

Webcams and ooVoo: What is that?

By Robert Hugh Farley, M.S.
Consultant to the VIRTUS® Programs

Introduction

A webcam connected to a computer allows parents and children to chat with friends or relatives in real time... but webcams can also be very dangerous.

A webcam is a video capture device that is connected to a computer often using a USB port. In some computer brands or models, the video capture device is actually built into the monitor. Most webcams today have a microphone feature allowing audio. A computer, with the appropriate software installed and a webcam attached, will allow the user one-on-one, live video communication over the Internet. Webcam features and capabilities vary by the type of video software, the type of computer operating system, the computer's processor capabilities, and also by the strength of the Internet connection.

One inherent danger of webcams was seen in the 2010 nationally reported Lower Merriion School District "WebcamGate" case. Parents charged two suburban Philadelphia high schools with secretly spying on their students—by surreptitiously and remotely activating **iSight** webcams built into school issued MacBook laptops that the students were using at home. According to media reports, school administrators admitted to secretly snapping approximately 66,000 photographs, including shots of students in their bedrooms.

An additional danger is that a webcam can be used by a cyberbully to humiliate a victim. Recently, a Rutgers University student committed suicide when he became aware that a college roommate had used a hidden webcam to document a dorm room encounter that was then streamed across the Internet.

ooVoo

ooVoo is the latest free, audio and video, webcam instant messaging software that can be used with Microsoft Windows and with Apple operating systems. **ooVoo** is similar to **Skype** video software and Apple's **iChat** video software in that it allows you to have webcam conversations with friends.

ooVoo instant messaging software is also different from **Skype** and **iChat** in that it allows multi-party, video and audio calls with up to twelve locations at the same time—six on video and six on telephone.

One social networking site recently created an app (or application) that now allows "friends" to connect face to face and in live time using **ooVoo**.

Dangers

The foremost danger with **ooVoo** is the built-in recording feature that is imbedded into the software. In the past, child molesters would need third party software installed in order to record webcam conversations with children or teens. Not so with **ooVoo**, which has a video messaging feature that allow messages up to five minutes in length to be recorded and then sent to someone via email, or it can be shared with others via the Internet. In addition,

ooVoo has a video call/chat recording feature that allows a participant to record and then store the video calls on one's own hard drive. The only limit is the size of the hard drive. Portions of the video chat can then be uploaded to the Internet or posted on child molester web sites.

In addition, there is a very dangerous webcam specific Windows virus called **W32/Rbot-GR**. A child molester utilizing this virus or Trojan horse can identify that a child or teen has a webcam attached to the computer. The molester is then able to remotely activate a young person's webcam without their knowledge.

Conclusion

A computer with a webcam attached should always be placed out in an open area like the family room or kitchen and never be located in a bedroom. Parents should always monitor any webcam activity that goes on in the home because it allows an open window into the activities and lives of children and teens.

Unfortunately there are many ways to gather information from the personal items that are located in the background during a webcam video chat. This information, such as the name of a school, can be used by a child molester to locate your child or identify where your family lives.

Children who have grown up with access to social networking sites and related features may easily get carried away with the instant messaging freedom that a webcam allows, such as talking, dancing, or even dressing in front of the webcam. Furthermore, a teen with "different standards of privacy" may feel comfortable about performing risqué acts, such as between a boyfriend and girlfriend, while using a webcam.

Teens and children must understand and parents must reinforce that a webcam video stream can be saved and later watched by someone who was not the intended recipient. The video can even be posted on the Internet where, for all practical purposes, it is there forever.

Brought to you through the National Catholic Risk Retention Group, Inc. and its VIRTUS® programs with the goal to help prevent, address, and mitigate wrongdoing in the community of faith and to help adults become protectors of children and to help communities become safe havens for children.