





学生网路安全指南 (STUDENT ONLINE SAFETY GUIDE)











苏格兰警察
守护民众安全

POLICE SCOTLAND
Keeping people safe

POILEAS ALBA

简介

苏格兰警察旨在为您提供有关如何避免成为犯罪受害者的重要安全建议。

现今，学生们经历着的常见欺诈行为可以从更易于识别的面对面欺诈到某人匿名在线进行的欺诈。

技术进步使您能够更轻松地执行日常任务，但经常被对您的个人信息和金钱感兴趣的欺诈者所利用。

本指南将为您提供信息和建议，以提高您的认知，准备您能识别潜在的欺诈行为，并防止您有价值的数据，被有心人意图窃取。

内容

网络钓鱼
当犯罪分子使用欺骗性的电子邮件，短信或电话欺骗毫无戒心的个人时。

租赁欺诈
当在没看过住宿环境就要求学生提交预付费时，表明有潜在的租赁欺诈。

包裹欺诈
学生收到关于警方在调查中发现了针对他们的非法包裹的通知。

洗黑钱
个人同意披露其银行详细信息，使非法资金存入其帐户中。

门票欺诈
购买活动门票时，请注意并保持警惕注意欺诈活动的指标。

假工作骗局
当求职者面向旨在以窃取个人信息或金钱为目标的欺诈广告时。

购买论文
让第三方写你的论文，使您面临潜在的骗局。

性勒索
犯罪分子操纵受害者分享明确的图像或让受害者认为他们有裸照，并以勒索义务。

网络警戒意识 6

什么是骗局和欺诈? 7

欺诈危险信号
常见的欺诈指标和警告 8

网络钓鱼
HMRC的假税退款
学生贷款网络钓鱼骗局
英国签证 /伪内政部/假警察骗局
学费支付骗局
银行账户会有危险 10

租赁欺诈 14

包裹欺诈 16

洗黑钱 18

加密货币骗局 20

门票欺诈 22

欺诈性工作骗局
预付费用骗局
高费率电话面谈骗局
身份欺诈和身份盗用 24

性勒索
給性勒索受害人的建议 26

英国 SIM 卡相关建议 29

支持和福祉 30

其他資料, 建议及指南 31

网络警戒意识

英国国家网络安全中心对有关如何在在网路上保持安全的建议：

- **使用三个随机单词作为您电子邮件的强大且不同的密码**
  结合三个对您意味着某些意义的随机单词，是创建易于记住但难以破解的密码的好方法。
- **为您的电子邮件打开2步验证（2SV）**
  可以为您提供两倍的保护，因此，即使网络罪犯拥有您的密码，他们也无法访问您的电子邮件。您不会在每次查看电子邮件时，都被要求这样做。
- **将密码保存在密码管理器中**
  将密码保存在密码管理器中 密码管理器可以存储您的所有密码 安全，因此您不必担心记不住它们。
- **备份数据**
  备份数据备份是您存储的重要数据的副本 通常在网路（云存储）或可移动媒体上（例如USB，SD卡或外部硬盘驱动器）上的单独安全位置。
- **更新您的设备**
  按时依制造商指示更新您的设备的包括保护来自病毒和其他恶意软件，通常会包括改进和新功能。

更多信息
网络警戒意识-
NCSC.GOV.UK

什么是骗局和欺诈?

骗局和欺诈是用于个人利益的犯罪。通常是通过欺骗来赚钱或获取信息。随着技术的改进,欺诈者变得越来越复杂。存在许多类型的骗局和欺诈。

通过了解各种骗局的动机和迹象,您可以保护您的个人信息免受可能在国际边界进行操作的骗子盗取。这些欺诈背后的罪犯没有歧视;他们将针对任何人,并完全无视其行动的影响或后果。

在使用网路时考虑您的行动,如果某事似乎感觉不对,则可能不对。

任何欺诈和其他金融犯罪都应通过致电101向警方报告。



欺诈危险信号

常见的欺诈指标和警告。

- 警惕任何来自英国税务海关总署 (HMRC)、警方或银行等机构的意外来电。
- 警方或银行绝不会要求您提取资金或移交款项以协助调查，也不会要求您交出您的银行卡。
- 如果您在网上聊天或与您有关系的人向您索要钱财或礼品卡，他们就是诈骗分子。切勿代表他们收款或转账——这是洗钱。
- 一个真诚的人或机构绝不会要求您对朋友/家人撒谎，或要求您与“机构”保持私密联系。
- 在您成为诈骗受害者后，可能会有人联系您，声称他们可以帮您取回钱财（当然需要付费）。这被称为“追回诈骗”。
- 犯罪分子可能会要求您下载远程访问工具，以便他们完全控制您的设备，并坚称这是为了帮助您“解决”问题。
- 一个真诚的人或机构绝不会催促您或让您惊慌失措。
- 诈骗分子冒充值得信赖的官员是很常见的。警惕任何来自英国税务海关总署、警方或银行等机构的意外来电。
- 任何试图联系您进行投资的人都要格外小心——这很可能是骗局。
- 警惕任何通过电话索要个人信息的人。



网络钓鱼

诈骗电子邮件的目的通常是让您单击链接。这可能会将您带到假网站，或者可能将恶意软件下载到您的设备上。这被称为“网络钓鱼”。

HMRC的假税退款

HMRC警告您要警惕潜在的骗局，尤其是如果您从事部分工作，并且是与代理商互动的新手。在所有税收骗局中，几乎一半是提供了假退税款，HMRC永远不会通过简讯或电子邮件提供这个。

如有疑问，HMRC建议不要直接回复任何可疑的东西，而是通过GOV.UK与HMRC马上联系。

将可疑电子邮件转发给 report@phishing.gov.uk

学生贷款网络钓鱼骗局

您可能会收到一封似乎合法询问银行详细信息的电子邮件。

电子邮件里写着由于您的学生信息不完整导致您的帐户已被暂停，以敦促您使用一个网路链接 来更新您的資料此链接可能会导致一个旨在收获个人信息的假网站。

不要假设任何通过电子邮件发送给您的人就是他们自称的人。如果电子邮件要求您付款，登录在线帐户或提供优惠，请务必谨慎。

请记住，没有银行会通过向您发送请求密码或敏感信息的电子邮件来要求您单击链接并访问一个网站。

如有疑问，请通过询问公司本身来检查它的真实性。

切勿遵循可疑电子邮件中提供的链接，请使用单独的浏览器和搜索引擎找到官方网站或客户支持号码。

请记住，欺诈性官方的电子邮件其公司或组织的可能质量，语法，图形设计或图像质量较差。

为了欺骗您的垃圾邮件过滤器，他们可能会在电子邮件主题中使用奇怪的“spe11ings（拼字）”或“cApiTals（大小写字母）”。

垃圾邮件电子邮件也可能以“向我们的贵重客户”发送，或者使用您的电子邮件地址而不是您的姓名当收件人。

英国签证 /伪内政部/ 假警察骗局

假装为警察或内政部官员的罪犯可以通过电子邮件与您联系，并告诉您您在进入该国时未完成正确的文书工作，必须支付罚款或被驱逐出境。

其他骗局涉及打电话或留下语音留言的诱饵，声称是警察，HMRC或法院，并要求支付罚款以避免起诉。

有些骗子可能会说服您说您正在与执法人员交谈，或者指导您到 假网站显示带有您的照片和详细信息的驱逐引渡页面。要验证警察的身份，请致电101。

学费支付骗局

这些骗局是与您联系并提供折扣或“帮助”以支付学费。您可能会被告知如果您提供您的银行详细信息，您可以拥有助学金。

骗子有时会自称是政府机构，并要求“国际学生关税（international student tariff）”付款。他们威胁如果不付款就要撤销您的签证，付款是以通过汇票，电汇或其他难以追踪的方法进行的。

如何避免骗局：

警惕愿意代表您支付学费或承诺付款时给您折扣的人。如果听起来好的不真实，则几乎可以肯定是骗局。

避免使用在您的祖国个人和公司广告中列出的但没有在大学列出或大学授权的学费支付服务。

在同意通过第三方处理任何付款之前，请务必与大学联系。

切勿与大学缺乏可验证关系的任何人分享个人，银行或财务信息。 始终验证您与谁交谈。

始终保持警惕对于骗子可能会接近您的方式（亲自，电话，通过社交媒体）和地點（移民线，国际学生会议等。）如有疑问，请联系大学。不要受到截止日期或报复威胁感到压力。

银行账户会有危险

骗子可以电话声称来自您的银行说明您的帐户有被攻击的风险。他们建议您将钱转移到他们为您设置的“安全帐户”上，但实际上是骗子的银行帐户。

银行永远不会意外的与您联系，询问密码，帐户详细信息或要求您移动钱。

挂断电话，並从银行卡后面的电话号码打电话给您的银行。

警察永远不会要求您转钱或用代金券付款。



租赁欺诈

找一个安全，方便且负担得起的地方生活可能是您的主要问题之一。不幸的是，骗子知道学生住宿的重要性，并且可以尝试利用您想找到房屋的需求。

您可能会被要求在看住宿环境前就提前支付费用。实际上，该物业可能不存在，可能已经出租或已将其租给了多个受害者。

然后，您将损失您已支付的预付费用，并且无法租用您认为已获得的住宿地點。

保护自己免受租金欺诈的侵害：

仅当您确定此网路广告租房是真实的，才向人们汇款。如果您需要确保定下了此住宿 来自海外找的英国的住宿，寻求您雇主的帮忙或询问大学或学生会的帮助，联系或亲戚来检查该物业是否存在并且可用。

仅在您或可靠的联系人与代理商或房东访问该物业后才付款。

避免被迫转移大量资金。如果要求您通过汇款服务汇款，请持怀疑态度。



包裹欺诈

冒充警察或海关官员的罪犯可以通过电话或短信与您联系。他们可能会声称您因由您的祖国寄给您的包裹已被停止而您正在接受刑事调查。

他们可能会发送假警告/身份证的图像，并指示您不要将“调查”告诉任何人。

然后，他们可以指示您将钱转移到您祖国内的银行帐户，以便可以检查以确保其合法。这笔钱不会被退还；相反，会被要求需要更多。

保护自己免受包裹欺诈的侵害：

这种骗局使学生遇到了严重的财务困难。不要以为这些人就是在电话上或短信上自称的人，尤其是当他们索取个人或财务细节时。

警方永远不会要您的银行帐户详细信息，护照信息，地址或通过电话要求监视您的移动。

如果您不确定任何电话，电子邮件或消息，请不要遵照任何请求。与您信任的人或警察谈谈。



钱骡（洗黑钱）

该计划涉及一个同意分享其银行详细信息以将钱存入其帐户的人。然后将资金取出并继续转移 - 帐户持有人的因合作而保留了一部份百分比的钱。

学生之所以成为目标，是因为年轻人不太可能拥有犯罪历史，而且他们干净的帐户使银行不易怀疑。

招聘通常是通过：

- 未经请求的电子邮件寻求帮助
- 通过社交网站联系
- 在网站上广告合法企业的虚假空缺
- 看起来合法的在媒体和网路上的分类广告。

您可能会看到真正的网路广告，但不要上当。

花点时间考虑广告里提供的东西。

诸如“从您自己的家中赚钱”“必须愿意提供银行详细信息”和“每周赚250英镑 – 无需经验” 之类的术语是危险信号，这可能表明您是作为洗黑钱的目标。

另外，还要警惕那些试图引诱你使用手机数位钱包在超市自助收银台购买大量礼品卡的人。

手机中很可能装有被盗的数位钱包，购买的礼品卡随后会被兑换成可以带出境的商品。

如果您有任何有关洗黑钱的信息，请拨打 **101** 给警察，在紧急情况下拨打 **999**。

您还可以通过 **0800 555 111** 匿名，也可以上网在 www.crimestoppers-uk.org 与灭罪热线联系。

请记住，在返回您的祖国时，请勿将您的银行帐户详细信息分享给家人/朋友。

转移违法的钱是一种犯罪。虽然这似乎是一种赚钱的简单方法，从事这样的活动可能导致获得犯罪记录。

有关更多信息，请访问：www.nationalcrimeagency.gov.uk/moneymuling



加密货币骗局

加密货币是一种可以在线购买和交易的数字货币。加密货币投资骗局是针对学生群体增长最快的骗局之一。

这些骗局往往始于看似随意的接触——例如 Instagram 上的私信、一条“发错号码”的短信，或是在约会软件上的匹配。许多此类骗局手段高明，有时会利用人工智能（AI）生成的内容，并利用学生面临的经济压力（如学生债务）以及人们渴望快速获利的心理进行诈骗。

与传统银行业务不同，加密货币投资通常不提供退款或保障机制，一旦出现问题，往往无法挽回损失。

警惕以下迹象

- 虚假网红——骗子冒充富有的网红或商业大咖，甚至利用埃隆·马斯克（Elon Musk）等公众人物的 AI 生成视频来推广虚假的投资机会。
- 不切实际的回报——警惕任何“保证”获利或承诺“资金翻倍”的说法。没有任何正规投资能保证回报。
- 制造紧迫感——营造紧迫感是骗子常用的手段。如果有人催促你立即采取行动，那很可能就是骗局。
- 虚假网站和应用程序——骗子会制作看起来非常逼真的网站、交易平台和投资组合页面，以此窃取你的资金。
- 索取访问权限——切勿泄露你的钱包助记词、密码或账户信息，也不要允许他人远程访问你的设备。

如何保持安全

- 在投资前，先研究加密货币的运作方式并了解相关风险。
- 保持掌控权——不要让其他人代你创建加密货币钱包或管理投资。
- 避免远程访问——切勿让他人控制你的设备或代你安装软件。
- 仔细核实信息来源——名人或网红的代言往往是虚假的或经过操纵的。
- 从容行事——不要仓促进行投资。
- 只投入你输得起的资金，因为加密货币投资通常不像传统金融产品那样拥有完善的保障机制。

如果某件事让你感觉过于仓促、过于简单，或者好得不真实，那它很可能就是骗局。如果你决定投资加密货币，请务必谨慎、从容，并做好充分的研究。



门票欺诈

如果您正在考虑购买现场活动的门票，请记住要注意门票欺诈的迹象。

犯罪分子经常建立假网站或社交媒体个人资料，以欺诈销售音乐会或体育赛事或不存在的门票。

网站甚至看起来像是真正的组织，但是網址的细微变化可能表明它是欺诈性的。

罪犯可能使用了看上去很真实欺诈的门票的图像。

他们可以通过文字，电子邮件或传單与您联系，以宣传假票。他们在社交媒体上创建假帖子或页面，以骗那些寻找门票的人。通过官方卖方，票务代理商和零售商协会（STAR）的官方卖家预订门票总是最安全的，因为其他任何事情都可能是骗局。

如何发现门票欺诈：

- 您会在电子邮件或消息/传单中看到票价。
- 为您提供高需求或售罄的活动的门票以“好到不真实”价格。
- 您被要求您仅通过银行转让付款，而不是通过信誉良好的在线零售商建议的安全付款方式。
- 您会看到一个看起来类似于真正组织的网站，但网址URL有细微的变化。
- 有人告诉您，将安排客户代表在会场外与您会面。



欺诈性工作骗局

简而言之，这是针对求职者为了窃取个人信息或金钱的伪造的网络上求职广告。

假招聘广告旨在针对求职者，以窃取他们的个人信息或金钱。

骗局已经变得非常复杂，使得很难分辨真假。

机会主义者使用令人信服的谎言来针对潜在受害者的背景，试图收集个人信息并介由欺骗来得到金钱。

常见的骗局

预付费用骗局
欺诈者要求预付钱来写履历，管理费或进行背景安全检查之类。当人们希望在国外工作时，他们也可以声称是旅行社。

高费率电话面谈骗局
诈骗者向您发送短信或未接电话，要求您致电高费率号码以进行初始电话面谈。您在电话上等了很长时间，将通话持续到一个小时。造成毫无戒心的受害者的费用总计可达数百英镑。

请，记住：

- 切勿预先付钱以进行背景调查或管理费。
- 如果被邀请参加电话面试，请确保面试官打电话给您 – 否则您可能陷入高费率骗局。

身份欺诈和身份盗用
欺诈者假装作为雇主，要求个人信息，银行对帐单，护照详细信息和驾驶许可证作为雇佣检查。

请，记住：

- 不要在社交媒体资料上让人看到个人和敏感的信息。
- 直到您面对面见面，只有在确定这是一家真正的公司时，才能共享任何信息。



性勒索

网路上性勒索是性勒索的一种形式。它涉及通过约会应用程序，社交媒体，文字或电子邮件来针对您的罪犯，并操纵您分享性图像/视频，后来他们用来威胁要在公众曝光要求您付款。

社交媒体欺诈是指创建虚假在线身份以欺骗和操纵您。如何减低风险遇到潜在的骗子，您可以将您的个人资料私有化，限制能访问的个人信息并使自己成为一个不吸引人的目标。

罪犯可能会使用虚假的身份在线与您成为朋友，然后威胁要向您的家人和朋友发送图像。

如何保护自己：

- 使用互联网时要谨慎。仅在您想要的时候激活相机功能。确保在不使用时始终“关闭”或使用网络摄像头盖子。永远不要让自己被欺骗去参加以后会后悔的活动。
- 如果使用视频聊天应用程序，请注意以下事实：“联系人”并不总是与他们说的一致。如果您允许建立关系，如果对方提出异常请求，要对其请心生警惕。
- 如果您使用网络摄像头与某人聊天，请对您的说的和做的事情要有所警惕。

給性勒索受害人的建议

立即与您的当地警察联系。警察将认真对待您的案件，保密处理，而不会评价您的情况。

不要与犯罪分子进行进一步的沟通 - 屏幕截图有关您的所有沟通。

停用您的帐户而不是关闭帐户将表示保留数据，并将帮助警察收集证据。请注意，有关性勒索的大规模网络钓鱼电子邮件很常见，应转发到NCSC的可疑电子邮件报告服务（SERS）
report@phishing.gov.uk

不要付钱 - 许多已付钱的受害者会继续收到要求更高金额的需求。

保存证据 - 注意罪犯提供的所有细节，例如电子邮件地址，号码，联系您的社交媒体帐户，金钱转移控制号码（MTCN），任何银行帐户详细信息，任何已发送的照片/视频等。

保护您的帐户 - 有时犯罪分子将在信件中包含您的密码，以使其看起来更合法。他们可能是从以前泄露的数据中发现的。您可以检查您的帐户是否已被侵入，并通过访问-www.haveibeenpwned.com 来获取未来的通知。

拉黑并举报 - 将它们报告给他们与您联系的平台，并在平台上 /联系人中拉黑此人。

不要删除任何联系的信件。

如果您或您认识的某人是性欺诈的受害者，不要觉得很尴尬，因为会有能帮助和支持的地方。不要恐慌。对于某些人来说，这可能非常令人痛苦，但是会有能提供帮助，建议和指导的地方。您并不孤单。



英国 SIM 卡相关建议

请注意，不法分子有时会利用国际学生在抵达英国前购买的 SIM 卡进行犯罪活动。诈骗者可能利用这些号码实施“SIM 卡置换”（SIM swapping）诈骗，从而窃取个人信息、入侵重要账户并进行冒充诈骗。

为降低此类风险，请务必在抵达英国后，直接从正规、信誉良好的移动网络运营商处购买英国 eSIM 或实体 SIM 卡。您可以在英国的各类超市及移动网络运营商的官方门店轻松购买到 SIM 卡。

支持和福祉

请向您的大学/学院健康服务寻求帮助，以寻求帮助和指导。

撒玛利亚人（Samaritans）

针对在英国和爱尔兰的任何人，可提供24/7每年365天免费的，机密的情感支持服务
致电 116 123
www.samaritans.org

喘息空间（Breathing Space）

为苏格兰的任何遭受情绪低落，抑郁或焦虑的人提供免费的保密服务。它有一个服务热线和网络聊天；请看网站可用的时间
www.breathingspace.scot

CALM

试图降低自杀率的运动，尤其是男性。CALM有一个服务热线和网络聊天，下午5点 - 午夜，一年365天
www.thecalmzone.net

UKCISA

UKCISA 是英国国际学生事务委员会（UK Council for International Student Affairs），这是一个致力于为在英国际学生及其相关工作人员提供支持的全国性组织。
www.ukcisa.org.uk

Student Minds

一家为英国大学学生提供心理健康支持的慈善机构。
www.studentminds.org.uk

更多信息，建议和指导

NCSC 性勒索电子邮箱
www.ncsc.gov.uk/guidance/sextortion-scams-how-to-protect-yourself

网络钓鱼
www.ncsc.gov.uk/collection/phishing-scams

打击色情求助热线-性勒索（Revenge Porn Helpline – Sextortion）
www.revengepornhelpline.org.uk

网路安全（Get Safe Online）
www.getsafeonline.org

受害者保健卡
www.victimsupport.scot

Take Five
www.takefive-stopfraud.org.uk

钱骡（Money Mules）
www.nationalcrimeagency.gov.uk/moneymuling

苏格兰警察（Police Scotland）
www.scotland.police.uk/advice-and-information/internet-safety

苏格兰警察
守护民众安全

POLICE
SCOTLAND
Keeping people safe
POILEAS ALBA

由苏格兰警察于 2023 年 8 月 1 日创建

19963_26_psm