Internet Safety

Internet Safety and Children

The Internet can be a truly valuable resource for kids, as it can provide educational material, fun games, and ways to connect with their friends. However, it can also be a playground for cyber-bullying, malicious content, and criminals and predators who seek to prey on kids and their families

The first and most fundamental principle is that children never, under any circumstances, browse unaccompanied. They have phones/tablets or devices at which they are more adept at using than most adults I know. But these devices should be set up to forget the wifi access code so that they cannot get online without a parent/guardian present.

Teach them the importance of keeping information private

Posting personal information and photos on the Internet can be dangerous, as it can be leveraged by those who want to do harm. In addition, once information is posted, it can have damaging effects later, as it can be hard to remove once it's in the public domain. Be sure to also check their **privacy settings** on social media sites to prevent strangers from accessing personal information. These settings may not always be set up properly by default. Ensure that your kids understand:

Never give their name, phone number, email address, password, address, school name, or picture without your permission.

Don't respond to malicious or hurtful posts.

Don't open emails or attachments from people they don't know.

Don't agree to get together with anyone they "meet" online.

The Internet is filled with websites that are inappropriate for *anyone*, much less children. Kids get into trouble online all the time, even when they aren't looking for it.They know the internet is a magical entity capable of answering obscure questions; providing printable templates of pretty much any animal to colour in; and serving up endlessly-repeatable videos of startled cats, Stampy's Minecraft exploits and loom band tutorials.

What they don't know is anything about viruses, online privacy, phishing, social networking etiquette, and any other internet safety and/or security issue you can think of.

"Kids are implicitly very trusting, so it's possible that they are more likely to fall prey to a social engineering attempt and as such they need to be taught to spot them and not be afraid to question or challenge the need for disclosing things like passwords or other sensitive information in response to an e-mail, text, IM or social networking message.

Further, it's important for them to understand that anything that is put online should assumed to be permanent and they must be careful what they expose and that their identity and all that goes with it is precious.

In the case of certain environments, considering the use of a Pseudonym, not disclosing one's age or gender, and limiting identifying information for some of their interactions online is important."

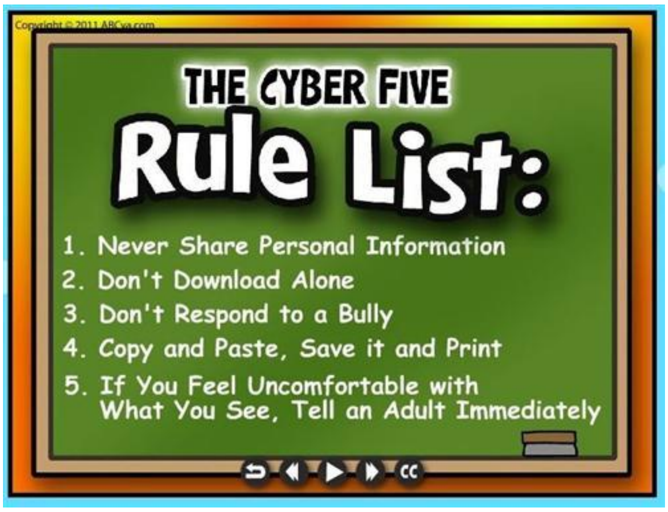
Chris Hoff, vice president, strategic planning, security, Juniper Networks

As parents, we all know it is difficult to monitor the little ones activity at all times, be sure to check browser history on a regular basis and talk about any questionable sites.

As I said at the beginning the internet has a wealth of information and can be invaluable at times so long as we regulate and monitor our children's time spent online.

(This is only a guide.

All situations are not the same.)



Copyright © 2011 ABCya.com

THE CYBER FIVE

Rule List:

1. Never Share Personal Information
2. Don't Download Alone
3. Don't Respond to a Bully
4. Copy and Paste, Save it and Print
5. If You Feel Uncomfortable with What You See, Tell an Adult Immediately