TET1 Task 1: Ethics

Charles Rich

5 November, 2016

A Written Project Presented to the Faculty of the Teachers College of
Western Governors University
TET1 Task 1: Ethics

For Department of Defense employees keeping up with information assurance and the safe use of technology can be a daunting task. We must be aware of the pitfalls of obtaining information through the Internet, and the risks to our computers such as viruses, spyware, adware, and mobile code. As government employees we are also charged with protecting sensitive information from those who are actively trying to get at it. Additionally, we need to be cognizant of how our students use technology (especially mobile phones) and any risks associated with that.

Instructional Setting

The Defense Language Institute English Language Center (DLIEC) is located on Lackland Air Force Base (AFB) in San Antonio Texas. Our institute is one of the largest in the world with the mission of training students in English as a Second Language (ESL) and English for Specific Purposes (ESP). At any one time there are hundreds of teachers either on our campus or on overseas training assignments.

Our students and instructors are dependent on technology and the Internet for research and reference on the job fields we talk about in our classes and it is important that we be able to advise our students on how to obtain the information they seek safely.

Audience

The primary audience for this paper is the teaching staff at Defense Language Institute English Language Center. Our teachers are well trained in ESL, but they have different levels of skill in dealing with the ethical and legal concerns we face when using technology. While our information technology department does a pretty good job of informing us about the handling of privacy act information and how to safely navigate the Internet, we still have had incidences and security infractions despite the training we receive.
Protective Measures for Safeguarding Electronic Resources

Three of the threats or concerns we and our students need to be aware of at DLIELC include viruses and spyware, information security, and responsible use of technology and social networking.

Viruses and spyware are unfortunate realities for anyone accessing the Internet these days. Even given the fairly strict protections and policies placed on our systems in the workplace, students and instructors sometimes stumble into sites they didn't realize were harmful and come away with a virus or spyware “gift” they didn't want.

Threats exist that may not be readily apparent to us. There are those who are actively seeking to get at the information stored on our computers and it is our job to protect that data. It may not seem like much, but even a student roster in the wrong hands can be dangerous for some of our students.

Mobile or cell phone and portable device use at DLIELC is one of the most contentious arguments with students using them when they shouldn't be, or using them inappropriately. Mobile phones have become so prolific that our students sometimes seem to go into withdrawals when we tell them they can't text and check their Facebook constantly. The bigger problem is that there is the potential for students to use phones in potentially dangerous ways as well.

Safe Practices for Use of Instructional Technology Tools

First of all we need to establish what our instructional technology tools are. Instructional technology is everything we use to access or create information in our classes. It can be our desktop or laptop computers, the Smart board, or even the phones in our pockets. Because information can be generated and shared on all of these and they are connected to each other through a wireless network a vulnerability in even one of these devices can jeopardize all of them.

So, how can we protect our instructional technology? We have virus scanning software and the government otherwise secures our computers, right? Just like preventing real viruses and illness
in our bodies it takes more than just automated protection to keep our technology healthy. It takes active prevention on our part too. Most people wouldn't run into a room they know to be full of infectious viruses without covering their faces or otherwise protecting themselves from it, but often the same people would go to a website they suspect might be unsafe. These days it is not a matter of whether your technology has been exposed to these bugs but of how often and how badly. We should treat any website we visit for the first time as if it is a room full of disease and bacteria.

We need to take a few precautions like turning off the web browser’s ability to run mobile code like JavaScript, Active-X, and Flash, scanning all downloaded files for viruses before accessing them or evaluate whether downloading the file is worth the risk in the first place, and avoiding sites we suspect may be a threat. Even when proper precautions are taken we should run routine virus scans to clean up anything we didn't quite manage to prevent from sneaking into our computers.

These protections are even more important when we are not at work. Teachers and students tend to email documents and presentations to each other as a workaround because we are forbidden to use flash drives and other portable devices to transfer files. This actually adds another layer of potential risk if teachers and students don’t maintain the same level of security at home or on their personal devices. While most webmail programs scan files before sending them this is not a guarantee that the files are safe. All files should be virus scanned before sending and after receipt as an added layer of prevention.

Intrusion into your work and home machines happens more often than you might think. Data protection is more than just logging off when you leave the room. It’s not a matter of whether someone can get to your data; it’s a matter of how many have gotten in while you weren’t looking. Simply running a network logging program on your own Internet connection can be a shocking experience as you see literally hundreds of attempted connections to your machine in a fairly short
period of time. Many of these attempts are from random scans of other users on your Internet service checking for open or unsecured ports they can use to access your computer. Make sure your Windows firewall is updated and enabled. Keep people out of your windows by putting up walls.

It’s should also go without saying that you need to use secure passwords on your network routers and computer. The most common hacks are those using scripts to guess a person’s password based on common names, number sequences, and random words from the dictionary. Most users forget to change the administrator password on their computers, or they use a weak password on their own login. This makes the work of the hacker’s scripts quick and easy. Further, it does no good to create this secure password and then write it on a post-it note stuck to your monitor or bottom of your keyboard. You may laugh at the thought that someone might do this, but I have personally found many of these little slips of paper laying around our classrooms and imagine our whole network going up in flames every time I see one.

The last issue to discuss here is teacher and student use of portable devices. We tend to forget that iPads® and mobile phones are basically just little computers. These computers are very small and easy to hide and they are often capable of more than a normal desktop computer. You wouldn’t pull a desktop computer out of your pocket and snap a photo of a classmate sleeping in class, for instance. It goes beyond this, though. What if a student or teacher then takes that photo and posts it to a social media site? At the very least that photo could get the student in trouble with his or her commander back home, but it could also make them a target of an enemy who until now didn’t realize that student had traveled to America and was attending classes at our institute. Not only that, but the phone probably added geo-location and time meta data to the picture from the GPS on the phone identifying in exactly which classroom the student was napping.

How do we protect our students from their phones? So far the answer has been to tell students not to use their phones in class, or some teachers collect phones in baskets at the door. But
more and more teachers are having students use their phones for activities in class for online tools like Quizlet. It’s no wonder that our students are confused about our cell phone policies. Either way we have simply forgotten to discuss the proper use of these devices with our students. Students and teachers should know that our phones need to be secured in just the same ways as our desktops and laptops are and that privacy must be properly protected.

Every Monday morning we brief students on how to exit the building in an emergency and where on campus they can smoke, but we don’t discuss firewalls, virus scanners, cell phone cameras, and social media. This can be added to this briefing, but teachers must also emphasize these things throughout the week.

**Establishing Behavioral Expectations in a Technology Environment**

The Air Force already tells us how they want us to keep their network and computers secure through annual online training, but our students don’t get this training and we need to think about it more than once a year. We often tell our students to put away their phones and other devices, but how often do we take the time to talk to them about safe and secure use of these devices? We should talk to them about it at least once in the time we have them in our classes because if they send us files, or even send attachments through FaceBook we run risks.

There are a number of ways we can pass this information on – through short presentations, maybe a short chat about it the first time we ask students to use technology, and certainly by modeling safe behaviors ourselves. However we do this we need to have a plan and we need to be consistent. It only takes once for an unsafe act to return our classrooms to paper and pencil while our classroom technology is being fixed because we didn’t think about it.
References

Department of Defense *Employee Cyber Awareness Challenge*.


Department of Defense *Phishing Awareness*.
