

**Neighborhood Networks Quarterly Consortia Conference Call**  
**"Internet Safety"**  
**March 6, 2007**

On March 6, 2007, Neighborhood Networks held the second of four Quarterly Consortia Conference Calls for the 2007 fiscal year. The call was entitled "Internet Safety" and focused on the effects of Internet safety on children at Neighborhood Networks centers, the dangers associated with the Internet, how an organization can promote a cyber-safe community and means through which effective education strategies for community members and parents can be implemented. Guest speakers discussed strategies that center staff can employ to protect residents from Internet predators and other dangers on the Web.

One of the guest speakers, Bil Mooney-McCoy, director of TechMission's Safe Families Program, provided an overview of approaches for nonprofit organizations to protect children from online dangers. Carolyn Walpole and Dennis Shaw, guest speakers from i-SAFE, discussed Internet safety concerns from an adult's perspective, focusing their discussion on privacy issues, spam, computer security, and the use of netiquette with e-mail communication. Both organizations are Neighborhood Networks national partners.

***Highlights from the call:***

- Internet safety is an effort to primarily keep children safe from dangers to which they can be exposed on the Web. There are a number of dangers that affect children's safe online experiences. Online perpetrators, for example, interfere with a child's safe experience on the Web. One in five children has been approached by a pedophile online. Two out of five victims of abduction between the ages of 15 and 17 initiated contact with the kidnapper through the Internet. Other problematic sites promote drug use, guns or violence, gore and pornography. Such content online can be avoided through education and the promotion of child friendly sites.
- Children viewing pornography is a serious issue. Ninety percent of children between the ages of 8 and 16 have viewed pornography, mostly unintentionally. Youth with significant exposure to sexuality were more than twice as likely to have intercourse between the ages of 14 and 16 as those that did not view pornography. This is having a serious impact on sexual and at risk behavior for the children exposed to these sites.
- Child pornography is another significant problem. There are approximately 100,000 Web sites offering illegal child pornography. More astonishing is that child pornography is estimated to be a \$3 billion annual industry in which children are being exploited online.
- TechMission's Online Safety Checklist provides resources that Neighborhood Networks centers and consortia may use to enforce children's safe online experiences and include:
  - Internet filtering software that should be installed on computers in the centers and act as the first line of defense for dangerous sites. TechMission provides a free Internet filter on its Web site ([www.techmission.org](http://www.techmission.org)), called We-Blocker, and is available for downloading.
  - Prohibiting the use of chat rooms, file-sharing, and instant messaging which can lead to connections with pedophiles. The Internet is a powerful resource and can be utilized more effectively as a learning tool for children.

- o Deciding whether or not the Neighborhood Networks center's computers can be utilized to check personal e-mails, play games, view social networking sites such as MySpace, and enforce these rules.
- o Developing an Acceptable Use Policy (AUP) which states what users can and cannot do in the center, and the consequences of ignoring the center's policies. The AUP should be reviewed and posted at the center, and signed by center users. The signed copy should be kept on file in the event that a policy is abused. AUP places the burden of responsibility on the user for his/her violation.
- o Creating an online safety orientation that center staff conducts with every user. The orientation would be customized by age, with instructions about the importance of Internet safety, privacy, and the center's policies.
- o Always keeping a lab monitor in the room when computers are being used, especially by children. The monitor should be able to view the computer screens to make certain that children are not violating the center's policy.
- Mooney –McCoy highlighted several sites that could be promoted for children, such as [www.netsmartz.org](http://www.netsmartz.org), which features games, racially ambiguous characters, and trivia. Several other sites, [www.wiredkids.org](http://www.wiredkids.org) and [www.blogsafety.com](http://www.blogsafety.com), discuss ways to be safe on MySpace and other social networking groups.
- i-SAFE is a nonprofit organization that offers free Internet safety education to children in kindergarten through high school. As a federally funded organization, i-SAFE provides professional development for teachers, awareness outreach programs for parents and law enforcement, and training for the Federal Bureau of Investigation (FBI) and for local police departments on Internet safety concepts. i-SAFE also provides online programs for parents, such as a foundation program called Cyber Citizenship, which focuses on the known risks and threats from cyberspace.
- Walpole discussed e-mail netiquette which is a set of rules that the Internet community developed to guide the behavior of online users. E-mail netiquette plays a big part in Internet safety, because e-mail is a pervasive part of many online activities. There are basic e-mail netiquette terms with which Internet users need to be familiar.
  - o *Flaming* is committed when an individual sends a mean or hurtful e-mail to another person. This occurs frequently on the net, and is a form of cyber bullying. E-mail communication is instantaneous and people find it easier to say things they might not say in person.
  - o *Spam* is a type of junk e-mail, such as jokes, hoaxes, urban legends, or other inappropriate material that a person sends to many people at once. It is proper netiquette not to forward spam to others.
  - o *Forwarding* is the act of sending a received e-mail message to others, usually without editing. E-mail users should not indiscriminately forward messages for several reasons.
    - When one forwards e-mail, he/she can be giving out personal information, such as the e-mail address of the person who sent the message plus the addresses of others in the original list of recipients.
    - Indiscriminate forwarding is considered "spamming". One needs to make certain that any e-mail forwarded has a particular message that he/she would like to convey. In some cases, forwarding is necessary, however, one

has to make sure he/she knows and understands the complete contents of the e-mail including any attachments, and not include the e-mail addresses of others. Once a message is forwarded, the recipient may forward it also, which is going to provide the e-mail addresses to strangers. To avoid indiscriminate forwarding, cut and paste the content into a new message and then send it.

- *Privacy issues* are important because messages can be retrieved if they have been "deleted". They are stored on the computer's hard drive and if an adult has personal information in a message such as credit card information, social security number, and/or bank information this could lead to identity theft.
- *Phishing scams* are e-mails that seek personal information in order to defraud the recipient. The big risks range from monetary theft to identity theft. Awareness is the common protection, and never responding to e-mails from a bank or any other reputable organization requesting personal information via an e-mail reply is also strongly encouraged. These e-mail scams are very convincing, but no financial institution would ask for personal information via an e-mail communication.
- Walpole concluded the discussion by highlighting the importance of protecting computers from virus infection. As users indiscriminately download and attach files, potential viruses attached to these can eventually be encrypted into the computer. To protect computers from infections, the following safety measures should be performed:
  - Install a firewall on the center computers which will prevent virus transmission through e-mail communication to recipients.
  - Update the computers' operating system regularly.
  - Install anti-virus and anti-spyware software on the computers.

The call concluded with a general question-and-answer period for participants. The next Quarterly Consortia Conference Call will be held on June 5, 2007, when the topic will be "Changes in Internal Revenue Service (IRS) 501(c)(3) Code".