Oversharing: How Much Information is too Much on Social Media?

Social media can be a fun way for kids to connect with each other, but it's important to understand the risks involved in sharing information over the internet in order to prevent identity theft and have a safe experience. The Office of Privacy Protection offers the following tips on managing your digital footprint:

What information should remain private: Just like when we were taught how to safely cross the street when we were little, look both ways before you post. Be aware of the information your child shares online. Disclosing personally identifiable information on the internet such as name, address, Social Security number, date of birth or phone number could put your child at risk of identity theft. Warn your child about opening emails from strangers or clicking on links for unfamiliar sites. It is important that your child choose a screen name and email address that does not include their real name.

Think before you post: Once it is out there, you can't take it back. Educate your child on the public nature of the internet. Emails, photos and video can easily be copied and posted elsewhere. With each post, like, share, check-in or status update, your child reveals bits and pieces about them self and their family. Talk to your child about what "personally identifiable information" is in order to help them understand what is appropriate to share and what is not. Encourage your child to think about the implications before each post.

Online actions have consequences: Information shared online is difficult to erase and may leave a lasting impression. It's fun to be the first to share a photo from a great weekend or a silly video of friends, but it could end up in the wrong hands. Photos and video can provide insight into the names and locations of family and friends through GPS data embedded in the digital file. An identity thief can use this data to access your personal information and commit fraud. Be sure to disable GPS location services on your digital devices and remember: even if you think you deleted information from a site, older versions may exist on someone else's computer. What happens on the internet, stays on the internet.

Use privacy settings: Most social media websites and mobile applications have privacy settings, make sure to review them with your child. If your child is under 13 years old, you can decide if you consent to their use of social networking sites. Adjust privacy setting so that information is viewable only by friends and family. Also, disable location settings and use a secure Wi-Fi network. Help your child to create strong passwords that include numbers, symbols and a mix of upper and lower case letters. The motto is "long and strong". Remind your child never to share their passwords with anyone.

Talk to your kids: Start talking to your child about their online activity early and talk about it often. Establish an open environment where your child feels comfortable discussing their internet habits. Explain the implications and risks involved in sharing personal information in public forums. Create a contract with your child outlining the rules of computer use, including time limits and appropriate sites to visit. It is a good idea to keep the computer in a central location in the house where you can monitor your child's actions. Above all, be patient and demonstrate an interest in your child's online activity.

For more information, visit us online or call the Consumer Protection Hotline at 1-800-422-7128.