以色列 BGU 研究人员创建了评估用户安全意识的新框架

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Researchers Create New Framework to Evaluate User Security Awareness		
原文作者	杰·维贾扬（Jai Vijayan）	**原文发布日期**	2020 年 8 月 6 日
作者简介	杰·维贾扬是一位经验丰富的技术记者，在 IT 贸易新闻领域拥有 20 多年的经验。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/endpoint/researchers-create-new-framework-to-evaluate-user-security-awareness/d/d-id/1338603		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

以色列 BGU 研究人员创建了评估用户安全意识的新框架

杰·维贾扬

2020 年 8 月 6 日

基于问卷调查和自我评估的方法并不总是有效，无法评估用户防御社会工程威胁的能力。

以色列本古里安大学（BGU）的研究人员开发了一个新框架，用于持续评估最终用户对网络钓鱼等社会工程攻击的防御能力。

现有安全意识评估技术通常高度依赖问卷调查和用户自己报告行为，而该新方法则基于真实的数据。这些数据是从最终用户的智能手机、PC、设备的进出网络流量以及攻击模拟中收集的。

在本周美国举办的黑帽大会上，BGU 网络安全研究中心首席研究经理罗恩·比顿（Ron Bitton）发表了演讲，指出该框架解决了现有评估方法的一些缺点。

比顿说，现有评估方法通常不区分攻击类型或平台，并且是静态的。他指出："这些方法存在若干局限性。例如，问卷和调查都依靠用户自己报告行为，因此是非常主观和有偏见的。"

同样，模拟攻击旨在衡量用户防御社会工程攻击的能力，也容易受到环境因素的影响。此外，强制用户参加安全意识培训研讨会等活动，会导致用户的参与度降低。

在开发新框架时，研究人员首先确定了用户安全意识的所有指标，然后评估不同指标在防御不同类型攻击方面的权重。

为确定这些指标，研究人员分析了诸多社会工程案例，确定了攻击者在社会工程攻击中通常利用的"人的"漏洞和技术，以及可以用来防止这种漏洞利用的对策。

通过分析，研究人员提出了安全意识的 30 种指标。用户具有良好安全意识的示例包括：仅从受信任源下载应用程序、不安装具有危险权限的应用程序、仅使用 HTTPS 网站、避免浏览被浏览器标记为危险的网站、定期更新口令、不将未知存储介质（例如 USB）连接到计算机等。

得分与评估

确定安全意识指标之后，研究人员开发了一种程序，对每种用户行为防御四种攻击的有效性进行评分。这四种攻击包括：口令攻击、基于应用程序的攻击、网络钓鱼和中间人攻击。他们发现，在不同类型的攻击中，用户的防御行为也应是不同的。

例如，在防御网络钓鱼攻击时，用户可以避免通过 HTTP 网站发送敏感信息，避免在未经验证的网站上填写私人信息等。但在防御中间人攻击时，上述防御措施则没什么效果；真正有效的防御措施是从设备中删除未知证书，不批准未知数字证书等。

在确定了测量指标和评估方法之后，BGU 研究人员开发了两种探针来分析用户行为。一种是端点代理，该端点代理可以从设备中收集多种探针数据，包括已安装的应用、应用许可、应用源、排名、邮件活动、安全设置和社交网络活动。

另一种是侵入性较小的网络监视器，该监视器使用各种方法（包括深度数据包检查和对应用程序级协议进行评估）来检查进出最终用户设备的流量。通过这些探针，研究人员可以获得丰富的数据，详细了解用户的安全意识。

研究人员还开发了一种模拟攻击框架，该框架能够实施 20 种不同类型的攻击，包括权限滥用，以及涉及恶意 Word 宏、PDF 文档、网络钓鱼邮件和 SMS 消息的攻击。

研究人员在七到八周的时间内对 162 位用户进行了测试。首先，每位用户需要提供一份自我评估问卷作为基线。研究人员通过新框架对用户的安全意识进行评分，并根据得分将其安全意识评为低、中或高。之后，他们通过攻击模拟框架，计算每位用户防御各种攻击的成功率。

比顿说，结果显示，得分较高的用户比得分较低的用户更有能力防御攻击。然而，基于问卷对用户安全意识进行的分类，与用户防御攻击的能力几乎是没有关联的。

“受试者的自我报告行为可能与他们的实际行为有很大差异。”比顿说，“相比之下，从客观指标（例如从端点和基于网络的解决方案中收集的数据）得出的安全意识分值，则与用户防御社会工程攻击的能力高度相关。”

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com