



Internet Safety Workshop – Handout

Firewall Options – Key point: use a firewall, any firewall

- Windows firewall, McAfee, ZoneAlarm

Content Filters – Key point: deploy filters for obvious inappropriate content

- Set Google and Yahoo Safe Searches
- AOL content files, Net Nanny
- Consider blocking certain chat rooms or MySpace.

Spyware/Virus – Key point: run software to check for and remove malware

- Don't download files or programs you are unsure about. This includes opening attachments from suspicious e-mails.
- Use antivirus software (McAfee, Norton, etc.)
- Regularly run anti-spyware programs (McAfee, Spybot, Ad-Aware, etc.)
- Maintain the anti-virus and anti-spyware software up to date

Physical PC Security – Key point: supervise computer usage

- Keep computer in common areas of home
- Check internet usage history / cookies, etc.
- Tell children to never give out personal information or pictures or meet with someone you met on-line without asking their parents or guardians.
- Consider invoking "online contracts" for Parents and Children like the ones found at <http://www.safekids.com/contract.htm>. Use www.safekids.com for more information on this topic.

Identity Theft – Key point: protect personal information

These recommendations and websites are based on the collective research and knowledge of the St. Ambrose School technology committee.

The final selection of what sites, concepts, ideas, precautions, software, etc. to use on their computer and share with their children should be determined by the children's parents or guardians.

- Don't give out passwords to anyone
- Do not respond to suspicious e-mails (or phone calls). Ensure the identity of the person/organization before providing sensitive information (SSN, account info, etc)
- Report suspicious e-mails to the appropriate authorities or bank – Internet Crime Complaint Center – www.ifccfbi.gov.

Other key web sites with more information

- www.wiredkids.org – for children using the internet
- www.ftc.gov – Federal Trade Commission – for reporting possible identity theft
- www.annualcreditreport.com – for getting the latest copy of your credit report. “Big Three” credit reporting agencies – www.experian.com, www.equifax.com, www.transunion.com
- www.antiphishing.org – background information on some common phishing scams
- www.missingkids.com/cybertip - National Center for Missing & Exploited Children Cyber Tip Line.
- PNC Bank Security Center – www.pnc.com, then click on “security center” at the top of the page – excellent site with lots of background information on internet security
- www.isafe.org – more information on Cyber Bullying

Who to Contact?

- **Technology issues:**
 - **St. Ambrose School Technology Committee:**
 - tech@stambroseschool.net
 - **Web sites with good Internet security information:**
 - <http://www.firewallguide.com/>
 - <http://www.wiredsafety.org/>
 - http://www.download.com/Security/2001-2023_4-0.html?tag=dir
 - Also see handout for additional sites
- **Safety questions:**
 - **Old Bridge Police Department: (732) 721-5600**
 - **FBI – Newark Field Office (973) 792-3000**
 - **FBI – Crimes Against Children Unit (202) 324-3666**
 - **National Center for Missing & Exploited Children
1-800-843-5678**
- **Emergencies:**
 - **911**