Staying Safe with Social Media

Thomas MacEntee, of Genealogy Bargains
http://genealogybargains.com genealogybargains@gmail.com

The ability to connect with others through the Internet and, namely social media, brings great opportunities, but also issues, complications and problems which can turn a fun journey of sharing into a bad experience. It all comes down to common sense really: educate yourself, act responsibly and take action when needed.

Best Practices

The formula for a successful online experience involves these basic components:

- **Educate yourself**. Know the terms of service and privacy settings for each site; know your friends and followers; know how your information is being used, etc.
- **Act responsibly**. Avoid e-mail links and offers to build followers; reveal shortened URLs before clicking; don't play games and quizzes; don't use location-based services; limit the information you share, etc.
- **Take action**. Block some applications and even some followers when necessary; set security precautions including using dummy e-mail addresses or an alias; be proactive rather than reactive, etc.

In-Person vs. Online

Many users forget that our actions online via e-mail, social media sharing, etc. cannot communicate the same way that in-person interaction can. There are no non-verbal cues, no way to easily interpret actions, etc. How often has the meaning of an e-mail to a friend been misinterpreted accidentally?

Now take that same situation and apply it to social media which can compound the problem 1,000 fold (or however many friends and followers you might have). Interacting with others online is very different than interacting in-person and we often forget this. Again, common sense rules and sometimes we just need to pause and think before we click the Send or Enter button.

Ways to Stay Safe

Here are some tips and tricks and words of advice on how to stay safe online, especially when using social media sites:

Terms of Service and Settings

- **Read and understand the terms of service (TOS) agreements at all sites**. It is your duty before signing up and using a service to know how your information will or will not be used by that site.

© 2020, copyright Thomas MacEntee. All rights reserved.

- **Be responsible – know the privacy settings available for each site you use**. It is your responsibility to understand how privacy settings work and then decide which settings are best for you. Do not automatically accept the defaults provided by the site. When in doubt, check the Help section of the site.
- **What types of information are gathered on social media sites?** It really depends on the site but it is still your responsibility to know. Once you add an application, on Facebook for example, immediately go to Privacy Settings and see what data the app is collecting. Very often you can change the settings to block some or all of the collecting features. Or simply remove the application if you don't feel comfortable with the collecting arrangement.
- **Stay up-to-date on changes to a site's policies**. This means reading the e-mails about updates to a site's TOS or privacy policy. Some sites have forums or RSS feeds where you can subscribe and get alerts. Again, you need to stay in the loop on what a social media site is doing with your information. Check out the site Terms of Service Didn't Read (https://tosdr.org/) to compare various websites and their terms of service policies.

Privacy

- **Limit the amount of personal information you display**. This means information you display publicly and to friends or followers. Don't include your birth date, hometown and other items of information used to verify personal identity. Remember: once posted, often it's always posted.
- **What does your employer see about you on social media?** More and more employers are doing research about their employees on social media and they don't always like what they find. Make sure you don't share information publicly and make sure you know who you are allowing to see your personal information.
- **Be anonymous if you want**. This isn't always easy to do but no one said you have to use your real name. Some sites like Facebook don't allow fake names and will either shut down your account or convert it to a Facebook page. Still, you might consider adopting an alias for social media accounts.
- **Is your birth date public?** Facebook requires you to enter your birth year when signing up (to verify that you are over 13 years of age to meet their terms of service requirements) but make sure you go to Privacy settings and set the display settings to not show your birth year, at a minimum.
- **Never give out your e-mail password – even to a social media site**. Facebook and others try to convince you to find all your friends via your e-mail address book. Sounds like fun, right? Not if that site later on uses your contacts to send advertising e-mails etc.
- **Don't post your daily routine**. Again, just like location-based check-ins, don't let strangers know your daily habits such as walking to work, etc.

© 2020, copyright Thomas MacEntee. All rights reserved.

Friends and Followers

- **Use sites that are permission-based**. This means you need to allow people to follow you or see your content/information. Example: With Facebook, you can grant permission before another user becomes your friend and has access to your information.
- **Do you really know your friend's friends?** Remember what Mom used to say about knowing your friends' friends? Do you really know them? The same is true with social media. Avoid privacy settings that allow anyone who isn't your friend to see your information or to even comment on status updates and photos.
- **Mutual friends matter**. When receiving a friend request on Facebook, do you have mutual friends? If so, it is likely that the person is legit. Ask the person how they know you and why they want to interact with you on the site.
- **Don't race to build followers**. Sure and steady wins the race, as they say. Who said you had to have 5,000 followers right away? Almost all e-mails offering to increase your followers are scams and they only want your login credentials to that social media site. Besides, what would you really do with 5,000 followers?
- **Unfriend when needed**. Have no qualms about pruning your friends or followers list especially if a person does not respect your privacy or shares information about you inappropriately.

Games and Applications

- **Games can be misleading**. Do you really know what you get into when you agree to download a game app in Facebook or another social media site? Again, read the Terms of Service. Many games seem like fun but they are collecting data on what you click on within Facebook or another site and some games even follow what else you do on your computer or on the Internet.
- **Understand how 3rd party applications work**. A site may ask you to authorize using it with another site via an application so that when you post content to one site it may appear on your Facebook page etc. Take time to read the Terms of Service for that application as well as how it will be using your content!
- **Quizzes: wrong answer!** They seem like fun don't they? You answer questions about yourself and share it with friends on social media. But have you ever looked closely at what type of data is being collected? Birthplace, birthday, school info . . . all items that can be used to steal your identity. Avoid quizzes and don't perpetuate them by sharing with others.

Pitfalls and Stuff to Avoid

- **Avoid e-mail links to add friends/followers or to add applications**. This is a common way to pick up a computer virus. Go to the original site and you should use the notification there to add friends and content.
- **Check-in or check-out?** Location services are a hot ticket these days with many folks stating where they are and who they are with, but who's watching the house

© 2020, copyright Thomas MacEntee. All rights reserved.

or minding the store? Don't advertise your location activities publicly, especially concerning vacations and the like.

- **Beware of shortened URLs**. With the increasing popularity of social media, spammers have taken advantage of the increase use of shortened URLs to hide their links. Use a program that can reveal the true web address of a shortened URL (like **Check Short URL** at https://checkshorturl.com)
- **What about copyright and social media?** Yes, copyright still applies when using social media. This means you should use the various share buttons associated with a web page or blog post instead of copying the text and pasting it into a status update. Share content responsibly and legally.

Take Action

- **Block and report spam posts and spammers**. Most sites have mechanisms to mark an update as spam or in violation of the site's Terms of Service. In addition, report specific users if they violate the rules of the site.
- **Reserve your name on social media sites**. Sign up with multiple sites in order to protect your identity. Use a site like **NameChk** https://namechk.com) or **Know'em** (https://knowem.com/) to see which sites are already using your name.
- **Social media is not kid's stuff**. Know what your children are doing on social media and monitor their activity when appropriate. The minimum age for Facebook is 13 years, although many children younger than that age are using the service. Make sure your children understand all the rules including yours!
- **Learn to post privately**. This means knowing the difference between a public post and a private post. And don't forget that when you post publicly, on Facebook for example, it will remember that setting! Always check the setting before posting and change back to private when needed.
- **Use a "burn" e-mail address**. Set up a dummy e-mail account that you only use with social media. Forward the account to your real e-mail account.
- **Use strong passwords**. Take time to construct a password that is easy for you to remember but not for a hacker to guess at. Avoid names of family members, locations etc. Use combinations of letters, numbers and special characters.
- **Fake your security information**. When asked for security information, either use fake data or provide information that others would not know about you. Example: for mother's maiden name, who said it has to be your mother's maiden name? Be consistent with usage across all social media sites.
- **Install a good antivirus and spyware protection program on your computer**. You don't need to spend a lot and some programs are even available for free!

© 2020, copyright Thomas MacEntee. All rights reserved.

Resource List

- **Check Short URL**
  https://checkshorturl.com/
- **Electronic Privacy Networking Center**
  https://epic.org/privacy/socialnet/
- **Facebook Account Security**
  https://www.facebook.com/help/security
- **Facebook Privacy**
  https://www.facebook.com/about/privacy/
- **How to Use Facebook Privacy Settings – Consumer Reports**
  https://www.consumerreports.org/privacy/facebook-privacy-settings/
- **Know'em**
  https://knowem.com/
- **NameChk**
  https://namechk.com/
- **OnGuard Online.gov**
  https://onguardonline.gov/
- **Privacy Rights Clearinghouse**
  https://www.privacyrights.org/
- **Social Networking Privacy: How to be Safe, Secure and Social**
  https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social
- **Stay Safe Online**
  https://staysafeonline.org/
- **Terms of Service Didn't Read**
  https://tosdr.org/

© 2020, copyright Thomas MacEntee. All rights reserved.