August 2010

MONTHLY Cyber Security Newsletter

Security Tips

Mississippi Department of Information Technology Services

Division of Information Security

This issue…

This month's newsletter provides you with information regarding online protection for children.

Get involved…

Now more than ever, parents must monitor their children's internet activity – teens included.

Many kids are hooked on social networking sites such as MySpace, Twitter and Facebook, but most are unaware of the dangers associated with the Internet and these various Web sites.

Protecting Children Online - What are the threats online?

Children are spending more of their time online than ever before. According to one study, 8-18 year-olds spend an average of 1.5 hours a day using a computer outside of school[1]. As use of the Internet and online technologies becomes more ingrained into our everyday lives, it is important we ensure that our youth understand how to use these powerful tools and how to protect themselves from becoming cyber victims. Children of all ages face online risks, including the following:

- **Inappropriate Contact**: Children may come in contact with individuals with malicious intent, such as bullies and predators.
- **Inappropriate Content**: Children may be exposed to inappropriate content while online, such as violent or sexually explicit material.
- **Inappropriate Conduct**: Children have a sense of anonymity while online and may do things that they would not do when face to face with someone.
- **Identify Theft**: Because of the perceived sense of anonymity online, children may post personal or identifying information that can then be used by identity thieves.

How do I keep my children safe?

There are steps parents, educators and others who work with children can take to help keep children safe on-line:

- **Computer Location:** Keep your computer in a central and open location in your home.
- **Establish Rules:** Create guidelines for computer use. Include the amount of time that may be spent online and the type of sites that may be visited. Post these rules near the computer.

---

[1] "**Generation M2: Media in the Lives of 8- to 18-Year-Olds**"
http://www.kff.org/entmedia/mh012010pkg.cfm

this newsletter is brought to you by…

MS-ISAC

www.msisac.org

www.its.ms.gov/services_security.shtml

- **Supervise Access:** Supervise computer access for children and monitor the types of sites visited. Consider using parental control tools on your home computer. These tools are provided by some Internet Service Providers or are available for purchase as a separate software package. You may be able to set some parental controls within your browser. As an example, in Internet Explorer click on **Tools** on your menu bar, select **Internet Options**, choose the **Content tab**, and click the **Enable** button under **Content Advisor**. (For other browsers, contact the vendor to determine what parental controls are included.)
- **Personal Information:** Teach children not to post or share personal information such as their photograph, address, age or activity schedule. Create a safe screen name that does not reveal personal information about the child.
- **Web Filtering:** Use web filtering software that restricts access to inappropriate websites and content.
- **Communication:** Maintain an open line of communication. Encourage children to come to you if they feel threatened online.
- **Cyberbullying:** Teach children not to respond to cyberbullies. Report incidents of cyberbullying to school administrators and local law enforcement when appropriate.

Additional Information:

Here are some resources focused on protecting children online.

- NET CETERA: Chatting with Kids About Being Online: **http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec04.pdf**
- iKEEPSafe Internet Safety Coalition **http://www.ikeepsafe.org/PRC/**
- StaySafeOnline **http://www.staysafeonline.org/content/protect-your-children-online**
- GetNetWise **http://kids.getnetwise.org/safetyguide/**
- Netsmartz **http://www.netsmartz.org/index.aspx**

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to redistribute this newsletter in whole for educational, non-commercial purposes.