



How to Protect Yourself, Your Children, and Your Business When Using Social Media

An increasing majority of the American population uses social media to connect with their friends, relatives, colleagues, teachers, clients, and people they may have never met. Users are sharing unprecedented amounts of information including photographs, videos, and geographical data, often with few privacy settings or filters in place. Therefore, private information is available on the public domain with consequences that many adults, children, and businesses may not realize.

For many adults, privacy is the number one concern when using social media. It is very difficult to delete or remove information from the internet once it has been posted, which lengthens the lifespan and consequences for posts. However, most adult users are aware of these dangers and normally practice restraint.

Children are a different story. Many use social media at a younger age than ever before and parents are primarily concerned about their children's safety online. Most children do not understand the implications (both short- and long-term) of the information they share online and the potential risks to themselves and those around them. Since computers and digital devices are an integral part of our culture and children can use them for educational purposes as well, they cannot be ignored.

Reputation is the number one concern of most companies online. Businesses are in a unique position with respect to social media – it can be an incredibly powerful marketing tool, but can also open the door to liabilities, lawsuits, and risk from competitors. Unfortunately, businesses can no longer avoid the online community without missing major opportunities.

The following tips can help protect you, your children, and your business in navigating the online world, especially on social media sites:

1. Actively Monitor

- For yourself – Examine how much time you spend online, where you are accessing the internet, and how you might be sharing something that could invade your privacy.
- For children – Keep computers and digital devices in communal spaces and frequently check the favorites and internet history on web browsers, as well as text messages on cell phones.
- For business – Make sure you have a clearly stated and enforced computer and digital device use policy and that all employees understand the limits of their expectations of privacy and the appropriateness of online business-related posts.

2. Risks of Sharing

- For yourself – Be aware that everything you say online may be archived and used later. It can be helpful to think of yourself as a

politician being elected to office and that any angry posts, re-tweets, or risqué photographs may be shown during your campaign.

- For children – Have discussions about all of the consequences of online posts for them and everyone around them. Make sure they know that even seemingly innocuous information (such as an address) can become dangerous when used in the context of other posts (such as a time they will be leaving on vacation) – in that instance, a potential thief now knows your address and exactly when your family will be out of town.
- For business – Examine potential posts or tweets from your competitor’s standpoint. Could they take business, customers, methods, procedures, or anything else that would be a competitive advantage based on what you are sharing online?

3. Know the Technology

- For yourself – Know the capabilities of your digital devices (including your cell phone) and take extra caution when using a public wireless network - many do not have any type of security and you may be inadvertently revealing your passwords. Recognize that many digital devices have GPS tracking and some apps are designed to broadcast that information.
- For children – Teach them the same things you just learned about your own devices, and remind them of the risks of sharing (above). This is particularly true if their online identity is tied to any devices with GPS capability. Note that many gaming systems have internet access and group user capabilities.
- For business – Don’t just assume the IT staff has secured all the computers, servers, and devices at your offices. Protect proprietary information by restricting access to only those that really need it.

4. Know the Access

- For yourself - Be aware of all the places you access the internet and edit your use for the particular situation – for example, don’t work on a confidential business document at a coffee shop or on any other public wireless network.
- For children – Know all of the places your children can access the Internet and (where possible) ask questions about any available filters or blocked sites. Most schools have sophisticated systems in place, but the computers at their friends houses may not.
- For business – Know what sites you and your employees can visit while at work. Ensure that everyone is aware of the risks of sharing corporate information and who is in charge of the company’s online presence.

5. **Equip Yourself, Your Children, and Your Business to Judge** - After examining the places that internet access is available, the types of posts that are appropriate on social media, and the consequences of social media use, you have given yourself the best tools to judge proper Internet use. Remember, no one can be anonymous on the Internet and it is very important to balance the risks and benefits of posts in every context.

Avansic has developed an in-depth presentation on this topic that can be given at schools, organizations, and professional groups. Please contact us at beth.downing@avansic.com or 888-808-0337 for more information.