Should You Hand Over Personal Information?

Everything you do online generates data. Every time you shop, click, scroll, like, message, play and more, you are generating data. This personal information has tremendous value to businesses. When creating online accounts, we are always asked for basic information and to agree to Terms of Service conditions. Should we click “agree” or is it better to “not agree?” Check out the top five questions to consider before handing over personal information.

1. **What is this company doing with my information?**
   - Ever wonder why you get so many spam phone calls or pieces of junk mail from places you’ve never heard of? That’s because companies often sell and trade data including your email addresses, phone numbers, or home addresses. Most people do not have time to thoroughly read a Terms of Service Agreement. You can use the website “Terms of Service: Didn’t Read” for a short summary of how the most popular websites and apps use, protect, and store your information when you click “agree.”

2. **Does this company own my content?**
   - The truth is anything you agree to in a Terms of Service agreement is binding. Instagram, for example, does not take ownership of your photos, but by posting images to their platform you are giving the company license to distribute, modify, publicly display, translate, copy, and create remixes with them.
   - One way to ensure your content is used in ways you approve of is to skim the terms of service. You can do quick searches for key terms like “Permissions You Give to Us” to read up on how the company uses your content.

3. **What is this company’s reputation?**
   - Before buying anything from the internet and handing over your credit card number or bank account information, take a few moments to do an internet search on the name of the company you are purchasing from. What do previous customers have to say? Are there any red flags in your search?
   - You can also add a layer of protection to your web browsing with a tool like the Norton Safe Web browser extension which gives websites safety ratings.

4. **Is my child protected from identity theft?**
   - Children are attractive targets for identity thieves and the more frequently children hand over their personal information, the more likely they are to become a victim. Read this article from LifeLock by Norton about how to protect your child from identity theft.

5. **Am I giving more information than I need to?**
   - Many apps and websites ask for permission to access your location, microphone, camera, and contacts. If you will not benefit from sharing this access, don’t.
   - Anytime you choose to log into a site using your Facebook or Google credentials, you are sharing data between the companies. Consider setting up separate usernames and passwords on each site if you have a privacy concern. Use a password manager to help you keep track.

Remember:

- Privacy settings should not be something you set once and never think about again. It’s a great idea to revisit your privacy settings on a regular basis to ensure you have control over your information.
- Watch this video tutorial for 4 Easy Steps to Keep Your Devices Safe.
- When possible, talk through your privacy decisions with your children. Model how to modify settings and explain your choices as you do so.