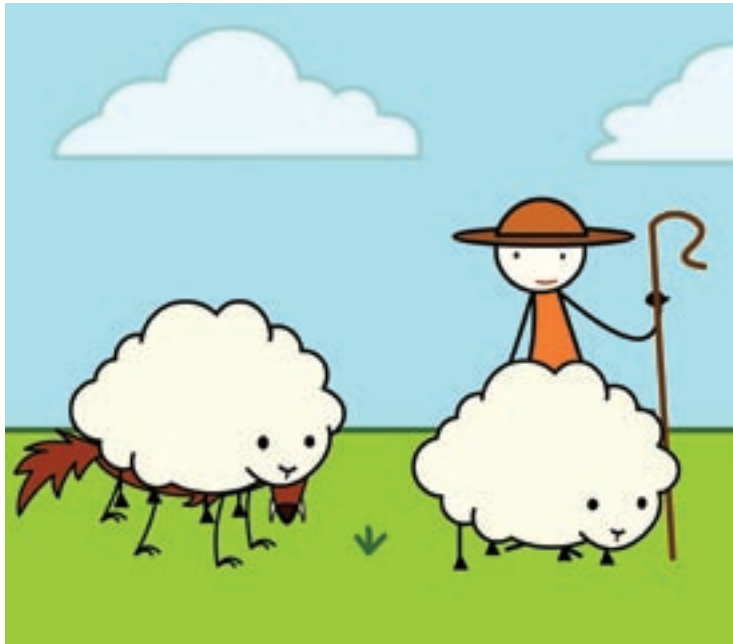




# 上网安全

保护您的身份、个人信息和家庭。

安全 • 简单 • [makeITsecure.org](http://makeITsecure.org)



## 网络钓鱼

### 什么是网络钓鱼？

网络钓鱼是一种犯罪活动。不法分子（网钓客）伪装成诸如银行和信用卡发行公司等合法组织，骗取您的个人详细资料（如银行帐号或卡号）。

网钓客是指伪装成合法组织骗取您的个人详细资料的不法分子。

网钓客通常向您发送电子邮件，要求您“核实”或“重新提交”您的个人信息。

他们可能要求您填写一份在线表单，并可能提供一些有吸引力的“诱饵”（例如现金奖励或旅游奖励）作为您填写在线表单的回报。

当有人要求您提供银行帐户信息、银行卡号、信用卡号、密码、身份证号码或社保卡号时，您一定要谨慎处理。

网钓客会使用这些信息冒充您，并可能从您的银行帐户中非法划款或用它来支付网上购物款。他们甚至可能将这些重要的信息出售给第三方。

### 如何知道我已“被钓”？

相信您的直觉。如果发现某封电子邮件很可疑，请立即删掉它；或者如果发现似乎有“天下掉馅饼”这样的好事，就值得怀疑是假的。如果发现似乎来自您的银行或信用卡发行公司，请立即告诉他们的客户服务部门。

### 下面是一些在网络钓鱼电子邮件中可能会用到的词：

“核实您的帐户”。

“在 48 小时之内答复，否则将被销户”。

“尊贵的客户”。

“单击下面的链接以访问你的帐户”。

### 如何避免被网络钓鱼诈骗？

相信您的直觉。请记住，有名的公司都不会要求您通过电子邮件提供个人详细资料。

绝不要通过电子邮件或传真提供个人详细资料，也不要通过回复弹出广告或向可疑网址提供个人详细资料。

一定要检查您的信用卡和银行声明，以了解任何违法情况。

请使用最新的防病毒软件和防间谍软件，以防止恶意软件入侵。网络钓鱼过滤器能够阻止已知网络钓鱼网站或发出相关警告，从而防止您上当受骗。

### 如果怀疑自己“被钓”则应该怎么办？

如果怀疑自己“被钓”，请马上通过座机电话、手机或另一台计算机通知相关公司。然后与当地警察局联系，或者如果是在北爱尔兰，请与北爱尔兰警察总局 (PSNI) 联系，电话是 0845 600 8000。

有关详情，请访问 [www.makeITsecure.org/phishing](http://www.makeITsecure.org/phishing)

弹出广告是指在一个新打开的浏览器窗口中弹出来的网上广告。

# 社交网络

## 什么是社交网络？

社交网络服务网站帮助建立由 Internet 用户组成的网上社区并对其提供支持。

**Bebo** 是爱尔兰著名的社交网络服务网站，它的主要会员都是 13-24 岁的用户。必须年满 13 岁才能建立一个帐户。

**Facebook** 是一个社交网络服务网站，虽然建立帐户的最小年龄限制为 13 岁，但大多数会员都是 25 岁以上的用户。

**Nimble** 是一个爱尔兰社交网络服务网站。

**博客** 又称网络日志。博客可以是个人日记、政治辩论论坛、突发新闻发布或一组链接。简而言之，博客是一个网站，您可以持续不断地在这里创作和发布信息。

诸如 Bebo、Facebook 和 Nimble 等网站吸引了成千上万的、各个年龄段的 Internet 用户，这些用户可以通过这些网站与朋友（甚至是陌生人）在网上进行交流。取决于上述这些网站提供的不同功能，网站的会员可以互相分享各种兴趣爱好，并且可以通过网站进行聊天、传递消息、收发电子邮件、上载和下载照片和视频、博客、讨论和分享信息。

## 如何运作？

当您在社交网络服务网站上创建个人概况时，通常会上载一些关于您自己的基本资料，例如，用户名、您来自哪里以及您喜欢的音乐和其它兴趣爱好。然后您可以决定是要将您的个人概况公开还是保密。如果您选择将您的个人概况保密，那么没有人能够访问您的个人资料，除非您首先批准并将他们添加到您的亲友列表中。

## 有哪些风险？

社交网络服务网站必定会要求您提供一些个人信息。当决定在网上提供多少个人信息时，用户可能没有像在现实生活中那么谨慎。例如，绝不要提供您的家庭住址或电话号码，并且请始终将您的个人概况设为保密以确保您总是知道在跟谁交流。

## 如何保护自己？

在网上提供个人信息时请始终保持谨慎。请记住，Internet 是一个公共资源。请提供尽可能少的个人信息，仅提供一些别人看了不会对您造成不好影响的信息，以防身份被窃。

## 如何保护孩子的网上安全？

如果您的孩子在网上提供个人信息时保持谨慎，那么社交网络其实是一个可以从中享受到乐趣和学习的地方。

您需要告诉他们不要相信在网上看到的任何信息，因为有时网上的用户可能会隐瞒自己的身份。

劝告他们在没有值得信任的成人的陪同下绝不要与网友见面。

警告他们不要与在网上聊过天的陌生人见面。

您可以结合孩子们正在使用的这种技术，跟他们讲讲与 Internet 相关的知识。请记住，现在手机上以及在家里都可以上网。

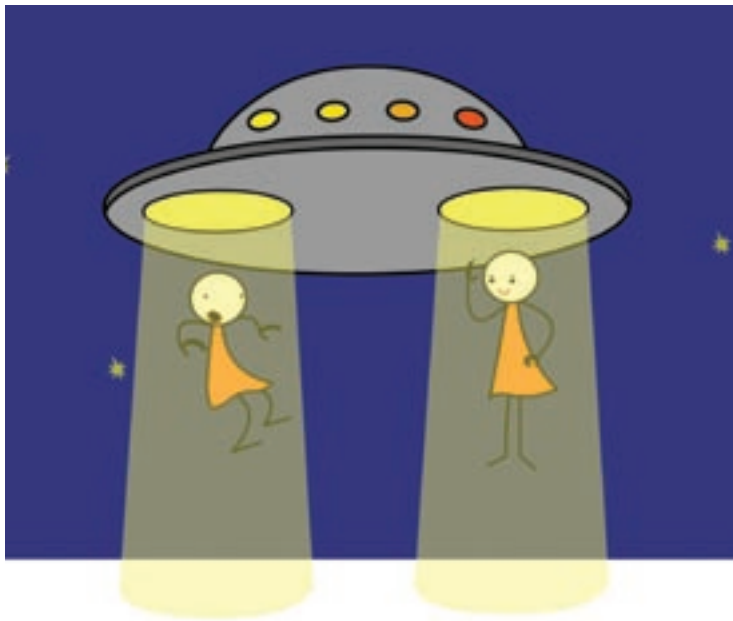
了解您的孩子曾经访问过的网站，并查一查他们是否适合访问这些网站。

现在大多数 Internet 浏览器都有家长控制功能，您可以借助这些功能来限制孩子们对 Internet 的访问。建议您了解一下这些功能并加以利用。

有关详情，请访问

[www.makeITsecure.org/socialnetworking](http://www.makeITsecure.org/socialnetworking)





## 身份窃取

### 什么是身份窃取？

身份窃取是指这样一种情况：不法分子窃取您的个人信息，然后冒充您从您的银行帐户中非法划款或用它来支付网上购物款。他们甚至将您的个人信息出售给第三方而从中获利。

### 如何识破？

很遗憾，当您识破它的时候，您可能已经成为受害者了。他们的惯用伎俩包括：

- 拒绝您的信用或贷款申请。
- 派收帐公司联系您，要求您付清莫名其妙的到期欠款。
- 您可能收到一些有关公寓、工作或房子的莫名其妙的信息，而这些信息其实跟您一点关系都没有。

### 如果我是身份窃取的受害者，应该怎么办？

立即致电警察局或北爱尔兰警察总局 (PSNI)，报告有关身份被窃的事宜。

建议致电或写信给与您有财务业务往来的相关银行或金融机构。

书面通知发生身份窃取的相关组织或网站。

撤消您知道或相信已经被非法利用的银行卡或帐户。

### 如何避免身份被窃？

在网上提供个人详细资料时保持谨慎。

在网上购物时确保连接是安全的。状态栏上应出现一个锁形图标，并且地址栏上的字符应以 `https://`（而不是 `http://`）开头。

请检查公司应显示明确的隐私和安全策略。

请使用安全密码，并且不要把密码告诉任何人。密码最好是由数字、字母和标点符号随机组合而成，并且至少有 8 个字符。

为网上购物和新闻组设置特殊的电子邮件地址。这样，当您需要更改这个电子邮件地址时，不会影响到您用来通信的主要电子邮件地址。



`http://` 和 `https://` 是位于网站地址中开头的字符。当通过 Internet 提供信用卡信息时，安全的网站将会在其网址的开头显示 `https://`。

有关详情，请访问 [www.makeITsecure.org/identitytheft](http://www.makeITsecure.org/identitytheft)

## 保护 Internet 访问的安全

当访问 Internet 并不十分安全时，需要采取一些简单的措施来保护您的计算机或设备的安全，并减少您的信息或数据泄露的风险。

### 始终使用最新的防病毒软件和防间谍软件

计算机病毒是指跟随一些真实的程序（如字处理程序或电子邮件应用程序）一起进入电脑的软件程序。除了可能会损坏、复制或盗窃您的数据之外，它们甚至可以复制自身并感染其他用户。

**间谍软件**是一种软件，它在您不知不觉中秘密地收集您的信息并通过 Internet 连接传出这些信息。

间谍软件是指在您不知不觉中下载到您的系统中的一种小应用程序。它会收集您的个人信息，并通过 Internet 将这些信息发回给其发起者。

间谍软件和计算机病毒常称为恶意软件。

**防病毒软件**是一种您安装在计算机中的软件，它会扫描所有文件和程序以查找病毒，然后删除找到的病毒。

防病毒软件和防间谍软件在您的系统中查找并删除恶意软件。因为病毒和间谍软件会持续不断地演变，所以一定要让您的防病毒软件和防间谍软件保持最新。所有防病毒软件和防间谍软件应用程序都会提供通过 Internet 进行更新的方法。

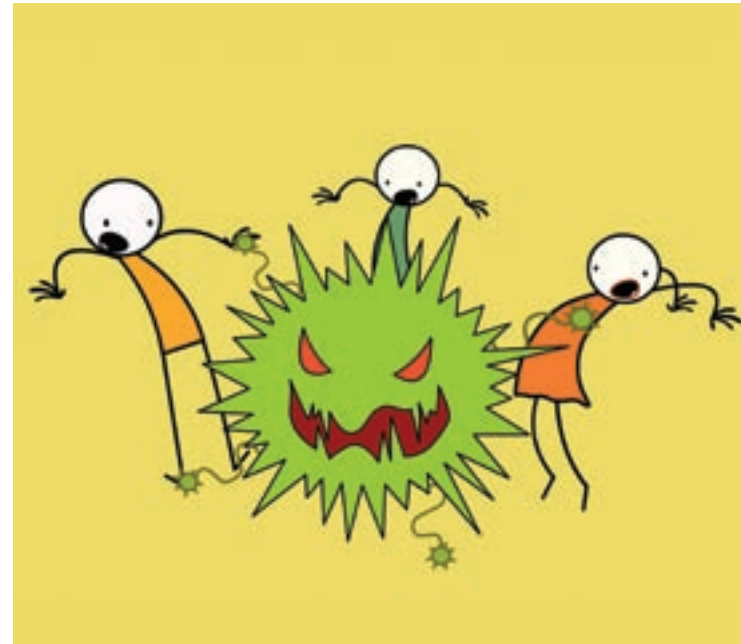
### 始终应用信任的应用程序安全更新

**操作系统**是为计算机程序运行而提供的软件基础。例如，Microsoft® Windows、Linux 和 Mac OS。

您的计算机或设备上运行了许多程序，包括操作系统。操作系统充当应用程序（如字处理程序、游戏或 Internet 浏览器）的平台。

因为恶意软件会持续不断地演变并产生新的威胁，所以应用程序开发人员也会持续不断地创建安全更新以阻断感染。

因此，一定要始终应用由软件开发商发布的合法安全更新，从而确保保持您的系统最新。



### 始终使用 Internet 防火墙

Internet 防火墙就像是一个虚拟的门卫。它持续不断地过滤从 Internet 进入到计算机的数据，并只允许批准的数据进出系统。大多数现代操作系统或安全软件包都将包含防火墙。始终确保在访问 Internet 时防火墙是打开的。

**防火墙**是指一些设备或程序，它们专门设计用来在计算机上网时防止对计算机的未授权访问。

