you should NOT download all files indiscriminately; in particular, be careful not to download attachments containing execution files (i.e., those which have an .exe extension).

- Never share your password with anyone, and choose a password which cannot be guessed by someone who knows you: Using your child's name or the date of your birthday or wedding anniversary, for example, is a bad idea. It is best to choose a password which appears to be a random combination of lower-case and upper-case letters, numbers, and special characters, and which contains at least 8 characters. (One way to do this is to use an acronym consisting of the first letters of the words from a sentence that you can easily remember.) Change your passwords occasionally, and do not use the same password more than once.
- Whenever you are using a public computer, be careful never to choose the "remember this password" option, and take special care to sign out of your inbox/dashboard/etc. when you are finished.
- Avoid clicking on advertisements.
- Never click on a link in emails; instead, if the email appears to be from someone you don't know, delete it, and if it appears to be legitimate, *copy and paste the link* into an open browser. Be very wary of any email which requires you to provide your password, even if it appears to be genuine. Also, be wary of emails claiming to be from your bank and requesting information; emails claiming to be from a friend who has been robbed on a trip and needs financial assistance; those claiming that you have won a prize; those telling you to click on a link to stop receiving similar messages; etc. In fact, you must even be suspicious of emails appearing to be from your email service provider itself, telling you that due to suspicious activity in your account, you need to click somewhere in the email to update your password and that otherwise they will be forced to shut down your account! A tip to remember: Fraudulent emails often contain spelling, typing, or grammatical mistakes, or make use of an inconsistent writing style (for example, inappropriately colloquial language in a formal letter).
- Learn how to ascertain the *authenticity* and *reliability* of the websites you are using. How can you do this? I'll tell you next time…

References

Adware. (n.d.) In *TechTerms.com.* Retrieved August 11, 2012, from http://www.techterms.com/definition/adware

Cennamo, K. S., Ross, J. D., and Ertmer, P. A. (2010). *Technology integration for meaningful classroom use: A standards-based approach.* Belmont, CA: Wadsworth.

Computer worm. (n.d.) In *Wikipedia.* Retrieved August 10, 2012, from http://en.wikipedia.org/wiki/Computer_worm

Malware. (n.d.) In *Wikipedia.* Retrieved August 5, 2012, from http://en.wikipedia.org/wiki/Malware

Marandi, S. S. (2012a). Appropriate online behavior: Beyond netiquette rules. *Roshd FLT, 26*(4), 1-7.

Marandi, S. S. (2012b). Netiquette rules: Avoiding online communication breakdowns and misunderstandings. *Roshd FLT, 26*(3), 7-13.

Palloff, R. M. & Pratt, K. (2007). *Building online learning communities: Effective strategies for the virtual classroom.* (2nd Ed. of *Building learning communities in cyberspace*). San Fransisco, CA: John Wiley and Sons.

Richardson, W. (2010). *Blogs, wikis, podcasts, and other powerful web tools for classrooms.* (3rd ed.). London: Corwin.

Spyware. (n.d.) In *TechTerms.com.* Retrieved August 11, 2012, from http://www.techterms.com/definition/spyware

The difference between a computer virus, worm, and Trojan horse. (2011) In *Webopedia.* Retrieved August 11, 2012, from http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp

The responsibilities of a CALL teacher

Now that you know about different types of malware, email scams, and other online threats, what should you do about them? Remember that one of the first responsibilities of a good CALL teacher is teaching learners appropriate online behavior. This includes teaching them how to stay safe on the Net. Therefore, take care to establish clear *acceptable use policies* (AUPs) for your students. Make sure these policies are both understandable and understood by all stakeholders, such as the school/institute authorities, as well as the learners and their parents. Preferably, everything should be stated clearly in black and white, including the penalties for flouting the AUPs.

Next, be careful to monitor your students' use of the Internet, especially if they are minors. At home, parents are advised to place computers where they can easily be checked (for example, in the living room, with the monitor facing the room); however, on a networked system such as in school computer labs, there are numerous kinds of software which can allow you to see what your students are doing, and which can limit their uses of the Internet. Try to keep yourself up-to-date on cyberspace security and ethical issues. And familiarize yourself with chat room abbreviations, so you won't be caught off guard if a student tries to evade you by using codes or *netlingo*. (Visit http://www.netling.com/top50/acronyms-for-parents.php for a list of the "top 50 Internet acronyms parents [read *teachers*] need to know.") For example, it might be helpful to know that PAL means *parents are listening*, CTN means *can't talk now,* and 143 means *I love you.*

Finally, bear the following points in mind, and take care to publicize and popularize them among your students, as well:

- Do not trust cyber strangers. Remember that people are often not what they seem online, and that on the Net, it is not uncommon for people to lie about their name, gender, age, looks, personality, education, etc.
- Malware is often spread through cyber junk mail, or *spam*, so avoid opening emails from people you don't know. Also, remember that you may receive email which appears to be from a friend or acquaintance but in fact isn't. Therefore, do not open emails with vague or suspicious subject lines, either.
- Install a *firewall* on your computer or network server. Firewalls can prevent unauthorized access to your computer/network.
- Install reliable anti-virus software on your computer, and take care to update it regularly. It is also a good idea to perform a virus scan every so often, to ensure that your system is malware-free. Scanning email attachments for viruses before downloading them is also important. And in any case,

adware is a kind of software which runs advertisements. Usually the adware is financially supported through these ads and is therefore free, which is one reason that adware is often downloaded by users. And while the mere existence of ads may often be overlooked or tolerated, adware frequently functions as a kind of spyware, recording your personal information and computer habits, and transmitting them back to hackers. Often this is done for marketing purposes; that is, the developers of the software use the information as feedback on their product, which would influence their future product development decisions ("Adware," n.d.; Cennamo, Ross, & Ertmer, 2010). However, such uses of adware are potentially harmful, and without a Terms of Use and gaining informed consent, such acts constitute an illegal breach of online ethics, similar to all spyware. And in case you were wondering, it is adware which accounts for all those times that you noticed with surprise that you are suddenly receiving many advertisements which seem to be relevant to your area of interest, or which are related to the topic of an online search you have recently done, etc.

Email fraud: Phishing

Another common online threat is called phishing (pronounced *fishing*). Phishing is a kind of email scam which fools the user into providing sensitive personal information, often leading to identity theft. The email usually appears to be from a genuine, trustworthy Internet address, (and may even contain the logos and trademark signs of reputed entities); and the requests in the emails often seem innocuous and justified (such as verifying your personal information). However, the phishing email usually directs the user to a fake website which is very similar in appearance to the original website, leading her/him to provide private information, such as passwords, credit card details, etc. (Cennamo, Ross, & Ertmer, 2010). Figure 1 below is an example of an email scam from someone impersonating Yahoo.

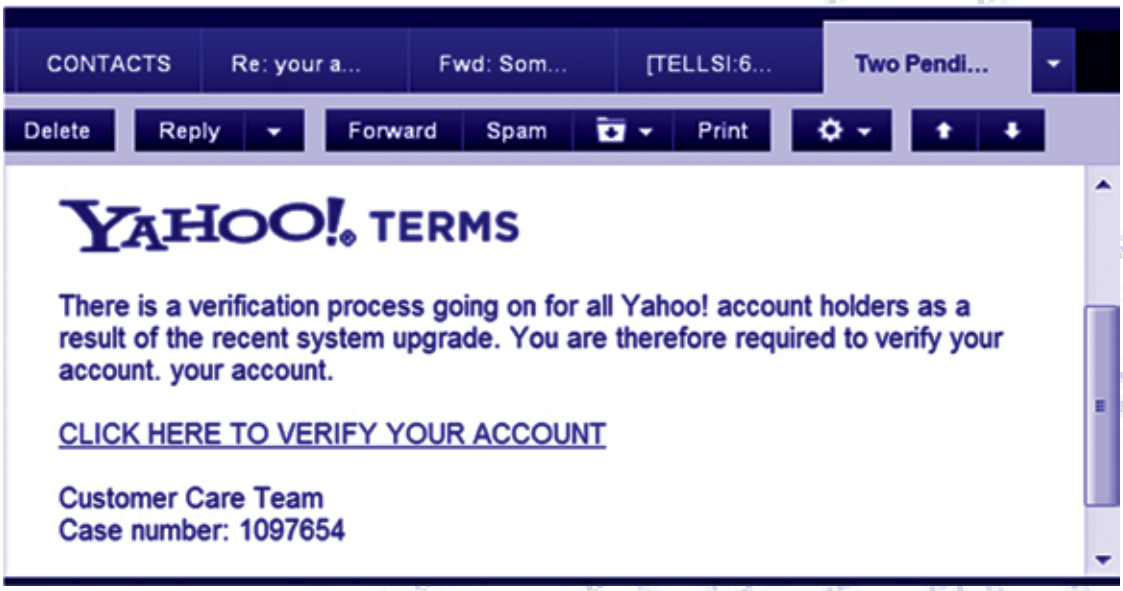

***Figure* 1. A sample phishing email, impersonating Yahoo**

and its people. Thus the Trojan horse has become symbolic of dangers which have a benign appearance, gift-bearing enemies, etc. Similarly, the *Trojan horse* malware is a destructive program which parades as a benign one. To put it another way, in order for the malware to be able to achieve its destructive purposes, it shouldn't be detected by the user, since then it might be deleted or destroyed. Therefore, a hacker designs the destructive program in such a way that it masquerades as a desirable program and, in fact, the user willingly installs it her/himself! This especially happens on the Internet, when a person innocently downloads what appears to be a useful application or a legitimate file, but which is in fact concealing malware giving hackers remote access to her/his computer. Scary, isn't it? This means that we must be very careful not to download files from just any online source, no matter how straightforward and innocent the website might seem. This is extremely important to bear in mind, since many of us constantly download free games, utilities, movies, songs, books, etc. from the Internet, without knowing whether the source is a benign one or not.

Task 2: Think back to the last time you downloaded something from the Internet. How sure are you that the source was reliable and safe? How do you know?

The good news about Trojan horses is that, contrary to viruses and worms, they don't self-replicate, nor do they reproduce by contaminating other files. The bad news is that, similar to worms, they are known to create a backdoor through which hackers can remotely access the infected computer ("The difference between a computer virus, worm, and Trojan horse," 2011).

As the name implies, *spyware* is a kind of malware which spies on you, gathering information about your computer usage patterns such as your browsing habits; or your personal information, such as user IDs and passwords, credit card information; etc. It can be spread through infected email attachments, similar to a virus, or as a Trojan horse parading as a legitimate, advantageous software (Cennamo, Ross, & Ertmer, 2010; "Spyware," n.d.). And as you may probably have guessed by now,

Be*ware* of mal*ware*!

These days, most people know that viruses are no longer exclusive to human beings, and that a *computer* virus can sometimes make life even more unbearable than the old-fashioned human virus! What many people do not know, however, is that often their malfunctioning computer is not down due to the notorious "virus" at all, but due to a different form of *malware*. In fact, viruses are just one type of malware, although we often erroneously use the term "virus" for all forms of malware. This is while ***mal***icious soft***ware***, alias ***malware***, is an umbrella term "used to refer to a variety of forms of hostile, intrusive, or annoying software," including "computer viruses, worms, trojan horses, spyware, adware, and other malicious programs" ("Malware," n.d.). Each of the above is spread differently and presents a different type of threat, so it is important that we become familiar with the various types that exist:

For example, what is the difference between a virus and a worm? The SANS Glossary of Security Terms defines a *virus* as: "A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting – i.e., inserting a copy of itself into and becoming part of – another program. A virus cannot run by itself; it requires that its host program be run to make the virus active." (See: http://www.sans.org/security-resources/glossary-of-terms) On the other hand, the same dictionary defines a *worm* as, "A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively." Therefore, as you can see, both viruses and worms can self-replicate, but the term *virus* is applied to a usually malicious computer program that can only be spread through human intervention (i.e., through running an executable software), whereas a *worm* automatically spreads itself through the security deficiencies of networked computers ("Malware," n.d.). Also, a computer worm doesn't need to attach itself to an executable file (e.g., files with an .exe extension) to spread itself ("Computer worm," n.d.), and it can also expose a compromised system to further attacks by installing a "backdoor" through which hackers can gain access to the infected computer more easily, gaining also remote access to personal or private information (Cennamo, Ross, & Ertmer, 2010).

Task 1: Are you familiar with the story of the Trojan horse from Greek mythology? Based on your knowledge of the Greek myth, try to guess what kind of malware might be called a *Trojan horse.*

Many of us remember reading the famous story of the Trojan horse in our English textbooks at school. Briefly, after nearly a decade of war on Troy, the Greeks (i.e., Spartans) built a huge wooden horse and left it in front of the gates of Troy, full of hidden warriors. The Trojans took the wooden horse to be a peace offering, a sign of the defeat of the Spartans, and dragged it happily into the city. They then spent the night celebrating their supposed victory, until the Spartans came out of hiding and destroyed the city of Troy

Respect your own privacy

In the preceding article it was mentioned that a good CALL teacher should teach her/his students about the dangers of cyberspace, and should ensure that they know how to take care of themselves online. It was revealed that many people use false identities on the Internet, scamming and abusing others. For this reason, a responsible CALL teacher will take care to make the learners understand the perils of sharing personal information online, and will seriously discourage them from sharing their personal photos, address, school name, phone number, etc. (Marandi, 2012a). This is especially crucial in the case of minors, whose use of the Internet needs to be monitored, and whom Richardson (2010) believes should withhold their full names, engaging in class-related online activities only with the express written permission of their parents. Cennamo, Ross, and Ertmer (2010) concur, and claim further:

> Sometimes, students participate in online activities that they may not realize are threatening…. Children who visit and participate in a website devoted to playing games—even simple games, such as checkers or chess—may actually be communicating with adults who are collecting information from them, such as their interests and hobbies. Building trust with someone who seems to like the same things you do may inadvertently lead to providing contact information. The same is true of chat rooms or social-networking sites, such as the popular MySpace.com or Facebook.com (p. 257).

In the previous article, it was indicated that privacy on the Internet is in any case a frail and fragile concept, and users should assume that whatever they send out in cyberspace might one day come back to haunt them! This should prompt us to exercise the utmost caution and discretion in using the Internet generally, and particularly in sharing information, photos, etc.—even with trustworthy friends. Cennamo, Ross, and Ertmer (2010, p. 240) claim, "You should never consider your e-mail to be private or confidential." Palloff and Pratt (2007, p. 62) affirm, "One suggestion that is often made is to avoid posting something you would not want your mother to read or that you would not want to see on the front page of the *New York Times*."

Remember, however, that your online privacy and comfort will not be assured merely through your practicing reticence. Even if you merely lurk online without sharing anything personal, you can still be the object of cyber attacks, if you are not careful. Therefore, another important responsibility of CALL teachers is teaching their students how to combat various types of malware.

Do-it-yourself: Computer-Assisted Language Learning (CALL)

Online Safety and Privacy

Classroom Techniques

By Seyyedeh Susan Marandi, Assistant Professor of TEFL, English Department, Alzahra University, Tehran, Iran
Email: susanmarandi@alzahra.ac.ir

اشاره

مقاله‌ای که پیش روی شماست پنجمین مقاله از مجموعه مقاله‌های مربوط به آموزش زبان به کمک فن‌آوری است. در دو مقاله پیشـین رفتار مناسـب آن‌لاین (بر خط) مورد بررسی قرار گرفت و گفته شـد که رفتار مناسب بر خط نیازمند رعایت نمودن قوانین Netiquette و همچنین آشنا شدن با قوانین مالکیت مجازی همچون Copyleft و Creative Commons Licensesمی‌شود. بخشی از مقاله پیشین هم به امنیت و آسایش اینترنتی اختصاصی یافته بود، موضوع مهمی که در مقاله حاضر به آن بیشتر می‌پردازیم.

Abstract

The article before you is the fifth of a series of CALL-related articles to appear in *Roshd FLT* magazine. In the previous two articles, appropriate online behavior was discussed. It was suggested that appropriate online behavior necessitates practicing netiquette rules (Marandi, 2012b), as well as familiarizing oneself with online ownership laws, including copyleft and Creative Commons licenses (Marandi, 2012a). Part of the previous article was also devoted to safety and privacy on the Net (ibid.), an important topic which will be developed further in the present article.

Key words: appropriate online behavior, online safety and privacy, malware, viruses, worms, Trojan horses, phishing