Redefining Computer Literacy in the Age of Ubiquitous Computing

Laurie Werner
Miami University
1601 University Blvd
Hamilton OH 45011
513-785-3136
wernerla@muohio.edu

ABSTRACT

Most computer literacy courses encountered by college students in a non-technical major encompass a foundation set of computing skills including efficient use of word processing, spreadsheet, database, and presentation software. Yet current college graduates are facing fresh challenges as end-users in a work force transformed by legislation that is revolutionizing digital data communication, by nearly boundary-less computer systems that include mobile and static devices, and by employer expectations for safeguarding critical data resources. For example, data privacy legislation affects all end-users of computer systems in the workplace. As employees, new graduates will have access to critical data to perform their jobs, yet they could be the weakest link in an otherwise effectively secure computer system, primarily because of inadequate education, negligence, and inexperience. Technical and mathematical computer security has progressed substantially in the last few years, but new graduates are typically lacking in the knowledge of computer security as a fundamental component of their workplace roles. This paper proposes a computer literacy course content and structure that incorporates substantial practice in end-user computer security.

Categories and Subject Descriptors

K.3.2 [**Computers and Education**]: Computer and Information Science Education – *Curriculum*, *Literacy*
K.4.1 [**Computers and Society**]:Public Policy Issues – *Abuse and crime involving computers, ethics*

General Terms: Management, Economics, Reliability, Experimentation, Security, Human Factors, Legal Aspects.

Keywords

Home computer security, pedagogy, laboratory activities

1. Introduction

A few months ago, the most pervasive viruses came in email attachments, this week the greatest number of threats arrived via instant messaging. America Online (AOL) advertises that they provide a "better internet" by maintaining complete protection of users' systems, thus minimizing, if not eradicating, threats to users' computer security [3]. The advertising lulls home users into thinking that by delegating the responsibility for securing their home computers becomes invisible and ignorable. However, even AOL directs users to download and install software, which users must interact with regularly for it to be effective. If the AOL methods for protecting users worked, we should see a significant drop in Malware for AOL users. Unfortunately, that is not the case. The McAfee virus and firewall protection provided to AOL users leaves open vulnerabilities. One of these is its failure to scan instant messages for threats.

Some of the AOL subscribers are non-technical students at, or graduates of, our colleges and universities. Many have taken, or will take, a computer literacy or technology course as a requirement in their curriculum. Are these students and graduates any less vulnerable than the average home user? There is no evidence to indicate that the computer literate graduates possess greater proficiency at securing a computer system than other end-users.

Who is responsible for securing the vast resources of the internet? Is it hardware vendors? Is it software vendors? Is it home users? Is it the government? Is it business users? Is it the ISP? Is it the IT professionals who secure enterprises? Debates ensue regularly in the literature about who or what is to blame, bad software, unsophisticated users, insufficient IT support within organizations – the list is nearly endless. Regardless of whom one accuses, insecurity about computing is having a negative impact on IT growth, in part because users lack confidence in secure transactions via the internet [13].

Research supports the claim that Non-technical home users deserve some of the blame for security breaches [2]. Unprotected computers are used to launch targeted attacks on systems that contain vast amounts of information, as in the recent attack on CardSystems Solutions that compromised 40 million credit and debit cards [1]. On-line criminals are constructing more focused attacks for three reasons [10]:

1. Organized criminals are able to intimidate playful hackers and redirect them to launch a persistent attack.
2. Focused attacks are under the radar of Internet security firms that monitor the internet.
3. Focused attacks provide sufficient detailed information to enable a clever criminal to hoodwink a non-IT trained employee.

All it takes is a Spyware Trojan on the right machine to glean passwords and account numbers that the criminals can immediately use [14].

SIGITE'05, October 20–22, 2005, Newark, New Jersey, USA.

In a National Cyber Security Alliance (NCSA) and AOL survey, 77% of respondents felt they were "safe from on-line threats" [15]. However, when their computers were inspected, the facts overwhelmingly revealed otherwise:

- 67% of computers lacked current anti-virus software
- 1 in 5 were infected with virus
- 80% of were infected with Spyware or Adware
- 88% didn't know they were infected with anything
- 49% of broadband users lacked firewall protection

Ignorant home users are perceived to be such a problem that at a June 2005 Forum presented by SC Magazine, a technology company CSO suggested that the average home user "is clueless about IT Security" and should be required to obtain "a license to log on to the internet"[5]. As much as requiring users to pass a test and get a license to use the internet is ludicrous, it is entirely feasible to "point to constant education, training and awareness…for making employees understand the importance of controls outside the company, providing users with information on issues that might come up at home…After all…employees are the real corporate asset."

Despite the growing threats and cyber crimes, we are on the edge of a "third wave of computation, displacing the era of mainframes and personal computers" in which "computer use is focused on a single device." This new era of "Ubiquitous computing… anticipates that an individual's computational needs will be met by tens or hundreds of computational components working together; security is both an inherent problem in this sort of combinatorial system, and a practical concern for end users" [7].

IT educators have an excellent opportunity to foster this third wave of computing by not only educating IT professionals prepared to support information security in the workplace, but also by providing the end users of tomorrow with the critical thinking and basic skills to collaborate with vendors and IT professionals who provide them with the vigilant security tools. To do so means redefining basic computer literacy and technology courses for the non-technical majors to embrace a robust focus on computer security that includes practice with and prudent evaluation of security tools.

2. The Gap in Current Literacy Courses

Most college majors require a technology course or computer literacy course presented by the IT or CS department. Some institutions tailor technology courses for various non-technical programs. For many years, CS and IT departments have developed and provided courses to assist non-technology majors in using computing to support their career goals because computing is inexorably linked to information critical to students' lives today and to their professional lives tomorrow.

Typical literacy courses are valuable to students in many ways, such as learning to use specialized software, perform research on-line, and communicate with the IT professionals, but they are dangerously outdated. If end users of computers are not knowledgeable enough to maintain reasonable security on a home computer, from updating software to recognizing phishing frauds and virus-payloaded emails, how will they stay abreast of computing policies in the workplace of the near future? PC security practices may be discussed, but rarely implemented, inside a non-technical literacy class. Because IT security today generally uses conventional approaches to system security, such as access control lists, firewalls, network based access policies which are separate from the working activities that the security policies protect, responsibility for security is delegated to the IT organization in the workplace. However, this approach is insufficient as computing becomes more pervasive. In ubiquitous computing, "security requirements depend on the specific circumstances of action and are subject to continual reflection and revision…Rather than being transparent then, security technologies need to be highly visible – available for inspection and examination seamlessly as a part of work" [7].

3. Motivation

The gap in computing literacy of our non-technical students became apparent to me personally quite recently. In the last few years, my academic focus turned to data communications, networking, and information security and away from non-majors courses. In summer 2004 and summer 2005, I taught a few sections of the computer literacy variety of courses in a summer session. I was appalled to find that many of the students were seniors, not freshman, taking the only technology course that was required in their major program. Is there one word about computer security in the course? NO! Is there internet searching! YES! Have these students been using computers at home and at school for at least five years, – YES – all of them have been. Do any of them know what a firewall is? Unfortunately, the answer to that question is less than half. These students roughly matched the NCSA and AOL survey that identified the end user's lack of sophistication with securing a home computer. [15]

4. A Plan to Reduce the Gap in Computer Literacy Courses

There are two foundation principles that permeate the design of a successful computer security component of a non-majors course [9]:

- The students should have a higher success rate than a technically intense major's course component.
- The course component should be designed to influence student behavior and attitudes towards computer security in the future.

To ensure the success rate, and to influence behavior, the security component of a computer literacy course requires lecture, lab and project work to equal about one credit hour of a 3 or 4 credit hour computer literacy course.

4.1 Laboratory Needs

The plan to enhance the computer literacy experience of non-technical students includes project and lab work that will provide them with up to date information and hands-on experience with common tools. Since we would not expect students to become proficient in MS Office without using a computer, how can we expect them to become security literate without practicing in a computer lab environment? The lab experience with security tools could present a temporary roadblock. Typically, literacy courses use lab environments where students have no administrative rights. Using security tools requires them to install, test and evaluate those tools as consumers. Is there a possibility that we have lab space that is idle for a few hours a week due to our recent low enrollments? Using removable hard drives in a computer lab enables each user to boot up and maintain a personal configuration. If your curriculum includes a network security class, chances are you have such a lab on campus. Finding some

funds for a few more removable hard drives may be needed, but that is a small expense. On my first presentation of the security literacy component, I was fortunate to have each student at a personal workstation, with a removable hard drive.

4.2 Major Lecture and Laboratory Topics

In order to accomplish some depth of security literacy in ten to fifteen hours of class and lab time, students are expected to perform outside readings and actively contribute to the lab practices. Books on reserve in the library, handouts, or an additional relatively inexpensive text could provide the necessary background reading. In my first attempt at presenting security literacy, I asked students to purchase a non-textbook by Greene [8]. Since such trade books will be readily available to non-tech users throughout their non-technical careers, following the text recommendations in lab, as well as questioning and criticizing them, supplies a positive model for continued literacy. The context for each laboratory activity is provided by a recent article from the news about a security breach that has impact on everyday users.

Lecture topics are dependent on student project topics. The first class meeting of this course component, while installing Windows on the workstations, the topic list is presented for students to peruse. Each student must select one topic. Two students can form a team if the class is large. The projects are informal. The goal is to have students research and then edit what they find. They can copy and paste from websites, journals, and vendor documents or ask professionals at work for their opinions. Whatever they collect, they edit and analyze. When they bring the information to class, it must be in electronic form to copy to the lab server. A Windows 2003 Server houses the student accounts and a shared writeable folder for them to upload project information. The server is not accessible outside of class, but it does provide an internet connection during class. The entire class participates in discussing the topic of the day; everyone installs one of the recommended tools to try it out. Not all tools have a trial version, but there is typically at least one trial version of every type of end user security tool with which to experiment.

After each student has installed windows on the assigned workstation, students configure Windows XP security options by systematically following the chapter in Greene entitled "From Newbie to Power User" [8].

Greene [8] influenced major lecture topics as well. Other books that were on reserve in the library were Whitman and Mattord [16] and Cobb [6]. Major topics researched by students:

- On-line Tools to Enhance Security
- Defeating Viruses
- Using a firewall
- Defeating Spyware
- Email Insecurity
- Protecting Sensitive Data
    - Social Engineering
    - Data Hygiene
    - Backups
    - Phishing

4.3 Project Topic Assignments

Project assignments correspond to the lab activity of the day. After secure Windows installation, topics 1 through 6 became the focus of lecture and lab activities. Social engineering is not a standard laboratory style topic, but it is extremely destructive to computer security. Since social engineering can undermine all the tools and best practices that we can teach and employ, it is vital to research and discuss it in detail [4]. At a minimum, class dialogue can alarm students into awareness of potential liabilities for them [12].

1. A website with tools to test your Operating System security: www.grc.com
    a. Review the free tools at grc.com and pick the best tools for a home workstation.
    b. Write up for each tool that you determine is worth installing:
        1) What it does
        2) Why we need it?
        3) How will it influence our system's performance?
        4) How much maintenance does it require?
2. What are firewalls?
    a. Software Firewalls
        1) What are they?
        2) How do they work?
        3) What types are there?
        4) What vulnerabilities do they minimize?
        5) Find a website with a free or trial download of a firewall for us to install in class.
3. What are viruses?
    a. Find at least three AV software vendor sites, and find out what is new in virus protection from them. Summarize your findings for the class.
        1) Symantec
        2) McAfee
        3) Kaspersky
        4) Panda
    b. For each of three vendors, In addition, answer these questions for the vendor:
        1) list its recommendations for maintaining your computer as virus free as possible
        2) How will the AV software influence our system's performance?
        3) How much maintenance by the user does it require?
            a) Time
            b) Licensing rules, expense
        4) What are the unique features
    c. Pick one product that offers a trial version and demonstrate how to install and configure it for the class
4. Email Security (or insecurity)
    a. How do you secure your email client?
    b. Select an email client, and demonstrate how to secure it.
    c. Discuss email traces. How do you eliminate these?
    d. Check out zmail features, and compare your chosen client to zmail. https://zsentry.com/email_security.htm
        1) Is zmail better? What features does it have that your client does not have, if any?
        2) Is it worth switching?

5. Spyware
    a. What is it?
    b. Why is it undesirable?
    c. Find three Anti-Spyware tools and evaluate them. You will find reviews at places like download.com, pcworld.com
    d. Pick one product that offers a trial version and demonstrate how to install and configure it for the class.
6. Protecting sensitive data
    a. Backups
        1) We know these are important, but how can we make it easy to back up data?
        2) Find/suggest/try some procedures to back up sensitive data
    b. Encryption
        1) Can you encrypt files/folders?
        2) Is it practical?
        3) How does an average user encrypt files?
    c. Social Engineering
        1) What is it?
        2) How prevalent is it?
        3) How much damage has it caused?
        4) How do you prevent it?
    d. Phishing
        1) Define and find examples
        2) Anti-phishing resources

4.4 Grading

Students evaluate each other's projects and grade themselves. As shown in Table 1, the evaluator awards a maximum of five points for each of seven qualities, for a possible thirty-five point total.

There is one open resource test at the end of the security literacy course component in which students evaluate insecure scenarios and discuss what they would do. Grades on this component of the course are higher than what IT majors would probably attain, but the goal is to have the students come away with a lot of useable information, and awareness of their role in securing computer systems at home and at work.

Table 1

Criteria	Rating
Thoroughness of comments: Are the comments superficial or do they demonstrate deeper processing? Are there applications or relationships to other materials?	
Completeness: Have all the important points been discussed?	
Understanding: Does the discussion and write-up show depth of understanding?	
Personal Connections: Is the information connected to personal observations, such as brought out in an article or white paper?	
Growth: Is there evidence that your understanding has increased because of the project?	
Inquiry: Have you thought of other questions to investigate because of the project?	
General Quality	
Total (35)	

5. Conclusion

The IT field has been in decline for several years, with our graduates struggling to compete with experienced IT workers laid off in the .com bust. Happily, the demand for IT and CS graduates has improved producing an IT worker shortage because the numbers of CS and IT majors plummeted as much as 60% in the last five years [11]. The optimism probably will not bring us more students immediately. In the meantime, we can use our facilities and our skills to make a positive contribution to Information Technology by reviewing the content of our computer literacy courses, and ensuring that the graduates of our institutions are prepared for the third wave in ubiquitous computing.

6. References

[1] Acohido, Byron, and Jon Swartz. Are Hackers Using Your PC to Spam and Steal? In *USA Today,* 8 Sept. 2004. *Available* <http://www.usatoday.com/tech/news/computersecurity/2004-09-08-zombieuser_x.htm>.

[2] Acohido, Byron, and Jon Swartz. Home PCs Not As Protected As Owners Think. In *USA Today,* 25 Oct. 2004. *Available* <http://www.usatoday.com/tech/news/2004-10-25-internet-security_x.htm>.

[3] America Online. Available <http://www.aol.com/optimized/safetyandsecurity.adp>.

[4] Anti Phishing Working Group. *APWG Phishing Activity Trends Report*, 28 Mar. 2005. Available <http://antiphishing.org/APWG_Phishin_Activity_Report_Feb05.pdf>.

[5] Armstrong, Illena. It's Not Just Home Users Who Are To Blame. *SC Magazine,* June 21, 2005. Available http://www.scmagazine.com/features/index.cfm?fuseaction=FeatureDetails&newsUID=fc2a83f9-69ae-4343-bc58-5227c9fab5eb&newsType=Features

[6] Cobb, Chey. Network Security for Dummies. Wiley, New York, 2003.

[7] Dourish, Paul, et al. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem, *Personal and Ubiquitous Computing* 8 (Sept. 2004), 391-401.

[8] Greene, Thomas C. Computer Security for the Home and Small Office. APress ,New York, NY. 2004.

[9] Guzdial, Mark and Andrea Forte. Design Process for a Non-majors Computing Course. In *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education. (SIGCSE '05)*(St. Louis, Missouri, February 23-27). ACM Press, New York, NY, 2005, 361-365.

[10] Computer Technology Industry Association. *Internet Security Threats Increasing in Maliciousness and Criminal Intent, Computing Technology Industry Association Study Reveals*. Available <http://www.comptia.org>. Path: Press Releases.

[11] Kan, Michael. IT Field Now Faces Worker Shortage. In *Richmond Times-Dispatch,* 27 June 2005. Available <http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1031783515110&path=%21business&s=1045855934855>.

[12] Orgill, Gregory L., et al. The Urgency for Effective User-privacy Education to Counter Social Engineering Attacks on Secure Computer Systems. In *Proceedings of the 5th Conference on Information Technology Education*. (Conference on Information Technology Education) (Salt Lake City, Utah, 2004). ACM, New York, NY, 2004, 177-181.

[13] Perez, Juan Carlos. Gartner: Security concerns to stunt e-commerce growth. In *Computerworld,* 24 June 2005. Available http://www.computerworld.com>. Path: QuickLink# 55252.

[14] Sullivan, Andy. Hackers Score Big by Thinking Small, Experts Say. In *Computerworld*, 21 June 2005. Available <http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,102654,00.html>.

[15] Weinstein, Andrew, and Susan Engley. Largest In-Home Study of Home Computer Users Shows Major Online Threats, Perception Gap. National Cyber Security Alliance. 25 Oct. 2005. Available <http://www.staysafeonline.info>.

[16] Whitman, Michael E., and Herbert J. Mattord, Principles of Information Security, Thomson Course Technology. Boston, Massachusetts, 2003.