Reclaiming "Old" Literacies in the New Literacy Information Age: The Functional Literacies of the Mediated Workstation

Ryan Shepherd and Peter Goggin

For many writing faculty, electronic or digital literacies may not play an overtly significant role in their course designs and teaching practices, but these literacies still play a significant role in how students write. Whether or not writing teachers want to accept it, functional computer literacies are an important aspect of teaching writing. In order to test how well acquainted writing instructors were with these literacies, two informal surveys were conducted on writing instructors knowledge of computer peripherals and security. These surveys found that writing instructors may need to reconsider the role of functional literacies in their classrooms.

As Peter Vandenberg notes, the evolving definition of *literacy* is always accompanied by a deep-seated belief in its ameliorative guarantee. "We tend to see a less benevolent disciplinary face only in the rearview mirror" (547). Perhaps no aspect of Writing Studies illustrates this idea more than education in digital literacies. As newer and "better" technologies come along, they enhance brave new possibilities for teaching, learning, and theorizing the study of writing. Not surprisingly, scholars quickly turn their attention to these new technologies and the potential they promise. After all, academia rewards innovation, and scholarly publishers are always on the lookout for the newest creative finding for literacy research and teaching. But the emphasis on technological innovation which has so powerfully influenced the study of digital literacy has accelerated the decline in the perceived disciplinary significance of technologies and literacies that are not on the "cutting edge" of innovation. The result is that older, still vital, technologies and their related still-existing issues that generated so much scholarly investment not so long ago are no longer viable in contemporary discourses other than as remnants of a previous era. At the same time, the shift to the innovative runs the risk of Writing Studies losing sight of the very aspects of those older discussions of digital literacies that have given shape to newer discussions. As David Kaufer and Kathleen Carley have pointed out:

> There is an unfortunate "futurist" bias that impels many to assume qualitative differences between older and newer communication technologies before exploring whether their differences might lie on common quantitative continua. The result of this tendency is to think of new technologies

> as a rupture from the past and to cluster the technology immediately superseded closer to the technologies it itself superseded. (17)

For many writing faculty who teach in traditional classrooms, electronic or digital literacies may not play an overtly significant role in their course designs and teaching practices, but these literacies still play a significant role in how students write. All writing faculty, even those in unmediated classrooms, are assumed to have (and care about) the functional skills that enable them to sustain their computing systems, administer their courses, and communicate with students via their office (and home) computer workstation. As Ilana Snyder points out, "preparing the current generation of students to become literate is difficult, not only because it is uncertain what the literacies of the future will be, but because the task falls to educators who are not fully literate themselves in the use of these new technologies" (3-4).

Whether we view the proliferation of system security peripherals (such as virus protection programs, product and system updates, backup systems, and firewalls) as undesirable background clutter or desirable computer-mediated composition (CMC) technologies, the demands for increased knowledge and use of these peripherals adds to the already complex multiple literate, pedagogical, and administrative practices that comprise writing instruction. These functional literacies are significant elements in the ecology of technological literacy that Cynthia Selfe (*Technology*) exhorts us to pay attention to but, as Staurt Selber notes, have, for the most part, been left out of our conversations on new information literacies.

In recent years, much scholarship has been written in the field of computers and writing on the subject of technological literacy. The idea of "technical literacy" in writing as the basic abilities to operate keyboards, computer systems, and various hardware and software applications has morphed into the idea of a more critically reflexive "information literacy" that strives to account for the multiple dynamics of social/ideological contexts that are overtly and tacitly embedded in the technologies that shape and mediate every facet of written communication. Notable scholars such as Faigley, Selfe and Hawisher, LeBlanc, Wysocki and Johnson-Eilola, and Sullivan and Porter, to name a few, have helped to promote reflexive questioning about what it means to be digitally literate.

The technologies and scholarly investment in digital literacies associated with bulletin boards, Web site design, HTML, online writing labs, and even e-mail have, for the most part, been superseded by wikis, blogs, texting, gaming, and social networking sites. But even those earlier technologies superseded scholarly prior interest in word processing, hypertext, and electronic textbooks. To oversimplify for the sake of perspective, Writing Studies as a field has generally shifted from emphasis in the functional/how-to literacies to an emphasis in social and critical literacies. But in the ecology of writing and Writing Studies, the functional is still there. This goes right down to the mechanical how-to knowledge, the basic nuts and bolts of

digital communication, from the act of tapping on a QWERTY keyboard and clicking a mouse to running virus protection and other security protocols. This essay makes the case that we need to reclaim some of the interest in the essential basic functional literacies of the digital media we use, not necessarily for instructive purposes, but rather as consumers and managers of those technologies. For this we focus on just one basic key function—system security peripherals—to make the argument for why Writing Studies needs to include a literacy of mundane functionality to re-establish an important element in our discussions of digital literacies.

Crisis to Commonplace

A little over a decade ago the nation faced a "technological literacy crisis," as it was termed by the Clinton administration, when the heady rush to mediate America's classrooms and thrust college writing into the digital age gave widespread credence to the already well-established scholarship, research, and teaching of writing and digital technologies. This "crisis" also signaled an end to the days of the techie gurus in writing programs—the few who understood, or at least enjoyed dabbling in, the mechanics of hardware, software, and the rapidly evolving technologies and interfaces of the Internet. Their emphasis was very much on "how to" approaches that emphasized functionalist literacies, that is, the mechanics of text production through the new media, or personal growth literacies that validated traditional approaches to writing education via the new technologies that validated them (see Goggin). Now, just about anyone who teaches in higher education in the U.S. has come to use computer technology for a variety of teaching, administrative, and research purposes. With this now widespread and commonplace dependence on digital technologies has also come the sort of general disciplinary disconnect from digital writing instruction that was already being attributed to traditional writing instruction (see Connors; Graff; Vandenberg).

CMC scholarship and pedagogy asks us and our students to critically examine the sociopolitical agendas that are embedded in writing technologies and to consider the multiplicities of cultural perspectives and contexts. But as digital writing studies has moved further into the realm of social criticism, it has also divorced itself from the emphasis on functional technical skills that so marked its early years. Sheridan-Rabideau, McLaughlin, and Novak studied some of the resulting confusion that such a departure has caused. They note that in university writing courses, instructors typically teach students from a range of disciplinary backgrounds. The disciplinary values, methods, and expectations that students bring into the writing class become evident in Web authoring courses as the students and their instructors struggle with competing ideologies, definitions, and assumptions of what it means to be technologically literate (348-9). For many instructors, the growing preference for social/ideological theories of literacy, and post-process theories of composition have redefined what we mean when we speak about literacy.

Technological literacy as an ideological model of critical/social theory, it seems, cannot readily coexist with what are now understood as autonomous literacy approaches (see Street, *Literacy in Theory and Practice*; Street, *Social Literacies*) that view computer-based literacy merely as a set of mechanically acquired skills. This is understandable. As Selber notes:

> Functional literacy has been reduced to a simple nuts-and-bolts matter, to a fairly basic skill based on mastery of technique […] This view understands functional literacy in much the same manner that current-traditional rhetoric understood written texts: not as socially or rhetorically embedded but as expressions of grammar, style, and form, all of which could be learned in prescriptive and decontextualized ways. (32)

Functional literacy skills have, for many teachers, become an invisible part of the writing process.

The tendency has been to ignore the important aspects of necessary functional knowledge and awareness of the increasing options in writing for digital technologies. Function itself has come to be recast as a mere afterthought (if thought of at all) of the more scholarly relevant subject of a social/critical technological literacy model. Selber argues that students need to be exposed to multiple ways of conceiving literacy, both functional and critical literacies as well as other types of literacies like rhetorical and visual literacies involved in Web site design and production (35). Selber, however, does not propose that we approach functional literacy from a functionalist perspective. He is not suggesting that we return to a narrow focus on text production, grammar drills, or spelling and punctuation exercises. Rather, he is arguing for a postcritical stance, that is, a contextual reckoning through which we view functional literacy in computer-based writing as an integral and necessary aspect of the broader social problems and concerns that are addressed as technological literacy.

From such a postcritical perspective, we would further argue that we not only pay attention to functional literacy for the sake of our students, but that we also need to recognize that our own functional literacies in the technologies we use for teaching, for instance, system and workstation security, are integral and necessary aspects of the work we do. With few exceptions[1] we have paid little attention to the impact that system peripherals and institutional expectations for technological know-how have on our own day-to-day communication and teaching practices. Composition's role in transdisciplinary discourse on technological innovation and design futures in the academy is that of passive recipient unless we can demonstrate functional/mechanical know-how to accompany our theoretical arguments.

Because the field of Composition seems reticent when it comes to acquiring the literacies of what Gunther Kress terms the New Media Age, the field risks squandering the gains in scholarly and pedagogical value it has made in the academy as what we do with technology becomes merely the new "business as usual." One symptom of this has been the pendulum

swinging too far away from emphasis on the "how to" aspects of writing with technologies. Understandably, in view of the general shift in recent years to critical and social theories of literacy, there is a general tendency to ignore the ecological role of functional literacies associated with the day-to-day technologies that inform the study and teaching of written communication.

In its narrowest sense, literacy may be seen merely as the basic ability to read and write certain forms of scripted text. This view stands in contrast to other ideological constructs of literacy such as those based on activism, criticism, personal growth, or cultural gatekeeping. Yet the key common feature across literacy ideologies is that literacy always involves making and doing and, therefore, requires some degree of functional knowledge and ability within the making and doing.[2] Selber argues that rather than the sort of functional approaches to writing instruction often equated basic skills learning and teaching methods fostered by current-traditional rhetoric, "functional literacy need not be disempowering and that functional and critical literacies need not be mutually exclusive" (497-98).

For writing instruction professionals, as basic educational computing has become increasingly mainstream, non-techie friendly, and highly automated, the technologies and the infrastructures that sponsor them have become increasingly commonplace and rhetorically invisible. Just as Selfe and Hilligoss predicted more than a decade ago:

> It is possible to imagine that computers (or some related word like hypermedia) may become a linguistically "unmarked" term for devices of reading and writing, even for text, as paper, pen, and type have been.…What we have here named as knowledge will evaporate into the tacit practices of any number of fields, with both losses and gains for us and, more important, for those who come after us. (340)

An example of the crucial day-to-day technologies that we pay little attention to are computer security peripherals. System security hardware and software have become increasingly necessary for supporting digital writing practices for students and instructors alike. In terms of access and success, these technologies have become increasingly, and some might say insidiously, invisible gatekeepers of technology-based writing instruction and new-media composing. They serve as barriers, only visible on breakdown, for students and instructors who do not fully understand how they function. So, why haven't we paid more attention to them? Research and teaching in composition is already demanding enough. Do we now have to be the technicians also? Well, if we want to be players in the transdisciplinary conversations that are shaping the directions of higher education, then yes. And we need to focus with some awareness of the infrastructural frameworks that we operate in and how those infrastructures both shape and are informed by the basic functions of our own workspaces and the systems we depend on (DeVoss, Cushman, and Grabill 16). Even for writing instructors who already have, or wish to, move into the realm of new-media

composing that has students reinvent the possibilities for writing (such as video editing, podcasting, and other forms of multimedia presentations), functional technological literacy is a crucial element for inclusion in institutional design. DeVoss, Cushman, and Grabill state:

> To understand the contexts that make possible and limit, shape and constrain, and facilitate and prevent new-media composing, new-media teachers and students need to be able to account for the complex interrelationships of material, technical, discursive, institutional, and cultural systems....Our claim is that in order to teach and understand new media composing, some understanding of new-media infrastructure is necessary. Without such an understanding, writing teachers and students will fail to anticipate and actively participate in the emergence of such infrastructures, thereby limiting—rhetorically, technically, and institutionally—what is possible for our students to write and learn. (37)

DeVoss, Cushman, and Grabill contend that without a means to recognize, comprehend, and account for the infrastructural contexts of new-media composing, students (and instructors) can never fully come to grips—both critically and functionally—with the social, political, cultural, and material aspects of technological literacies that composition has the potential to explore.

This essay takes DeVoss, Cushman, and Grabill's argument for an infrastructural framework in Composition Studies to a micro level by looking at one aspect of the composition instructor's mediated environment—workspace system security. It is one aspect of the day-to-day "clutter" that is integral to the institutional/pedagogical infrastructure, yet seemingly invisible—until the system is compromised. It is our contention that implementing a successful infrastructural framework for mediated composition studies will require greater disciplinary appreciation for the value of such mechanical micro-knowledge of the "mundane" systems that inform every aspect of the teaching we do. An assessment of such current functional micro-knowledge literacy practices suggests that we may have some ways to go.

A case-study survey and a short online follow-up survey (described here in the following pages) were conducted on awareness of computer security peripherals by writing program faculty at a large state university. These surveys illustrate just how far outside of the loop we already are when it comes to mechanical know-how of the very technologies that inform our teaching and scholarship. The purpose here is not to offer yet another account of "problems" that composition instructors have with technology. Mediated composition for the most part is pretty old hat now. Technical skills and pedagogical applications and outcomes are accessible and simple to acquire for anyone who wants to and has the support (and/or mandate) from their institution. Rather, this essay underscores Selber's view that theoretical awareness on its own in Composition Studies is no longer sufficient. Mechanical awareness, if not expertise, about the most basic computer

functions is also crucial to awareness of the social and cultural impacts of the shift in meaning making from page to screen. Technological literacy in all aspects of electronic discourse will determine our discipline's ability to reinvent writing in the New Media Age and ensure that we are active participants in a multimodal future.

"Protect your chicken from Dokken"

This slogan is one in a series of ads produced by Norton Internet Security. Other slogans include "Protect your caterpillar from Kimbo Slice," "Protect your unicorn from Dolph Lundgren," and "Protect your oscillating fan from David Hasselhoff." While these ads present the information in a rather absurd and humorous way, the commercials effectively communicate that your computer is weak and vulnerable, and viruses and other malware are strong and dangerous. These ads feed into the public's growing concern for online security, as do other ads by companies such as K7 TotalSecurity, Trend Micro, and McAfee. All of these companies are effectively communicating the same message: you are vulnerable to attack, our company can protect you, update now. The ads are stating that you are already in danger: your finances, your credit, your records, and even your very identity may be compromised, hacked into, stolen, or destroyed. If it hasn't happened to you already, it's only a matter of time until it does.

Scare tactics to sell product aside, computer system security is clearly an important issue as more and more institutions and individuals go digital. A 2004 cover report on security products in *Consumer Reports* titled "Protect yourself online," warns, "Shielding your computer from online hazards is no longer an option. It's a necessity. What were once annoyances—viruses and spam—have become major concerns" (12). Just a year later, *Consumer Reports* issued a second exclusive feature rating security products, this time titled "Net Threat Rising," stating, "Use the Internet at home and you have a 1-in-3 chance of suffering computer damage, financial loss, or both because of a computer virus or spyware that sneaks onto your computer" (12). Recent events with online hackers such as the collective known as Anonymous or the group Lulzsec have shown that even groups such as Fox News, Public Broadcasting, Bank of America, and even governmental agencies are not safe. Anonymous and Lulzsec have exploited gaps in the Internet security of these groups to embarrass them and bring attention to these vulnerabilities. Their lax security has resulted in serious leaks, such as company emails and other documents and private information about individuals within these groups.[3]

This is not to say that it is only people in these high-profile positions that need to be aware of internet security and the functions of their computers. System and online security may be the most pervasive yet least visible aspects of mediated writing instruction. Advertised security and virus protection services and *Consumer Reports* cover stories are strong indicators that personal system security has become a mainstream issue as more and more of the public rely on online services and are potential victims of

phishing, pharming, spying, spamming, adware, and so forth. Of course, personal workstation/system security is something most writing scholars and teachers have long had to cope with, particularly as more and more of our academic institutions require online and networked correspondence. As education professionals, the separation of workplace between home and office is blurred, perhaps more than most professions. Cross-contamination between workplace and home systems, corrupted student files, and increased visibility via institutional Web sites increase the potential for risk for security problems. Further, even in the "official" workplace, proficiency in installing, operating, and maintaining the hardware and software peripherals that are necessary for security at the user end of academic information technology systems is often the responsibility of faculty, even for systems that are owned, managed, and serviced by the institution. At the same time, we suspect it is unlikely in many academic institutions that non-technical faculty are actually consulted in the computing infrastructure policies and designs that office workstations are dependent on. Selber suggests that, "If universities are not quick to consult humanists on technical issues, then teachers of writing and communication must look for ways to enter the conversations that shape technical infrastructures on their campuses" (195).

Selber is quite right about the need for faculty to be aware and involved of computing technologies as they concern institutional policy, but for day-to-day routine instructional and administrative purposes functioning, the divide between computing specialist and writing faculty may already be too great. Selfe even goes so far as to say that "technology is either boring or frightening to most humanists" ("Technology and Literacy" 1164), and Chris Anson, in an interview with Coley and Erickson, states that humanists often feel that learning about technology "take[s] time from their work." While some in Writing Studies may actually welcome opportunities to serve as system watchdogs for their institution and take the time to stay current with security updates, backup systems, spam filters, ad-buster software, and the like, we suspect they are relatively few. "Computer maintenance technician" is not posted in most writing instructor job descriptions, and it is fair to say that the majority of our profession would be uncomfortable (perhaps fearful) with the suggestion that they accept such a role. Our top academic journals value scholarly theoretical knowledge over practical, applied knowledge so there is little disciplinary incentive, in terms of promotion and tenure, to sacrifice commitment to the former to devote publishing effort to the latter.

An interesting thing about computer technology is the tacit assumption that faculty teaching on behalf of an academic institution will take on the functional skills necessary for protecting the security of the institution's data network. There is no other high-end technology for literacy education that requires such a commitment. Copiers, telephones, projectors, and all those other technologies that are essential for teaching require minimal operating skills, and less responsibility for maintenance. Sure, instructors may handle minor maintenance problems like removing a feeder-tray paper jam

or changing a burned out projector bulb, but in terms of actual servicing, it's "hands-off instructors, bring in the mechanic." Yet, when it comes to computers, there is an assumed level of technical ability for instructors, not merely as users and work station administrators, but as front-line protectors against hackers, spammers, crackers, phreakers, cyberpunks and malware writers. Somehow, the "personal" in personal computing, even in institutional settings, implies that if the machine sits on your desk, it is nominally yours, but the photocopier in the workroom belongs to the department/university. So, why isn't this issue something we talk about more? While most writing instruction still takes place primarily in traditional classrooms the technologies on our office desks are no less pedagogically relevant for writing instruction than the technologies of the mediated classroom or the digital contexts of the Web.

Even DeVoss, Cushman, and Grabill while arguing for an infrastructural lens for composition instruction focus primarily on the student/classroom perspective on infrastructure. The instructor workspace setting receives only scant attention. Obviously workplace situations and conditions are determined by their local contexts, but personal and anecdotal experience suggests that most writing programs do not have *carte blanche* for all their technological needs and desires. Much of what determines workspace setups has less to do with individual instructors or program directors than with departmental administrators and the decision-making on macro and micro levels that go on behind the scenes. Budgetary concerns, office administration politics, personal and technological favoritism, seniority, unforeseen crises, upper administrative directives, to name a few are a constant fact of life in university departments. Multiple decisions, directly and indirectly, are made involving workspace technologies that are part of the infrastructural framework that is the underlying context for pedagogical practices. Yet these day-to-day workplace realities (and functional workplace literacies) are generally ignored in our literature because they are so localized and seemingly separate from the teaching part of what we do.

A Case of Basic Functional Know-How

We wanted to find out just how much time, effort, and responsibility writing instructors were putting into their office workstation security peripherals in order to ensure the technologies would support their teaching. The motive behind the two surveys was to see just how functionally tech-savvy full-time composition instructors were with basic workstation security. It seemed to us that if Selber's call for a postcritical stance on composing and DeVoss, Cushman, and Grabill's call for an activist approach to infrastructure are to be implemented in programmatic and individual levels in the new information literacy age, we need to see just where we stand to know where to begin. As system security is an underlying factor affecting all aspects of innovation, policy, and practice in institutional computing, an

assessment of basic functional awareness of end-users would illustrate how prepared composition professionals to effectively respond to those calls.

The initial informal survey (see Appendix 1) was a small-scale case-study survey conducted in 2008. This survey was conducted by Peter through face-to-face interviews in the subjects' offices. Each participant had a computer in the office issued by the university's English department. The survey began with a few general questions to establish frequency of use of computer technologies for teaching and then went on to ask specific questions relating to basic critical security functions such as scanning for update of the operating system, virus protection, and firewall. The next group of questions related to e-mail and Internet security settings, the use of backup systems, and estimates of overall time spent on securing and updating the computer workstation. The last questions related to technical assistance and any changes to course design or teaching practices mandated by institutional policies or changes affecting instructional software. For comparative purposes, in addition to questions about office computer security, Peter also asked the participants about their attention to security on their home computers.

The follow-up survey was conducted by Ryan anonymously online in 2011 (see Appendix 2). The purpose was to both update information and add additional insights toward our central claim. The survey followed a very similar pattern to the initial survey, starting with general questions about computer use and maintenance and then moving into more specific questions about operating system updates, virus protection, firewalls, and additional security measures.

Both surveys drew their participants from full-time instructors, lecturers, and professors teaching in the writing programs at a large state university. Twenty-eight instructors participated in the initial survey, and 18 participated in the follow up. Because the second survey was conducted anonymously, it is unclear how many of the respondents participated in both surveys. However, it is safe to assume that there is some overlap. All of the participants in both surveys had university-issued computers. The faculty taught a range of writing courses including general university requirements, first-year writing, upper-division writing, and a number of writing program electives at the undergraduate level.

For the initial survey, Peter interviewed each of the 28 instructors in their offices rather than having them respond to a questionnaire on their own. He found that for questions concerning awareness of individual computer workstation security settings, this approach helped to prevent the participants from checking their office machines and self-correcting. The result was a lot of ambiguous and inaccurate responses about system security from a group of writing instructors who are otherwise very proficient in operating computers, particularly for teaching purposes. Many of the participants apologized in advance for not knowing settings or attempted to check the accuracy of their responses during the interview despite assurances that the survey was not a test and that findings would be confidential. The unease many expressed

about lacking expertise and due care of their computer security peripherals suggest that on some level there is an expectation that they should be more technically savvy and devote more time to operational maintenance of their office machines—this despite the fact that they all already teach full time.

It is important to note this unease, inaccuracy, and ambiguity when reflecting upon answers given for the anonymous and more general second survey. There was no way to verify the answers that the respondents gave, as Peter was able to in the first survey, but the anonymity provided by the second survey does offer some protection and ease that the initial survey did not.

Almost all of the instructors who participated in the initial survey reported a high use of multiple computer functions for teaching, including word-processing, e-mail, online instruction, discussion boards, document preparation, Web site development, file transfer, electronic editing, assessment, and so forth. Most of the full-time instructors at the university who teach for the writing program teach in computer labs, teach online, or teach hybrid courses for at least part of their workload. Only 2 of the 28 instructors said they did not teach any designated CMC courses and used their computers mostly for e-mail and document preparation. All of the instructors said they used computers daily for teaching functions.

In both surveys, all of the security and privacy settings about which we asked the instructors were, from our perspective, fairly basic. They included such subjects as virus scans, firewalls, browser security, and back-up systems. When we say that the settings were "fairly basic" we realize that the term is relative. We are not talking about the sort of system management that requires specialized technical knowledge, but basic, low-tech user awareness of the off/on switches and settings for essential security applications. To use an automotive analogy, it is the equivalent of checking the tire pressure; to put it in terms of cooking, it is the equivalent of following instructions for microwaving a prepared frozen dinner. Technical expertise with computers in the initial group Peter surveyed ranged from participants who saw their computers as little more than turbo-charged typewriters and expected to use them for teaching support with minimal user maintenance (to continue the automotive and cooking analogies think passive seatbelt restraints or pizza delivery), to instructors who built their own computers and spent a great deal of time keeping peripherals maintained and updated. Most, however, fell into a mid-range of writing professionals who were proficient in using their hardware and software in multiple ways for a variety teaching purposes and were at the very least aware of such things as virus scans, firewalls, and e-mail filters.

In the follow-up survey, the range was equally broad. Exactly 50% of respondents said that they had a "strong" or "good" sense of Internet security, with the other 50% saying they had "some," "a weak," or no sense of Internet security. Only 33% of respondents said that they were in charge of the security on their university-issued computer, despite 50% admitting that they were the ones who should be responsible for this. This is an even more

surprising finding when considering the fact that 83.3% of instructors stated that Internet security was "a subject about which English/writing instructors should be knowledgeable" and not a single respondent responded that they should not be knowledgeable in this subject (the remaining 16.7% stated they were unsure). This finding reiterates Peter's previous finding: the instructors felt a sense that this was a subject about which they should know, but they were not entirely comfortable with their current knowledge on the subject.

All of the instructors that Peter met with face to face had self-purchased computers at home which they used extensively for teaching purposes. Almost all of the home computers were PCs. Only two instructors had purchased Macintosh computers for their home use. Both of these instructors stated that they understood PCs were more vulnerable to virus attacks and had purchased Macs primarily because of security concerns for their personal investments in their home computer systems. A number of the instructors, even those with university-issued wireless laptops, mentioned that they used their own home computers more than the office computers. This was especially the case for instructors who taught online or hybrid courses. Overall, the instructors spent far more time maintaining their home systems and were far more aware of security needs and settings on their home computers than on their office computers. Results of the second survey reflected this: 72.2% of the instructors stated that they were in charge of the security for their home computers or personal laptops, while only 33.3% stated that they were in charge of the security on their university-issued computers.

Fourteen of the participants in the initial survey said that they ran a firewall application on their home computers, while only 4 said they ran a firewall on their office computer, and when Peter checked actual settings on office computers, one instructor unknowingly had the firewall turned off. Eighteen instructors said they did not know if they were running a firewall on their office computer. Out of those, 10 actually were but did not know it. This carried over into the second survey where 27.8% of respondents were also unsure of whether or not they were running a firewall.

Only 6 participants said they ran spyware and adware blockers on their office computer (only 2 actually did), while 14 said they ran blockers on their home computer. Peter was able to assume that this information was accurate because they were able to identify the software application they ran at home. In most cases they cited Spybot and/or AdAware. In the follow-up survey, 83.3% said that they ran pop-up blockers, 33.3% said that they ran adware blockers, and only 22.2% said that they ran script blockers. Pop-ups seemed to be a greater concern than more pressing Internet security issues. Only 2 of the 18 respondents to the second survey could name additional software that they had outside of those mentioned above to protect their computers.

Only 1 participant in the initial survey had a full backup system for the office computer, while 7 said they had one at home. (2 participants thought the office system was automatically backed up by the department—it isn't). This response differed greatly in the online survey where 75% of respondents

said that they backed up files onto an external USB drive and an additional 8.3% of respondents said that they backed up files onto a Web-based hosting service.

On the whole, office systems did not fare well in terms of user awareness and maintenance. Seventeen of the participants in the initial survey were running Microsoft XP as their operating system, 3 had Windows 2000, and 5 had Windows 98. Because the XP operating system provides many automated features with Service Pack 2 that had been set up by computing administrators before issuing them to instructors, many of the office computers were set to automatically scan and install critical security updates. Those with older operating systems were less likely to manually access Windows Update and run a scan (only 11.1% of respondents in the second survey ran manual system updates; this is likely due to a larger prevalence of automatic system updates in newer operating systems, but it is unclear whether or not users were actually taking advantage of the automatic updates).

Non-automated tasks further highlighted the discrepancy. While all the office computers ran virus protection at start up, 19 subjects in the initial survey said they had never run a full virus scan of the hard drive and 31.3% of the subjects in the second survey were unsure when the last anti-virus scan took place. When it came to virus protection updates, 7 of the participants in the initial survey did not know if their virus protection was updated, while 9 said they never updated their virus protection. It turned out that 8 of the "nevers" and "don't knows" were automatically updated. The interesting thing about this was that while the participants were more attentive to security needs on their home computers, actual virus infections were pretty much equal at both home and office. Thirteen instructors said their office computers had been infected at some point, and 14 experienced this on their home computer. These similar numbers may suggest that ownership still might not result in better maintenance. A number described infections serious enough to slow down or crash their systems requiring hard drive reformatting, and in at least two cases causing irreparable damage. One participant described a relatively "benign" virus that infected his workplace computer though an e-mail attachment. A soft drink manufacturer logo would pop up, along with music, and the CD drawer would open. "The virus also attached itself to most of my computer's sub-directories. I called tech support, and they came over and cleaned it out. But by then I had already sent it out to a whole lot of other people on a national listserv. Whoops!"

Only 2 out of all the instructors in the initial survey were aware of what their Internet security and privacy settings were on their office computer. This number was far higher in the second survey (only 16.7% stated that they were unsure of their settings), but follow-up questions revealed that as high as 50% of the respondents were unsure of settings for running scripts, blocking ads, and real-time spyware/virus scanning.

Another discrepancy turned up in the amount of time participants spent on peripheral matters. When participants were asked how many unsolicited

(i.e., spam) messages they received on a daily basis, results averaged at around 33 messages per day in the initial survey and only about 4 per day in the second survey. When Peter asked participants in the initial survey if they had a spam filter installed, 16 said they did, 6 said they did not, and 6 didn't know. Out of the 16 who said they did filter spam, 7 did not actually have a spam filter set up. In the second survey, however, nearly everyone (93.8%) stated that they had a spam filter. This, most likely, reflects a change in e-mail providers between the first and second surveys.

When Peter asked the participants in the first survey how much time they spent with e-mail they felt was "a waste of their time," that is scanning, opening, reading, and deleting mail that they deemed irrelevant or unnecessary, the average came out to 98 minutes per week (but only 11 minutes per week in the second survey), while the amount of time they spent maintaining and securing their computer systems averaged 27 minutes per week (about 22 minutes in the second survey). Aside from the obvious difference in how this non-teaching time is prioritized, the grand total for peripheral time usage on a weekly basis for 28 instructors is 3403 minutes, almost 57 hours. That is an average of 2 hours a week per instructor—almost 2 full class sessions. This is not insignificant considering that the time spent maintaining security, both at home and in the office, is not recognized as work time, like grading and course preparation, even though it is necessary to ensure effective conditions for teaching. There is a tacit understanding that devoting such time to securing and maintaining the technologies for teaching is institutionally required and is just an unquestioned part of the job—merely the price one pays for the benefit of working with computers. As one survey participant suggested, the demands of computer technologies for educators was like going back to the days where the teacher of the one-room schoolhouse had to chop wood, mend furniture, and do many other chores simply to keep the schoolhouse in functioning condition in order to do their job.

On a related note, Peter also asked the participants if they had ever had to change or compromise their writing course design or teaching practices due to institutional policies or changes in instructional software or hardware. Eighteen in the initial survey responded that they did, and cited online discussion and teaching systems that get dropped in favor of another, security policies that require learning new Web editing programs, and desktop publishing and word-processing programs that get dropped. Three in the second survey also stated that they did, all 3 citing Blackboard constraints. Generally, instructors were not happy about having to give up practices they had become comfortable and proficient with and forced to learn new ones on their own time in order to do their jobs. They were particularly frustrated in having to discard lesson plans and projects they had spent a lot of time developing because they were incompatible with the new programs. One described having to restructure his dissertation in progress because of his university's new IT constraints, and another stated, "I don't want any more

mid-term surprises. I don't believe it when they say the system will run forever. We should have more input in tech support for the work we do."

Following the initial survey, Peter conducted an interview with the Humanities Computing Facility (HCF) Technology Support Analyst Coordinator who supervised technical support for a number of departments in the College of Arts and Sciences, including the English department. HCF maintains about 600 machines and works with about 500 faculty and teaching assistants. HCF for the college consists of two full-time staff and one part-time student worker. The coordinator explained that a big part of the problem with security issues was that with so many departments, programs, and individuals in the college, there was no accurate inventory on who was operating what machines. The HCF coordinator did report, however, that there was a good deal of ongoing discussion among university administrators and information technology specialists about security, and a number of ideas for future policies were being considered. One possibility was to require all university system subscribers to use complex passwords (combinations of upper and lower case letters, numbers, and punctuation) that would automatically expire after a certain time and require updating to continue access (this requirement has since been implemented). Another possibility being considered was to remove administrative permissions on personal workstations so that faculty and staff would only function as users. This would mean that any time someone wanted to download a program they would have to call HCF to approve and install the new software. Although highly restrictive, the effect would be to prevent backdoor intrusions. Although this seems rather drastic and likely unworkable given current technology support conditions, in theory it would effectively absolve individual instructors from the responsibility of securing their workstations. Whether this would actually be true in practice or not is debatable. The obvious impact would be on the sense of personal identity that instructors imbue their computers with and the teaching they do with those computers.

In the meantime, the HCF coordinator explained that the university considered users responsible for the security of their workstations, even though there is no unified security concept in place. He reckoned it would probably require 1 hour per person to train and explain security settings and maintenance—that's for 500 people just in humanities. He estimated that up to 50% of the work that HCF did was related to security prevention and cure. The coordinator's observation on the cause for the security problem was that when it comes to the functional side of computer technology in the university, people on all levels make decisions about computers and usage in a vacuum. "As people learn more about technology," he stated, "they implement it without being aware of the consequences." The coordinator's view of the future was that of more policies on computer use to be handed down to instructors that would require even more attention to peripherals and more user responsibility for maintaining security.

Paying Attention to Technology

A review of articles over the past decade in Writing Studies journals reveals little to no scholarly attention or interest in technologies related to computer security. If discussed at all, system security is only obliquely mentioned in the context of providing secure password-protected environments for students to write in, but for the most part the subject is neglected. In Garza and Hern's *Kairos* article on the use of wikis as tools for collaborative writing, the authors address the pedagogical potential for students to function differently in the "open environments" of wikis from the "closed environments" of other learning formats. They also acknowledge resulting institutional reaction and concern for student protection. The originally open wikis the authors present as examples of their collaborative venture are now password protected. However, there is no overt discussion in the article about just exactly what the concerns of their institution are and how these may have impacted on teaching practices. In the same *Kairos* issue, Hewett and Powers address principles and processes for training online writing instructors. While training methods, both functional and theoretical, are discussed in detail, the focus is on the pedagogical issues of instructor training. There is no discussion of instructors' work setting functions and the realities of the workstation administration and system security aspects of maintaining and sustaining online instruction. The sense one gets in reviewing the literature on mediated composition studies is that the mechanics of computing and computing systems, the security protocols, and support technologies are not worthy of intellectual consideration—that somehow these things are not relevant to pedagogy.

By comparison, Selber points to a computer competency test offered by the computer science department at Florida State University that has substantial components of its study guide devoted to important security issues including, "Computer Virus, Macro Virus, Worm, Denial of Service attacks, Antivirus Software, Virus Hoaxes" (16-17). This is not to suggest that every article in writing journals should include functional aspects of computer mediated education, or that writing instructors should necessarily take on the role of computing specialist. But the absence of any emphasis on protection and system security highlights that these very issues that are considered significant and basic elements of digital literacy are not recognized as significant elements, both for our students and ourselves. Requirements for security software and hardware both limit and necessarily validate continued use of computer-mediated writing studies, yet these functional elements of the workplace appear to have received little validation in the discipline.

While it is in the best interests of the individual academic institutions to provide security and backup peripheral services for all subscribers to its system, writing and technology scholars Charles Moran ("Emerging") and Mark Werner have pointed out that funding to support peripheral technologies and upgrades may come at the cost of additional faculty lines, internal grants,

student support services, and learning materials that are not compatible with the technologies. Further, because in-house tech support is often sparse or stretched to the limit, institutions often require that faculty themselves keep their workstations' security systems upgraded, often with little or no training. For example, at the large state university where we conducted our surveys on knowledge of workstation security, faculty and students were warned during a virus attack that they would be "kicked off" the university system if it was determined that their computers were infected or vulnerable to infection. The university's writing program offers around 400 sections per semester. Roughly 20% of those are designated CMC courses, although all of the instructors we surveyed utilized computer support. Shortly after the virus attack, new security protocols were put in place that required faculty to install new software and reconfigure access procedures to online accounts. In another move, WebBoard, an online discussion board subscribed to by the English department and used by many writing instructors teaching hybrid and online courses, was cancelled in favor of the university supported Blackboard system. Access to, and use of, the new discussion board is controlled not by individual programs or departments, but by the university's Information Technology office which disabled many of the "manager" options and features that had previously been available to instructors.

It would seem that Selber's call for a postcritical approach to computer literacy not only creates a space for bringing awareness and questions of technology and education design into the writing classroom, but can also be implemented for examining the multiliteracy (critical, functional, social, rhetorical) aspects of the workspace. It is the functional literacies that seem to get the least amount of attention. DeVoss, Cushman, and Grabill effectively illustrate this point in their account of a breakdown in security policies and technological needs between the institution and multimedia composition instruction on the subject of memory storage in mediated classroom workstations. The authors and their students bring an analysis of preexisting institutional policies and infrastructures to negotiate change and introduce a new structure for new-media composing. The authors' skill, experience, and technical know-how in mediated instruction and system management, along with their commitment to multimedia composition, provide a functional as well as scholarly/pedagogical basis from which to transform a rupture (their term) in institutional policies into a teachable opportunity for themselves and their students. But for most writing instructors who use computers for their teaching and administrative duties, technology needs (predominantly e-mail, word-processing, and Internet-based research) are relatively more discrete than those invested in new-media composing. However, the necessary peripherals for such needs are no less than those for more high-tech end users in other disciplines such as engineering, the sciences, and business. Increasingly, writing instructors (including full time, adjunct and teaching assistants), who are often among the lowest paid university faculty, are having to learn to be end-user technicians or lose their required

access "privileges," pay out of pocket for necessary home computer work stations, personal back-up systems and other peripherals, and redesign, reconstruct, or abandon teaching materials that are rendered obsolete by mandated university computing policies.

Conclusions

Evolving technological infrastructures and the challenges for composition professionals to play a role in determining the future of mediated education highlight the necessity for functional technological literacy. For instance, as this survey shows, with the increasing threats to system security, identity theft, and institutional expectations for end-user/employee technical skills, it seems likely that the technologies we use to teach writing will require even greater attention to the functional aspects of digital literacy than we already do. A postcritical perspective may provide the theoretical space in which Writing Studies may play a role in new information literacy designs, but at the same time, we should not privilege only the deeper philosophical questions at the expense of awareness and discussion of the basic functional knowledges and literacies. Despite the fact that most of us get along just fine with our workstation "black boxes" and are happy to let tech support and our lurking software agents keep the systems running, it is clear from the survey that in practical terms, many writing instructors who are already devoting a great deal of time to non-teaching related peripherals may lack sufficient knowledge and awareness about even basic security operations on their workstations. Perhaps this will come as no great surprise to those who read this essay, and therein lies the crux of the problem. The lack of know-how of basic computing maintenance in the survey results reveals a blind spot in the perspective that many writing professionals have in their relationship with technology: it appears as though many of those involved in the survey did not have a personal relationship with what have essentially become the tools of our trade, computers. The results of the survey should come as a shock—that so few of the participants were aware of and actively maintained their computer workstations while simultaneously considering maintenance a significant and necessary part of their jobs as Writing Studies professionals. But we suspect that this is the case for writing instructors in most institutions. Selfe states, "if teachers pay attention to technology and literacy problems on a local level, they can collectively work to construct a large vision of these issues on a professional level" (*Technology* 147). But this can only work if the problems are first recognized as problems. We first have to know that there are blind spots and then we can pay attention to them and come up with strategies to address them.

But the pragmatic question that still remains for many Writing Studies professionals is *how*? How do they find the time and motivation to do this? Computer technology provides wonderful opportunities for instructors to teach and for students to learn in exciting and innovative ways, but should

writing instructors have to devote substantial amounts of personal time and personal resources to maintain the systems that are essential to do their job? Should they have to assume increased personal responsibility for risks of security breaches in an institution that requires instructors to use computers for correspondence, administration, grade reporting, self-evaluations, and so forth, but does not provide adequate technical support? Most of the writing instructors we surveyed indicated that they felt they could be more functionally literate and vigilant when it came to security peripherals, but were concerned about the extra time this would take beyond the time they were already devoting to security and maintenance. They all recognized the importance and value of computer security, but there was no consensus on just how much they were responsible for the university's property. It is unlikely that problems such as these will be solved universally, but if, as Selfe suggests (above), specific problems can be tackled creatively on a local level (and we would add here that it is the responsibility of those already technologically savvy to lead the way in this), then we can claim more disciplinary space that includes functional literacy. For instance, in the very act of conducting an interview survey on workstation security, many of the participants came face to face with their own levels of awareness and proficiency of this functional aspect of their professional work. As a result, many of the participants not only acquired new knowledge of their security software and hardware peripherals and ways to maintain and update them, but expressed desire to learn more and to keep up with ongoing and future developments in system management. In this case, the key to recognizing and dealing with a technical blind spot was simply to talk to people and see firsthand what their actual awareness was. It is a good place to start.

Here's the thing. If, as writing professionals, we are to have a place at the table when it comes to infrastructural awareness and transdisciplinary discourse on new information and multimedia designs in teaching and scholarship, then we are responsible for making that space. We need to be proficient in the functional literacies that allow for critical analysis of the infrastructures that sponsor and implement institutional policies and electronic technologies. We need, as one survey participant observed, to be willing to reacquire the role of the teacher of the one-room school house. We need to be active participants in all the literacies of digital writing, from the functional knowledges of the material workspace (both office and classroom) to the institutional infrastructures that the workspaces are embedded in, to the disciplinary and transdisciplinary theories and questions that inform scholarly discourse in digital composition and new media studies. If we are going to work with computers, if these technologies enable us to reinvent writing and envision the myriad potentials that technological innovations can offer for practical, social, and critical pedagogies, then we need to know how and why they do what they do. In his review of the twentieth anniversary of the journal, *Computers and Composition*, Moran observes that scholarship on mediated writing studies has generally moved from emphasis on eliminating

the "drudgery" of writing, improving student writing, and improving the marginal status of writing instruction to a more recent emphasis on looking "less at and more through technology" (345). Perhaps the pendulum has swung too far away from the "looking at" of technology and writing. Perhaps it is time to apply the critical lens of looking through to reclaim a new emphasis on the functional aspects of mediated writing studies.

It is certainly a dilemma, and one, which more and more writing professionals and the field will be forced to face, whether they want to or not as computer peripherals become an increasingly overt aspect of writing instruction. Selfe's (*Technology*) call that we pay more attention to the social and political agendas that construct and drive the connections between technology and literacy is important and necessary. As Writing Studies professionals, we do need to make sure we are active participants in shaping what it means to be technologically literate. Likewise, Selber's call for a postcritical stance by writing instructors underscores the need for Composition Studies to have a voice and an investment in computer literacies and educational technology designs. Additionally, we also need to address the institutionally functional literacies and technical skills that are inherently and integrally bound to the technologies themselves and to question how those functions are relevant to social context. Functional knowledge of security peripherals and other system maintenance software and hardware is increasingly relevant for a field that relies so much on computer technologies for teaching and research. We need to bridge the disconnect between the privileged pedagogical literacies of the mediated classroom that warrant significant space in our scholarly journals, and the day-to-day, mostly invisible, functional literacies of our office workspaces. It is important and necessary that when it comes to digital literacies our scholarship also pays attention to the whole ecology of writing—and that includes the functional.

Appendix 1 – Initial Survey Questions

Name

Date

1. How do you use your office and/or home computer for any aspect of teaching writing, including e-mail, online instruction, document preparation, assessment, information retrieval, and so forth?

2. How often, per day/per week, do you use the computer for these functions?

3. Do you scan your office computer for critical updates? **Yes No**

If yes, how often?
How about your home computer?
Do you scan? **Yes No**

If yes, How often?

4. Do you have a virus protection application on your computer? **Yes No** *(If no, go to 4a)*
If yes, What kind/version?
Do you have it set to run on access (when you turn the computer on)? **Yes No**
How often do you run a full system scan?
How often do you update your virus protection?

4a. Have you ever had a computer virus on your office computer? **Yes No**
What kind?
What happened?
How did you solve the problem?
How do these questions apply to your home computer?

5. Do you have a firewall application on your computer? **Yes No**
If yes, what kind/version?
Do you have it set to run on access (i.e., when you turn the computer on)? **Yes No**
What level of protection/security are your firewall filters set at? **High Medium Low**
How often do you update your firewall software?
How do these questions apply to your home computer?

6. How often do you correspond with students or colleagues by e-mail?
Do you have a SPAM filter your e-mail? **Yes No**
About how many unsolicited e-mail messages do you get on a daily basis?
How often do you check the filter and delete suspected SPAM?
Have you ever opened a message that turned out to be SPAM? **Yes No**
About how often does this happen?
About how much time per day/per week do you spend on e-mail messages you consider to be a waste of your time? At the office? At home?

7. Do you access the Internet? **Yes No**
What are your Internet options for security and privacy set at? **High Medium Low**
Do you ever discover unwanted spyware on your computer? **Yes No**
If yes, what kind?
How often do you delete cookies, your temporary Internet files, your history folder?
How do these questions apply to your home computer?

8. Do you have backup system for your office computer? **Yes No**
Home computer? **Yes No**
If yes, what kind? How often do you back up your system at home or at work?

9. How much time overall, at the office, at home, do you spend securing and updating your system?
How often do you seek out technical assistance from humanities computing, information technology, instructional support? **Yes No**
If yes, how effective has technical assistance been from these sources? Please explain.

10. Have you ever had to compromise or change your writing course design or teaching practices due to institutional policies or institutional changes to instructional software?
Please explain.

Computer Checklist

Hardware
Operating System
Firewall Software
Security Level
Version/Update
Virus Protection
Software Version/Update
Last Scanned
Scheduled Scan
Spam Filter Version - On or Off
Spyware Filter Version/Update
Internet Settings
Browser
Security Level
Privacy Level
Pop Up Blocker
Backup System
Version Scheduled/Last run

Appendix 2 – Follow-Up Survey Questions

1. How do you feel about your knowledge of Internet security?
2. Do you feel that Internet security is a subject about which English/Writing instructors should be knowledgeable?
3. Primarily, who is in charge of Internet security on your home computer or personal laptop?
4. Primarily, who is in charge of Internet security on your office computer or university-issued laptop?
5. Who do you think holds the responsibility for the security of your office computer or university-issued laptop?
6. Is your office computer or university-issued laptop password protected?
7. Do you scan your office computer or university-issued laptop for critical operating system updates?
8. If you answered yes (either manually or automatically) to question number 7, how often are these scans performed?
9. Does your office computer or university-issued laptop have anti-virus software installed?
10. If you answered yes to question 9, who provided this software?
11. Please provide the type of anti-virus software installed on your office computer or university-issued laptop.
12. Approximately how often is this anti-virus software run?
13. Do you have a firewall on your computer?

14. Have you ever had a virus on your office computer or university-issued laptop?
15. If you answered yes to question 15, please explain the type of virus, what it did to your system, and how the issues were resolved to the best of your ability.
16. Do you regularly use wifi on your personal or university-issued laptop?
17. If so, do you adjust security settings when connecting to a public network?
18. Do you store sensitive student information (grades and/or personal information) on your office computer or university-issued laptop?
19. If you answered yes to question 18, what type of service do you use to do so?
20. Do you back up these files elsewhere?
21. Which Internet browser do you use on your office computer or university-issued laptop?
22. What are your browser security settings set to?
23. When using your browser on your office computer or university-issued laptop, do you use a pop-up blocker?
24. When using your browser on your office computer or university-issued laptop, do you use a script blocker (such as No-Script)?
25. When using your browser on your office computer or university-issued laptop, do you use an ad blocker (such as Adblock)?
26. When using your browser on your office computer or university-issued laptop, do you use a real-time virus scanner, often part of your virus protection suite?
27. When using your browser on your office computer or university-issued laptop, do you use a Web site advisor that lets you know if sites have been reported as dangerous (such as McAfee SiteAdvisor)?
28. Do you generally adjust the privacy settings on Web sites that contain your personal information (such a social networking sites, dating sites, or any other sites that contain a profile)?
29. Do you browse Facebook or other sites with your personal information in secure mode when given the option (https:// at the beginning of the address instead of simply http://)?
30. Do you use an e-mail system that filters spam messages?
31. On average, how many spam e-mails do you think that you receive per week that are not caught by your filter?
32. On average, how much time do you think you spend per week deleting or dealing with these spam e-mails?
33. How often do you open spam messages thinking that they are legitimate e-mail messages?
34. How often do legitimate e-mail messages accidentally get routed into your spam folder?
35. Have you ever accidentally downloaded a file attached to a spam message?
36. Have you ever accidentally opened a link in a spam message?
37. How often do you seek assistance for your office computer or university-issued laptop from humanities computing, information technology, or instructional support?
38. How effective has this assistance been?
39. How much total time per week do you spend securing and updating your office computer or university-issued laptop?

40. Have you ever had to compromise or change your writing course or teaching practices due to institutional policies or changes to instructional software? Please explain.
41. Have you ever had problems with a class you were teaching due to computer problems or computer security issues? Please explain.
42. Do you think that the security on your office computer or university-issued laptop is related to Internet security for your students? Please explain.

Notes

1. For instance, Moberly's article examining spam in the context of often conflated concepts of public speech and commercial speech offers an interesting perspective on filtering technologies for integrating functional and technological literacies into a teachable moment.
2. In *Professing Literacy in Composition Studies*, Goggin differentiates between functionalist literacy, "that views the acquisition of certain reading and writing skills as the way to learning and as the solution to learning 'problems,'" and functional literacy, "as a component of a multiliteracy view in which the acquisition of discrete learning skills can contribute to various forms of learning" (71-3).
3. Our own institution knows these breeches too well. On June 29, 2011, our university sent out a campus-wide e-mail reminding instructors of the importance of security in light of recent Lulzsec attacks. The e-mail stated, "The recent attacks on computer systems across the country, including here in [this state], by the LulzSec group highlights the need to take appropriate steps to safeguard our own systems from intrusion and theft of sensitive information," and went on to remind instructors that "each member of the faculty and staff have the responsibility to secure their own servers, desktop, and laptop machines" (Wishon). The online university login system was hacked less than 6 months later on January 18, 2012. Many users' passwords were downloaded, forcing every user on campus to reset his or her password. The extra traffic from this brought down the login system for several days. Classes that depended on online course materials were disrupted, and online instruction was effectively cut off until the system was restored some days later.

Works Cited

Anson, Chris. Interview by Toby Coley and Joe Erickson. "New Media and Multimodality in Compositions Students: An Interview with Chris Anson." *Computers and Composition Online*, 2009. Web. 14 Jun. 2011.

Connors, Robert J. "Crisis and Panacea in Composition Studies." *Composition in Context: Essays in Honor of Donald C. Stewart*. Ed. Ross Winterowd and Vincent Gillespie. Carbondale: Southern Illinois UP, 1994. 86-105. Print.

DeVoss, Danielle N., Ellen Cushman, and Jeffrey T. Grabill. "Infrastructure and Composing: The When of New-Media Writing." *CCC* 57.1 (2005): 14-44. Print.

Faigley, Lester. "Literacy After the Revolution." *CCC* 48.1 (1997): 30-43. Print.

Garza, Susan Loudermilk, and Tommy Hern. "Using Wikis as Collaborative Writing Tools: Something Wiki This Way Comes—or Not!" *Kairos* 10.1 (2005): n. pag. Web. 15 Dec. 2005.

Goggin, Peter N. *Professing Literacy in Composition Studies*. Cresskill: Hampton, 2008. Print.

Graff, Harvey J. *The Legacies of Literacy*. Bloomington: Indiana UP, 1987. Print.
Hewett, Beth L., and Christa Ehmann Powers. "How Do You Ground Your Training? Sharing the Principles and Processes of Preparing Educators for Online Editing Instruction." *Kairos* 10.1 (2005): n. pag. Web. 15 Dec. 2005.
Kaufer, David S., and Kathleen M. Carley. *Communication at a Distance: The Influence of Print on Sociocultural Organization and Change*. Hillsdale, NJ: Erlbaum, 1993. Print.
Kress, Gunther. *Literacy in the New Media Age*. London: Routledge, 2003. Print.
LeBlanc, Paul. "The Politics of Literacy and Technology in Secondary School Classrooms." *Literacy and Computers: The Complications of Teaching and Learning with* Technology. Ed. Cynthia L. Selfe and Susan Hilligoss. New York: MLA, 1994. 22-36. Print.
Moberly, Kevin. "Spam Wars: The Sooper Sekrit Rhetoric of Frea Speech." *Kairos* 9.2 (2005): n. pag. Web. 20 Apr. 2005.
Moran, Charles. "*Computers and Composition* 1983-2002: What We Have Hoped For." *Computers and Composition* 20.4 (2003): 343-58. Print.
- - -. "Emerging Technologies: Some Implications for Writing, Learning, and Teaching in the Disciplines." Conference on College Composition and Communication. Denver. March 2001. Presented paper.
"Net Threat Rising: Crime Abounds But You Can Fight Back." *Consumer Reports* 70 Sept. 2007: 12-18. Print.
"Protect Yourself Online." *Consumer Reports* 69 Sept. 2004: 12-19. Print.
Selber, Stuart A. *Multiliteracies for a Digital Age*. Carbondale: Southern Illinois UP, 2004. Print.
Selfe, Cynthia L. "Technology and Literacy: A Story about the Perils of Not Paying Attention." *The Norton Book of Composition Studies*. Ed. Susan Miller. New York: W. W. Norton, 2009. 1163-85. Print.
- - -. *Technology and Literacy in the Twenty-First Century: The Importance of Paying Attention*. Carbondale: Southern Illinois UP, 1999. Print.
Selfe, Cynthia L., and Gail E. Hawisher. *Literate Lives in the Information Age: Narratives of Literacy from the United States*. Mahwah: Lawrence Earlbaum, 2004. Print.
Selfe, Cynthia L., and Susan Hilligoss. *Literacy and Computers: The Complications of Teaching and Learning with Technology*. New York: MLA, 1994. Print.
Sheridan-Rabideau, Mary P., Rachel McLaughlin, and Jennifer Novak. "Contested Knowledge: Technological Literacies and the Power of Unacknowledged Disciplinary Investments." *Computers and Composition* 19.3 (2002): 347-59. Print.
Snyder, Ilana. *Silicon Literacies: Communication, Innovation and Education in the Electronic Age*. New York: Routledge, 2002. Print.
Street, Brian V. *Literacy in Theory and Practice*. Cambridge: Cambridge UP, 1984. Print.
- - -, ed. *Social Literacies: Critical Approaches to Literacy in Development, Ethnography, and Education*. London: Longman, 1995. Print.
Sullivan, Patricia, and James Porter. *Opening Spaces: Writing Technologies and Critical Research Practices*. Greenwich: Ablex, 1997. Print.
Vandenberg, Peter. "Taming Multiculturalism: The Will to Literacy in Composition Studies." *JAC* 19.4 (1999): 547-68. Print.
Werner, Mark. "Challenges in Supporting Faculty Who Use Technologies in Composing Communities." Conference on College Composition and Communication. Denver. March 2001. Presented paper.

Wishon, Gordon. “Information Security Update.” Message to Peter Goggin. 29 June 2011. E-mail.
Wysocki, Anne F., and Johndan Johnson-Eilola. “Blinded by the Letter: Why are We Using Literacy as a Metaphor for Everything Else?” *Passions, Pedagogies, and 21st Century Technologies*. Ed. Gail E. Hawisher and Cynthia L. Selfe. Logan: Utah State UP, 1999. 349-68. Print.