Cybersafety: Educating individuals with aphasia or cognitive-communication disorders

The Internet poses risks, also known as cyberthreats. Everyone is vulnerable to cyberthreats, including individuals with aphasia (IwA) or cognitive-communication disorders (IwCCD). When speech-language pathologists introduce Internet into treatment plans for IwA or IwCCD the ASHA Code of Ethics dictates they "shall fully inform the persons they serve of the nature and possible effects of services rendered and products dispensed". Yet safe-use products and protocols designed to inform or educate IwA and IwCCD about cybersafety are not reported in the literature. In this project we examine cyberthreats and cybersafety as they affect IwA and IwCCD by1) reviewing literature on cyberthreats; 2) reporting anecdotes from IwA and IwCCD who are Internet users; and 3) proposing strategies to support safer Internet use. We examine information and knowledge needed to create adaptations and scaffolds supporting safer Internet-use for people with language/cognitive-communication disabilities, and propose strategies for teaching cybersafety concepts. Issues drawn from the human-computer interaction (HCI) literature will facilitate discussion of privacy, accessibility, and universal design (Hochheister & Lazar, 2007).

The Internet revolutionized the way people communicate, share and access information, conduct business, and socialize (Buckely & Duncan-Clark, 2009). Individuals with disabilities, including those with acquired language/communication disorders following a stroke or traumatic brain injury can be taught to use the Internet to connect with peers, gain and share information, participate in support groups and, in so doing, to feel less isolated from others and more supported by friends and family members (Egan, Worrall & Oxenham, 2004, 2005; Spaniol, Klamma, Springer & Jarke, 2006).

Conversely the e-Revolution potentially leaves individuals vulnerable to cyberthreats such as hacking; phishing (acquiring information by posing as a trustworthy source); spoofing (masquerading as another by falsifying information to gain illegitimate advantage); or introducing a virus, malware (harmful software), worms, spyware or Adware such as pop-ups (Gantz & Rochester, 2005). Cyberthreats arise from technical and social vulnerabilities (Emigh, 2005; Jagatic, Johnson, Jakobsson & Menczer, 2005). Technical vulnerabilities compromise the electronic system, for example by keylogging (a program installs itself into a web browser, collects data and sends it to a phisher); or cache poisoning (a program supplies data to an unintended cache thereby "poisoning" it and sending faulty data). Even sophisticated computer users may be unable to detect cyberattacks through technical vulnerabilities. Social vulnerabilities place the burden of safe-use on the Internet user, and arise from the characteristics of the Internet user such as unfamiliarity with cybersecurity measures, inappropriate level of trusting information sources, or personal behavior such as limited self control or low socioeconomic standing. Education and awareness are the best tools to deflect cyberattacks arising from social vulnerabilities.

Brain injury introduces additional cognitive, linguistic and social vulnerabilities which may invite cyberattacks for IwA and IwCCD Internet users. We identified six categories of vulnerabilities which will be defined, with examples, in the poster: 1) Visual or reading deficits that preclude careful review of a website or impair comprehension of graphic or printed material; 2) Attention or memory deficits, i.e. selective attention impairments may interfere with attending to computer screens filled with multiple features, while anterograde memory impairments confound the ability to learn and retain the steps necessary to access the Internet (Sohlberg, Elhardt, Fickas & Sutcliffe, 2003; Todis, Sohlberg, Hood & Frickas, 2005); 3) Careless use of

adaptations, for example referring to written models of passwords, with the risk of this information being viewed by others; 4) Impulsive responding, impaired judgment or decreased error monitoring resulting in minimal observance of safety precautions; 5) Limited ability to generalize computer skills, for example training in one application such as Facebook™, and to transfer these skills to anti-phishing software; 6) Restricted opportunities to use a computer and become familiar with protocols.

Our group has engaged in several Internet projects with IwA and IwCCD, primarily involving email and Facebook™ (Avent, Glista & Goldblum, 2008; Goldblum & Patterson, 2009), which has become the most-used digital social network with over 200 million active users (Kinkoph Gunther, 2010). We have watched IwA and IwCCD enthusiastically embrace Internet platforms or shy away from them. We collected anecdotal information about successes and frustrations with Internet platforms and considered them within the context of education about cyberthreats and cybersecurity.

The project underway in three sites internationally, and which will be reported in this poster, presents results of guided discussions with IwA and IwCCD to educate them about cybersecurity. Education evolves with awareness of the complex factors that support the use of technology with these individuals. For example, Sohlberg and colleagues (2003; 2005) noted how electronic communication "remains largely inaccessible to individuals with severe cognitive-communicative disabilities" and that barriers existing for computer access for IwCCD can be inferred given the range of problems they exhibit. Two tools used in this project are: 1) a list of questions guiding discussions; and 2) surveys administered before and after the series of discussions that investigate real and perceived barriers to Internet access; individuals' technical and social vulnerabilities; Internet usage patterns (i.e. email, shopping); and cybersecurity awareness.

Finally we will offer suggestions for teaching individuals with language or cognitive impairments to develop skills and knowledge for safety in computer usage. HCI research suggests game formats are better teaching tools than tutorials for information on phishing (Sheng et al., 2007). Cybersecurity training for IwA or IwCCD has not been described in the literature, however approaches for teaching general computer skills have, for example, using direct instruction (Sohlberg et al., 2005) or tutors (Egan et al., 2004). While the most effective approach is not known, Sohlberg et al. (2003) refer to a user-centered approach to match individual needs to the selection and development of assistive technology, which may be a useful process in training safer Internet- use.

References

Avent, J., Glista, S., & Goldblum. (2008, November). *Linking People with Aphasia & Cognitive-Communication Disabilities Using Technology*. Paper presented at the meeting of the American Speech-Language-Hearing Association, Chicago.

Buckley, P. & Clark, D. (2009). *The rough guide to the Internet*. London: Rough Guides Limited.

Cruice, M. (2007). Issues of access and inclusion with aphasia. *Aphasiology, 21*(1), 3-8.

Egan, J., Worrall, L., & Oxenham, D. (2004). Accessible internet training package helps people with aphasia cross the digital divide. *Aphasiology, 18*(3), 265-280.

Egan, J., Worrall, L., & Oxenham, D. (2005). An internet training intervention for people with traumatic brain injury: Barriers and outcomes. *Brain Injury, 19*(8), 555-568.

Emigh, A. (2005). *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*. Identify Theft Technology Council. Retrieved from http://www.anti-phishing.org/Phishing-dhs-report.pdf.

Goldblum, G. & Patterson, J. (2009). *Facebook experience: Linking persons with neurogenic communication disorders across continents.* Paper presented at the meeting of the American Speech-Language-Hearing Association, New Orleans.

Gantz, J. & Rochester, J. (2005). *Pirates of the Digital Millenium.* Upper Saddle River, NJ Prentice Hall.

Hochheiser, H., & Lazar, J. (2007). HCI and societal issues: A framework for engagement. *International Journal of Human-Computer Interaction, 23*(3), 339-374.

Jagatic, T., Johnson, N., Jakobsson, M. & Menczer, F. (2007). Social phishing. *Communications of the ACM , 50*, 94-100.

Kinkoph Gunther, S. (2010). *Sam's Teach Yourself Facebook in 10 Minutes.* Indiana, Pearson Education, Inc.

Pollens, R., Glista, S., Czap, A., Glick, A., Littlejohn, J., McCormick, J., & Sharp, M. (2008, November). *Developing Email communication for individuals with aphasia: Case studies.* Poster presented at the meeting of the American Speech-Language-Hearing Association, Chicago.

Sheng, S, Magnien, B., Kumaraguru, P., Acquisti, A., Canor, L.F., Hong, J & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. Proceedings of the Association of Computing Machinery Conference, Pittsburgh.

Sohlberg, M. M., Ehlhardt, L. A., Fickas, S., & Sutcliffe, A. (2003). A pilot study exploring electronic (or e-mail) mail in users with acquired cognitive-linguistic impairments. *Brain Injury, 17*(7), 609-629.

Sohlberg, M. M., Fickas, S., Ehlhardt, L., & Todis, B. (2005). The longitudinal effects of accessible email for individuals with severe cognitive impairments. *Aphasiology, 19*(7), 651-681.

Spaniol, M., Klamma, R., Springer, L., & Jarke, M. (2006). Aphasic communities of learning on the web. *International Journal of Distance Education Technologies, 4*(1), 31-45.

Todis, B., Sohlberg, M.M., Hood, D. & Fickas, S. (2005). Making electronic mail accessible: Perspectives of people with acquired cognitive impairments, caregivers and professionals. *Brain Injury, 19*(6), 389-401.

Tonkovich, J. (2009). Use of social networking sites as a clinical tool. Poster presented at the annual meeting of the American Speech-Language-Hearing Association, New Orleans.