E-Learning and Security Threats

Ateeq Ahmad [1] and Mohammed Ahmed Elhossiny [2]

[1] Faculty of Science
Department of Computer Science, Northern Border University, Arar, Saudi Arabia
[2] Faculty of Specific Education,
Department of Computer Teacher, Mansoura University, Egypt.

Abstract
E-Learning is a method of learning which ultimately depends on the Internet in its execution. The Internet has become the venue for a new set of illegal activities, and the E-learning environment is now exposed to such threats. Security is one of the most pressing Information Technology issues that E-education faces today, but it's especially a concern for student, instructors, teachers, lecturers and learners who find it difficult and increasingly complex to find the recourses needed to protect against growing number of security Threats. The basic aim of this article is to protect learners and instructors from unauthorized Security Threats.

Key words:
Security Risk, Security Threats, E-Learning, Definition.

1. Introduction

E-learning is the term used to describe the use of the web and other Internet technologies in terms of enhancing the teaching and learning experience. The development of E-learning has a way of learning and, at the same time, has given equal opportunities to everyone to become learners. With such methods of learning now available, it is said that information can be reached easily. However, despite the Internet as a place to obtain all necessary information and knowledge, it has also become the venue for a new set of illegal activities. Information on the Internet is continuously exposed to security threats. As a consequence of E-learning having to depend on the Internet via web applications, the E-learning environment has also become affected by security threats. The concept of E-learning and security Threats, which involves secure technologies, secure instructor facilitation, and secure learners. Security is a critical part of the E-learning, to protect learners and instructors from unauthorized Threats. The idea of E-learning and security threats, that to ensure the safety and security of the learners.

2. Definition

One of the early definitions for E-learning was provided by the American Society for Training and Development (ASTD), which proposes that elearning covers a wide set of applications and processes, such as web-based learning, computer based learning, virtual classrooms, and digitals collaboration.
Collaborative knowledge creation and innovation can occur when team members take risks. Educationally sound software must promote a psychologically secure environment" (Kildare, Williams, & Hartnett, 2006, p. 101).
E-learning also needs to happen in an environment where people's privacy is protected (As per the Family Education Rights and Privacy Act or "FERPA").
E-learning is the implementation of technology in order to support the learning process, whereby knowledge or information can be accessed using the communication technology. The learning process can be continuous, provided that the content is available on the net. (Eklund, J., Kay, M. and Lynch, H. M. 2003).

3. Objectives

The main purpose of this article is to learn the tools and motives involved in security Threats and share the lesson with the University student and Instructors, those who are involved in research related to security risk of E-learning. There is a commitment to moving far beyond theory and providing solid information about common security threats that are involving with E-learning.

4. E-Learning Security

E-Learning security is the process of preventing and detecting unauthorized use of your computer System. Prevention measures help you to stop unauthorized users from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done. The online learning should not involve the incurring of legal liabilities. Ultimately secure learning enables learner success.

Manuscript received April 5, 2012
Manuscript revised April 20, 2012

Security refers to freedom from harm. Harm, in the e-learning context, may refer to the following points.

- Corrupted or lost communications, messages, grades, data, or work.
- A compromised learner or instructor identity.
- Stolen personal or private information.
- Stolen or compromised student ideas and innovations.
- Corrupted social technical systems.

5. E-Learning Security Threats

Online E-learning security Threats are relentlessly inventive. Masters of disguise and manipulation, these threats constantly evolve to find new ways to annoy, steal and harm the system. Now a day's growing of E-learning security threats online. There are some kinds of threats that are related direct or indirect with E-learning system.

5.1 Virus Threats

Threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to your computer in the process.

5.2 Spyware Threats

Spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. We've amassed a wealth of knowledge that will help you combat spyware threats and stay safe online.

5.3 Hackers

People, not computers, create computer security threats and malware. Hackers are programmers who victimize others for their own gain by breaking into computer systems to steal, change or destroy information.

5.4 Phishing Threats

Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Internet Based Attacks While your computer is connected to the Internet it can be subject to attack through your network communications.

5.5 Viral Web Sites Threats

Users can be enticed, often by email messages, to visit web sites that contain viruses or Trojans. These sites are known as viral web sites and are often made to look like well known web sites and can have similar web addresses to the sites they are imitating. Users who visit these sites often inadvertently download and run a virus or Trojan and can then become infected or the subject of hacker attacks.

5.6 Adware, Advertising and Trojans Threats

Adware and Advertising Trojans are often installed with other programs, usually without your knowledge. They record your behaviors on the Internet, display targeted ads to you and can even download other malicious software on to your computer. They are often included within programs that you can download free from the Internet. Spyware doesn't usually carry viruses but it can use your system resources and slow down your Internet connection with the display of ads. If the Spyware contains bugs it can make your computer unstable but the main concern is your privacy. These programs record every step that you take on the Internet and forward it to an Ad Management Centre which reviews your searches and downloads to determine your preferences. The Ad Management Centre will build up a detailed profile of you, without your knowledge, and can pass this on to third parties, again without your knowledge. Some Spyware can download more serious threats on to your computer, such as Trojan Horses.

5.7 Online Social network sites Threats

Sometimes hackers go right to the source, injecting malicious code into a social networking site, including inside advertisements and via third-party apps. On Twitter, shortened URLs can be used to trick users into visiting malicious sites that can extract personal information if accessed through a work computer. Twitter is especially vulnerable to this method because it's easy to retweet a post so that it eventually could be seen by hundreds of thousands of people.

6. How to Secure E-Learning System

To implement and enforce an acceptable usage policy covering the use of E-learning media sites. It will help prevent data leaks and reduce the chances of a online

networking based attack from succeeding. The best way to ensure your policy works is to develop it through consultation with your employees and strictly enforce it. Employees are less likely to circumvent restrictions if they understand the logic behind them and have been involved in developing the overall policy. There are some common method is also used for securing the system from Threats.

6.1. Securing from Threats

- Recovering from Viruses, Worms, and Trojan Horses
- Avoiding Social Engineering and Networking Attacks
- Using Caution with USB Drives

6.2. Securing from Email, Communication

Using Caution with Email Attachments

- Reducing Spam
- Using Caution With Digital Signatures
- Using Instant Messaging and Chat Rooms Safely
- Staying safe on social Network Sites.

6.3. Securing from Browsing

- Evaluating Your Web Browser's Security Settings
- Web Site Certificates
- Bluetooth Technology
- Reviewing End-User License Agreements

6.4. Securing Privacy Control

- Protecting Your Privacy
- Effectively Erasing Files
- Supplementing Passwords
- Install and Use Anti-Virus Programs
- Use Care When Reading Email with Attachments
- Install and Use a Firewall Program
- Make Backups of Important Files and Folders
- Use Strong Passwords
- Use Care When Downloading and Installing Programs
- Install and Use a File Encryption Program and Access Controls
- Safeguard your Data
- Real-World Warnings keep you safe online.
- Keeping Children Safe Online

Conclusion

A few years ago, due to resource limitations, risk assessments, and time restrictions, it may have been impractical to deploy security of E-learning media. However, the risks and time involved with deploying security of E-learning are minimal when using current technology. The conclusion of this article that a E-learning can be implemented and protected against unauthorized security threats by using various security tools.

References

[1] Edgar Weippl, Martin Ebner, Proceedings of E-Learn 2008, Las Vegas, p. 4001-4007, 2008.

[2] Najwa Hayaati Mohd Alwi, Ip-Shing Fan, “E-Learning and Information Security Management”, International Journal of Digital Society (IJDS), Volume 1, Issue 2, June 2010.

[3] Jianming Yong, “Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes”, Journal of Universal Computer Science, vol 17, no. 2 (2011),296-310.

[4] Annie I. Anton, Elisa Bertino, Ninghui Li, Ting Yu, “A Roadmap for Comprehensive Online Privacy Policy Management”, Communications of the ACM,Vol. 50, No. 7, July 2007, pp109-116.

[5] Aqqal, A., Rensing, C., Steinmetz, R., Elkamoun, N., Berraissoul,A.,”Using taxonomies to support the macro design process for the production of WebBased Trainings”, Journal of Universal Computer Science, 2008

[6] Bella G. "What is Correctness of Security Protocols?", Journal of Universal Computer Science, Vol. 14, num. 12, 2083—2107, 2008.

[7] Hal Berghel, “Better-Than-Nothing Security Practices”, Communications of the ACM, Vol. 50, No. 8, August 2007, pp15-18.

[8] Chen L. et al, "Cryptography in Computer System Security", Journal of Universal Computer Science, Vol. 14, num. 3, 314--315, 2008.

[9] Geyer, W., Filho, R. S. S., Brownholtz, B. and Redmiles, D. F. “The Trade-Offs of Blending Synchronous and Asynchronous Communication Services to Support Contextual Collaboration”. In: Journal of Universal Computer Science, vol. 14, no. 1 (2008), 4-26.

[10] Lalana Kagal, Tiom Finin, Anupam Joshi, Sol Greenspan, “Security and Privacy Challenges in Open and Dynamic Environments, Computer”, Vol. 39, No.6, June 2006, pp89-91.

[11] Alfred Kobsa, “Privacy-Enhanced Personalisation”, Communications of the ACM, Vol. 50, No. 8, August 2007, pp24-33

[12] Novak, J.; Wurst, M. “Supporting Knowledge Creation and Sharing in Communities based on Mapping Implicit Knowledge”. Journal of Universal Computer Science, vol. 10, 2004, no. 3, p235-251.

[13] Eugene Volokh, “Personalisation and Privacy”, Communications of the ACM, Vol. 43, No. 8, August 2000, pp84-88.

[14] Xiaokui Xiao, Yufei Tao, “Personalised Privacy Preservation”, SIGMOD 2006, June 27-29, Chicago, Illinois, USA, pp 229-240.
[15] Yang G., Wong D.S. and Deng X. "Formal Security Definition and Efficient Construction for Roaming with a Privacy-Preserving Extension", Journal of Universal Computer Science, Vol. 14, num. 3, 441--462, 2008.
[16] Jianming Yong and Elisa Bertino, “Replacing lost or stolen Epassports”, IEEE Computer, October 2007, Vol. 40 No. 10 pp. 89-91.
[17] Acquisti, A, & Gross, R (2006): Imagined communities: “Awareness, information sharing, and privacy on the Facebook”: Cambridge, UK: Robinson College.
[18] Manson, R. and Rennie, R. (2006), “E-learning: the key concepts”, Routledge, Abingdon Great Britain.

Ateeq Ahmad received the Master degree in computer science in year 2003 from India. Currently he is working as a Lecturer in Faculty of Science, department of Computer Science, Northern Border University, Arar, Saudi Arabia. His research interests include Social networks, Computer Network and Network Securities.

Mohammed Ahmed Elhossiny received the B.Sc. degree in educational technolog in 1998, and the M.Sc. in educational technolog in 2005, from Ain Shams University, Egypt.. and the Ph.D. degree from the university in Ain shams 2010, He is a Lecturer at Department of Computer teacher Faculty of Education, Mansoura University, Egypt. Currently he is in Facuty of Science ,NBU,KSA. His research interests include Pattern Recognition, Computer Vision, E_Learning, Management of Data Base and Image Processing.