WEB SPEAK

Want to sound savvy? Add these words to your vocabulary.

Chat rooms: a form of real-time communications where participants type what they want to say, and it is repeated on the screens of all other participants in the same chat room.

Download: the transfer of information from a remote computer to the user's computer

Email: mail sent through the Internet

Instant messaging: Instant messaging, often called "IM" or "IM-ing," is the exchange of text messages through a software application in real-time. Usually included in the IM software is the ability to see whether a chosen friend or "buddy" is online and connected through the selected service.

Social networks: a service that connects individuals using various Internet software. Features include:

- Creating profiles
- Creating "communities" or groups with common interests
- Sharing (by uploading) photos, videos, and other information

MySpace (www.myspace.com) and Facebook (www.facebook.com) are the most popular social networks.

Upload: the transfer of information from a user's computer to a remote computer

Anti-virus software: software that searches the hard drive and other disks for any known or potential computer viruses

Firewall: software that protects a private network from the Internet by managing/blocking some communications from the Internet

Filtering Software: software to control content displayed, block websites, and set up passwords. Visit this site to learn about your options: http://internet-filter-review.toptenreviews.com/

Password: a secret code of letters and/or numbers that is needed to gain access to a user's profile or account

Spyware: programming that is put in someone's computer (either through a software virus or when installing a new program) to secretly gather information

Virus: a destructive program that reproduces itself and infects other programs or disks.

Morris and Rose
Goldman Computer Department
www.att.org/goldman.asp
beyondbytes@att.org

Associated Talmud Torahs
2828 West Pratt
Chicago, IL 60645

Beyond Bytes Explores **Internet Safety**

[Rabbis and educators have cautioned us about the dangers of the Internet. However, the Internet is everywhere—at work, school, libraries, and even cell phones—and is a wonderful resource for learning, informing, and communicating. Unfortunately, along with its benefits, the Internet can also be dangerous, especially for the uninformed user. The question is how do we balance the Internet's benefits with its safety issues. In the coming months the Associated Talmud Torahs will unveil a major community initiative on Internet Safety.]

* Broaden your technology knowledge at the Goldman Lab! *

DID YOU KNOW?

- The ATT's Goldman Computer Department has been authorized to approve technology plans for the Illinois Coalition of NonPublic Schools.
- The ATT is proud to host the Chicago Community Calendar on its website: http://www.att.org. To view the calendar, click Events Calendar on the home page. To submit an event to the calendar, click the "click here" at the top of each calendar page.

For more information call the Goldman Department at 773-973-2828 or email goldman@att.org.

BeyondBytes

March 2007 :: Vol. 2

BROUGHT TO YOU BY:
Goldman Computer Department of the Associated Talmud Torahs of Chicago

Internet Safety

It is fun to communicate with friends. The Internet makes it easy and in many cases spontaneous and in real time. However, most children do not consider all of the risks of sharing information. The following are safety tips when using email, instant messaging, chat rooms, and social networks (i.e. MySpace, Facebook):

- **Choose a user name that reveals nothing about you** including gender, age, location, and school.
- **Never give out personal information** including your name, email address, phone number, and school to people you do not personally know.
- **Never give out your password** to anyone (even close friends) except to parents.
- **Never arrange a face to face meeting with someone you met online.**
- **Do not post photos;** But if you do, be very selective – photos like text can be forwarded to others; they can come back to haunt you. Email is like a postcard – you never know who reads it!
- **Do not post information about yourself, family, and friends.**
- **Only add people to your "buddy list"** if you first know them in real life.
- **Be suspicious of anyone who tries to turn you against parents, teachers, or friends.**
- **Do not respond to SPAM** or any messages from unknown senders.
- **Check privacy settings of social networking sites** so you are the only one who can add a friend and that only friends can see your profile.

Remember:

- Do not do or say anything online that you would not say or do offline.
- Information that you give out can be used against you to gain your trust or to intimidate and threaten you.
- The Internet is anonymous - you never really know who is on the other side.

Tips for Parents

Being an up-to-date technology user is hard. However, according to research and experience, parents are the first line of defense in protecting their children against Internet abuse. Therefore:

- Establish strong communication and trust with your child.
- Set up a specific list of ground rules for computer use including when it can be used, for what it can be used, and how much time it can be used.
- Keep any computer with Internet access in a common room, where you can see it!
- Model good behavior while on the Internet; spend time online with your child.
- Understand the online services that your child uses; learn everything you can about the Internet (even ask your child for assistance).
- Investigate blocking and screening services offered by your Internet Service Provider (ISP) and other filtering software.
- To keep your computer safe, use a password, anti-virus software, a firewall, and anti-spyware.
- When asking about your child's day, also ask about online time as well; encourage your child to share his/her online activities with you.
- Discuss with your child whom he/she meets on line.
- Encourage your child to come to you if he/she encounters a problem while on the Internet.
- Have access to your child's online account and randomly check it.
- Find out about other computers that your child uses.
- Emphasize to your child that if he/she does not know the person in the real world, he/she does not know the person at all.
- Remember you were once your child's age – be reasonable and set up reasonable expectations.

Internet Dangers include:

- Internet addiction
- Cyberbullying
- Commercial exploitation
- Sexual predators
- Pornography

Internet use increases daily. Reality dictates that most of our children will need to use it during their lifetime. Therefore, it is our responsibility as teachers and parents to educate our children so they will not suffer Internet abuse.

SITES TO EXPLORE

NetSmarz NetSmarz Worskhop is a wonderful resource for educators, parents, and kids on Internet safety. All of the information and activities are designed on multiple levels to be age appropriate. This site include sections entitled "Keep Kids and Teens Safer," "Learn About the Issue (Internet Safety)," and "Teach Internet Safety." There is also a section entitled "Real Life Stories" documenting teens' Internet abuse experiences and flash cards and games to reinforce Internet safety rules for kids. To learn more about NetSmarz, visit http://www.netsmartz.org/.

Stop Cyberbullying It is important to be aware that adults are not the only one threatening children on the Internet. Children are also abusing other children. "Stop Cyberbullying" is a comprehensive site dealing with this potential danger. It defines cyberbullying, explains how it works, explores why children become cyberbullies, provides preventive measures against cyberbullying, and explains the role of the school and the parent to help avert cyberbullying. Visit http://www.stopcyberbullying.org.index2.html to explore this site.