January 2013

Community Literacy of Ontario

80 Bradford Street #508

Barrie, Ontario, L4N 6S7

Tel: 705-733-2312

Web: www.nald.ca/clo

Email: clo@bellnet.ca

Twitter: @Love4Literacy

Facebook: www.facebook.com/CommunityLiteracyOntario

INSIDE THIS ISSUE:

Community Literacy of Ontario

Our Voice

Reducing Risk/Protecting People
Focus on Cyber Risks

Community Literacy of Ontario is pleased to share the second of four newsletters as part of our project entitled ***Reducing Risk/Protecting People: Resources and Tools to Build Risk Management Capacity.*** This project is funded by the Ontario Ministry of Training, Colleges and Universities (MTCU).

Risk management is an extremely important topic: to LBS agencies, to MTCU, to other government ministries and to the general public. CLO's ***Reducing Risk*** project is designed to give LBS agencies tools, resources and training to help them to improve their risk management processes and policies.

As part of the *Reducing Risk/Protecting People* project, CLO will be producing four webinars and four newsletters on the topics of:

⇒ **Privacy** (November 2012) The newsletter is available at www.nald.ca/clo/newslet/dec_2012_our_voice.pdf and the recorded version of the webinar can be seen at https://vimeo.com/52630059

⇒ **Cyber Risks** (January 2013)

⇒ **Safety and Security** (February 2013)

⇒ **Risk to Reputation** (March 2013)

The webinars will be delivered live and a recorded version will be freely available online. The newsletters are also available online via CLO's website.

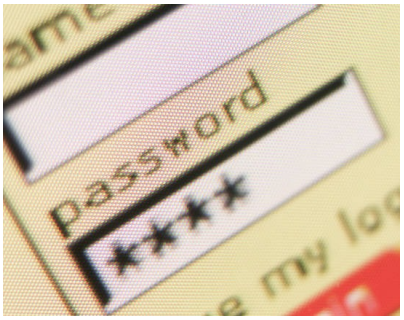
Technology is an integral part of teaching and learning in the 21st century. Literacy students are taking online courses, downloading applications to help them practice their skills, communicating via email and text messages and so much more. Technology has become an important tool at school, in the workplace and in the home. And while technology has many positive benefits, it also comes with risks. These risks can run from the minimal (the annoyance of receiving unwanted email) to the more serious (theft of money, loss of personal information and more).

In this newsletter, we will share ideas, tools and resources to help literacy practitioners and learners stay safe while learning and exploring the many riches that technology has to offer.

> "Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they'll do wonderful things with them." (Steve Jobs)

Focus on Cyber Risks

Passwords



Passwords are a key component of cyber safety. Strong passwords can help keep unwanted people from accessing your online activities and accounts. One of the first strategies in choosing passwords is to use something different for each of your important accounts. If you always use the same password, someone who hacks your account or who finds out your password would have access to all of your accounts.

A second strategy is to change your passwords regularly. Some workplaces and even some websites require you to do just that. However, now that so much of what we do in our day-to-day lives is online, this can become difficult! It can also be hard to remember all of your different passwords. Here are a couple of ideas to help you create, remember and maintain multiple passwords:

- Write them down! Although this may seem counter-intuitive, you may not always remember your passwords, so keep a list of them. Of course, you're going to want to keep that list somewhere safe so other people can't easily access it. You will want to let at least one trusted person know how to find that list, however. In the workplace, if you are ill or leave your job, someone else will need access to your files. As an individual, if you become ill, a family member may need to access your information.
- Use a root word to help make passwords easier to remember. Then add something related to the account or website. For example, a banking password could be "literacybank," or a learning website password could be "literacyspelling" and so on. However, some sites require additional security such as numbers, capital letters or special characters, so you would have to modify this strategy accordingly.
- Use compound words. They are more difficult for someone else to figure out. For example, use "newspaper" rather than "news." Or "ladybug" rather than "lady."
- Don't use obvious words or phrases like "password" or "abc123." Don't use your email address, your Social Insurance Number or your name.
- Longer is better. Shorter passwords are more likely to be hacked. Google's "Good to Know" site (www.google.com/goodtoknow) reports that there are almost one quintillion possible 10-character passwords! That's a lot of possibilities.
- Mix up numbers, letters and symbols. This also adds to the possible choices. "Good to Know" says that an eight-character passwords made up of a combination of numbers, symbols and mixed-case letters provides more than 6 quadrillion possibilities.
- Turn a phrase into a password. For example, choose a phrase such as "I like to attend ABC Literacy five days a week" and create a password using letters and numbers for each word: IltaABCL5daw.
- Don't share your passwords!
- Use Microsoft's Safety and Security Centre to check the strength of your password: www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

For more information about creating strong passwords, see "10 Rules for Creating a Hacker-Resistant Password" from the Privacy Rights Clearinghouse: www.privacyrights.org/ar/alertstrongpasswords.htm

If you can't think of any strong passwords yourself, why not try the "Strong Password Generator" tool at http://strongpasswordgenerator.com

Focus on Cyber Risks

Safe Clients: Understanding Internet Safety for At-Risk Clients

By Bruce Roxburgh, Manager, GreenIT. Modified with permission.

Internet safety is a vast topic because of its many fingers of influence in everyday life. When it comes to the safety of those we serve as clients, it is a matter of understanding what is at risk. How can we help adults exploring the internet to understand the risks?

We can teach our clients about internet safety. For example, you can make sure that clients know to log in and log off of public access computers and set the computers up to refresh and lose all the previous information so that the next client gets a clean slate. You can lock up any confidential information—digitally with a password and with a lockable cupboard or room for hard copies of information. You just have to develop a plan.

Sometimes, the individual online practices of the people we serve can be harmful to their future. Often agencies are called to teach people to use social media like Twitter or Facebook to help clients connect or communicate. Do we help our clients to understand that what they say on social media can be examined by a potential employer or taken out of context? There are many instances where etiquette breaches by unsuspecting clients have implications for work, even costing some their jobs in a tight economy. Helping clients navigate the internet and build online presence should come with a playbook that says, "*Go explore all you can, make the most of what is available and get excited about what you find… but understand that you are a fish in a vast ocean of shared knowledge and that you must be careful about how you share your personal information in this digital new world.*"

Speaking of "Fish" … A few years ago, I was overseeing some local training for persons with disabilities in my community training lab. As tech services manager, I was looking for ways to tailor our training to the nuances of each client; this put me shoulder-to-shoulder with several clients and I was astonished at the risks that many of these clients took on without realizing. Adult clients with intellectual disabilities were being openly encouraged in their group home environment to sign up for "*PlentyOfFish*" dating. Offering to meet people they met online. Sharing personal information with complete strangers. Shudder!

Whatever your role in providing people access to online services, take frequent stock of how much you know about the sites and services you are using and how the information is accessed. Try accessing your own information as an outsider and see what comes up on Facebook, LinkedIn or Twitter... or better yet, try logging in on a computer after one of your friends and see how much you can find out.

The force be with you! People are counting on you…

Bruce Roxburgh is the Manager of GreenIT, a unique technology service for Nonprofits that is leading the TechTogether (www.techtogether.ca) project. GreenIT offers free webinars and other resources to help nonprofit organizations effectively use technology.

In January 2013, CLO delivered a one hour webinar on **CYBER RISKS**. In this webinar, we overviewed issues to consider and shared examples of good practices, checklists, real-life examples and sample policies on social media and digital learning.

You can access the **CYBER RISKS** webinar here:
https://vimeo.com/user10532952

Focus on Cyber Risks

Safe Surfing

Here are some tips and ideas from CLO to help you stay safe online:

- Stay up-to-date. Update software regularly (e.g., Windows Update) and set security software to run scans at least weekly.
- Do not download programs or software from unfamiliar sites because it may contain malware or viruses.
- Do not click on email links that ask you to verify your banking account information. Banks will NEVER send this type of request.
- Do not click on email links or open email attachments from someone you don't know.
- Even if your best friend posts a link on Facebook, think twice. If the posting and tone are out of character for that person, don't click on the link.
- Do not click on links that offer to show your favourite Hollywood star doing something interesting.
- Be careful of links on Twitter, particularly if you don't know the source. (Trusted news sites such as television networks and large newspapers are generally safe.) Or use a Twitter client application like TweetDeck that shows you the full URL before you click on it.
- Be careful with video and music downloads. Use trusted sites such as iTunes to purchase digital content. YouTube and Vimeo are good choices for free video content but be careful with YouTube links to movies or television shows. File sharing sites that offer free content (e.g., Pirate Bay, Torrentz) are especially dangerous. If you want to watch a movie or television show, look for it on a reputable network website (CTV, CBC, Global, etc.).
- Be careful with web searches. Although search engines such as Google, Bing and others are very useful tools when it comes to finding information on the internet, occasionally they may also inadvertently provide you with search results that lead to malware and other problems. Most security software will alert you to dangerous websites, but in general, choose search results from trusted sources and familiar websites where possible.
- Use caution when installing applications on Facebook. There are no legitimate "do not like" buttons and no legitimate profile viewers on Facebook. Avoid these applications along with quizzes about which Harry Potter character you are, or similar applications that require you to download and install anything. A good source of information about Facebook scams and dangerous applications is Facecrooks (http://facecrooks.com).
- If it looks too good to be true, it probably is. Avoid scams such as "click here for a free $100 gift card." Companies simply do not offer that kind of deal! Often these links are simply a way for spammers to get your email. A good source of information on scams and other questionable internet content is Snopes (www.snopes.com).
- Be careful where and how you share your personal information online. Everyone has a different comfort level when it comes to what they are willing to share online. Some people are comfortable using sites such as Facebook and Twitter. Some people use their real names in full and post personal pictures in their profile, while others prefer to use an avatar. Do not post your home address or telephone number on social media sites.
- Create an email address specifically for social media sites and for website registration. Even legitimate and trusted sites may use your email to send you information or advertising that you are not really interested in. Many people create an email specifically for their online activity to keep their main email clean and uncluttered.
- Finally, be a little paranoid! This isn't advice we usually give, but it doesn't hurt to be too careful.

Focus on Cyber Risks

Security Software

Literacy educators, administrators, learners and volunteers are spending increasing amounts of time online. So how do we know what is safe? How can we avoid clicking on an interesting link and unknowingly downloading a virus or malware to our computer?

The first line of defense to staying safe while browsing or using websites is to install reliable security software. There are some free and low-cost options available, but often they offer limited protection and you will need to spend a bit of money to have more security. Many software providers will provide the option to download a free trial so you can test out the software and see if it's right for you and your agency. You can also purchase licenses to protect multiple computers in your agency. Most security software will alert you if a link or website is potentially unsafe. Some of the popular security software choices are:

- AVG Security (www.avg.com)
- BitDefender (www.bitdefender.com)
- McAfee (www.mcafee.com/ca)
- Norton (Symantec) (www.symantec.com)
- Trend Micro (www.trendmicro.com)

Top Ten Reviews offers a comprehensive review of security software at http://internet-security-suite-review.toptenreviews.com/?cmpid=ttr-snd

For more information on choosing the right security software for your needs, see About.com's article at http://antivirus.about.com/od/antivirussoftwarereviews/a/virusprotect.htm and TechNews Daily's article at www.technewsdaily.com/7966-best-internet-security-software.html

Learner Internet Safety Pledge

In the next several pages, we will share some sample policies that you can adapt and use as best suits your agency. For more information on creating internet-related policies, see Elisa Birnbaum's article entitled "*Social media: What's your policy*?" on Charity Village (https://charityvillage.com/Content.aspx?topic=social_media_what_s_your_policy_&last=531)

The Northwest Territories Literacy Council (www.nwt.literacy.ca) has created a *Learner Internet Safety Pledge*. It was written for all ages. We have adapted it below for use in an adult literacy agency.

- I will avoid giving out personal details that will identify who I am, such as my address, phone number or photographs.
- I will not knowingly link to any websites that contain offensive content.
- I will not reply to any messages or bulletin board items that include offensive content.
- I will not engage in online conflict.
- I will not accept any online offers of money, free gifts, prizes, etc.
- I will not order anything online or provide my credit card or other financial details.
- I will not enter chat rooms or participate in instant messaging during school hours except for approved learning activities.
- I will not arrange any face-to-face meetings with anyone I meet on the internet.

Focus on Cyber Risks

Sample Social Media Policy

Thank you to the Adult Learning Association of Cape Breton County (www.adultlearningcapebreton.ca) for so generously sharing their social media policy with us.

This document establishes a policy for staff and volunteer use of social media. It is written to encourage the safe and effective use of social media by ALACBC employees and volunteers. The Adult Learning Association of Cape Breton County encourages the use of social media technologies to enhance communication, collaboration, and information exchange in support of the ALACBC mission. The use of social media technology follows the same standards of professional practice and conduct as are already practiced by our organization, including existing confidentiality and harassment policies.

Social media means the online technologies and practices that are used to share information and opinions and build relationships. It can involve a variety of formats, including text, pictures, video, audio and real-time dialogues. It includes, but is not limited to, such things as social networks, discussion forums, blogs, wikis and podcasts.

When considering launching a social media initiative, management and employees should be clear about the purpose and the resource implications that maintaining and monitoring the effort will entail.

This staff use agreement applies to:

- All staff whether part-time, full-time or temporary.
- Volunteers working in the organization.

Posting material

- All material and links published on ALACBC social media should be appropriate to the ALACBC work environment.
- Such material can be posted only by those given the authority to do so by the Executive Director.
- Any employee or volunteer who brings ALACBC into disrepute on any social media platform could be subject to disciplinary action.
- Senior management will be responsible for ensuring that social media services initiated by and/or created by and within the control of ALACBC are moderated, and to ensure the timely removal of any defamatory or objectionable submissions. The reasons for content deletion will be stated.

All employees and volunteers should recognize that anything posted on the internet is permanent. Even if you attempt to delete the post, photo, comment, etc., it is likely that it has been stored in any number of other places. Content posted to the internet should be thought of as permanent.

Personal Social Media Space

ALACBC employees and volunteers should recognize that what they publish on the internet may reflect on their employer. Employees and volunteers who use social media for personal purposes should:

- Use a disclaimer anywhere there may be uncertainty about the capacity in which they are acting. A disclaimer, such as: "The postings on this site are my own and do not represent the views or opinions of my employer" can help protect you.
- Avoid sharing ALACBC material in a personal space. Try and keep your personal online presence and your work online presence separate.
- Recognize that if you publish inappropriate comments that reflect badly on your employer in your personal space, on your personal time, that disciplinary action could follow.

Sample Digital Technology Policy

Community Literacy of Ontario researched various policies, then developed this sample digital technology policy.

ABC Literacy wishes to encourage the correct and proper use of digital technology and expects staff, volunteers and learners to use technology during the normal course of work and learning. We wish to encourage appropriate internet use and to increase individual skills, competency and understanding. This policy outlines how ABC Literacy staff, volunteers, contractors and learners can use digital technology professionally, ethically and lawfully, while maintaining the safety and security of information and property, without compromising confidentiality.

ABC Literacy provides internet access for its staff, volunteers, contractors and learners for learning, teaching and administrative purposes. ABC Literacy permits limited personal use of the internet during designated break times provided that the material accessed is appropriate and is not potentially offensive to others and is consistent with our code of conduct. Internet use may be subject to monitoring, including sites visited, as allowed by Canadian law. Any individual using the digital technology inappropriately could put ABC Literacy and/or its employees, volunteers and learners at risk.

Staff members, volunteers, contractors or learners shall not:

- Use instant messaging or other "chat" software unless it is being used for learning and teaching purposes.
- Access, display, print, upload, share or download offensive or inappropriate material. This includes (but is not limited to) material related to pornography, mature content, gambling, illegal substances, racism, sexism, violence and/or illegal activity.
- Knowingly create, download, upload or transmit data or material that can corrupt or destroy other users' data and/or hardware.
- Download software and/or other material without permission. All hardware and software remain the property of ABC Literacy.
- Access or use peer-to-peer file sharing sites (e.g., to find movies or books).
- Disclose financial or operational information that is not public.
- Disclose or share personal information about other employees, volunteers, contractors and/or learners.
- Publish or reproduce material that belongs to others without their knowledge and permission. Any material that is shared will be attributed and sourced appropriately and accurately.

All learners, volunteers, staff members and contractors shall create and use strong, secure passwords. These passwords will be kept confidential and only be shared as needed with approved individuals.

Social Media

- Staff members, volunteers and learners who participate in social media are encouraged to establish a separate social media profile for agency use. This can help maintain personal privacy.
- Staff members, volunteers and learners may communicate and interact with each other using social media only as appropriate for learning and teaching.
- Staff members, volunteers and learners who participate in social media will ensure that strong privacy controls are used and that these controls are reviewed and updated regularly.
- Only authorized staff members, volunteers, contractors and learners may post updates to ABC Literacy's social media accounts, website and other online presences.
- Any information posted to ABC Literacy's social media profiles, website or other online presences will avoid controversial topics, inappropriate photographs and/or inappropriate language.
- No staff member, volunteer, contractor or learner may create a social media account for ABC Literacy without approval.
- No staff member, volunteer, contractor or learner may post or tag the name, photograph or other identifying information of another staff member, volunteer, contractor or learner without that individual's knowledge and permission.

Focus on Cyber Risks

Cyber Risks Newsletter—January 2013

Research and writing by Vicki Trottier

Editing by Joanne Kaattari

OUR FUNDER

Community Literacy of Ontario is funded by the Government of Ontario, under:

EMPLOYMENT ONTARIO

Sample Facebook Policy

CLO's Draft Guidelines for Facebook

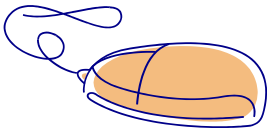
Only people approved by CLO's management may make social media postings on behalf of CLO. It is the responsibility of CLO's management to ensure that all postings made by CLO are appropriate.

CLO considers the following types of postings by us or others on our Facebook page or other social media sites to be unacceptable:

- Defamatory or offensive postings, including swear words or verbal abuse
- Postings that are against the spirit of the Ontario Human Rights code
- Postings that are politically partisan in nature
- Postings from others that are intended to solicit business for an external individual or company (Note: CLO can promote its own social enterprise activities)
- Spam comments

Such comments will be removed from our site. Repeat offenders will be warned and, if necessary, banned from our site.

Additional Resources



- GCF LearnFree's Internet Safety Module: www.gcflearnfree.org/internetsafety
- Imagine Canada's Insurance & Liability Resource Centre for Nonprofits: Technology and Social Media: www.nonprofitrisk.imaginecanada.ca/node/891
- Google's Good to Know: www.google.com/goodtoknow
- Must Have Resources on Teaching Online Safety: www.educatorstechnology.com/2013/01/must-have-resources-on-teaching-online.html
- Get Safe Online: www.getsafeonline.org
- CommonCraft: www.commoncraft.com. They offer a series of videos on staying safe. Click on "net safety" to view them.