Privacy and Safety

Welcome to '*Social Media Privacy and Safety*', one of the training modules from Community Literacy of Ontario's *Social Media Marketing* project.
This project is designed to develop resources to help Ontario's literacy agencies, and others, use social media for marketing.

Introduction

Now that you have begun exploring the many exciting possibilities of social media when it comes to agency marketing and promotion, you will also want to take some to learn about how to stay safe online. Although social media marketing offers many benefits and advantages to literacy organizations and other non-profit agencies, there are also associated risks with any online activity. In this module, we will share tips, tools, information and resources about creating strong passwords, security software, social media policies, and more to help keep your organization safe online.

Online Privacy

One of the biggest concerns that people have about being online is protecting their privacy. Everyone's comfort level is different, so some people will willingly share a lot of information about themselves while others may use a pseudonym or share very little information.

It is important for every person to educate themselves about the risks and decide what information they are comfortable sharing online.

Privacy and Safety

One of the best ways to safeguard your personal privacy when using social media to market your non-profit agency is to use organizational profiles and accounts rather than your personal account. Not only does this protect your privacy as an individual, it also makes it easier to share the administration of organizational accounts because multiple staff members, or even volunteers, can be given access to log-in information.

As an individual, you may be reluctant to share things online. However, when it comes to social media marketing as a nonprofit organization, it is important to share because you are trying to let people know about your agency and the great work that it does. But remember -- organizational online privacy and personal online privacy are not the same thing! You can administer organizational social media profiles without impacting your personal online privacy. For example, when you create an organizational social media account or profile, be sure to register with an organizational email rather than using your personal email address.

Always post, tweet and share as the organization, rather than as an individual. Each of CLO's modules clearly outlines how to set up an account as an organization for each of the various social media channels described in the modules.

It is also a good idea to regularly review privacy policies for all social media tools, as they have a tendency to be changed and updated frequently. Click on the name of each social media platform to access their privacy information:

- Facebook
- Twitter
- LinkedIn
- Pinterest
- Instagram
- YouTube

Privacy and Safety

Passwords

Strong passwords are one of the first lines of defence when it comes to online activity. After all, if hackers cannot access your profiles and accounts, they can't cause trouble. Below are some strategies to help you choose and use effective organizational (and personal) passwords.

1. Do not use the same password for all of your accounts! In reality, however, many of us do this simply because it seems impossible to remember a long list of different passwords. One strategy to combine reality with good practice is to use a common root word and then add something different for each account. For example, if the root password is "safari" then your Facebook password could be "safarifb" while your Twitter password would be "safaritw" and so on.

   If you choose to use this root password system for your organizational accounts, you can make it even more secure by adding numbers to your system. For example, "safarifb2014" is more secure than just "safarifb" and makes your password harder to guess or hack, even if someone is aware of your root word system. For an even greater level of security, add a special character (!, @, #, $, %) and use a mix of upper- and lower-case letters. "safariFB2014#!" is now a much more secure password than the original "safarifb" option.

2. Keep a list of your passwords. This may seem counter-intuitive; however, you may not remember each of your passwords as time goes on. Also, while some online accounts allow, and even encourage, the use of special characters as suggested above, others do not allow them. Therefore it may become difficult to keep track of the various root word combinations you have created.

   In the case of organizational passwords, it is good practice for at least two staff members to have access to the password list. This is one of the few times it may be more beneficial for you to use pen-and-paper technology. Rather than creating a Word document with your passwords that someone could access, actually write them down on paper. Be sure to keep the list of passwords in a safe place

Privacy and Safety

3. Another strategy for staying safe online is to change passwords regularly. Some workplaces and websites are set up so that passwords expire after a set amount of time and you have no choice except to change them. Once again the reality is that few people do this because it can seem like a lot of work. Maintaining a complete list of each organizational account and its individual password, as suggested above, can help make the job of changing passwords more manageable.

4. When creating passwords, use compound words. They are more difficult to figure out. For example, “newspaper” is stronger than “news”, and “adultliteracy” is stronger than “literacy”. But don’t make it obvious! It would be easy for someone to guess a password along the lines of “ABCLiteracyAgency”.

5. Don’t use obvious generic words or phrases like “password” or “abc123”. (You’d be surprised at how many people do this.) Don’t use your email address, your Social Insurance Number, or your name. For a list of more commonly used “bad” passwords to avoid, visit Top 25 common, attackable passwords (via ZDNet).

6. Longer is better. Short passwords are more likely to be hacked. Google’s “Good to Know” site reports that there are almost one quintillion possible 10-character passwords! That’s a lot of possibilities!

7. Mix up numbers, letters and special characters. This makes passwords harder to crack. For example, “belleville123safari#” would be more secure than just “bellevillesafari”.

8. Turn a phrase into a password. For example, choose a phrase such as “Our adult literacy agency offers classes five days a week” and create a password using the corresponding letters and numbers: Oalaoc5daw.

9. You can use online tools such as Microsoft’s Safety and Security Centre to check the strength of your password.

10. If you’re stumped, and you can’t come up with a strong password, give the Strong Password Generator tool a try.

Privacy and Safety

Safe Surfing

When you are involved in marketing and promoting your agency using social media, you are also going to be "surfing the 'net", looking for resources, reading blogs, visiting other agencies' social media sites, sharing posts and Tweets, and so on. Here are some tips and ideas to help you stay safe online and keep your computer virus-free.

1. Stay up-to-date. Take advantage of built-in updating tools provided by both Windows and Mac operating systems and by mobile providers. Often, the updates provided by these systems include security patches that can help you stay safe.

2. Do not download programs or software from unfamiliar sites. They may contain malware or viruses.

3. Never click on email links that ask you to verify banking account or PayPal information. Banks and payment companies will NEVER send this type of request. You can always verify your account by logging in through a website, but never follow a link from an email.

4. Don't open email attachments or click on links from someone you don't know. If you do know the sender, but the email isn't in character for that person, don't click on the link.

5. Don't click on links that offer to show your favourite celebrity doing something "interesting".

6. Be careful of links on Twitter, particularly if you don't know the source. Trusted news sites such as television networks and newspapers are generally safe. Some applications (e.g., TweetDeck) will show the full URL before you click on it, which can help you determine if it's a safe link.

7. Be careful when downloading music and videos. 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 or broadcast website (CTV, CBC, Global, Netflix, etc.).

8. 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.

9. Use caution when installing applications on Facebook. There are no legitimate "do not like" buttons and no legitimate applications that let you see who viewed your Facebook profile. Avoid these applications along with quizzes about which Harry Potter character you are, or similar applications that require you to download and install anything. Facecrooks is a good source of information about Facebook scams and dangerous applications.

10. 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.

11. 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. Some people are comfortable using sites such as Facebook and Twitter. Some people use their real names and post personal pictures, while others prefer to use a pseudonym and/or an avatar. Do not post your home address or telephone number on social media sites. As mentioned earlier, you can avoid using your personal social media accounts by setting up organizational accounts.

12. 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. When posting from your organizational profile or account, be sure to use a generic organizational email (e.g., info@myagency.com) rather than your regular work email.

13. Finally, be a little paranoid! This isn't advice we usually give, but it doesn't hurt to be too careful.

Privacy and Safety

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 online is to install reliable security software. If your computer comes with security software already installed, be sure you know how to set it up and use it. There are some free and low-cost options available, but often they offer limited protection, so you will need to spend a bit of money to gain more security. Many software providers will allow you to download a free trial to test out the software. You may also purchase licenses to protect multiple computers in your agency. Most security software will alert you if a link or website is potentially unsafe, which can save you time, trouble and money.

Some of the popular security software choices include:

- AVG Security
- BitDefender
- McAfee
- Norton
- Trend Micro

Top Ten Reviews offers a comprehensive review of security software. This list, which is updated frequently, may help you choose the right product for your needs and budget.

If you need more information to help you make that choice, be sure to read the following helpful article from About.com.

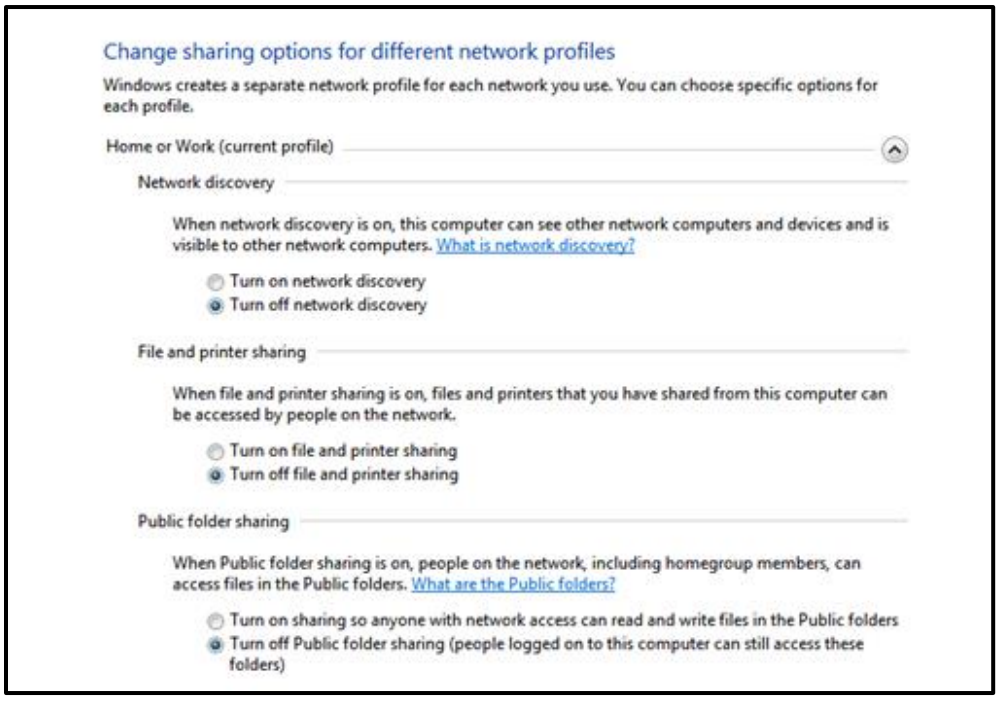
Staying Safe With Wi-Fi

Isn't it wonderful that we can be connected almost anywhere we go, thanks to wireless internet connections and mobile devices? However, just like everything else associated with digital technology, the benefits also come with risks. Within your workplace, wireless connections should be set up as secure networks to that only authorized people can access them. This not only helps protect your privacy and your data, it can also keep unwanted people from using your account beyond its pre-paid limits, which could cost your organization a lot of money!

When you are travelling and away from your organization's network and you need to use another wireless connection (e.g., in a hotel, a coffee shop, or an airport), here are some tips to help keep you safe:

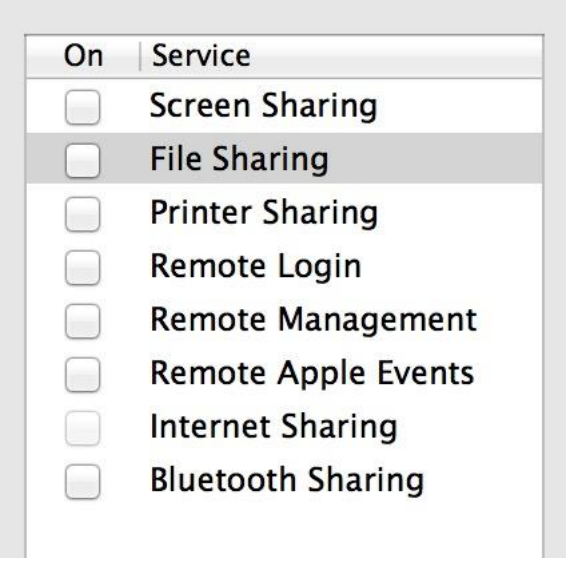
- **Turn off file sharing.** That way, no one can access your data on a public or shared connection.

On a PC, open your Control Panel and go to "Network and Internet". Then, from the menu on the left side, choose "change advanced sharing settings". Here you will find a variety of options, including file sharing and public folder sharing that you can turn off when travelling. You can easily turn them back on if you share files at home or with other trusted users.

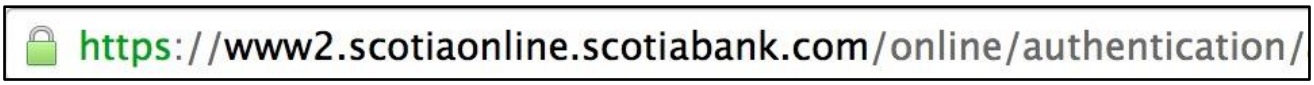


Privacy and Safety

On a Mac computer, go into your System Preferences, and then choose “Sharing”. Make sure that the “on” button is not ticked beside file sharing.



- **Turn on firewall protection**. This stops any attempts to connect to your computer.
- **Keep your security software running**. This ensures that attempts to access your computer are blocked.
- **Password protected connections are generally safer than open connections**. Look for the locked padlock icon on the list of available networks. Of course, you’ll need to know the password to be able to use these networks!
- **Avoid accessing highly sensitive information**, such as bank accounts, on a public network. If you do need to access sensitive information, look for a locked padlock icon in the corner of the browser window and make sure that the web address begins with https (this indicates a secure site), as in the example below.



Privacy and Safety

- **Consider purchasing and setting up a Virtual Private Network** (VPN), especially if your work requires you to travel frequently. This is the most secure way to use public networks. PCWorld's Eric Geier wrote a helpful and informative blog entry about VPNs that explains why you should use one and how to set one up.

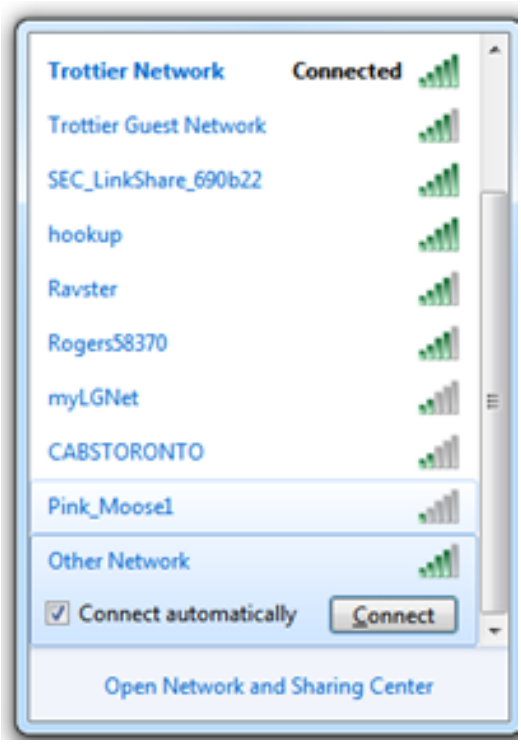
- **If you don't need to use the internet, turn off your wireless connection** so that it doesn't connect without you knowing.

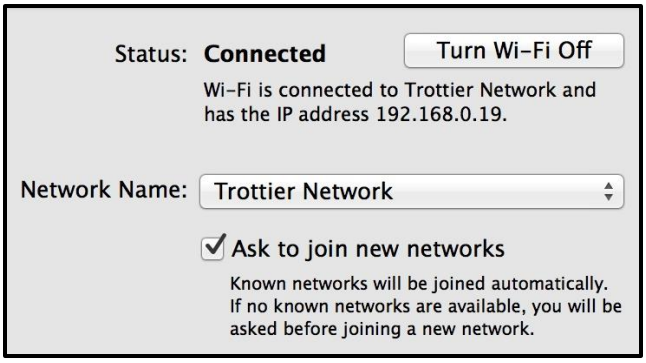
  Avoid the "automatically connect" setting so that your computer doesn't connect without you knowing.

  On a PC, go into the Control Panel and choose the Network and Sharing Centre. Then, choose "connect to a network". You will see a list of all available wi-fi networks.

  When choosing the network in your home or a trusted location, leave the "automatically connect" option checked, but when choosing a network in a public setting such as a hotel, airport or coffee shop, uncheck the "automatically connect" box.

  On a Mac, open your System Preferences, and then choose the Network icon. In the dialogue box that appears, you can choose to turn wi-fi off, and you can also select the option to be asked if you want to join new networks that are available.





- If you are using a free Wi-Fi connection in a public setting, **be sure that you are connecting to the right network**. Sometimes hackers will set up a fake network that gives them access to your information. Ask the store or restaurant employees what the name of the network is.

Privacy and Safety

Risk to Reputation

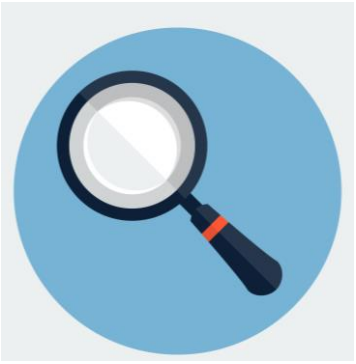
> *It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.*
>
> ~ Warren Buffett

Social media allows organizations to create an online presence and to interact with global communities on a virtually instant basis. While this makes social media a very powerful tool for marketing for non-profit agencies, it also represents a real risk to organizational reputation. Here are some strategies to help you develop and maintain an effective and vibrant organizational social media profile without damaging your agency's reputation.

Many people use tools like HootSuite or TweetDeck which allow you to post from both your personal and organizational social media profiles without having to log in and out of each one separately. While these are terrific time-savers, always be sure that you are posting from the right profile. There are plenty of examples of staff members accidentally posting personal tweets and comments on the organization's account!

Think before you click. Sometimes, you might want to share a bit of humour with your organizational followers. Take a moment to consider if the humour might be offensive to some readers. Fortunately, there are plenty of non-controversial photos and funny posts circulating on social media that you can share.

Monitor your social media accounts. While it's great to post regularly, it's also important to read what your followers might be posting to your account. Sometimes people will post spam or inappropriate content, so you want to remove this as soon as possible. Leaving your accounts unmonitored leaves you exposed to reputational risk. You can easily set up alerts from your social media profiles that will let you know when someone has posted to your wall or mentioned you in a tweet, so you can easily keep an eye on your accounts without having to log in multiple times each day.



Privacy and Safety

Appoint a social media spokesperson or “lead”. One or two people in your organization should be given the responsibility to maintain your social media accounts. This allows for consistency in messages and makes it easier to adhere to your social media policies. It also reduces your exposure to reputational risk.

Sharing pictures and personal stories on social media can be a very powerful tool for non-profit agencies when it comes to marketing and promotion. However, be sure that you have the proper consent from anyone appearing in any photographs or videos that you post on any of your social media accounts or on your website. Be sure that everyone understands that their picture may be shared far and wide by hundreds or even thousands of people. Always double-check to make sure that everyone involved – staff, students, clients, volunteers – is aware of just where their picture will be shared and how it will be used.

In terms of pictures and images from external sources, them with **caution**. Ensure that you are infringing copyright. Do not use images from Google images, Pinterest, etc. in your social media postings as many of these are not copyright free. Instead take your own pictures, purchase pictures and images legally, checking copyright before posting, or create your own beautiful images using free tools such as Canva.

Remember! Once you have hurt your reputation, it can be difficult to re-establish it, so use care and judgement in your social media activities and postings. Developing strong social media policies for your nonprofit organization is a great first step towards managing your online reputation!

Privacy and Safety

Sample Policies

If you haven't yet created a social media policy for your agency, Community Literacy of Ontario encourages you to use our Social Media Guidelines to help you develop your policy:

Community Literacy of Ontario believes in using social media in a way that informs, inspires and shows respect for people.

To ensure a professional online presence, CLO's social media accounts will follow these procedures:

- No staff member or volunteer may create any kind of a social media account in CLO's name without approval from management
- Only people approved by management may make social media postings on CLO's behalf
- CLO's management will ensure that all social media accounts have proper security and privacy controls
- It is the responsibility of CLO's management to ensure that all postings made by CLO are appropriate

All social media postings made by CLO will:

- Show respect for human dignity
- Respect the spirit of the Ontario Human Rights Code
- Respect CLO's core values
- Respect people's privacy and confidentiality

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

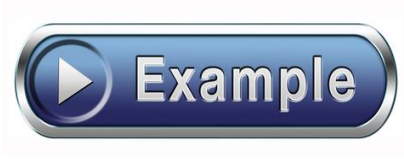
- Defamatory or offensive postings, including swear words or verbal abuse
- Postings that are racist or sexist in nature or are a violation of human rights
- Postings that are against the spirit of the Human Rights Code
- Postings that are politically partisan or sectarian in nature
- Postings from external individuals or organizations that are intended to solicit business for an external individual or company
- Spam comments

Unacceptable comments will be removed from our social media accounts. Repeat offenders will be warned and, if necessary, banned from our social media accounts.

Privacy and Safety

Sample Social Media Policy

This policy was created based on a number of examples that CLO found during the course of its research for this project.



Our workplace supports the responsible use of social media. Therefore, we have prepared the following policies to guide the use of social media.

- In order to maintain personal privacy, staff members who participate in social media in the workplace are encouraged to establish a work-related social media profile that is separate from their personal profile.
- Staff members who participate in work-related social media will ensure that strong privacy controls are used, and that these controls are reviewed and updated regularly.
- Only authorized individuals may post updates to our organization's social media accounts, website and other online presences.
- Any information posted to our organization's social media accounts, website or other online presences will avoid controversial topics and will respect human rights and dignity.
- Inappropriate photographs and/or language will be deleted from our organization's social media accounts.
- No staff member, volunteer, client or student may create a social media account for our organization without approval from management.
- No staff member, volunteer, client or student may post or tag the name, photograph or other identifying information of another staff member, volunteer, client or student without that individual's knowledge and permission.

Privacy and Safety

Sample Digital Technology Policy

The following policy was developed by CLO staff, based on numerous examples that we found in our research. It is a very comprehensive policy and may include more detail than some agencies need, but it can be adapted to suit individual agency needs.

Our workplace wishes to encourage the correct and proper use of digital technology and expects that technology is used during the normal course of work. We wish to encourage appropriate internet use. This policy outlines how our staff and volunteers can use digital technology professionally, ethically and lawfully, while maintaining the safety and security of information and property, without compromising confidentiality.

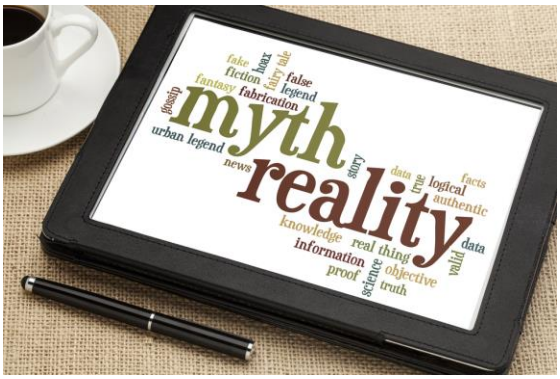
Our workplace provides internet access for its staff, volunteers, clients and students for learning, teaching and administrative purposes. Internet use may be subject to monitoring, including sites visited, as allowed by law. Any individual using digital technology inappropriately could put our workplace and/or its employees, volunteers, clients and students at risk.

No one shall:

- 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;
- Disclose financial or operational information that is not public;
- Disclose or share personal information about other employees, volunteers, clients and/or students;
- 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; and
- All volunteers and staff members shall create and use strong, secure passwords. These passwords will be kept confidential and only be shared as needed with approved individuals.

Privacy and Safety

Myth Busters



There are plenty of myths around cyber risks and technology in general. In this section, we'll separate some of the common myths from fact.

I installed security software years ago, so I'm safe.

Security software can be very valuable and can definitely help you avoid dangerous websites or unsafe files, but in order for it to be effective, it needs to be updated regularly. New internet viruses and scams are constantly being invented, and good security software companies will provide updates to keep you protected from the latest threats.

I use a Mac, so I'm safe

While Apple and Macintosh products are less likely to become infected, Apple and Mac users can transmit infected files or links (often without knowing). If you are a Mac user, be sure to take precautions to avoid inadvertent sharing of viruses and infected files. You don't want to be known as the Typhoid Mary of the internet world!

I never download anything, so I'm safe

Unfortunately, computer "infections" can be caught from more than downloads. Some websites are set up as "phishing" sites, which means that they look like legitimate websites but are, in fact, designed to steal your information. Good security software can help identify these dangerous sites so you can avoid them. It is also good to know some communications basics, such as the fact that banks will never send you an email asking you to go to a website to update or verify your password. This type of email should be deleted immediately.

I don't go to porn or gambling sites, so I'm safe

Legitimate websites can be compromised or hacked into, so it is possible to be scammed at any website. There are also dangerous websites that pose as legitimate sites, and it can be difficult to identify them without security software.

Privacy and Safety

I've been online for years, so I'm safe

Don't get complacent! New security threats crop up regularly, so it's important to stay up-to-date and keep your security software current.

Social media is a waste of time

It's true, people can lose hours of time following their friends on Facebook or checking out Twitter links. However, social media is also a very valuable marketing tool, and it's important that non-profit agencies take advantage of how it opens up the world, virtually for free.

Resources to Learn More

- Making a Good Password. Privacy Rights Clearinghouse, 2019.
- Birnbaum, Elisa. Social Media: What's your policy? Charity Village, May 3, 2011. This article provides some food for thought when developing your social media policies.
- Community Literacy of Ontario. Reducing Risk/Protecting People: Focus on Cyber Risks. This downloadable newsletter provides tips, tools and resources for staying safe online. (January 2013)
- Cyber Risks. This one hour, recorded webinar is part of a series of four produced for the Reducing Risk/Protecting People project. Tips, tools, resources and sample policies are included. (Community Literacy of Ontario, 2013)

Privacy and Safety

- Davidson, Cindy. Reducing Risk/Protecting People: An Annotated Guide to Risk Management Resources. This downloadable guide offers many resources for all areas of risk management, including cyber risks. (Community Literacy of Ontario, 2013)

- Get Safe Online provides information about staying safe on both your computer and your mobile devices.

- Internet Safety. This online module from GCF LearnFree is useful for administrators, tutors, learners and volunteers – in short, everyone will find it helpful.

- Kennedy, Bill. Heartbleed bug leads to much heartbreak for charities. Hilborn, April 23, 2014. This blog post provides a good overview of some of the risks and strategies charities (and non-profits) should consider when thinking about their online presence.

- Trottier, Vicki and Joanne Kaattari. Playing it Safe: Cyber Risks & Internet Safety. This Kindle e-book provides tips, tools and resources for staying safe online. (Community Literacy of Ontario, 2013)

- Wade, Jared. The Risks of Social Media: Self-Inflicted Reputation Damage. Risk Management Monitor, April 23, 2010. This blog post addresses ways you can control your agency's reputation online.

- How To Protect Your Social Media Privacy. This e-book from Trend Micro provides a good overview of privacy concerns that should be considered when using mobile devices.

- Wireless and Mobile Device Safety. GCF LearnFree.

Privacy and Safety

80 Bradford Street, Suite 508, Barrie, Ontario L4N 6S7
EMAIL info@communityliteracyofontario.ca
TEL 705-733-2312 | WEBSITE www.communityliteracyofontario.ca
TWITTER @Love4Literacy | FACEBOOK www.facebook.com/CommunityLiteracyOntario

Acknowledgements

Privacy and Safety was written by Vicki Trottier as part of Community Literacy of Ontario's Social Media Marketing project. All information and websites provided in this module were accurate at the time of publication. Date of Publication: March 2015.

CLO's Social Media Marketing project was funded by the Ontario Trillium Foundation.

Ontario Trillium Foundation / Fondation Trillium de l'Ontario

An agency of the Government of Ontario.
Un organisme du gouvernement de l'Ontario.

Connect with Community Literacy of Ontario via: