网络安全：

虚假新闻、自动程序、僵尸网络和点击欺诈

《纽约时报》[1] 近期发布了一篇报道，讲述虚假新闻如何影响除了名人和政治人物以外的普通人和企业。据报道，这则虚假新闻不负责任地指控一家华盛顿特区的比萨店被用作儿童性交易场所。虚假新闻发布后，一名男子携带突击步枪前往该披萨店进行调查，所幸执法人员逮捕了该男子，避免了一场重大灾难的发生。[2]

近期，美国财政部金融犯罪执法局就网络事件和网络犯罪问题向金融机构发布了警告，其中包括可疑活动报告提交示例和一些常见问题。本文将重点讨论虚假新闻给金融犯罪调查人员带来的挑战，并通过自动程序、僵尸网络和点击欺诈等途径，[3] 往往会伴随虚假新闻而来的网络安全威胁示例。[4]

虚假新闻

长期以来，以欺骗或隐瞒真相为目的制造虚假信息已成为一个竞争激烈的领域。但近期 Google、Twitter 和 Facebook 纷纷着手打击通过虚假新闻谋利的行为，[5] 这一情况已经引发金融犯罪调查领域的极大关注。

由于虚假新闻的存在，人们变得更不愿意相信传统新闻及社交媒体上的负面新闻。金融犯罪调查人员需要始终对欺诈性虚假信息、骗局和讽刺性文章保持警惕态度，因为上述信息会增加他们找到可靠负面媒体的难度。审查搜索结果（例如，[6] 某些在线声誉管理软件和服务提供商发布的针对个人或企业的负面评论，或保留未发布的正面评论，此行径的目的是为其产品和服务制造需求）时，采取合理的怀疑态度是一种妥当的做法。[7]

了解新闻时最好不要仅止步于新闻标题 [8]，此外，还应对陌生新闻媒体发布的在线新闻持谨慎态度。可通过在 WHOIS.net 上输入域名对网站注册人的身份进行调查，并使用 WHOIS Lookup 工具重复该步骤，查询域名注册商的相关信息。

另外，在浏览器中输入新闻网址或从搜索结果中选择新闻网址时要保持警惕。例如，人们可能本来想要输入 cnn.com，却手误输入了 cnn.om。由于 .om 是阿曼的互联网国家代码一级域名，因此 cnn.om 连接的可能会是一个虚假新闻网站。在一份据称为恶意 .om 网站的在线名单上，cnn.om 赫然在列。[9] 误植域名的网站无视知识产权和合法新闻媒体享有的 [10] 反不正当竞争保护 [11]，并向互联网用户发送虚假新闻 [12] 和恶意软件 [13]。

在查证一则新闻是否为虚假新闻时，应调查的信息包括作者的真实身份，其此前撰写的报道是否具有准确性，新闻来源是否可靠，有关事实、引言及出版日期的信息是否准确等。一些人为了掩藏不希望他人看到的搜索结果，可能会使用在线声誉管理工具，找他人代笔新闻博客或文章，将自己包装成为行业的思想领袖。[14] 无论是（个人或企业的）正面或负面新闻，都应对其准确性、完整性及相关性加以核实。

照片也应予以核实确认。互联网用户可以通过将图片拖放至 TinEye[15] 或谷歌图片 [16] 等基于网络的工具对图片进行反向搜索，以核实其来源和发布历史。互联网用户可以使用 Metapicz[17]

---

[1] Pui-Wing Tam，“Anti-Clinton Fake News Casts Pizzeria as Front for Crime”（反克林顿虚假新闻谎称披萨店为犯罪场所），*《纽约时报》*，2016 年 11 月 22 日，http://www.nytimes.com/2016/11/22/technology/anti-clinton-fake-news-casts-pizzeria-as-front-for-crime.html

[2] Keith L. Alexander 与 Susan Svrluga，“‘I am sure he is sorry for any heartaches he has caused,’ mother of alleged ‘Pizzagate’ gunman says”（“披萨门”枪手母亲说道：“我相信他对自己给他人造成的心痛感到愧疚不已”），*华盛顿邮报*，2016 年 12 月 12 日，https://www.washingtonpost.com/local/public-safety/i-am-sure-he-is-sorry-for-any-heartaches-he-has-caused-mother-of-alleged-pizzagate-gunman-says/2016/12/12/ac6f9068-c083-11e6-afd9-f038f753dc29_story.html?utm_term=.50c512a5f409

[3] “FIN-2016-A005 Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime”（就网络事件和网络犯罪问题对金融机构发布的 FIN-2016-A005 公告），*美国财政部金融犯罪执法局*，2016 年 10 月 25 日，https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

[4] “Frequently Asked Questions (FAQs)”（常见问题），*美国财政部金融犯罪执法局*，2016 年 10 月 25 日，https://www.fincen.gov/sites/default/files/shared/FAQ_Cyber_Threats_508_FINAL.PDF

[5] Abby Ohlheiser，“This is how Facebook’s fake-news writers make money”（Facebook 虚假新闻作者如何赚钱），*华盛顿邮报*，2016 年 11 月 18 日，https://www.washingtonpost.com/news/the-intersect/wp/2016/11/18/this-is-how-the-internets-fake-news-writers-make-money/

[6] “Lawsuit over negative Yelp review heads to Calif. Supreme Court”（针对 Yelp 负面评论提起的诉讼由加利福尼亚州最高法院受理），*美国 CBS 新闻*，2016 年 9 月 22 日，http://www.cbsnews.com/news/lawsuit-over-negative-yelp-review-california-supreme-court/

[7] Cheryl Conner，“The Dark Side of Reputation Management: How It Affects Your Business”（声誉管理的阴暗面：声誉管理如何影响你的企业），*《福布斯》*，2013 年 5 月 9 日，http://www.forbes.com/sites/cherylsnappconner/2013/05/09/the-dark-side-of-reputation-management-how-it-affects-your-business/#1f572fcc4b89

[8] Nick Robins-Early，“How to Recognize a Fake News Story”（如何识别虚假新闻），*赫芬顿邮报*，2016 年 11 月 22 日，http://www.huffingtonpost.com/entry/fake-news-guide-facebook_us_5831c6aae4b058ce7aaba169

[9] Endgame - List of malicious .om sites（恶意 .om 网站清单），*Pastebin*，2016 年 3 月 11 日，http://pastebin.com/q2WCuw6K

[10] William Needle，“Chapter No. 4.3 Trademark Primer”（4.3 章商标入门），*Concept Foundation*、*PIPRA*、*FIOCRUZ 与 bioDevelopments-Int. Institute*，http://www.iphandbook.org/handbook/ch04/p03/

[11] Florina Yezril，“Somewhere Beyond the ©: Copyright and Web Design”（介于版权和网页设计之间），*美国纽约大学知识产权与娱乐法律期刊*，2015 年 12 月 17 日，http://jipel.law.nyu.edu/vol-5-no-1-2-yezril/

[12] Elizabeth Weise，“Hackers use typosquatting to dupe the unwary with fake news, sites”（黑客利用误植域名的网站上的虚假新闻欺骗不谨慎的互联网用户），*USA Today*，2016 年 12 月 1 日，http://www.usatoday.com/story/tech/news/2016/12/01/hackers-use-typo-squatting-lure-unwary-url-hijacking/94683460/

[13] Lily Hay Newman，“Be Careful. Mistyping a Website URL Could Expose You to Malware”（当心！输错网址可能导致你接触恶意软件），*Slate*，2016 年 3 月 17 日，http://www.slate.com/blogs/future_tense/2016/03/17/hackers_use_om_urls_for_typosquatting_malware_attacks.html

[14] *Brand Yourself Concierge Service（Brand Yourself 在线声誉定制服务）*，https://brandyourself.com/info/about/howItWorks/concierge

[15] *TinEye*，http://www.tineye.com

[16] *谷歌图片*，https://images.google.com

[17] *Metapicz*，http://metapicz.com

和 Jeffrey Friedl 图片元数据查看器 (Image Metadata Viewer)[18] 等基于网络的元数据核实工具来核实图片的拍摄日期、时间及地点追踪数据。

互联网用户可以使用 Izitru 等基于网络的服务来验证图片[19]是否经过编辑以及核实图片的真实性。此类真实性证明对于拍卖网站和其他附有图片的在线卖家具有独特的意义，因为买家在购买产品和服务前需要参考图片。

虚假新闻可通过在线搜索、传统新闻来源以及社交媒体给互联网用户带来网络安全风险。应警惕伪装成新闻和其他通知形式的恶意软件，包括浏览器更新程序[20]、安全补丁[21]以及软件更新程序。[22]

想要识破恶意软件的伪装，用户需要多留意细节和提示出现的时机。有些恶意软件很容易识别，例如：带有错别字的更新提示、不专业的语言表达或与商标不符的徽标。应警惕引发强烈情绪或紧迫感的更新提示。如果更新提示无缘无故出现，请前往软件供应商的官方网站查看是否需要下载。美国联邦调查局提醒互联网用户，在使用公共热点或酒店互联网服务时要警惕可能伪装成软件更新提示的恶意软件。对于浏览免费媒体网站或下载免费软件的用户而言，恶意软件可能伪装成虚假的软件更新程序。应将安全软件设置为自动更新及始终保持运行，为笔记本电脑及移动设备等终端设备提供保障。由于恶意软件可以劫持自动更新程序，因此用户应不时查看自动更新状态。[23]

网络犯罪分子可能利用电子邮件[24]、新闻报道链接[25]、广告链接[26]以及词语搜索（包括个人姓名搜索）[27]在计算机上加载恶意软件、间谍软件和垃圾邮件，诱导用户访问恶意网站并向其报告用户的键盘使用情况及在线活动。此类报告可能影响美国联邦法律的可疑活动报告保密规定。[28]

自动程序和僵尸网络

计算机自动程序（又称“自动程序”）常被用作传播虚假新闻的手段。[29]

并非所有自动程序都是一样的。谷歌网页抓取自动程序 Googlebot 是自动程序的一个正面示例，它被用于发现新创建或更新后的网页并将其添加至搜索索引中。[30]

令人遗憾的是，由于经常被利用来控制受感染的计算机以达成非法目的，以致自动程序声名狼藉。由于恶意自动程序会通过网页数据抓取窃取网页内容、实施点击欺诈以及控制用户帐户，[31]因此网络公司在辨别真正的客户[32]和恶意自动程序上面临更加严峻的挑战。[33]在线赌博网站上，自动程序违反

[18] *Jeffrey Friedl 图片元数据查看器 (Image Metadata Viewer)*，http://exif.regex.info/exif.cgi
[19] *Izitru*，http://www.izitru.com
[20] Larry Loeb，“Firefox Malware Poses as Browser Update”（火狐浏览器恶意软件伪装成浏览器更新程序），*Security Intelligence*，2016年7月11日，https://securityintelligence.com/news/firefox-malware-poses-as-browser-update/
[21] Mark Jones，“Top Story:Watch out!Malware disguised as Microsoft security update”（头条新闻：警惕！恶意软件伪装成微软安全更新程序），*Komando.com*，2016 年 10 月 29 日，http://www.komando.com/happening-now/378364/watch-out-microsoft-security-update-disguised-as-malware/all
[22] “Keep getting fake Adobe update popup”（虚假 Adobe 更新提示不断弹出），*Adobe*，2016 年 9 月 7 日，https://forums.adobe.com/thread/2205736
[23] “Is That Software Update Actually Malware?”（这个软件更新程序真的是恶意软件吗？），*ZoneAlarm*，2015 年 3 月 11 日，http://www.zonealarm.com/blog/2015/03/software-update-malware/
[24] Elizabeth Shim，“South Korea police warns of malware in emails about Park Geun-hye”（韩国警方警告称内容涉及韩国总统朴谨惠的电子邮件中存在恶意软件），*合众国际社*，2016 年 11 月 23 日，http://www.upi.com/Top_News/World-News/2016/11/23/South-Korea-police-warns-of-malware-in-emails-about-Park-Geun-hye/7101479913990/
[25] “Visitors of NY Times, BBC, and AOL sites targeted by malware”（纽约时报、BBC 以及美国在线网站的访客成为恶意软件的进攻目标），*Lavasoft*，2016 年 3 月 17 日，http://www.lavasoft.com/mylavasoft/company/blog/visitors-of-ny-times-bbc-and-aol-sites-targeted-by-malware
[26] Laura Hautala，“How to avoid getting conned by fake news sites”（如何避免遭到虚假新闻网站欺骗），*CNET*，2016 年 11 月 19 日，https://www.cnet.com/how-to/how-to-avoid-getting-conned-by-fake-news-sites/
[27] “Celebrities Bring Us Entertainment, Laughter—and Malware”（名人给我们带来娱乐、欢笑以及恶意软件），*Intel Security*，2016 年 10 月 4 日，https://securingtomorrow.mcafee.com/business/celebrities-bring-us-entertainment-laughter-malware/
[28] 《美国法典》第 31 篇第 5318(g) 条；《美国联邦法规》第 31 篇第 103.18 条（美国财政部）；《美国联邦法规》第 12 篇第 21.11 条（美国货币监理署）；《美国联邦法规》第 12 篇第 563.180 条（美国储蓄机构管理局）；《美国联邦法规》第 12 篇第 353.1–353.3 条（美国联邦存款保险公司）；《美国联邦法规》第 12 篇第 208.62 条（美国联邦储备委员会）。
[29] John Markoff，“Automated Pro-Trump Bots Overwhelmed Pro-Clinton Messages, Researchers Say”（研究人员表示，支持特朗普的自动程序发送的推文数量远超支持克林顿的推文数量），*《纽约时报》*，2016 年 11 月 17 日，http://www.nytimes.com/2016/11/18/technology/automated-pro-trump-bots-overwhelmed-pro-clinton-messages-researchers-say.html?_r=0
[30] “Googlebot”，*Google Search Console 帮助中心*，2016 年，https://support.google.com/webmasters/answer/182072?hl=en
[31] “The 2016 Economics of Web Scraping Report”（网页抓取经济学 2016 年报告），*Distil Networks*，2016 年，https://forum.equinix.com/assets/images/files/distil-networks-2016-economics-of-web-scraping.pdf
[32] “The Bot Baseline:Fraud in Digital Advertising - Advertisers will lose $7.2 billion globally to bots in 2016”（自动程序基线：数字广告欺诈 - 2016 年全球广告商将有 72 亿美元收入流向自动程序），*美国广告商协会*，2016 年，http://www.ana.net/content/show/id/botfraud-2016
[33] Bryan Hooi、Hyun Ah Song、Alex Beutel、Neil Shah、Kijung Shin 与 Christos Faloutsos，“FRAUDAR:Bounding Graph Fraud in the Face of Camouflage”（FRAUDAR 算法），*美国卡内基梅隆大学*，2016 年，https://www.cs.cmu.edu/~neilshah/research/papers/FRAUDAR.KDD.16.pdf
[34] “Rise of the Machines:How Poker Bots Infiltrated the Online Game”（扑克牌自动程序如何侵入网络游戏），CardsChat，https://www.cardschat.com/poker-bots.php#sthash.tSAasWUK.dpuf

前金融犯罪执法局局长 JENNIFER SHASKY CALVERY 表示，可疑活动报告对于帮助美国联邦调查局识别与大规模洗钱活动犯罪分子操控下僵尸网络有关的电汇至关重要

使用条款与人类玩家对战，[34] 并规避年龄、身份核查程序及增强客户尽职调查程序。[35]

美国国会近期通过立法，禁止利用自动程序进行在线票券倒卖活动。[36] 2016 年 12 月 14 日，前美国总统奥巴马签署通过了《2016 优化线上售票法案》，公法编号：114-274。根据该法案的规定，使用自动程序预先购票后以高价转售属于《美国联邦贸易委员会法案》所述之“不正当的欺骗行为”。[37] 虽然这项法案的对象为被利用作在线票券倒卖工具的自动程序，但这一法案的通过也为类似禁止利用自动程序危害其他商品及服务在线销售法案的制定奠定了基础。

一台受感染计算机上的自动程序可能通过僵尸网络与其他受感染计算机连接，而僵尸网络可在全球范围内蔓延。通过僵尸网络，命令和控制服务器可作为主计算机远程控制被感染的计算机。不过，这种传统方式正衍生出一些新的形式。[38]

僵尸网络可能会通过收集互联网用户的个人财务信息（如信用卡卡号、银行账户信息和密码等）并将此类信息发送给有组织犯罪团伙和恐怖分子，对互联网用户造成不利影响。[39] 美国联邦调查局正联手私营机构、美国境内外执法部门以及其他美国联邦机构，积极应对此类网络安全威胁。[40]

前金融犯罪执法局局长 Jennifer Shasky Calvery 表示，可疑活动报告对于帮助美国联邦调查局识别与大规模洗钱活动犯罪分子操控下僵尸网络有关的电汇至关重要。其中就包括 GameOver Zeus 僵尸网络案件，仅在美国境内，该案件引发的资金损失就超过了 1 亿美元。[41]

美国联邦调查局的联合行动还缓释了 DNS Changer、Dridex、Dorkbot、Simda 僵尸网络以及其他可用于传播病毒（如勒索软件）的僵尸网络构成的风险。美国联邦调查局通过在海外派驻网络安全法务专员，携手外国执法部门和情报机构开展联合行动。[42]

关于美国网络事件协调的总统政策指令概述了应对网络安全威胁的公共 - 私人合作框架。美国司法部受指定为对网络事件构成的威胁进行响应的联邦领导机构，并由美国联邦调查局和国家网络调查联合特别工作组代表行事。美国国土安全部受指定为对网络事件进行资产响应的联邦领导机构，并由国家网络安全和通信集成中心代表行事。美国国家情报总监办公室受指定为提供情报支持的联邦领导机构，并由网络安全情报集成中心代表行事。[43]

美国联邦调查局正与一家私营机构在线欺诈防范公司 White Ops 展开密切合作，该公司近期发现了一个名为

[35] “You need to know your customers - remote casinos:Customer due diligence in remote casinos”（你需要了解你的客户 - 远程赌场：远程赌场客户尽职调查），*Gambling Commission*，2015 年 12 月，http://www.gamblingcommission.gov.uk/Gambling-sectors/AML/How-to-comply-AML/You-need-to-know-your-customers.aspx

[36] Ray Waddell，“Inside the Music Industry—and Congress’—Fight Against Ticket Bots”（音乐行业携手国会，共同打击票券倒卖自动程序），*Billboard*，2016 年 6 月 23 日，http://www.billboard.com/articles/business/7416096/ticket-bots-illegal-software-music-stars

[37] 待签议案 - S.3183 - 第 114 届国会（2015-2016 年）：BOTS Act of 2016（《2016 优化线上售票法案》），*Congress.gov*，https://www.congress.gov/bill/114th-congress/senate-bill/3183/text

[38] Botnets Today，*微软安全情报报告*，https://www.microsoft.com/security/sir/story/default.aspx#!botnetsection_p2p

[39] Joseph Demarest，“Taking Down Botnets”（取缔僵尸网络），美国联邦调查局，2014 年 7 月 15 日，https://www.fbi.gov/news/testimony/taking-down-botnets

[40] “International Cyber Crime—Iranians Charged with Hacking U.S. Financial Sector”（国际网络犯罪——数名伊朗黑客被控侵入美国金融部门），美国联邦调查局，2016 年 3 月 24 日，https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector

[41] Prepared Remarks of FinCEN Director Jennifer Shasky Calvery, delivered at the FSSCC-FBIIC joint meeting（金融犯罪执法局局长 Jennifer Shasky Calvery 在 FSSCC-FBIIC 联合会议上发表的预备演讲），*金融犯罪执法局*，2015 年 12 月 9 日，https://www.fincen.gov/sites/default/files/shared/20151209.pdf

[42] “DHS, DOJ Respond to Carper Inquiries on Agencies’ Response to Threat of Ransomware”（关于参议员 Carper 针对美国国土安全部和司法部对勒索软件的威胁所采取的行动提出的问询，两个相关机构作出回应），*美国参议院国土安全及政府事务委员会*，2016 年 3 月 30 日，https://www.hsgac.senate.gov/media/minority-media/dhs-doj-respond-to-carper-inquiries-on-agencies-response-to-threat-of-ransomware

[43] “Presidential Policy Directive—U.S. Cyber Incident Coordination”（关于美国网络事件协调的总统政策指令），*美国白宫*，2016 年 7 月 26 日，https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

Methbot 的僵尸网络，其造成的资金损失已超过 1.8 亿美元。[44]

美国联邦刑事诉讼程序规则第 41 条规则的最新规定于 2016 年 12 月 1 日起生效。电子前哨基金会 (Electronic Frontier Foundation) 声称，根据第 41 条规则的规定，只要某台计算机与僵尸网络相连，执法部门获取搜查令的程序将比以前更加简单，因此，应为这条新规定增设保证条款。[45]

点击欺诈

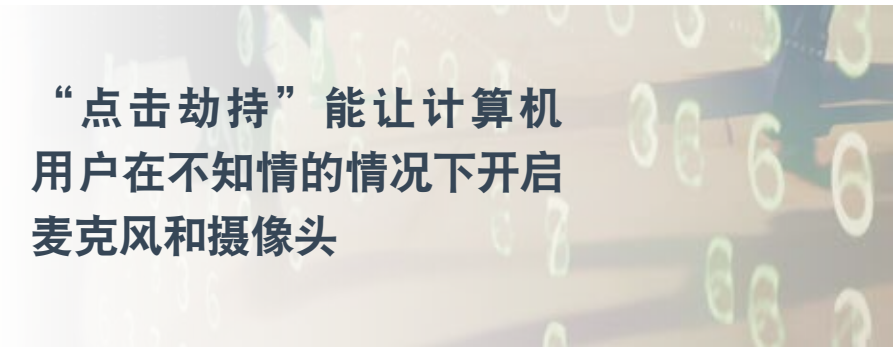
在线广告点击付费自动程序和僵尸网络为有组织犯罪团伙和恐怖分子提供机会，使得他们能够[46]通过点击欺诈来开展洗钱活动。[47]

例如，“点击劫持”（又名用户界面伪装攻击），可能与虚假新闻相关，被用作社交媒体点击欺诈的诱饵。[48]某有组织犯罪团伙借助一个覆盖 100 多个国家、连接 400 多万台计算机的僵尸网络，运行“点击劫持”恶意软件。该团伙利用该软件欺骗用户点击隐藏下的链接或按钮，以欺诈性手段得到 1,400 多万美元的广告点击付费收入。这群来自爱沙尼亚的犯罪分子伪装成一家在线广告公司，与该公司相连的十余家前台公司分布于塞浦路斯、丹麦、英格兰、爱沙尼亚、塞舌尔共和国、俄罗斯和美国；据传该团伙仍有一名俄罗斯籍成员在逃。[49]

“点击劫持”能让计算机用户在不知情的情况下开启麦克风和摄像头。“点击劫持”的防范手段包括：更新网页浏览器和 Flash 插件、安装用户界面伪装攻击侦查和防范软件。[50]

反洗钱 / 反恐融资调查员可能会对“点击洗钱”一词感兴趣。2010 年，微软普及推广了“点击洗钱”这个词语，用于描述另一种形式的点击欺诈，即将无效广告点击产生的收入伪装成来自合法来源的资金。[51]犯罪分子试图凭借“点击洗钱”手段避开 Microsoft adCenter 平台的欺诈侦测系统，该系统用于为在线广告商提供保障。从字面上看，“点击洗钱”与洗钱活动有相似之处，具体表现为，两者都试图将非法资金伪装成合法所得。[52]

综上所述，根据金融犯罪执法局近期发布的公告（该公告介绍了网络事件、网络犯罪和网络相关信息，并提供了可疑活动报告提交示例和一些常见问题解答），如发现通过自动程序、僵尸网络和点击欺诈等途径而伴随虚假新闻产生的网络安全威胁，可通过可疑活动报告进行汇报。



Miguel Alcántar, CAMS-FCI, 合规顾问，美国加利福尼亚州奥克兰，alcantar@aya.yale.edu

[44] Jose Pagliery，“Russian ‘methbot’ fraud steals $180 million in online ads”（俄罗斯 Methbot 欺诈窃取 1.8 亿美元在线广告资金收入），CNN 新闻技术频道，2016 年 12 月 20 日，http://money.cnn.com/2016/12/20/technology/ad-fraud-online-methbot/

[45] Jamie Williams，“Expanded Government Hacking Powers Need Accompanying Safeguards”（需为扩大的政府黑客入侵权力制定保证条款），*电子前线基金会*，2016 年 12 月 14 日，https://www.eff.org/deeplinks/2016/12/expanded-government-hacking-powers-need-accompanying-safeguards

[46] “Ad Networks:A New Avenue for Money Laundering”（广告网络：洗钱新途径），*Trulioo*，2015 年 10 月 27 日，https://www.trulioo.com/blog/ad-networks-a-new-avenue-for-money-laundering/

[47] “Clicks and impressions - Definition of invalid click activity”（点击和曝光率 - 无效点击活动的定义），*Google AdSense Help*，https://support.google.com/adsense/answer/16737?hl=en

[48] Susan Hogan，“Internet users falling prey to ‘click-jacking’ schemes”（互联网用户成为“点击劫持”诡计的受害者），WPRI 12 Eyewitness News，2014 年 10 月 20 日，http://wpri.com/2014/10/20/internet-users-falling-prey-to-click-jacking-schemes/

[49] “Estonian Cybercriminal Sentenced for Infecting 4 Million Computers In 100 Countries With Malware In Multimillion-Dollar Fraud Scheme”（爱沙尼亚网络犯罪分子因利用恶意软件感染 100 个国家的 400 万台计算机而被处以 14 年监禁，该欺诈案的涉案资金达数百亿美元），*美国司法部*，2016 年 4 月 26 日，https://www.justice.gov/usao-sdny/pr/estonian-cybercriminal-sentenced-infecting-4-million-computers-100-countries-malware

[50] Andy O’Donnell，“How to Protect Yourself From Clickjacking Attacks”（如何防范“点击劫持”），*Lifewire*，2016 年 10 月 20 日，https://www.lifewire.com/how-to-protect-yourself-from-clickjacking-attacks-2487178

[51] Nancy Gohring，“Microsoft Chases ‘Click Laundering’”（微软打击“点击洗钱”行为），*PCWorld*，2010 年 5 月 19 日，http://www.pcworld.com/article/196694/article.html

[52] Bill Harmon，“Microsoft Adds New Defendant in Click Laundering Lawsuit”（微软“在点击洗钱”诉讼案中增加一名被告），*微软*，2010 年 12 月 10 日，https://blogs.technet.microsoft.com/microsoft_on_the_issues/2010/12/10/microsoft-adds-new-defendant-in-click-laundering-lawsuit/