保工作时保持备份磁盘与计算机相连，以避免丢失任何数据。如果只是偶尔手动做备份，则很容易忘记做备份。建议养成保持备份磁盘始终连接在电脑上的习惯，让 Time Machine 或 File History 自动连续备份数据。

这种设置需要将外部磁盘连接到计算机上。如果发生入室盗窃或房屋失火，可能会同时丢失计算机和备份。所以我们还需要远程备份。

远程备份

远程备份可以避免这种风险。建议使用 Duplicati 创建加密的备份文件，这些文件可以存储在任何远程位置（例如，FTP 服务器），包括云存储（Backblaze、One Drive、Google Drive、Amazon S3 等）。Duplicati 是免费开源软件：https://www.duplicati.com/

使用加密技术保护数据

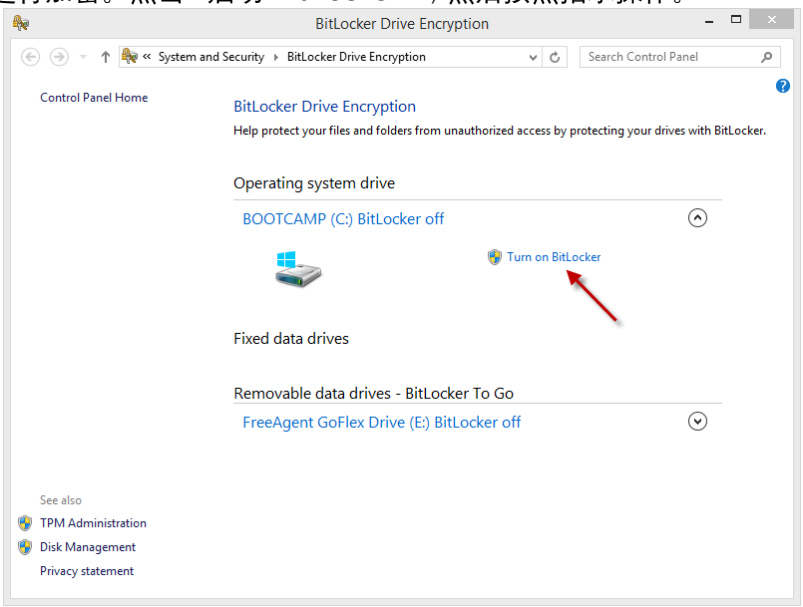
如果电脑或磁盘落入坏人之手，储存在其中的信息很容易被盗，除非对它们进行加密。

电脑或磁盘加密后，需要记住/保存加密密码。否则，没有人能够访问里面的数据。每次启动计算机或访问外部磁盘时，需要输入加密密码。

苹果操作系统用 FileVault 加密磁盘。在 Spotlight 中搜索 FileVault，找到后开始配置。确保把恢复密钥保存在安全的地方。

Windows 的专业版或商业版带有 BitLocker 磁盘加密，但是，家庭版上没有，如果需要这种保护，请考虑升级 Windows 版本以获得 BitLocker。可以从微软在线商店购买许可证进行升级，无需重新安装 Windows。

在适当的 Windows 版本上，按 Windows 键并输入 "bitlocker"，然后点击 "Manage BitLocker "，可以对内部磁盘和外部磁盘进行加密。点击 "启动 BitLocker "，然后按照指示操作。



使用密码管理器

管理密码的最好方法是使用一个密码管理器，例如 KeePassXC。

您只需要记住一个强壮密码以打开密码管理器。密码管理器可生成不重复的强壮密码用于所以其它地方。这样就避免使用弱密码或重复使用相同的密码，以及忘记密码和忘记密码存放的地方。

当您第一次启动密码管理器时，它会创建一个新空白密码数据库，并要求您提供一个强壮主密码。然后，您可以在数据库中为您现有的密码创建条目。以后都要使用密码管理器生成新密码。

这个密码数据库文件对您来说非常重要。保护它的最佳方法是使用云存储，如 Dropbox、One Drive、Google Drive 等。因文件本身是强加密，所从可以将其存储在云中。文件很小，用任何云存储的免费级别都绰绰有余。由于它存在云中，您可以在您的电脑或手机上使用，并会将在您的所有设备上自动同步。为避免潜在的同步冲突，最好仅在一台设备上进行编辑。

KeePassXC：https://keepassxc.org/

电子邮件客户端设置

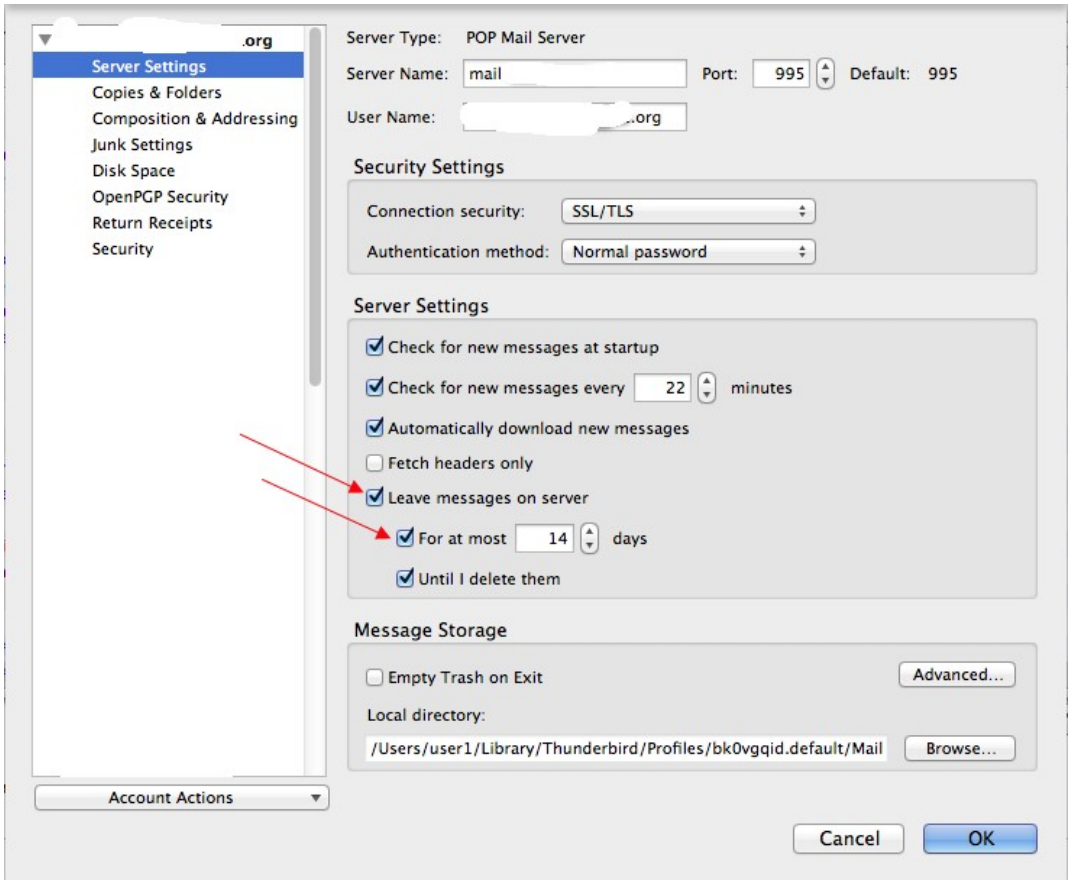
请勿用 Gmail 之类的电子邮件传送敏感内容。请改用我们内部电子邮件服务。我们内部电子邮件每天都会自动发送访问摘要。您应该在每次看电子邮件时查看访问摘要。这样及时可以发现您的帐户是否被邪恶侵入。

在安全的计算机上下载存档您的电子邮件。不要将电子邮件留在服务器上。否则，邪恶偷了邮件密码就可以远程阅读您所有保存在服务器上的邮件。

使用电子邮件客户端（如 Thunderbird 或 Apple Mail）下载和存档您的邮件。下载时使用 POP3（而不是 IMAP）。

如果您还想使用移动设备（如 iPad）查看电子邮件，请设置邮件在服务器上最多保留两周，并设置您的移动设备使用 IMAP 访问您的电子邮件。 （IMAP 将保留电子邮件在服务器上，而 POP3 则将邮件下载到本地计算机上。）

下面是 Thunderbird 的一些截图。添加电子邮件帐户时，选择 POP3，然后切换到手动设置模式。收取协议 POP3S 的加密端口是 995，发送协议 SMTPS 的加密端口是 994。



其它措施

案例：Stuxnet 的入侵方式。伊朗的核设施没有连接到互联网。敌人在停车场投放了一些小 USB。工作人员将从停车场捡到的 USB 插入电脑中，导致电脑中毒，进而导致大量提炼铀的离心机受损。

请勿将未知的 USB 闪存盘或 DVD 插入您的计算机。不要将未知的 FireWire 或 Thunderbolt 设备连接到您的计算机。

使用 uBlock Origin 浏览器插件以防范通过网页广告投放的恶意链接或代码。

苹果设备的语言设置：请不要用简体中文。如果用简体中文，苹果会将相应的 iCloud 数据存到中国的服务器。如果非用中文不可，建议用繁体中文。

移动设备

资料来源：美国国家安全局(NSA)移动设备最佳实践(2020 年 7 月 28 日)

部分做法也适用于电脑（PC 或苹果电脑）

蓝牙：不使用时关闭蓝牙（同理：不使用时关闭外设端口）。飞行模式并不总是关闭蓝牙。

Wi-Fi：不要连接到公共 Wi-Fi 网络。不需要时禁用 Wi-Fi。删除不再使用的 Wi-Fi 网络。

设备控制：保持对设备的物理控制。避免连接到未知的可移动外接 U 盘等媒介。（适用于电脑）

保护盒：考虑使用盖住麦克风的保护盒来阻止房间音频（以避免热麦克风攻击）。不使用时盖上摄像头。

对话：不要在未配置适用安全语音的移动设备附近进行敏感对话。

密码：使用强锁屏密码/密码：如果设备在 10 次错误密码尝试后自行擦除，则 6 位数字 PIN 就足够了。将设备设置为 5 分钟后自动锁定。

应用程序：安装最少数量的应用程序，并且只安装来自官方应用程序商店的应用程序。往应用程序中输入个人数据时要格外小心。不使用时关闭应用程序。（适用于电脑）

软件更新：第一时间更新设备软件和应用程序。（适用于电脑）

生物识别：使用生物识别（例如指纹、面部）身份验证有其方便之处，但只在保护敏感度最低的数据时予以考虑。（言下之意是不要使用）

短信：即使您认为内容是普通的，也不要在个人设备上进行涉及敏感工作的对话。

附件/链接：不要打开未知的电子邮件附件和链接。即使是熟知的发件人也可以意外地传递恶意内容，或者由于被恶意行为者破坏或冒充而传递恶意内容。（适用于电脑）

值得信赖的配件：仅使用从值得信赖的制造商处购买的原装充电线或充电配件。不要使用公共充电站。

位置信息：在不需要时关闭位置服务。请勿将设备带到敏感地点。

电源：每周一次关闭设备电源再从新开机。

修改：不要修改设备或操作系统的内置保护限制以取得额外权限（jailbreak or root the device）。

弹出窗口：像这样的意外弹出窗口通常是恶意的。如果出现，强制关闭所有应用程序（iPhone：双击主页按钮或从屏幕底部向上滑在屏幕中间略微停顿以选中应用再往上滑动以关闭；Android：单击最近的应用程序软键）。

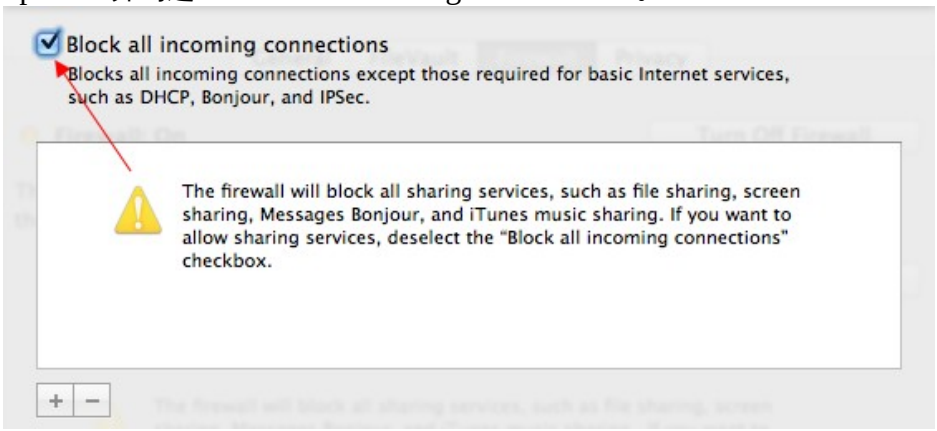
资料来源：https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/Mobile_Device_UOO155488-20_v1_1.PDF

苹果操作系统

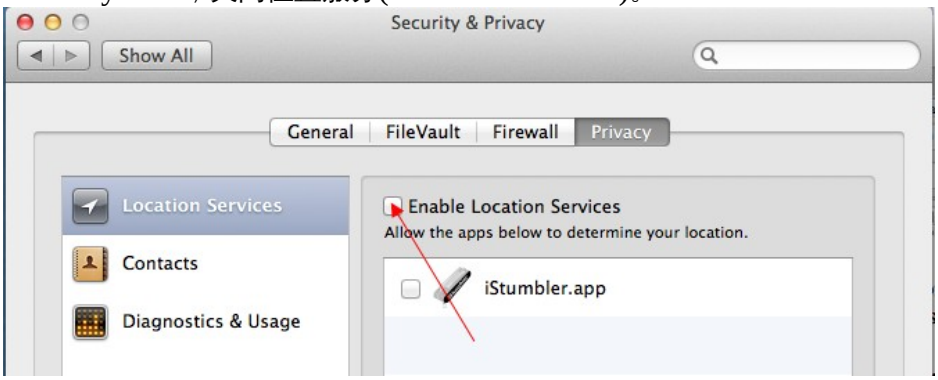
网络配置

启动防火墙，阻止所有内向传入连接。在 Spotlight 中搜索 firewall，找到后开始配置。

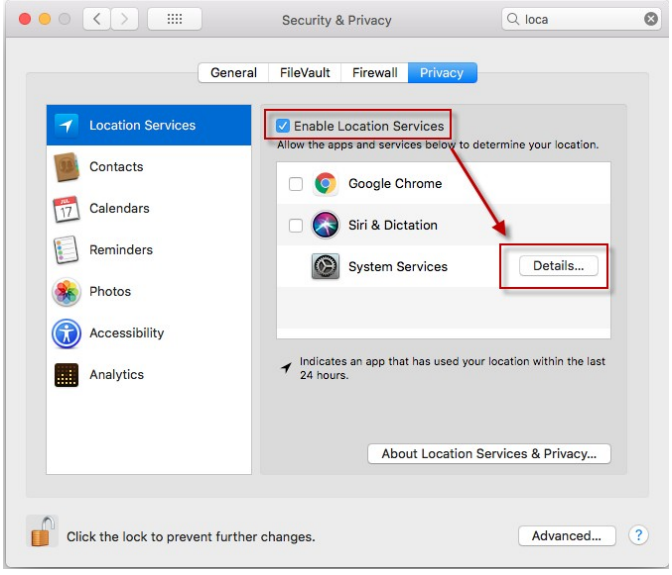
点击 "Firewall Options"并勾选 "Block all incoming connections"。

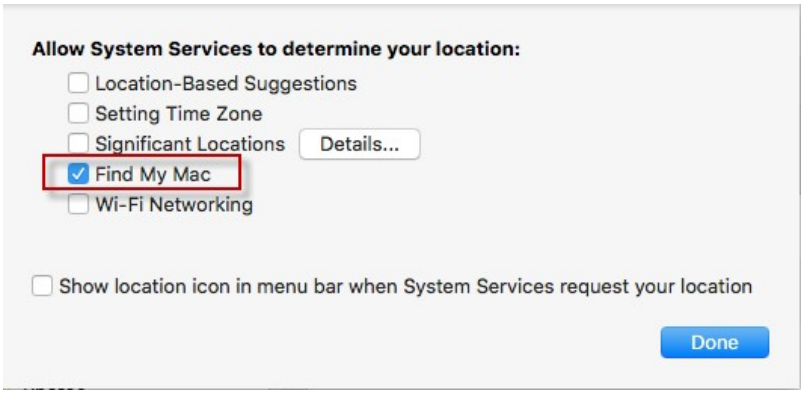


如果不希望使用 Find My Mac，关闭位置服务(Location Services)。

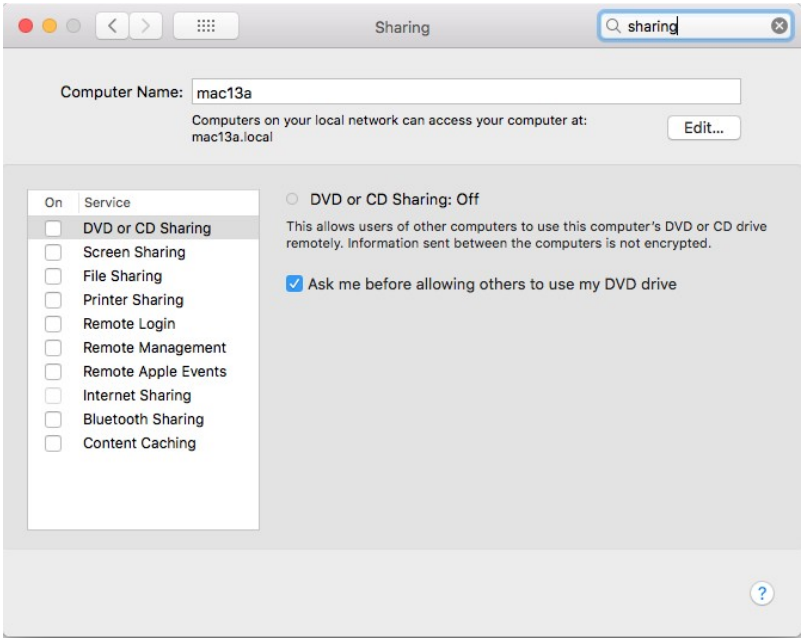


如果希望使用 Find My Mac，需要打开 Location Services，但取消勾选所有其它项目。





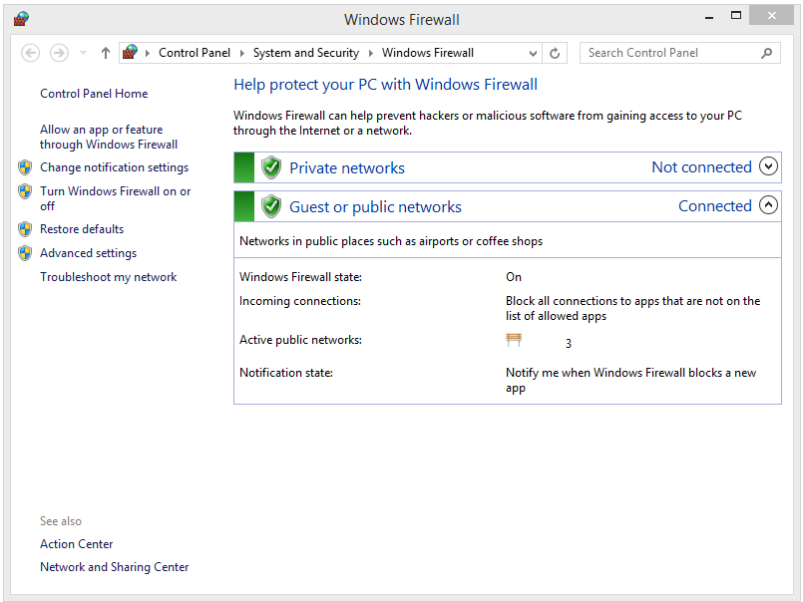
通过 System Preference -> Sharing 或在右上角方框中搜索 sharing，来关闭 File Sharing(文件共享)、Screen Sharing(屏幕共享)、Remote Login(远程登录)等。当您在防火墙选项中(Firewall Options)选择阻止所有传入连接时，它们都将被关闭。



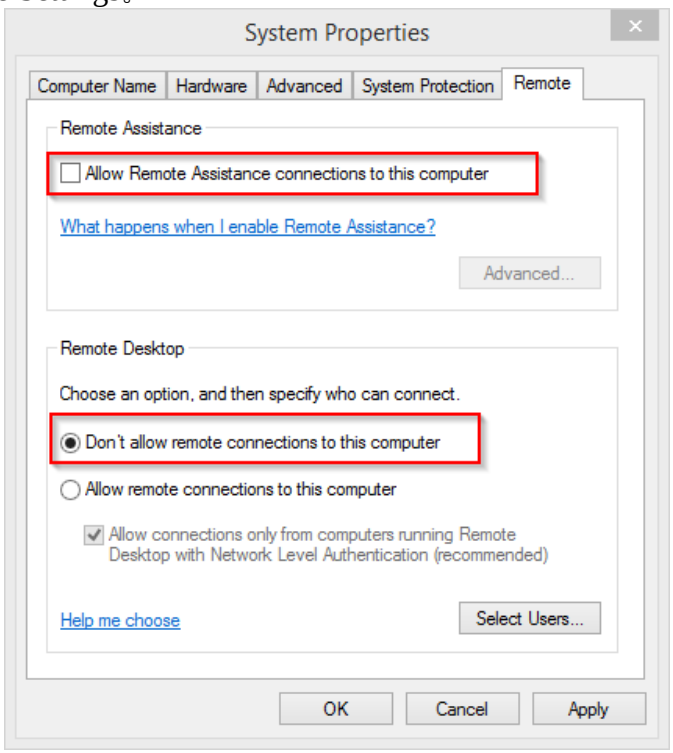
Windows 操作系统

网络配置

按 Windows 键，输入 "firewall"，在搜索结果中点击 "Windows Firewall"。



如果不需要远程访问计算机，建议关闭远程登录。按 Windows 键，输入 "system"，在搜索结果中点击 "System"，再点击 Remote Settings。



Windows 11 安全特性

如果您使用的是 Windows 设备而不是苹果设备，建议您升级到 Windows 11。一方面这符合保持操作系统和应用软体更新到最新的原则。另一方面，Windows 11 在安全上有极大的改进。有些改进来源于高要求的硬件比如 TPM 2，有些改进来源于操作系统的改进。

前面提到的终极防护是只运行受信任的应用。Windows 11 的智能应用控制（Smart App Control）简化了这个防护的实施。

勒索软件（Ransomware）会加密用户文件以索要赎金。因为是加密用户自己的文件，不需要管理员权限，所以即使是以非管理员登录也不能幸免。Windows 11 增加了受控文件夹的功能（Controlled Folder Access），只有受信任的应用才可以更改文件夹里内容。

Windows 11 还有应用隔离（Application Isolation），让高危文件和网页在一个容器里运行，即使有病毒也不对系统产生伤害。目前 Windows 11 的应用卫士（Application Guard）让 Word 文件，PowerPoint 文件，Excel 文件，Edge 浏览器在保护的容器里运行。