CYBER SECURITY
newsletter

PROTECTING YOUR FAMILY

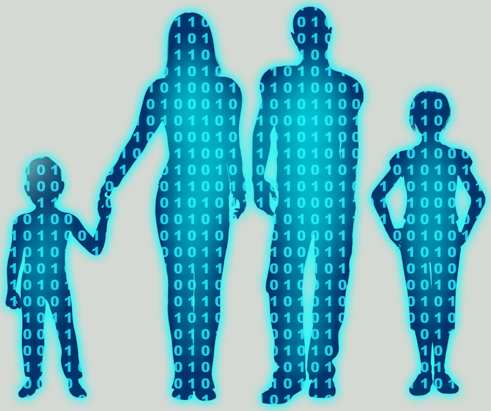
Problem

We understand that security is not just an issue at work, but also an issue for you at home. If you have children, they are most likely using computers and actively online. While we want them to develop the skills and experience they need to be successful in the 21st century, we also have to help protect them against today's cyber risks. In general there are three types of dangers that your children face when online; strangers, friends and themselves. We will explain each of these risks and how you can protect your children against them.

Strangers: Just like in the real world, there are strangers that may attempt to hurt our children, either physically or emotionally. These types of predators often pretend to be children themselves when online, then try to build trust with other children, such as in online chat forums. Once they have this trust they then exploit it for their own purposes.

Friends: Also just like the real world, your child's friends can also be a risk. Just as you may have been bullied when you were a child, so to may your kids, but online through cyber space. Other children may make fun of or harass your kids by posting mean comments on websites such as Facebook or send harassing messages via mobile phones. In addition you or your child may not even know who is posting these harassing messages.

Themselves: Finally, the third risk is your child themselves. In today's age your child may be sharing too much information. This information can lead to things such as identity theft or having online accounts compromised. In addition, as children get older the information they post about themselves can impact their future. For example, college admissions or new employers often conduct background checks by seeing what information kids have posted online about themselves.



Protecting Your Family

The Internet provides tremendous opportunities for your children, not only for learning but in their social life. However with these opportunities also come risks. We discuss the top three risks to your kids and what you can do to protect them.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

Facebook

Often one of the most common concerns we hear from parents is Facebook. As you most likely already know, Facebook is the world's largest social networking site with literally hundreds of millions of users. Social networking sites allow users to create an account, post information about themselves, then share that information with the rest of the world. Facebook states that children must be at least 13 years of age to use the site, but many kids lie about their age and start using it earlier.

One of the best ways to protect your kids is create your own account on sites such as Facebook, , then 'friend' your children. To 'friend' means to create a relationship and let you two share information with each other. This way you can watch and monitor your children's Facebook activities including what they post and whom they are sharing with. For younger children you may want to have additional rules, such as they must get your permission before 'friending' anyone else.

Fortunately, by following some basic steps you can help protect your kids against these online risks. We recommend the following.

First, and most importantly, be sure you and your children are talking. Make sure they are aware of the risks we just discussed, that they are careful whom they talk to and that they do not share private information. Ensure your kids feel comfortable to approach you if they have questions, are approached by strangers online, or are the victim of cyber bullying.

Second, have a dedicated computer just for your children to use. This ensures they do not accidently infect your computer which you may use for confidential activities, such as online banking. In addition, have their computer in a public, high traffic area so their activities can be monitored.

Third, establish some basic ground rules for online use, then have those rules posted by your kids computer. The rules can include things such as how long they can use the computer, who to report problems to, and what they can or cannot do online.

Finally, most operating systems now include filtering and monitoring capabilities, or you can purchase commercial software that does the same. Filtering allows you to control what your children can do online, such as what websites they can visit or whom they can communicate with. This is especially effective to prevent younger children from accidently accessing harmful content. Even more important is monitoring, make sure you log and review what your children are doing online. There are a variety of solutions now a days that can generate detailed reports, including what children are searching for, the videos they watch on YouTube, and their actual chats with their friends online.

The Internet is a powerful tool for children to grow and learn. In addition we want to ensure that our kids are armed with the skills and knowledge to be successful in the 21st century. By playing an active role in your children's online activities you can help ensure they are safe and successful.