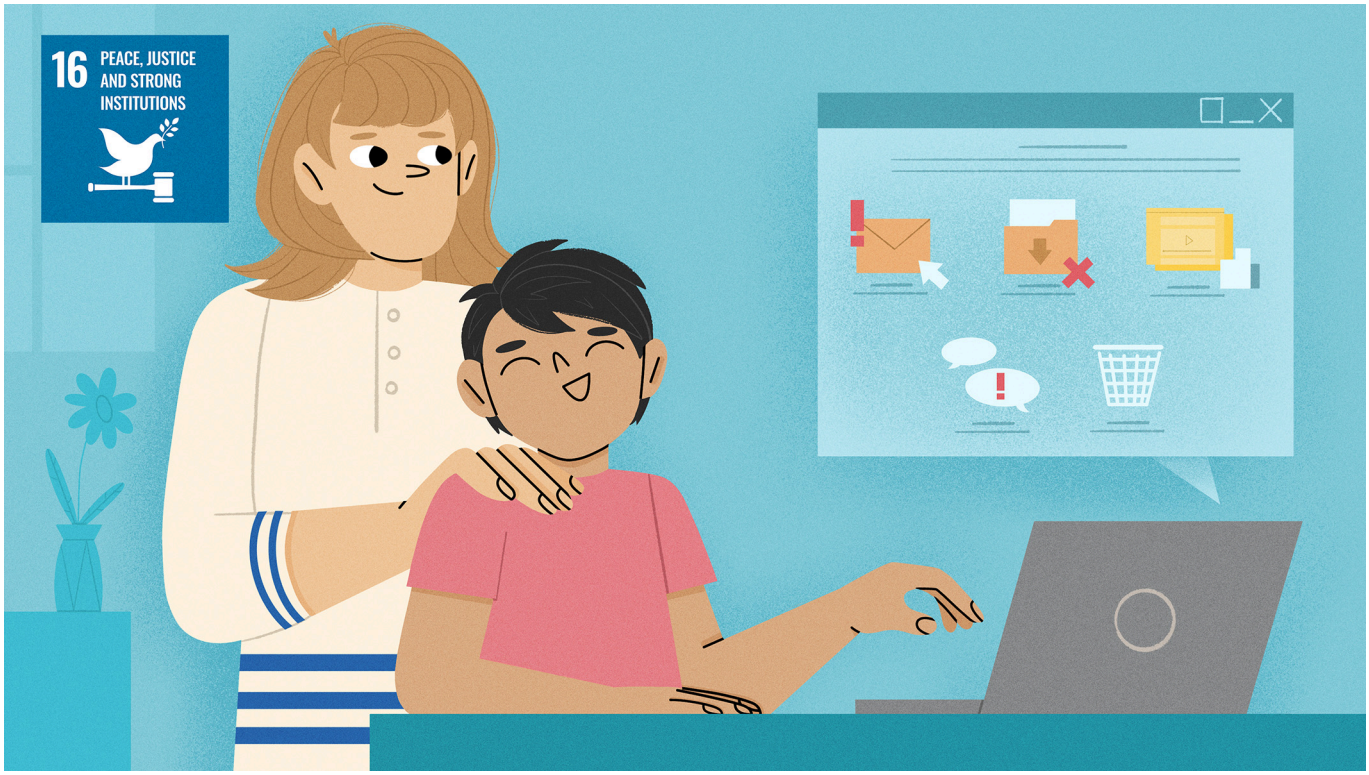
工程与技术
线上发布: 2025 年 12 月 12 日
doi: 10.3389/frym.2024.1396135-zh



助力实现第十六项可持续发展目标: 安全使用数字技术

Taous Madi, Charalambos Konstantinou * 和 *Paulo Esteves-Verissimo*

阿卜杜拉国王科技大学（*KAUST*），计算机、电气和数学科学与工程部（*CEMSE*）（沙特阿拉伯, 图沃）

联合国第十六项可持续发展目标（SDG 16）"和平、正义与强大机构"旨在确保所有人都生活在安全、公正且免受危害的社会中。信息通信技术（ICT）指的是我们使用的数字设备，它帮助我们借助数字服务完成各项任务，例如使用电脑和平板设备工作、购物或学习。然而,ICT 环境中存在许多安全威胁因素，私人信息被盗就是其中之一。要在数字世界中确保安全，必须留意这些风险并成为负责任的 ICT 使用者。本文旨在提升对 ICT 安全风险的认知，讲解科学家如何守护数字世界安全，以及每个人该如何防范这些风险。

欢迎观看本文作者的专访视频，获取更多精彩内容！（视频 1）。

数字技术暗藏风险

联合国于 2015 年提出的第十六项可持续发展目标（SDG 16）旨在为全人类构建安全、公平、无忧的社会。作为 1945 年成立的国际组织，联合国始终致力于维护世界和平安全、促进各国友好关系、推动社会进步、提升生活标准、保障全球人权。可持续发展目标包含 17 项全球性指标，由联合国成员国于 2015 年作为《2030 年可持续发展议程》的一

少年审稿人


AISYAH
年龄: 14


KATERINA
年龄: 9


SHIRHAN
年龄: 16


ZAHRAA
年龄: 16

视频 1
(Video 1)
观看本文 作者的专访视频, 获取更多精彩内容!

部分共同商定，涵盖贫困、不平等、气候变化、和平等相互关联的议题。SDG 16 的核心目标是创建以友好方式解决冲突争端的和平环境，特别强调消除一切形式的暴力（尤其是针对儿童的暴力），同时确保各族群与国家享有平等权利、身份认同和法律保障。通过在个人、组织与国家层面践行这些核心价值观,SDG 16 将确保社会健康发展 [1]。

社交媒体平台、即时通讯应用和线上购物网站等信息通信技术（ICT）在我们的生活中扮演着重要角色。尽管我们身处所谓的数字环境，但这个环境有时并不安全。ICT 使用者可能面临多重威胁，比如作为一种暴力形式的网络霸凌，或者威胁人身安全的隐私信息窃取。因此，谨慎使用 ICT 对实现 SDG 16 至关重要。

ICT 的使用风险

如今，越来越多不同年龄段的人通过技术手段参与各类活动。在许多学校，学生通过网站和电子邮件进行学习交流；移动应用程序被广泛用于娱乐、培训和健康监测等；朋友们在社交媒体上分享生活点滴，或在游戏平台相聚互动。虽然这些工具带来了便利，但作为年轻的 ICT 用户，你需要警惕其中潜藏的大量网络安全风险。

从网络安全角度而言，主要存在三大风险：首先，密码等本应保密的信息被泄露，好比陌生人复制了你家的钥匙，或试图冒用你的身份参加考试，这叫机密性风险。其次，文件资料（如学习报告）在未经所有者同意或知情的情况下被篡改，就像某同学暗中破坏了你的项目文件，

这叫完整性风险。第三，个人设备被他人私自占用，导致你无法正常使用，这叫可用性风险。

这些网络安全风险在日常生活中是如何体现的呢？

网站与电子邮箱

我们每天通过网站和电子邮箱处理事务、交流互动或获取资讯。然而，某些网站可能会损害设备或显示不当内容。例如，点击可疑链接可能跳转至不良信息页面，甚至自动下载恶意软件。这类软件五花八门，可能造成各种损害 [2]。

恶意软件可能会擦除文件内容，窃取身份信息、家庭住址或银行资料等敏感数据，也可能占用运算能力和存储空间等设备资源，导致系统瘫痪。以臭名昭著的木马软件为例（图 1），这种恶意软件相当于为黑客开辟数字通道，让这些网络窃贼肆意盗取个人照片、密码，甚至入侵政府系统，偷走无比重要的国家安全文件。

信息通信技术 (ICT) (Information and Communication Technology (ICT))

我们使用的所有电子设备，通过基于互联网的服务来完成各类任务。

数字环境 (Digital Environment)

由 ICT 构建的环境，为日常活动（如沟通、协作、预约等）提供便利。

网络霸凌 (Cyber-Bullying)

通过数字通信平台恐吓、骚扰或伤害个人或群体的行为，常表现为反复攻击或传播有害内容。

网络安全 (Cybersecurity)

保护 ICT 安全并抵御信息窃取、文件破坏等恶意行为的实践。

机密性 (Confidentiality)

确保敏感信息免遭未经授权访问或泄露，在 ICT 和网络安全领域指数据仅限授权人员查看和使用。

完整性 (Integrity)

保证数据准确、完整且未被篡改，在网络安全中指维持数据的一致性与可信度，确保数据免遭篡改和未授权修改。

恶意软件 (Malware)

未经用户批准擅自安装在设备上的有害程序，主要通过破坏机密性、完整性与可用性导致设备异常。

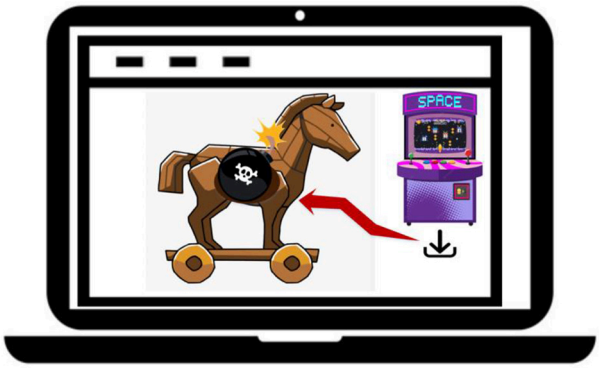


图 1

图 1
点击某些下载图标时，可能无意间将木马程序带入设备。木马程序一旦下载成功，便会开始执行恶意操作，例如为黑客打开访问个人设备的后门。"木马"这个名称源于一个古希腊传说：特洛伊人将巨型木马视为献礼迎入城内，不料深夜木马开启，潜藏的士兵悄然出动，最终攻陷了特洛伊城。

移动应用程序

众多 ICT 使用者会在手机端安装各类应用，游戏和运动追踪类程序尤为流行。但某些看似安全的应用程序可能内置自动点击器，这种恶意软件能模拟用户操作，同时触发多个指令（图 2），既会大量消耗系统资源，导致运行卡顿，还可能自动点击下载按钮，植入更多恶意程序，方便黑客窃取信息。令人担忧的是，含恶意软件的应用屡见不鲜：在已知的 56 个含恶意软件的应用中，竟有 24 款是儿童类应用 [3]。

图 2

图 2
自动点击器是一种如同多触手章鱼般执行自动化点击的程序，能同步点击应用程序内出现的广告横幅等元素。

这些安全威胁不仅危及数字环境中的个人，造成财产损失、阻碍用户获取关键服务，如果上升到国家层面，更将直接影响公民数据的安全性、完整性与私密性。由此可见，网络安全直接关系到社会能否实现安全、公平与稳健的发展。

科学如何提供帮助？

好在众多专业人士正携手构建更安全的数字环境。网络安全研究人员致力于守护数字世界：他们研发恶意软件检测和阻止机制，追查身份盗窃等数字犯罪源头。此外，为提升 ICT 的安全防护水平，研究人员正致力

身份认证 (Authentication)

类似出示身份证表明个人身份的过程，用于验证人员或设备的真实身份。

于完善身份认证机制，即验证用户身份的真实性，同时加强访问控制管理，例如限制特定资源或数据的访问权限。

在我们开展的一项研究中，团队尝试开发一款能抵御有害事件的防护软件，使 ICT 系统免遭破坏。换句话说，我们想知道能否打造出一款能保护设备抵御各类恶意活动的软件 [3, 4]。该软件包含检测与修复两大核心模块，犹如数字世界中的"警察"与"急救员"。检测模块持续追踪设备运行状态，识别异常行为并即时发出警报，修复模块则根据警报快速修复受损系统，使其恢复健康状态（图 3）。

图 3

数字卫士是由两大核心模块构成的防护软件：检测模块如同巡视道路的警察，持续监控系统状态；修复模块则像急救员，在紧急情况下提供关键救援。

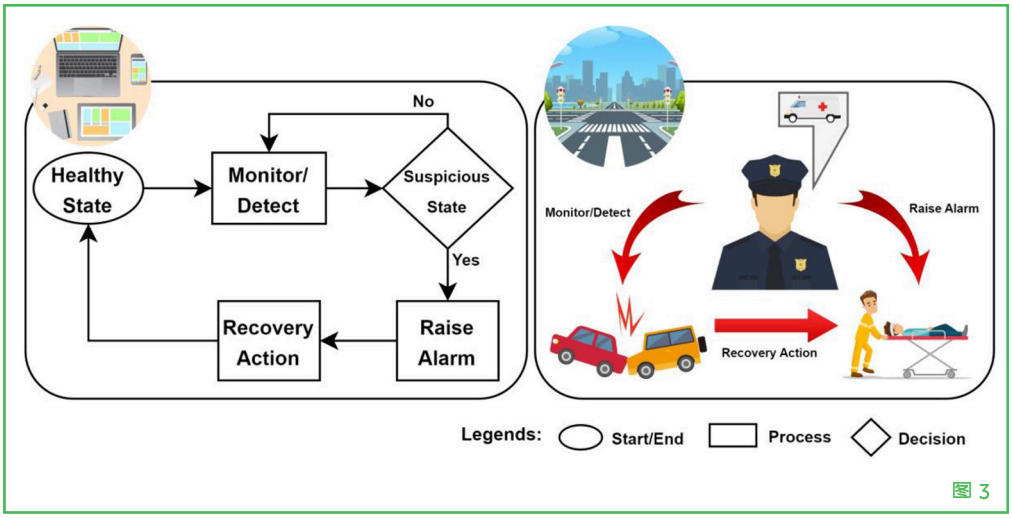


图 3

这好比现实生活中警察在事故发生后立即呼叫救护车，收到关键信息的急救人员抵达现场了解伤情并实施救援。在模拟攻击测试中，我们的软件成功检测到威胁并修复系统。简而言之，我们打造出了一位守护数字环境安全的"数字卫士"。

安全畅享数字生活

多家机构正积极推行保障 ICT 使用安全的方案。例如，联合国下属数字技术专门机构 ——国际电信联盟（ITU）发布了一系列指南，指导如何最大程度降低儿童使用 ICT 时的风险 [5]。美国制定的《儿童在线隐私保护法》（COPPA）明确禁止网站在未获家长同意的情况下收集儿童个人信息 [6]。

为了在畅享数字世界时避开风险因素，确保个人安全，建议培养以下良好习惯：谨慎访问网站与邮箱，仅访问老师/家长推荐的可信网站；不下载未知发件人的附件；控制设备中安装的应用程序数量；遇到网络霸凌或仇恨言论等异常情况时，及时告知老师/家长。

结论

ICT 既是学习工作的得力工具，也是带来乐趣的源泉，但其中潜藏的安全威胁不容忽视。本文揭示了一些常见数字风险，概述了科研机构在安全防护方面的探索，并提供了基础防范建议。当每个人都能安全使用 ICT 时，我们离 SDG 16 描绘的"强大可靠的社会"就更近一步——让所有人都能安居乐业。希望大家增强网络安全意识，并积极传递网络安全对于守护社会安全的重要意义。

致谢

谨向阿卜杜拉国王科技大学（KAUST）的 Nicki Talbot 致以诚挚谢意，感谢她在审校阶段提供的宝贵支持，本系列的完成离不开她的专业贡献。同时向 KAUST 可持续发展办公室与联合国开发计划署沙特阿拉伯国家办公室表示谢意，感谢他们始终致力于提升公众对联合国可持续发展目标（SDG）的认知，共同推动世界走向更可持续的未来。

AI 人工智能工具使用声明

本文中所有图表附带的替代文本（alt text）均由 Frontiers 出版社在人工智能支持下生成。我们已采取合理措施确保其准确性，包括在可行情况下经由作者审核。如发现任何问题，请随时联系我们。

参考文献

1. United Nations 2015. *Transforming Our World: The 2030 Agenda for Sustainable Development*. Available at: https://www.un.org/sustainabledevelopment/development-agenda/
2. Blancaflor, E., Beltran, S. S., Jayag, J. E., Obog, A., Salem, F. E., and Sungahid, M. D. 2022. "A security assessment on malwares disguised as children's applications", *2022 7th International Conference on Multimedia communication Technologies (ICMCT)* (Xiamen, China). p. 15–19. doi: 10.1109/ICMCT57031.2022.00012
3. Madi, T., and Esteves-Verissimo, P. 2022. "A fault and intrusion tolerance framework for containerized environments: a specification-based error detection approach", *2022 International Workshop on Secure and Reliable Microservices and Containers (SRMC)* (IEEE).
4. Konstantinou, C., Wang, X., Krishnamurthy, P., Khorrami, F., Maniatakos, M., and Karri, R. 2022. HPC-based malware detectors actually work: transition to practice after a decade of research. *IEEE Des. Test.* 39:23–32. doi: 10.1109/MDAT.2022.3143438
5. International Telecommunication Union n.d. *Child Online Protection Guidelines*. Available at: https://www.itu-cop-guidelines.com/
6. Children's Online Privacy Protection Act 1998. 15 U.S.C. §§ 6501–6506. Available at: https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act

线上发布: 2025 年 12 月 12 日

编辑: Rúben Martins Costa

科学导师: Emma Louise Nason

引用: Madi T, Konstantinou C 和 Esteves-Verissimo P (2025) 助力实现第十六项可持续发展目标: 安全使用数字技术. Front. Young Minds. doi: 10.3389/frym.2024.1396135-zh

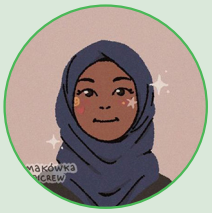
英文原文: Madi T, Konstantinou C and Esteves-Verissimo P (2024) Towards SDG 16: Safe and Secure Use of Digital Technologies. Front. Young Minds 12:1396135. doi: 10.3389/frym.2024.1396135

利益冲突声明: 作者声明本研究不涉及任何潜在商业或财务关系。

少年审稿人

AISYAH, 年龄: 14
我是一名小小的科学爱好者, 但最喜欢社会科学。在课余时间, 我喜欢做美食, 在羽毛球场上跳跃挥拍, 或是沉浸于编程学习。

KATERINA, 年龄: 9
我喜爱动植物, 始终怀着好奇心去探索身边的世界, 渴望了解更多科学奥秘。体操、游泳和校园活动构成了我的多彩生活, 而音乐、艺术与数学同样让我乐在其中。



SHIRHAN, 年龄: 16
在学校, 科学课是我的最爱, 特别是地球科学与植物科学, 而天文学始终让我很着迷。不钻研科学知识时, 阅读与创意写作便是我的精神乐园。能参与《Frontiers for Young Minds》项目并与众多优秀伙伴合作, 令我感到非常荣幸!

ZAHRAA, 年龄: 16
作为一名专注求知的学生, 我始终关注科学与数学在现实生活中的应用。很荣幸能加入《Frontiers for Young Minds》项目, 让我有机会对网络安全和周围世界有更深刻的认知。

作者

TAOUS MADI
Taous Madi 现任爱立信加拿大公司资深研究员，此前曾担任阿卜杜拉国王科技大学（KAUST）弹性计算与网络安全中心（RC3）的研究员。她持有蒙特利尔康考迪亚大学信息系统工程博士学位，主要研究领域涵盖 5G 及未来电信网络安全、机器学习与形式化验证。她曾与人合著一部专著，并在多家权威网络安全会议与期刊上发表数篇学术论文。

CHARALAMBOS KONSTANTINOU
Charalambos (Harrys) Konstantinou 现任沙特阿卜杜拉国王科技大学（KUAST）计算机、电气和数学科学与工程部副教授，兼任下一代弹性系统安全实验室（SENTRY Lab）首席研究员。他毕业于希腊雅典国立技术大学，获得电子与计算机工程硕士学位，并在美国纽约大学获得电气工程博士学位。在加入 KAUST 之前，他曾任佛罗里达州立大学先进电力系统中心助理教授。他的研究领域涵盖关键基础设施的安全与韧性，特别关注智能电网技术、可再生能源并网以及实时仿真。
*charalambos.konstantinou@kaust.edu.sa

PAULO ESTEVES-VERISSIMO
Paulo Esteves-Veríssimo 是阿卜杜拉国王科技大学（KAUST）教授，兼任弹性计算与网络安全中心主任。他还担任卢森堡大学 SnT 研究中心研究员及美国卡内基梅隆大学电子与计算机工程系客座教授。作为 IEEE 和 ACM 双料会士，他发表了 200 余篇同行评审论文并合著 5 部专著。当前，他的主要研究方向为弹性计算在多个前沿领域的应用：基于软件定义网络的基础设施、自动驾驶汽车、分布式控制系统、数字健康与基因组学，以及区块链与加密货币技术。

中文翻译由下列单位提供
Chinese version provided by