Three Threats Facing Your Children Online

We all want the best for our children, including the ability to leverage technology. With technology comes risk, though. As parents, it is our responsibility to ensure our children understand these risks and how to protect themselves. Since the majority of adults did not grow up in the same environment, with so much access to technology that connects us to other people, it can be challenging to know how best to protect them. We will attempt to explain the top three online threats to your children.

1. Strangers – The most common threat that parents think of when wanting to protect their kids online.

In this context they are individuals (usually adults) who establish online relationships with your children, in order to take advantage of them.

2. Friends – Friends can pose a serious threat as online bullies. The Internet amplifies the issue, as bullies can post harassing messages to the entire world (even anonymously) or hijack your child's identity online.

3. Themselves – Children can be their own worst enemy. Anything they post is accessible to the entire world, and may be difficult or impossible to remove.

Protecting Your Children Against Online Threats

Now that you understand the key risks, here are the steps you can take to defend against them:

- **Education**: The most important step you can take is education. Make sure your children understand these threats and that you are always talking to them about their online activities. Create an environment where your children feel comfortable coming to you with questions or problems they may have online.

- **Dedicated Computer**: Have a separate computer just for your children. This helps ensure that if they do accidentally infect their computer, your own accounts, such as online banking, are not impacted or compromised. Keep the children's computer in an open area in your home so that you can monitor their online activities. Make sure each child has and uses their own non-administrative account on the computer. This will allow you to track and enforce what each child is doing on the computer.

- **Mobile Devices**: Mobile devices can be more challenging to manage. Consider setting time limits when your kids can use them. When not being used, they should turn them in to the parents. Also consider taking the mobile devices at night so they are not tempted to go online when they should be sleeping.

- **Social Networking**: Track what your children are doing online by creating your own accounts on social networking sites such as Facebook, Twitter or Instagram and then have your children invite you so you can follow what they publish.

- **Rules**: Create a document that identifies the rules you expect your children to follow when online. Rules can include when they can use technology, for how long, what games or apps they can and can't play and what information they can or cannot post online. Consider posting how the rules will be enforced and possible consequences for violating the rules. Review the rules with your kids and post it by their computer.

- **Technology**: Lastly, there are technologies available to help filter and monitor your children's online activities. Most operating systems come with parental controls and there are additional free and commercial tools you can use, such as OpenDNS.
Tips & Tools

This section is used to provide information about security tips or tools that you can utilize on your personal computers. Please note, CEC does not support these tools (please don’t contact the Service Desk for assistance).

There are many tools to help protect your children from online content you don’t want them to see. One free solution that is widely used is OpenDNS. This allows you to customize the content filtering to your liking for all devices on your home network.

http://www.openddns.com