

引言

ChatGPT，给我出个题吧

我：猜猜看，在一切皆可伪造的时代，你如何分辨什么才是真实的？

ChatGPT：这是一个引人深思的问题。它不仅触及了深刻的哲学思考，还包含了实际的考量。我们今天所处的世界，技术能够创造出令人信服的幻象，我们被提醒要质疑我们所感知到的真实。为了分辨什么是真实的，我们常常依赖于背景、佐证以及批判性思维。这提醒我们要保持警惕，在假象中寻求真相，并珍视真实的东西。但在深入探讨之前，让我们先澄清一下：我们是在说隐喻，还是你在质疑现实中的某些具体事物？

我：哦，差点忘了告诉你，我正在写一本关于人工智能的书，讲述我们如何飞速迈向一个真假难辨的世界。这也引发了另一个困惑……如何在不被技术细节所困扰的情况下，讲述这样一项充满变革潜力的技术？

老实说，鉴于人工智能的飞速进化，写一本关于它的书是一项艰巨的任务。这种速度是指数级的，今天的新突破明天可能就成了旧闻。我曾目睹互联网的诞生与崛起，见证了从固定电话到移动通信的革命，经历了从龟速拨号调制解调器到流畅的光纤网络的跨越，以及从本地主机到云计算的巨大飞跃，我亲历了 iPhone 时代对手机行业的震撼，也亲眼看到了 Blockbuster Video 的衰退，以及 Netflix 等流媒体服务的兴起。然而，这一切都不及 2022 年 11 月 ChatGPT 的诞生带给我的震撼。从那以后，人工智能开始以

惊人的速度发展和普及。

那一刻，世界猛然意识到，曾经在科幻电影中只可遥想的奇思妙想，已经变得触手可及，或者说悄然逼近。不同的人会从科幻电影中获得不同的感悟。有人感动于《钢铁侠》中托尼·斯塔克与贾维斯之间的温情互动，看到了计算机与人类的情感链接；有人则迷恋《星际迷航》中的那些冷漠却别具一格的机器交流；另一些人则幻想着像《终结者》和《黑客帝国》这类电影描绘的末世景象。

不过，大家都承认，人工智能正在以惊人的速度改变着这个世界。正因为如此，在这样一个瞬息万变的领域，创造任何具有持久价值的事物，都是一项不小的挑战。那么，如何才能写出一本书，确保它在上架时尚未过时？^①

关键在于关注支撑这个新时代的基本真理，关于人类智能和人工智能本质的真理，关于它们合作方式和冲突方式的真理。虽然具体的技术会发生变化，但这些基本原则是永恒的。

人类智慧如同一座宝藏，充满了无限可能。我们在学习、推理和创造中展现出机器无法企及的深度与广度。我们天生具备理解上下文、洞察言外之意的能力，我们能够在纷繁的信息中作出似乎是直觉般的判断。这些闪光的智慧，正是我们在人工智能时代的独特超能力。

但是，人工智能也有自己的超能力。它可以在眨眼之间处理大量数据，发现人类无法感知的模式，并作出始终如一的决策。此外，随着技术的不断突破，人工智能系统正以惊人的速度在某些领域迎头赶上，甚至超越了人类的能力。

两种智能的故事

人类智慧与人工智能紧密协作的成果具有改变世界的力量；然而，当它

^① 顺便说一句，我可以向你保证，书在你的手中或床头柜上比在书店里更快乐。

们成为敌对力量时，后果却可能是毁灭性的。我们将在接下来的章节中看到，坏人已经在操纵人工智能，利用人类的弱点进行大规模欺诈活动。

这是两种智能的故事，各有优劣。在这个充满未知与挑战的时代，我们只有透彻理解这两种智慧的内涵，方能在变革的浪潮中从容前行。我们要借助人工智能乘风破浪，又要保护好自己免受威胁。

正是在这一历史性时刻，本书应运而生。在接下来的篇章中，我们将一同探索人类智慧与人工智能之间亘古不变的真理。我们将迎接它们急速融合带来的种种挑战。同时，我们将用知识和战略武装自己。系好安全带，准备好踏上这场穿越人工智能革命的壮阔旅程吧！未来已来，而我们，将是这个未来的创造者。

欺诈：旧貌换新颜

从古老的特洛伊木马，到今天层出不穷的诈骗新闻，欺诈是人类历史中一个永恒存在的主题。我们既被它深深吸引，也为其带来的恐惧所困扰。而如今，这类历史悠久的故事翻开了崭新的篇章，骗术越发精巧，虚假越发难以辨识。原因何在？因为欺诈找到了它的强大帮凶——人工智能。

人工智能并不会让钓鱼邮件和虚假广告等传统骗术过时。相反，它们比以往任何时候都更加猖獗。人工智能为不法分子提供了前所未有的强大工具，使得他们的作案规模更大，手段更高超。人工智能可以完美模仿老板的语气生成钓鱼邮件，或者制作出以假乱真的亲人求助音频。在人工智能的“加持”下，今天的骗局令人瞠目，过去的伎俩显得过时，甚至有些可笑。

人工智能拐点

此刻，我们正站在变革的十字路口，技术发展将迎来爆发式增长。人工智能不再是遥不可及的未来概念，它的影响力已经席卷而来，被用于善意或恶意的目的。从积极的一面来看，人工智能正在重塑医疗与教育等领域，带

来前所未有的洞察与效率。^①然而，它的阴暗面也正在显现，人工智能已成为前所未有的欺诈、操控与诈骗工具。

这是一个真假难辨的时代，事实与虚构的界限比以往任何时候都更加模糊。视频可以凭空生成，声音可以精确合成，图像可以被篡改得面目全非。我们的感官不再可信，客观现实的概念正在遭受前所未有的冲击。

阅读指引

跟随本书的脚步，我们将全方位了解深度伪造、虚假信息及人工智能骗局的复杂世界，一同剖析这些技术的运作原理、其应用者以及它们为何能够如此高效。然而，我们的初衷并不仅仅是敲响警钟，而是要赋予每个人在这片崭新领域中从容前行的智慧与韧性。

开启这段探索之旅后，你将被引领至一个由人工智能编织的迷雾世界，届时，真相与虚幻将交错难辨。每一章的开篇，都有一个悬念迭起的惊悚故事或一则震撼人心的新闻报道，刻画出角色在合成媒体的冲击中如何奋力挣扎。

这些开篇叙事通过细腻的场景和贴近生活的人物，生动地描绘了一个尖端技术被武器化、以前所未有的规模进行欺诈的未来。它们犹如直击心灵的警钟，有力地告诫我们，在与人工智能欺诈较量的战场上，风险远超所想。

但本书不仅仅是一本警世故事集。它是你在这个新的迷雾世界中前行的指南针。深入阅读每一章的主要内容，你将掌握必要的工具和知识来识别欺诈，保护自己和亲人的安全，并对抗骗子和操纵者的伎俩。

即使身处人工智能的时代，我们最大的财富依然是人类的智慧。

你将学会批判性地评估媒体、验证信息来源并核查事实真伪。你将识破

^① 在医疗保健领域，DeepMind 对 AlphaFold 的研究是一个卓越的典范。关于人工智能的革新实践，可参考可汗学院（Kahn Academy）创始人萨尔曼·可汗（Sal Kahn）对该机构如何运用人工智能的阐释。

欺诈者惯用的心理策略，更重要的是，你会发现如何加强自己的心理防线，抵御虚假信息的侵扰。

在共同探索的过程中，我们将领悟，纵使人工智能蓬勃发展，人类智慧始终是最强大的力量。

我对人工智能、生活和本书的独特视角

我坚信，人工智能对人类而言总体是有益的。它是一种工具，既能推动发展，也能造成破坏；既能成为助力，也可化为利刃。

作为一名安全专家，我的主要职责是理解并阐述事物如何走向偏差，工具如何被滥用，以及网络犯罪分子如何利用工具和人性对我们发起攻击。但技术终归只是技术。

技术会随着使用者的双手和意志而改变。早在 ChatGPT 发布之前，我就在工作和生活中运用人工智能来提升效率了。我将其视为重要的同事和创意伙伴。

沃顿商学院管理学教授伊桑·莫利克（Ethan Mollick）在其最新力作《共智：与人工智能共生共存》（*Co-Intelligence: Living and Working with AI*）一书中描述了与人工智能协同工作的两种基本方式：一种是成为“半人马”，另一种是化身为“半机械人”。两者之间的关键区别在于，“半人马”模式下的人类与人工智能之间始终有着清晰的分界线，他们将人工智能视作工具，随时可以拾取、使用或放下；而“半机械人”则完全不同，它是一种人类与人工智能之间流畅且无缝的互动，二者的界限逐渐消失，近乎融合成了一个统一体。

未来，每个人都会根据手头任务的不同，在“半人马”和“半机械人”模式间自如切换。尤其是在创造性任务的处理中，选择“半机械人”模式无疑更为高效。头脑风暴、创意迭代、研究分析、数据推演、草稿编写、重写、审阅等反复的工作过程非常适合人类与人工智能密切配合。这就像是在虚拟的写作工作室内与同行集思广益，或在需要时得到教练和专家编辑的专

业指导。

这就是我处理本书的方式。作为一名领域专家，我总能自如地完成创意碰撞与主题筛选。然而，盲点的存在使得我未必能完全认识到自己的盲区。在这些时刻，人工智能便成了我的得力助手，帮助我激发创意。作为一名作家，我擅长雕琢句子，然而，偶尔我也会创造出过于繁复的句子。此时，人工智能会提供建议，以简化语言或结构。我当然可以继续说下去，但你已经能理解我的意思了。

人工智能可以帮助我们更快地前进。

我对人工智能的好处非常乐观。只要负责任地使用，人工智能就是人类的财富。但同样，工具也会随着使用者的意愿和目的而改变。因此，人工智能同样为怀有不良动机的人提供了加速实现其阴谋的工具。

人工智能的到来已是不变的事实。精灵已经从瓶子里出来了。作为社会的一员，我们的任务是负责任地利用这一技术，驾驭人工智能的力量，以推动人类的共同理想，同时主动采取措施，防范或减少其被滥用的风险。

工具会随着使用者的意愿和目的而改变。

关 于 我

有时，科技进步的狂热步伐很容易让人忽略最重要的东西，以及谁能带来最大的改变（无论好坏）：人类。人和与人有关的因素是一切的核心。

这就是我的工作。我是一名网络安全专家和研究员，二十多年来一直在探索技术与人类的交集。

如果你浏览我的领英个人档案（<https://www.linkedin.com/in/perrycarpenter>）^①，你会看到我自称为“欺诈学家”。这缘于我从小便对欺诈、巧妙的手法、心

^① 在你浏览时，不妨关注我。我很乐意认识你。

理幻觉与影响充满了浓厚的兴趣。没错，我就是那个总是问别人“想看看魔术吗”的孩子。我有着强烈的好奇心，渴望了解是什么驱使我们行动，以及自以为聪明的我们是如何被愚弄的。

在我职业生涯的大部分时间里，我一直专注于安全领域的人为因素，尤其是社会工程学与欺诈的科学。我还因将心理幻觉（也称心理魔术）巧妙融入主旨演讲，以展示心理劫持的威力而声名鹊起。我的使命是帮助人们认识并为自己筑起防线，抵御那些不法分子操控人性的手段，而这些手段正在被人工智能越来越娴熟地模仿和运用。

从大型行业活动的舞台，到制定网络安全策略的会议室，我从未停止学习和宣传。我的目标是帮助构建一个这样的未来：让技术成为人类的增辉之力，而非掠夺之源；同时，使人类拥有应对数字欺诈的必要工具、资源与思维方式，从而免受其害。

人类直觉与机器智能的交汇点才是真实的故事发生地，而这正是我想带你去的地方。当我们翻开历史的一页，朝向一个充斥着深度伪造、虚假信息和人工智能操控的未来迈进时，我愿成为你前行的指引者。我的目标是解开技术的迷雾，赋予那些尚未涉足的人力量，并在这充满数字欺诈的世界中为你照亮通往真相的道路。

章节预览

人工智能驱动的欺诈行为错综复杂，且不断演变。为了帮助读者了解这一领域，本书分为三个不同的部分，每一部分都在前一部分的基础上展开，让读者对当前的问题有全面的了解。如前所述，每一章开头都有一个简短的故事，这个虚构场景生动展示了合成媒体的欺诈潜力及其影响。这些开篇故事通过独特的人物和情境，暗示了本章所涉及的主题。

虽然本书遵循逻辑顺序，但许多章节可以根据你的兴趣或需求独立阅读。在接下来的篇幅中，你将找到关键概念、真实案例、防御策略和前瞻性考虑因素，让你有能力直面人工智能驱动的欺诈挑战。

介绍和概述生成式人工智能和合成媒体：第 1 章至第 3 章

我们将从时间的长河中拾起线索，回溯欺诈的历史渊源，并揭示人工智能的崛起如何开启了一片崭新的疆域。稍后，我们将深入剖析人工智能的运作机制，介绍深度伪造和合成媒体等关键概念，并研究数字操纵者的思维模式和工具。

新兴威胁的风云变幻：第 4 章至第 7 章

在本部分，我们将深入探讨人工智能被用于欺诈的多种方式，包括虚假信息的传播和诈骗手段的演化。我们将通过现实案例，揭示骗局背后的精妙伎俩与策略。

在当下与未来守护自己、家人和朋友的安全：第 8 章至第 10 章

在这个部分，我们将把重点转向防御，讨论识别欺诈的策略、强调媒体素养的重要性，并阐明科技在应对人工智能带来的威胁中的关键作用。你将收获一系列切实可行的建议，可以保护自己在数字世界中安全前行。

新的希望

我希望，读完本书后，你将以全新的视角审视这个世界。你将拥有更加敏锐的媒体鉴别力，更加深刻的思辨能力，成为那些图谋不轨者无法轻易得逞的对象。

在这个谎言如野火般蔓延、诈骗手段愈发高明的时代，知识是我们最坚实的盾牌。本书将赋予你这种力量，让你在这个新的数字世界中游刃有余，理智而自信。因为在人工智能驱动的充满欺诈的时代，唯一值得信赖的武器，是一颗富有洞察力和批判精神的头脑。

当你翻开书页，进入第一个小故事时，请让自己完全沉浸其中。感受故事的脉动、人物和情境，体会他们所承受的压力与困境，以及他们正在解答的急切命题。每一个章节的展开，每一个真相的揭示，都是你武装自己、准备以智慧、坚韧和对真相的执着迎接挑战的契机。

让我们一起踏上这段旅程，迈向真实的未来。

佩里·卡彭特

2024 年 9 月

欢迎与我联系，获取更新，探索相关资源：

<https://thisbookisfaik.com>