20 Tips for Staying Safe Online

GENEALOGY BARGAINS HTTPS://GENEALOGYBARGAINS.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.

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.
- ☐ **What types of information are gathered on social media sites?** Once you add an application, on Facebook for example, 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.
- ☐ **Be responsible – know the privacy settings available for each site you use.** Understand how privacy settings work and decide which settings are best for you. Do not automatically accept the defaults provided.
- ☐ **Stay up-to-date on changes to a site's policies.** Sign up for and read the e-mails about updates to a site's TOS or privacy policy. Check out the site **Terms of Service Didn't Read** (https://tosdr.org/) to compare various website terms of service.

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, etc., used to verify personal identity. Remember: once posted, often it's always posted.
- ☐ **Never give out your e-mail password – even to a social media site.** Facebook and others offer 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.
- ☐ **Is your birth date public?** Facebook requires you to enter your birth year when signing up. Make sure you check Privacy settings and set the display settings to **not** display your birth year, at a minimum.
- ☐ **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.

Games and Applications

- [ ] **Games can be misleading.** 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 via an application so that when you post content to one site it may appear on your Facebook page etc. Understand how that application will be using your content!

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.

- [ ] **Quizzes: wrong answer!** 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 identity. Avoid quizzes; don't share online.

- [ ] **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 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 reveals the true web address (like **Check Short URL** at https://checkshorturl.com)

Take Action

- [ ] **Learn to post privately.** This means knowing the difference between a public post and a private post. When you post publicly on Facebook for example, it remembers that setting! Always check the setting before posting; change back to private when needed.

- [ ] **Use strong passwords.** 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.

- [ ] **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!

- [ ] **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.

- [ ] **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 actual maiden name? Be consistent with usage across all social media sites.

- [ ] **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.