PROTECTING YOUR KIDS ONLINE

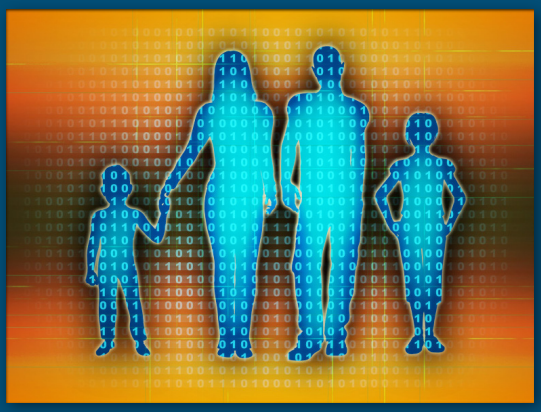
The Challenge

We know and 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 are 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, then cover how you can protect your children from them.

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.

Also just like the real world, your child's friends can be a risk. Just as you may have been bullied when you were a child, so too 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.



Protecting Your Kids Online

The Internet provides tremendous opportunities for your children, not only for learning but in developing 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.

Finally, the third risk is your child themselves. Children may often share too much information. This information can lead to things such as identity theft or having their 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 about themselves.

St Luke's

This newsletter is published by St. Luke's IT Security.

For more information or to report an IT Security incident, please contact the St. Luke's Cyber Security Incident Response Team (CSIRT) at csirt@slhs.org

© The SANS Institute 2013

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 with 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. Make sure your children do not have administrator rights on this computer and that it is properly secured.

- 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 you can use technology to filter and monitor what they do online. However, as children get older and have access to more devices both inside and outside the home, technology becomes less effective. Education is the most effective tool you have in the long run.

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.

Facebook

Often, one of the most common concerns of many parents is Facebook. Facebook is the world's largest social networking site, allowing users to create an account, post information about themselves, and share that information with the rest of the world. Facebook rules state 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 way 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 that enables you to share information with each other. You can then watch and monitor your children's Facebook activities, including what they post and whom they are sharing information with. For younger children, you may want to have additional rules, such as requiring they must get your permission before 'friending' anyone.

© The SANS Institute 2013