CHAT

Introduction

Online Chat. Is it a valuable service allowing for human interaction in an increasingly disconnected real world? Or a vast wasteland exceeded in worthlessness only by reality television?

Tough choice.

If you think of chat as an endless string of "Hi." And "Hi Back," or mindless banter among the young, the foolish or the lost, then you clearly believe in the wasteland category. But, perhaps you think of it as something else. Yes, in the early stages of chat, it may have been a mostly empty or even silly place, with but few notable exceptions. However, chat can be used in many productive and valuable ways.

- Distance learning classrooms.
- Collaborative work among distantly remote coworkers.
- Collaborative work among colleagues who share goals. Teachers or Doctors in small or remote areas getting assistance from those in areas with greater resources.
- Support groups for those afflicted with medical problems, rare or otherwise. Perhaps those without much local support in their small community.
- Support for individuals suffering from illnesses or mental problems of an embarrassing nature. (Anything from alcoholism and gambling to depression, mental illnesses or similar.)
- Finding and interacting with others of like mind on political or other intellectual issues.
- Finding and interacting with others in the pursuit of common activities: sports, hobbies, and yes, dating too.

So perhaps chat has come of age as something of value. Like any tool, its value depends on the goals and skills of its users.

As for risks, typical chat is generally free of technical risks. Though there are two clear risks which may be associated with chat software

(also referred to as chat "clients"). There could be a security flaw in the software which someone could exploit to do harm. And if your software allows for file transfers, there is a risk you could be tricked into opening a damaging file attachment. This could occur by accident from a friend/coworker, or intentionally and maliciously by persons unknown.

The more prevalent risk for chat users are "social hacks" (p. 261) (Also known as "social engineering.") That is, lies and trickery either to accomplish specific goals or merely attempts to annoy perpetrated by social misfits. Common social hacks include Emails trying to get you to give up your password by some means. Users will also embed links into chat rooms which, when you click on them, take you to places very different from what the link text said. (See the "Social Hacking" section for more details (p. 261).

As for chat room "harassment" or lack of civility, usually your best bet is to just not engage with hostile people. It is as likely as not they intend to make you angry. Or goad you into saying something. (This is sometimes referred to as "flame bait." Flaming is defined as attacking someone else in text. Basically, this is when a conversation gets out of control. However, flame bait is not out of control. It is just someone trying to get someone else to become angry or lose control.) Such folks may be among those of the online population that either forget how to behave when hiding behind a screen name or they may be of the sort that truly have mental problems. Often people will throw around words like "harassment" or "stalking" with regards to someone being hostile with their words. Most often nothing of the sort is occurring. Being a jerk does not constitute harassment. Be careful about letting things spin out of control in chat rooms. Whether you are in a serious chat room for high minded pursuits or a more frivolous room, at all times remember that YOU OWN YOUR WORDS. Do not assume your anonymity cannot be stripped away. And remember that anyone in that chat room, and possibly others, can keep logs of what you have to say. All that being said, if after sensible assessment you truly believe that someone online means you actual harm, you should contact your local law enforcement and make a formal complaint.

Taking Action

- Awareness is your primary defense.
- Do not accept files via your IM Chat client file transfer unless

you are sure you know where they are from. Even then be suspicious.

- If your chat software allows direct connections of any sort, do not use them unless you have a very secure trust relationship with the person you're talking to and a clear idea of what it is you are doing. A direct connection may allow for file transfers or other remote access to computer resources.
- Make sure your virus program is up to date.
- Do not send your password to anyone for any reason.
- Do not enter any passwords into online forms you come to by other than "official" means. That is, Emails claiming you need to re-enter your password–for whatever reason–and provide a link to a form are most likely lies.
- Do not immediately click on hyperlinks in chat rooms unless you know the person who put them there and are confident they go to where they say they will.
- You can most often test a hyperlink before clicking on it. For example, in Windows, you may be able to "RIGHT-Click" on the link and use the pop-up menu to copy the link's target to the clipboard. Then either open an editor like Notepad or place your cursor in the Web Address/URL field. Use the Paste function. You will now be able to see where the hyperlink will send you. At this point, you can choose whether or not to follow it with some degree of confidence.
- Review the Special Notes for Kids. Many of these suggestions are appropriate advice for adults.

Special Notes: Kids & IM/Chat

Many of these rules might just as well apply to adults. But adults supposedly have the sensibility to make their own proper decisions. Children, however, need to be given clearer guidance. You must decide for yourself what age means "child" within your household.

- Rule 1. Never, under any circumstances offer personally identifiable information. This includes full real name, address or any other information which could lead someone to the child.
- Make sure there is no personally identifiable information filled out in any online profile or directory. Do not allow your child

to send their photograph to strangers. (Depending on the age of your child and what other identifying information is there, consider not having the child's picture on any personal web sites. Yours or the child's.)

- Never agree to meet in person anyone whom they have met online without parental permission. Not in a private place. Not in a public place. Any consideration of this kind must be reviewed with parents.
- If your child is old enough to be allowed to go online unsupervised, then they must be old enough for what may be a difficult conversation. You have very likely already expressed to them how to deal with strangers in real life. Online is no different. They need to be impressed with the fact that there are those in the world who would mean to do them harm. Even after multiple chats, it is possible the person they are talking to is not who they say they are.
- Warn your child to inform you if anyone they are having conversations with asks them to keep their communication "secret."
- Warn your child never to give their password out to anyone for any reason. Explain that anyone asking for this for any reason is almost sure to be lying. Tell your child to let you know immediately if someone is asking them for this.
- If you suspect, for whatever reason, that your child may be involved with someone online in an inappropriate way, discuss it. Do not wait.
- Some services have special monitoring set up for chat discussion amongst minors. Remember that this is no guarantee others in the room are confirmed as who they say they are.
- Use a special account for your child. One with their own screen name. One that cannot be easily traced back to the child. One that can be abandoned if they begin to have problems that become difficult to deal with beyond using the "Ignore" feature.
- Should you note any changes in a child's behavior, among other causes you may be considering, look into whether something that happened online may be the cause.
- Decide whether to use "spyware/snoopware" and filtering software on your child's computer. While everyone, including children, has privacy needs, you as a parent get to decide the freedom vs. security question for your children. Do understand

though, even an early teenager may be savvy enough to detect and disable this sort of thing. (Note that filtering can be software installed on the computer or you may use an Internet Service Provider that has filtering rules at their end of the connection.)

- Make sure your home is not the only child-safe computing spot. Consider anywhere else your child may have access. This includes school, public places, and friends' houses. Discuss these issues with other parents.
- If you are personally not very computer literate, you must be sure to personally visit with your child during their online activities. Be sure they understand these issues and your rules.
- If you strongly believe something inappropriate or illegal has happened, you should not let anyone use the computer. Turn it off and unplug it. You want to make sure that any files or history is left undisturbed.
- Contacting law enforcement is a serious step. Do not take it lightly. However, if you sincerely believe your child is at risk, contact your local law enforcement agency. If at all possible, get someone in their computer crimes unit assigned to your case. They will likely do this in any case if they have such a unit. If this is not possible and you are not comfortable with your local law enforcement agency's actions, consider contacting the FBI.
- On a final note regarding child safety online: Make sure they turn off the computer and go out and play sometimes.

Additional Resources

Child Safety

Child Safety Experts: www.childsafetyexperts.com
CyberAngels: www.cyberangels.org
National Safe Kids Campaign: www.safekids.org
Safekids.com: www.safekids.com

Content Filtering Software

BrowseSafe: www.browsesafe.com
CyberPatrol: www.surfcontrol.com
CYBERsitter: www.cybersitter.com
Net Nanny: www.netnanny.com