关于中东教育环境中网络安全意识的研究

**摘要：**

信息安全意识在面对入侵者的网络攻击方面可发挥重要作用。本文的主要目的是分析中东教育环境中研究人员，本科生和员工的信息安全意识，试图了解他们的信息安全意识水平，对于机构的相关风险和整体影响。结果表明，参与者对信息安全原则的重要性及其在日常工作中的实际应用缺乏必要的知识和理解。然而，这种情况可以通过全面的意识和培训计划得到纠正，并在机构的各个层面采取所有必要的安全措施，以确保学生，学术和员工值得信赖，技术娴熟并注重数据安全。如果没有这样的培训计划和意识，将会对IT系统及其应用程序使用以及现在和将来的用户个人安全产生负面影响。从本次调查中发现的弱点出发，提出了一些必要的建议来纠正这种情况。

**关键词：**

网络安全；信息安全；安全措施；安全意识；安全培训政策；数字取证；分类和回归树（CART）。

**介绍：**

计算环境和计算机应用程序中的技术进步已使不受管制的社交网络能够在任何给定时间的同时容纳数千个活跃用户和应用程序。由于这些用户和应用程序处于不安全的环境中，所以有许多寻找并利用系统漏洞的网络犯罪分子、伪装者、黑客和反社会人士，尤其身处教育网络环境中的犯罪分子较为突出。

具有先进计算环境，网络和应用程序的此类技术的全方位普及对于当今的在线和在线教育的过程和交互至关重要。学生和教师可以查阅、接收大量信息，这不仅可以扩展他们的视野，还可以增加他们的生动的受教育经历。不幸的是，这些技术越来越难以防止恶意活动。有鉴于此，这些事件产生了很多不利影响，包括未经授权访问私人和机构数据，身份滥用，知识产权盗窃和金融欺诈构成对关键基础设施，公共安全和国家安全的潜在威胁。

除了提供必要的保护和安全机制外，良好的树立网络安全意识的计划必须经过适当地调查与研究，以便为用户和员工提供危机意识和积极的培训和教育计划。该计划应有助于在它们之间发展和传播安全意识，采用适当的对物理地址的访问控制，遵守机构或组织规定的安全政策和规则，以达到最高的安全级别。

人们普遍认为，信息安全意识与预防措施之间存在直接关系，而预防措施提高了安全绩效。这表明员工安全意识和评估应成为制定或加强任何网络安全策略的出发点。

员工遵守信息安全意识的意图明显受到他们的态度，规范信念和自我价值的影响，以使自己迎合整体的个人和组织效应。克鲁格发现信息安全概念知识与强化自我价值和整体可信度的行为之间存在显着的联系。

**背景：**

教育机构依靠计算机网络和技术为学生提供大学新闻、活动、电子邮件、课程、校历、学业成绩、学生成绩以及存储在计算机系统上的其他个人信息。因此，需要保护这些系统免受许多威胁，包括恶意软件、间谍软件、跨站点脚本（XSS）、病毒、蠕虫、特洛伊木马、网络钓鱼、拒绝服务（DoS）和分布式拒绝服务（DDoS）。这些系统可以被对手用来通过窃取敏感信息来影响组织的资产，同时也可以影响组织的财务系统。因此，每个使用信息系统的组织都必须认真对待信息安全。

过去十年间，利用网络安全漏洞的网络犯罪事件的数量也大幅增加。根据2014年战略与国际研究中心（CSIS）的刘易斯报告，Heartbleed是最近开放SSL中严重的网络安全漏洞，其中许多网站在使用被称为开放SSL软件的计算机代码库。此外，该软件被用于加密被认为较为安全的网站链接，比如那些负责发送和接收敏感信息的网站链接，如信用卡详细信息、在线后台交易、在线购买等。最重要的是，使用这些网站的用户认为他们是被保护的，由于软件是开源的，所以任何人都可以免费使用。这种安全意识漏洞鼓励黑客通过访问源代码来破解加密或破解软件，从而利用它来实现他的期望目标。鉴于此，一些公司，如Gmail，鼓励用户更改密码，甚至把在访问不同的安全网站时使用不同的密码作为预防措施，以免受Heartbleed风险的影响。

除此之外，中东当地媒体偶尔会报道某些人企图通过网站攻击或使攻击银行的电子系统宕机而黑入银行的电子系统。例如，巴林电信公司和国家科威特银行都是网络钓鱼攻击的目标。另一方面，阿联酋教育部网站被计算机病毒感染了，2010年阿联酋今日和2012年沙特阿美公司的计算机网络被称为Shamoon的计算机病毒感染，并且用了近两周的时间来修复漏洞，弥补损失。因此，信息安全意识，教育和培训目标在所有学科中都是重要并且必要的，这取决于机构的信息安全政策，以保护网络不受攻击和降低受到网络攻击的风险。

**相关工作：**

信息安全意识对于敏感的学术信息尤为重要，这些信息必须始终受到保护，免受网络攻击，否则黑客可能会将数据用于个人利益。本节简要介绍了教育领域内网络安全以及信息安全意识和培训方面的一些相关研究。

计算机安全协会（CSI）的Richardson在2011年发现，恶意软件感染仍然是最常见的ICT系统攻击。另一方面，恶意软件可以被证明是窃取私人，商业，金融信息和其他个人信息的攻击工具。例如，为了窃取人们的信用卡详细信息而发送垃圾邮件被用于监控用户的网络浏览行为。最近，卡巴斯基实验室在2013年引用了大约91％的组织调查报告称，他们的IT基础设施在过去12个月内至少成为一次外部网络攻击的目标。他们还报告说，与2012年相比，恶意软件，垃圾邮件，网络钓鱼，网络入侵和移动设备被盗的情况显着增加。

除此之外，Wilshusen在2012年强调了网络事件对企业的严重后果和影响。这些事件包括数据窃取，恶意软件感染和敏感的个人数据泄露，如信用卡和借记卡信息，这些数据必须防止未经授权的使用。此外，有必要确定威胁的来源，网络攻击的类型以及可用于防止此类威胁或减少网络攻击漏洞的常见网络安全技术。这些技术包括防病毒软件，恶意软件，入侵检测和预防系统，计算机取证工具，数字签名和证书以及生物识别技术。这些技术可以在提高安全水平方面发挥至关重要的作用。

Katz在2005年发现，大学在一直受到网络攻击，主要有两个原因：

（i）开放接受用户及其为公众提供的信息；

（ii）大量的计算能力值得被利用。

他强调，高等教育的初衷必须保持平衡，这种初衷可以让公众获得信息共享的权利，并确保自己的信息资产不会受到风险的影响。而Rezgui和Marks则表明，诸如信仰，文化价值观和社会条件等因素会影响大学学生在开展工作方面的行为，从而产生安全和隐私影响。因此，应认真构思安全和保障措施，并将这些措施作为学术机构教学策略的重要组成部分。

Kim在2014年对新英格兰的商科学生进行了一项调查，调查学生对信息安全意识的态度，以便开展有效的信息安全意识培训（ISAT）。这些结果表明，学生了解ISAT的必要性及其提高意识水平的重要性。然而，Aloul在2012年通过在学术界和学术界专业人士间进行的几项安全意识研究的结果，显示了中东学术界对安全意识的需求，尽管他们对如何最好地降低安全风险几乎没有经过培训。因此，信息安全意识的教育和培训至关重要，应成为组织或公司的各类管理员和用户对整体安全管理的风险评估计划的一部分，以最大限度地降低网络攻击可能带来的后果。

学术机构也容易受到网络攻击：受到攻击的案例中包括为学生和教授提供专利奖励，窃取学生和教师的私人信息。因此，除了适当的提高网络安全意识的相关计划，培训，教育和政策外，教育机构还必须使用各种安全措施，如保护措施，隐私，信任，身份管理，审计和数字取证，以满足法律和社会要求。

此外，“模拟工具”在提高学生，学术和专业人员的信息意识和保证水平方面发挥着至关重要的作用。这些工具有几个特点，易于使用并理解，允许学生和用户开展真实的实验，并使他们能够深入了解信息安全概念。其主要目标是增加和优化信息安全意识，教育，保证网络安全培训的水平，这不仅对学生，而且对有关学术方面员工也是如此。

互联网的使用日益改变了人们生活和工作的方式，并已成为我们日常生活中的必需品。不仅是为了娱乐，也是为了与我们亲近的人交流。互联网的使用在增加盗窃，欺诈和滥用职权方面起着至关重要的作用。另一方面，没有任何国家，行业，甚至个人可以免受网络安全事件的风险及其后果的影响。反过来，安全意识对于敏感信息尤为重要，这些敏感信息必须始终受到保护，免受网络攻击，黑客可能将数据用于个人利益，并且如何阻止这种现象的发生应该成为任何国家最重要的优先事项之一。

考虑到调查将有助于创造变革和新的观念，同时考虑到中东的特殊情况，将调查本地化是一种更好的方法，而不是参考有关该主题的外国调查。此外，本调查的一个重要方面是评估对网络攻击的响应速度，意识和理解程度中的行为的影响。行为的深度呈现出一种新的角度或视角，即深入了解对于教育和学习机构的网络攻击的根本问题和概念。此外，网络攻击的活力意味着机构必须及时了解网络攻击活动的发展以及与信息安全相关的问题。

全球范围的研究都集中在学术领域信息安全的有效性上。教育机构的性质是对用户的公开访问以及他们为广大公众提供的信息。因此，这种性质可以增加对包括学生中的领导者的研究记录和财务信息等私人数据侵入的机会，并且可能是网络安全事件和攻击者选择攻击学术机构的主要原因。考虑到调查将有助于创造变革和改变观念，以及更好的方法，而不是参考外国调查。此外，本调查的一个重要方面是评估对网络攻击方面的响应，安全意识和对网络攻击理解中的行为影响。不应忽视对网络安全事件及其后果的理解，因为理解对所有信息安全方面都很重要，而且它们的结果也可以使学术机构了解敏感的个人信息及其财务数据。这项研究的动机是通过关注其学术研究人员，研究人员，本科生和员工的行为来识别目标的反应程度来确定他们的识别等级，用于安全，包括安全的所有方面学术环境中针对网络安全事件的措施。此外，由于安全意识至关重要，因此需要特别关注该问题。

随着网络安全事件的数量迅速增加，并且变得越来越有威胁和频繁，提高信息系统的安全性正在成为当今的主要事项。为此，每个使用信息系统的组织都必须认真对待信息安全。事实上，信息安全是一门依靠专家，员工意识以及技术控制以确保组织的信息资产得到充分保护的学科。然而，在这个基于问卷调查的研究中，我们分析和评估了与所有信息安全措施相关的员工对于信息安全的理解程度，意识，使用方面的问题，以及位于中东不同国家的一些教育机构的弱点，以确保在那里了解针对教育和学习环境的网络攻击有关的问题。根据调查结果，我们将提供有助于概述影响信息安全行为的建议。此外，我们应当确定哪些学术领域需要进一步研究，以提高对网络事件和网络犯罪的防范和预防意识，并减少现在和将来可能造成的损害。

我们的研究基于以下两个问题：

*目标群体对网络安全事件方面的认识程度如何？*

*对于提高认知水平和合格标准可信赖程度有什么好的建议？*