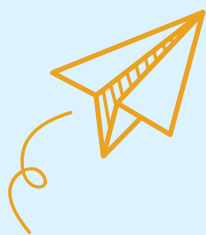


WWW



当心：

停一停、
想一想、问一问。

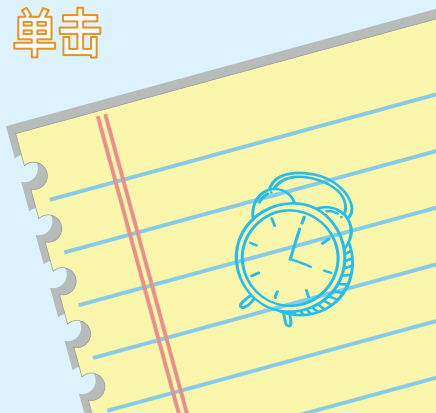


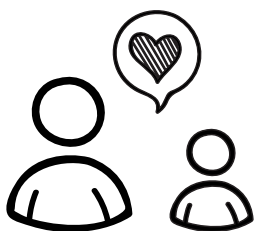
.com

SIMPLIFIED CHINESE



单击





要在生活中帮助您的孩子安全上网，
当心：停一停、想一想、问一问。有一些
想法可以帮助您与他们开始对话。
选择一节共同阅读，了解如何谨慎分
享、友好在线、防范网络欺凌以及在线
保护他们（和自己）的个人信息。这些
工具可以帮助您向孩子们展示如何做
出正确的选择、负责任地使用科技。
通过交谈，您可以让孩子知道一旦他
们犯了错误，有可以信赖的成年人会
帮助他们。

To help kids in your life be safe online,
Heads Up: Stop. Think. Connect. has some
ideas to help you start a conversation with
them. Pick a section and read it together to
see how to share with care, be kind online,
stand up to cyberbullying, and protect their
(and your) personal information online.
These tools can help you show kids how
to make good choices and use technology
responsibly. And, by talking with them, you
let kids know they have a trusted adult to
help them when they make mistakes.

上网是生活的一部分。人们会在网上观看和创建内容、发布照片和视频、玩游戏、与朋友和家人分享自己所在的位置和所做的事情。但在网上发布内容、娱乐和交流时会面临风险。网上的某些人和情形并非总是真实可靠的。

无论手指在键盘、手机或平板电脑上移动得有多快，头脑和时间才是避免网络风险最好的工具。停一停，认真想一想面临的情况可以帮助保护你自己、朋友和家人、你的账户和设备。否则，最终可能会分享过多信息，让自己或他人尴尬，产生电脑故障，或者与戴着假面具的人交谈。

✓ 谨慎分享

✓ 友善为先

✓ 防范网络欺凌

✓ 保护交流

谨慎分享



经过思考后再分享

网上的行为会产生真实的后果。分享的照片、视频和消息会影响你自己、你的隐私、你的声誉和周围的人——可能是现在，也可能是将来。发帖前停一停，想一想。

**关注你发帖的人
可能
比你想象的多。**

想要完全控制谁可以看到你的个人资料、图片、视频或文本是不可能的——即使用了在内容被查看后或在 24 小时内将其删除的隐私设置或应用软件也不可能完全

控制。任何看到你发帖的人都可以截图或录像。问一下自己：“想不想让某人在午餐时与全餐厅的人分享那张照片或者那个视频？”

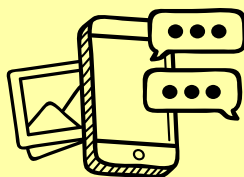
你分享的事物可能影响到其他人。未经当事人准许发送或发布照片和视频可能导致令人尴尬、不公平甚至不安全的状况。首先征得当事人的同意。发布前问一下他们：“您同意我在社交媒体上发布这个东西吗？”如果他们不同意，不要发布。

一旦在网上发布内容， 就无法将其收回

即使你删除了已经发布的内容，或者发布已过期，你不想让人看到的照片或评论也可能被保存、分享或在网上的其他地方存在 — 而且永存。

发送色情信息：不要这样做。

你可能在学校或者新闻中
听到过人们“发送色情信息”
— 用其手机发裸照。不要照做。



绝对不能这么做。创建、转发
甚至保存色情照片、视频或信息会使你面临
失去友谊和声誉的风险。更糟的是，你的行为
还可能违法。

关于社交媒体的注意事项



根据美国卫生部长的说法，使用社交媒体可能会对你造成伤害，具体取决于在社交平台上花费的时间，看到的内容类型，及其对人的健康至关重要的睡眠或锻炼等活动的干扰程度。

友善为先



礼貌很重要

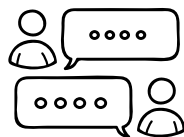
由于在网上看不到别人的面部表情、肢体语言或其他视觉线索,你可能会发布或说出不会当面说的话。但发短信、发帖、直接消息、玩电子游戏和发电子邮件与面对面的交谈在实施上是一样的。请注意自己的沟通方式,务必三思而后行。

慢下来。网上容易产生误解。在发送消息前,问自己:“其他人会对这条消息有什么感觉?”

考虑并尊重他人在网上的看法和情感 — 就像面对面打交道一样。记住:头像和个人资料名称背后都有真人。

低调一点。不要全部使用大写字母,也不用一连串的感叹号或粗大字体。网上书写的这种风格就跟面对面大喊大叫一样没有区别。

不要把所有东西都放在群聊里。在群发消息或点击“全部回复”前,停下来想一想:谁需要看到这条消息?



不要冒充他人

冒充他人(例如同学或老师)创建个人资料、评论或发贴是错误的,甚至可能造成伤害。

直言相告

如果看到朋友发送了轻率或不安全的内容,提醒他们。你可以帮助朋友减少麻烦和难堪。如果在网上看到不适宜的内容,报告并告诉可以信赖的成年人。大部分应用软件和平台都有报告有危险或不当行为的途径。



要注意礼仪! 😊

防范网络欺凌



无论是在网上还是实际生活中,每个人都有权利在与他人日常交流时有安全感。

如果有人发布刻薄的评论、伤人的表情包、尴尬的照片,或者发送关于你的聊天或私人信息,那就是欺凌。欺凌是不当的行为。向你信赖的成年人讲述这种情况,得到相应的帮助,并决定如何应对。

如果有人在网上骚扰你,采取以下做法:



不理此人或将其拉黑。



保存记录并向可以信赖的成年人求助。



报告这一情况。大部分应用软件和平台都有报告不当或危险行为的工具。

欺凌往往会让被骚扰的人感觉不好 — 也会让欺凌者形象不佳。

欺凌还可能导致校方或警方的介入。

如果你目睹了网络欺凌,想办法加以阻止 — 勇敢出面主持公道。如果有人能出面帮助被欺凌的人,恶劣的行为通常很快就会停止。

保护交流



保护自己的隐私

网上任何行为都会留下痕迹。通过以下步骤确保痕迹不会导致泄露不想分享的信息。

使用隐私设置。了解如何为设备、应用程序和社交媒体账户开启隐私设置 — 然后加以运用。它可帮助限制谁能看到你所在的位置、所发的帖子以及谁能与你联系。

检查自己的位置设置。有些应用程序能让用户看到其朋友所在的位置。它们还能分享用户的位置。想一想什么时候需要分享自己的位置。如果不需要,关闭位置

共享。设备上的功能(如摄像头)可能有拍照时所在位置的信息。如果不想每次自拍都让所有人看到自己的位置,请关闭手机摄像头上的位置功能。每次都扪心自问:“这个应用软件需要知道我的位置吗?”



将网友限制为自己生活中认识的人。通过短信、社交媒体或电子游戏交朋友可能很有趣 — 但有些人的实际身份与网上身份大相径庭。如果不小心,可能会与陌生人分享个人信息。

保护自己的信息

一旦给了陌生人自己的个人信息 — 例如
社保号、密码或者银行账户信息,就没有办法
再收回。

下面的方法用于在网上保护自己的信息:

不要回复索要个人信息的邮件。即使邮件像是来自认识的朋友、家人或公司 — 或者说不回复会有不好的后果也不要给出个人信息。很可能它们是假冒的,想要

窃取个人信息。向可以信赖的成年人求助，将邮件报告为垃圾邮件。

在下载该应用软件前，**检查应用软件想要访问的信息**。有些应用软件申请权限访问它们不需要的信息或功能，例如联系人列表、摄像头、存储、位置和麦克风。请可以信赖的成年人帮助阅读应用软件的隐私政策，查看如何使用你的数据，以及是否会分享该数据。然后确定那个文字游戏是否真需要访问你的照片。

在应用软件内购物之前先咨询可以信赖的成年人 — 尤其是在它们自行付费时务必先咨询成年人。

保护自己的账户

你的网上账户中有大量的个人信息。下面这些步骤可以防止他人侵入你的账户。

设置强密码。

密码越长，越难破解。至少有 12 位字符，而且同时含有大小写字母、数字和符号。考虑使用随机文字组成的密

码短语,让密码不易忘记。但不要使用常见的短语、歌词或电影台词,这些都很容易被猜测到。

使用独特的密码。不同的账户使用不同的密码。这样,如果有人得到了一个账户的密码,他们无法入侵其他账户。可以使用密码管理器来跟踪所有不同的密码。

不泄露密码。不要与任何人分享密码,即使是最好的朋友或恋人。

精心挑选安全问题。尽量选择只有自己能回答的安全问题。不要选择其他人可以在网上找到答案的问题 — 例如,自己的邮政编码、出生日期或母亲的闺名。如果无法避免这些问题,发挥创意!将它们当成密码,使用随机的长答案。但要确保自己能记住答案。

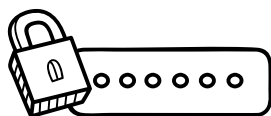


使用多重身份验证。许多账户通过使用“多重身份验证”为账户提供更多保护 — 除了密码,还需要其他

验证。多重身份验证 将你知道的事物 (例如密码) 和你有的事物 (例如应用软件生成的密码) 或你自身 (例如指纹) 组合到一起。

如果密码泄露, 请迅速更改。

如果公司通知你出现数据泄露, 黑客可能得到了你的密码, 请迅速更改该账户密码。同时更改任何使用类似密码账户的密码。



保护自己的设备

什么是最好的在线体验方式? 确保自己设备的安全。从些步骤着手:

将所有设备、互联网浏览器和操作系统的安全软件设置为自动更新。这样有助于防范新的安全威胁。

不要点击链接或打开附件。如果在网上收到陌生的短信、电子邮件或消息, 要你点击链接或打开附件, 切勿听信! 即使是免费优惠券也不要上当。链接和附件可能隐藏病毒或间谍软件, 它们可能会入侵你的手机、电脑或平板电脑。

用密码保护设备。这将有助于防止照片、消息和帐户落入坏人之手。

将它们存放在安全的场所。无论是手机、台式机还是平板电脑,都不要把它留在公共场所 — 即使是只有片刻。

登录了解更多信息

ftc.gov/KidsOnline



This booklet helps kids socialize safely online.
There's help on how to share with care, be
kind online, stand up to cyberbullying, and
protect their personal information. Get free
copies in English or Spanish at

ftc.gov/bulkorder



**FEDERAL TRADE
COMMISSION**

2023 年 8 月