

cybercops ...



Mirror Image

A Guide for Parents and Teachers

LIVE  **Wires**

CyberCops

Last year, Inspector Angie Howe received a call from a distraught father. While working on the family computer he had discovered explicit sexual conversations between his 13-year-old daughter and an adult man.

Detectives found several chats between the daughter and a man calling himself 'lowtheworld'. The conversations began romantically and soon the girl wrote she was "in love" with the man.

lowtheworld begged the girl to send him photographs of herself. He went to the family residence and left a cell phone in the bushes at the front of the house. Later he left a web cam. Then he asked the girl to undress in front of the camera while he watched.

So police laid a trap. Detectives created a fictitious profile of a 13-year-old girl, jessica13, and posted it on-line. A few days later, lowtheworld asked Jessica to meet him in a local restaurant. He said that later they would drive to a nearby motel.

On the day of the meeting, members of the Child Pornography team were watching the restaurant. At 8:10 p.m. the car pulled into the parking lot, the driver entered the restaurant, briefly glanced around and walked to the men's restroom. Police followed him. When the man realized an arrest was imminent, he fainted.

"When we told the teenager about the arrest, she was devastated," says Inspector Howe. "She thought this man was in love with her. It was a terrible blow to realize he was simply cruising the Internet for any teenager he could find."

Inspector Angie Howe leads the Child Pornography Section of the Ontario Provincial Police. She points out that: "The victim in this case suffered a serious, long-term depression, even though she had had no direct personal contact with the predator."



Profile of a Victim

In the early years of the Internet, researchers assumed that Internet predators lied to potential victims about their age and their interest in sex. Why else would young people exchange intimate details with strangers they met on the Internet?

In the summer of 2004, researchers at the University of New Hampshire released a report that radically altered our perceptions of how young people are lured. The study showed that 95% of predators told their victims that they were adults and 80% openly admitted a sexual interest in the teenager they were stalking.

After reviewing the data from 2,574 cases, the researchers uncovered two strategies that predators had used to lure potential victims: flattery and romance.

- Half of the victims said they were in love with the stranger they had met on-line.
- Predators also claimed to be modeling agents looking to help attractive young people gain a foothold in the industry.

Most shocking of all, the study revealed that 83% of the victims had met with the predators more than once, and fully 40% of the teens had gone to meet the predators more than three times. Clearly, the predators' on-line conversations had set powerful psychological forces in motion, so the young people became deeply dependent on their abusers.

The study "Internet-related Sex Crimes against Children" from the University of New Hampshire's Crimes Against Children Research Center was authored by Janis Wolak, David Finkelhor and Kimberly Mitchell. It was published in the Journal of Adolescent Health in 2004.



Flattery

Predators explore the Internet for photographs of good-looking teenagers. They email these teens with flattering comments, offering a modeling career. Once the teens are hooked, they can be persuaded to send photographs that are more provocative.

In a recent study undertaken with the U.S. National Center for Missing and Exploited Children, 20% of teens said it was safe to post personal information and photographs on the Internet.

- **Information and Images.** Unfortunately, digital images can be easily manipulated. A predator who finds an innocent face among the millions on a social networking website, can graft it onto a sexually-explicit photograph in minutes. Once that image has begun circulating through a child pornography network, it can never be regained.
- **Video Performances.** Predators sometimes provide webcams to potential victims as an incentive for the children to create videos about themselves. The predator follows a three-step strategy. First, he encourages children to perform: clowning around or 'mooning' the camera. Then, he praises the performances. Finally, he coaches them to try more sexually-explicit acts.
- **A Global Marketplace.** Over the last decade, police agencies have seen the rapid growth of an international marketplace. In some cases, images are swapped between individual predators. On other occasions, images are purchased from commercial child porn rings. Over time, a pedophile may amass hundreds of thousands of images of exploited children which he can use to fuel his sexual fantasies.

Agent Flint Waters of the Wyoming Internet Crimes Against Children Task Force has developed software that enables police agencies to track child pornographers. "In the last 24 months," he says, "we have identified 5.2 million transactions involving the trafficking of child sexual abuse images. We have found 1,700,000 unique IP addresses from around the world."



Romance

According to the FBI, over the last decade the number of Internet luring cases filed annually increased from 110 to 2400. With so many Internet safety programs now available, why does the number of victims remain high?

The answer, in part, lies in the nature of a seduction carried out first over the Internet, and then in person.

- **Romance.** Predators play on the romantic ideals of their teenage victims. They use symbols skillfully, promising flowers, jewelry and even marriage. Then, when the teen is 'hooked', the predator begins to send overtly sexual messages, describing what they will do when they meet. This gives the young victim a vivid mental image of the 'love affair', long before the child meets the predator in person.
- **Rewards.** Many young people become involved with predators thinking: 'I'll take the gifts, but if I don't like him I'll just walk away.' Few do. Once they meet, the predator increases the rewards, both emotional and monetary. When a pedophile makes suffocating demands, it may be almost impossible for a young person to break away.
- **Threats.** If the victim refuses to meet again, the predator can reactivate his skills as a stalker, threatening the child on-line and on the telephone. The victim lives in fear, afraid to go out of the house, to tell parents or the police. This situation may go on for months or years, leaving the victim with deep emotional scars.

Police officers use new cybertools to track children who have been lured from home. On our website, www.cybercops.net, Staff Sgt. Arni Stinnissen of the Ontario Provincial Police describes a case in which his e-Crime team discovered where a young runaway was headed, and arrived at the predator's house just as she got there.



Mirror Image was designed to open a dialogue about the tactics that predators use to manipulate potential victims. The game communicates three messages.

- 1. Recognize Predators' Tactics.** Mirror Image was designed to help teenagers recognize the tactics – such as flattery and romance – that predators use to exploit vulnerable teens.
- 2. Protect Yourself and Your Computer.** Mirror Image warns of the danger of providing personal information or photographs that a predator can use to track them. The game reminds teens to guard against incursions by using firewalls and virus protection.
- 3. Turn to a Trusted Adult.** Mirror Image demonstrates how cyberpolice officers can assist young people who find themselves in a dangerous situation.

This Guide introduces the three components of the Mirror Image program.

- The first chapter explains the five cybertools that students will use to win the Mirror Image game.
- The second chapter provides a synopsis of the Mirror Image game, with an Answer sheet so adults will know how to win!
- The final chapter, Behind the Headlines, provides interviews with a young victim of cyberstalking, her parents and the police who solved the crime.
- The Guide concludes with a template so students can design a poster with their own Internet Safety guidelines.

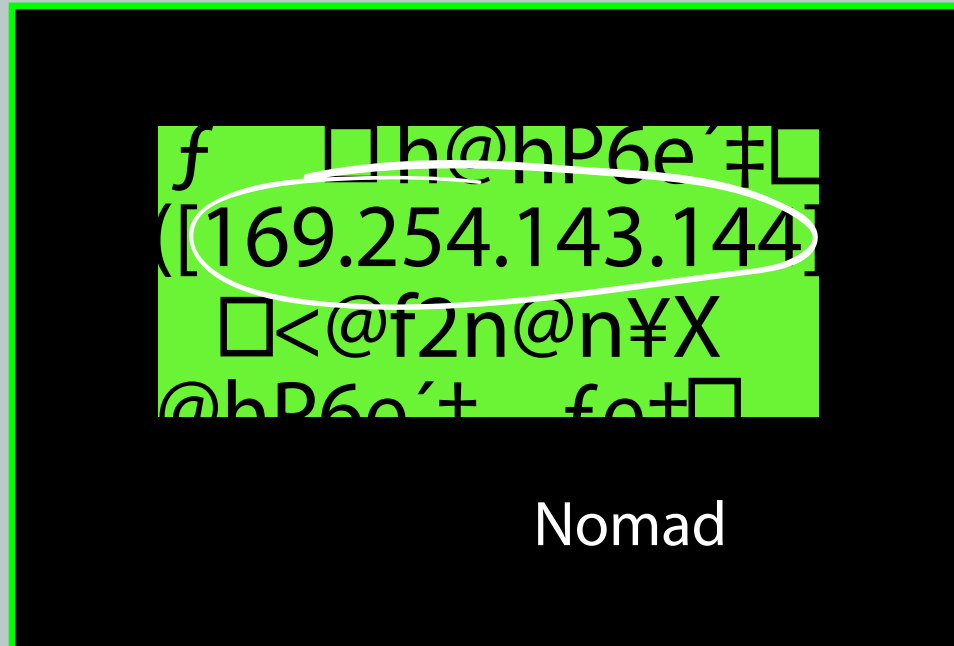
next steps...

Go to our website, www.cybercops.net and click on Why? Three interactive slide shows illustrate how young women can become victims of cyberstalking, child pornography and Internet luring.



We strongly recommend that parents, teachers and police officers review the Guide and the game before using it with young people. Mirror Image raises sensitive issues that may require careful consideration.

1. Detective's Notebook



The Detective's Notebook

“Cyberpolice officers use highly specialized forensic tools to gather and process digital evidence. Our job is one of the most challenging on the force.” Arni Stinnissen, Ontario Provincial Police

In the Mirror Image game, students are invited to take the role of a cyberspecialist and solve a crime simulation based on real events. To win, they will need to use five cybertools. Here is a brief explanation of each.

1. **Magnification.** Internet predators use fake emails and websites to fool recipients into revealing personal information. To combat this, cyberpolice look for errors, false information or spelling mistakes showing that the suspect has altered the document. Police also use magnification to compare the unique characteristics of original documents with documents seized from suspects.
2. **Directory Search.** The Internet offers hundreds of directories where a stalker can find information about a person he is targeting. But cyberpolice can use the same directories to find the predator. They cross-reference phone numbers, addresses, city maps, email and website information to build up a picture of the person they are trying to find.
3. **Domain Name Look-up: Whois.** If cyberpolice officers believe that a stalker is using a specific website to lure young people, they employ a “domain name lookup”, also called a Whois. This service provides all the information that was provided when the website was registered.

To activate the five cybertools, students click on icons on the game screen. The magnifying glass enables players to compare two pieces of evidence in detail.



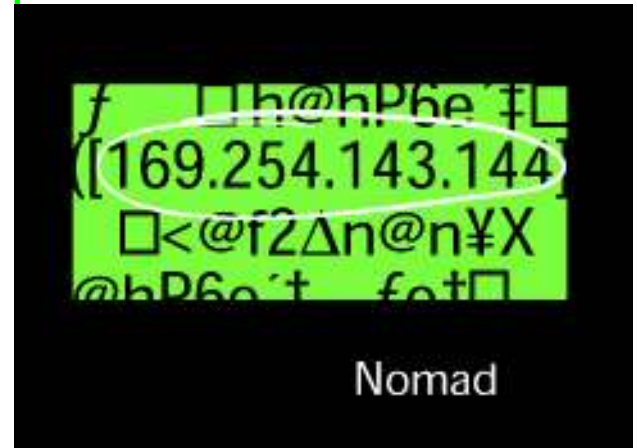
4. Information Retrieval Program: Scavenger

When a search warrant is issued, the electronic devices in the suspect's home or office are seized and brought to the police lab. Information entered into a computer remains there, even after it is deleted. Cyberpolice can regain this information by using retrieval programs. In the Mirror Image game we have given this technology the name: Scavenger.

5. Mapping Internet Transmissions: Nomad

An Internet message has an Internet Protocol address (or IP address) that identifies the route it took from sender to receiver. Each IP address is made up of four groups of numbers with a decimal between each group. When you receive an email, the IP address is embedded in it. When police officers want to track a cybercriminal, they obtain the IP address from one of his emails. This gives police the geographic location of the server that the criminal is using.

In order to track a criminal, cyberpolice officers use a program that maps the electronic route that an email has taken across the Internet. This Internet mapping technology identifies the route of a communication over the network from beginning to end, and lists all the intermediate routers a message passed through on its journey. In the Mirror Image game, this technology has been given the fictitious name: Nomad.



A Detective's Notebook worksheet is included on the next page. Each student should have a copy of the worksheet while playing the game.

next steps...

On the disk, the Detective's Notebook is a series of slides about the five cybertools police officers use to solve crimes. If students are playing the game alone, they may want to review the cybertools before they begin.

The Detective's Notebook

Fill in your answers as you play the game.

Challenge #1. What word proves the application form is faked? _____

Challenge #2. Where does Sheena work out? _____

What is the clue hidden in Sheena's photographs? _____

What is the address of Sheena's school? _____

Challenge #3. What is Mitch's website address? _____

What company is hosting Mitch's website? _____

What company is hosting the host of Mitch's website? _____

Who controls Sheena's images? _____

Challenge #4. What is an unusual word Mitch used in chats with Sheena or Megan? _____

What is Mitch's IP address? _____

Challenge #5. What is the latitude of Mitch's server? _____

What is the longitude of Mitch's server? _____



2. Mirror Image



Mirror Image

The Internet helps a predator search for a victim. He stalks his victim on-line, researching intimate details of the child's life. If he can discover a teen's dreams for the future, he can offer to fulfill them.

Mirror Image was designed to illustrate the tactics a predator uses to find a victim.

- **A Catalogue of Potential Victims.** In recent years 'social networking' websites have become very popular. Millions of teenagers have posted photographs and personal information about their interests. These sites become a 'catalogue' for predators, who comb these websites, looking for a vulnerable teen.
- **A Research Tool.** Once a predator has chosen a victim, he can assemble a dossier on his quarry before he makes contact. The Internet provides instant access to addresses, maps, telephone directories, and school websites. Many cyberstalkers create detailed lists of their victims' activities each day of the week.
- **A Mask.** A stalker who uses the Internet can be difficult to trace. He may mask his identity by relaying his email through a variety of servers and remailers. This makes it almost impossible for a teenager to confirm the identity of a stranger who has contacted them.

Mirror Image tells the story of Sheena and Megan, who were targeted by a stranger who found their photographs on-line.

Social networking websites are a popular place for young people to post personal information and photographs. One of the most popular social networking sites, MySpace, claimed almost 5 million registered users in 2005. That number had grown to 70 million a year later.



Clue 1

The Mirror Image game opens as the CyberCop is getting ready to end his shift. Suddenly he receives a call on his webcam. Two young women, Sheena and Megan, want to report a crime.

Sheena is being stalked by a man she met on the Internet. Mitch contacted Sheena after reading her profile on Instant Messaging. He claimed to be a modeling agent and offered to send her photos to a New York agency that was engaged in a "Search for New Faces". Sheena was thrilled. She filled in the application form Mitch sent her, giving him personal information.

Soon after, she noticed that a black van was following her in the street. Then she began to receive threatening phone calls. To protect herself from the stalker, Sheena turned to the cyberpolice.

Challenge: The CyberCop asks Sheena to send him the home page for the modeling agency and the application form that Mitch sent her. Students must compare the two documents to determine whether the application form really comes from the modeling agency or whether it was faked by Mitch.

Solution: Students click on the magnifier and compare the two documents, section by section. When they compare the right side of the two documents a sharp-eyed student should notice that the address of the modeling agency – Berkeley Street – is spelled wrong on the application form, proving that Mitch created it to fool the girls.

***TIP:** Mirror Image plays two simultaneous streams of video. In order to achieve a smooth playback of both video streams, use a computer with a minimum of 512 MB of RAM. The computer should be loaded with Quicktime 7.0. Type QT at any time to skip the video.*



Clue 2

Megan also posted her profile on Instant Messaging where it caught the eye of Mike. The two exchanged emails. Then Mike began to send Megan gifts, such as sexy underwear. Now Mike has invited Megan to a romantic dinner at an expensive restaurant.

Meanwhile, to persuade Mitch that she should be chosen to audition for the modeling agency, Sheena has paid her cousin to shoot a photo portfolio. She sent Mitch photos in her cheerleading outfit and in street clothes. Soon afterward, Mitch asked Sheena to pose for more provocative pictures, but she refused.

Challenge: The CyberCop asks Sheena to send him the profile that she posted on Instant Messaging. She also forwards the photographs she emailed to Mitch. The challenge is to determine whether Mitch would have been able to use this information to discover the location of Sheena's school.

Solution: The IM Profile indicates that Sheena goes to a Toronto school that is located close to her gym. The logo on her shirt suggests that either her school or her gym has the letters 'ing' in its name. When students use the telephone directory to look up the names and addresses of gyms and schools, they find that Springboard Gym is located on the same street as Glen High School.

Jan Sippel of the Vancouver School Board tested Mirror Image 'theater-style', on a single computer hooked up to a projector. With the students participating together, classes finished the game in less than 40 minutes.



Clue 3

The cyberpolice officer breaks the bad news to Sheena: her photographs have been altered and placed on pornographic websites all over the world. Her dreams of a modeling career are over.

Then, to the dismay of both girls, the cyberpolice discover that Mitch and Mike are the same man. He has been able to track the two girls because the application form for the modeling agency has placed a Trojan on their computers.

“Mitch” is able to open all of their files, read their Instant Messages, and activate their webcams to videotape them in their bedrooms.

Challenge: Students are asked what facts they can discover about the man who calls himself Mitch and Mike. They are given his email address and the website of his model search company.

Solution: Students click on the Whois icon to get the information that was filed when Mitch’s website was registered. They find that Mitch’s web host company is Moscownet. When they type ‘Moscownet’ into the Whois they learn that the host of that website is a dating service called Moscowgirls.

But when the students run Moscowgirls through the Whois, they reach a dead-end. The information is unlisted. However, the Moscowgirls website does show that Sheena’s photos are controlled by a man named Vladimir.

Scott Petronech, an IT specialist at the Calgary Science School, played Mirror image with students ‘theater-style’ and in groups of two. The students who played in pairs took twice as long to play the game and needed coaching.



The Arrest

The CyberCop warns: “We have to catch the predator with his hands on the keyboard or he’ll just claim someone else made the child pornography.”

Challenge: First, students must remember an unusual, specific word that was used in a conversation with Mitch: ‘Panorama’, ‘G-string’ and ‘mysterious beauty’ are options. Then students use Scavenger to search the hard drive of Sheena’s computer for the email that contains one of those words.

Challenge: Students search the code at the bottom of the email to find the Internet Protocol address of the server Mitch used. The IP address is: 156.114.152.256.

Challenge: Nomad technology gives us the latitude and longitude of the computer that Mitch is using. Students have to scour the satellite images for the Toronto, Canada, building at this location. When students run the cursor over the building, the IP address confirms the address where the police must go to make the arrest.

Solution: Students will have to remember the name of the computer: Keyhole. The cyberpolice enter Mitch’s office and arrest him while he is still deleting files from the computer.

All technologies used in the Mirror Image game are based on software tools used by cyberpolicing agencies. The E-Crime Section of the Ontario Provincial Police assisted with the design of the clues.



Discussion

Sheena:

- What information did Sheena initially post on her web profile? How did Mitch track her?
- What were the consequences of filling in the application form?
- Now that Sheena's photographs have been placed on pornographic websites, what will happen to her modeling career?

Megan:

- Think about the way Megan talked about Mike. What emotions was she experiencing?
- If Megan had gone on the date with Mike, would she have been as impressed with him?
- What additional inducements might Mike have offered Megan after their date?
- How will Megan respond to the next man who says he is in love with her?

CyberCop:

- Why did Sheena wait to talk to the police?
- What finally propelled Sheena and Megan to go to the police? Was this a good decision?
- What helpful tools and advice did the CyberCop give them?

next steps...

Go to our website, www.cybercops.net. There are several examples of Best Practices from parents, teachers and police officers in the United States and Canada.

The discussion encourages debate on the three themes of the Mirror Image game: personal responsibility on-line; computer security; and responding to trouble by talking to a trusted adult.



Answers

Question 1: What word proves that the application form is fake?

Answer: When Mitch created the fake application form he misspelled the address: Berkley.

Question 2: What is the address of Sheena's school?

Answer: Sheena goes to Glen High School at 7574 Glen Road.

Question 3: Who has control over Sheena's pictures?

Answer: Vladimir

Question 4: What is an unusual word Mitch used in chats with Sheena or Megan?

Answer: Any one of these words is correct: Panorama, t-backs, G-string, modeling career, icy mysterious beauty.

Question 5: What is Mitch's IP address?

Answer: 156.114.152.256

Question 6: What is the latitude and longitude of Mitch's office?

Answer: latitude: 43.76 N longitude: 79.02 W

Question 7: What is the name of the computer?

Answer: Keyhole

Lynne Van Meer, from Killarney Secondary School in Vancouver, Canada brought two classrooms into the school library to play the Mirror Image game together.



3. Behind the Headlines



Behind the Headlines

Rob searched the web for photos of cheerleaders in his home town. Pretending to be a modeling agent, he offered each girl a contract with a New York agency. If they agreed, he demanded sex. If they turned him down, he stalked them through the streets.

For months, Rob's young victims lived in fear. Some feigned illness and stayed home from school. Others experienced anxiety attacks. Yet for weeks, not one of the girls spoke to her parents – or the police – about the threats.

- **Caitlin.** When Caitlin's friends began to complain that Rob was harassing them, Caitlin offered to tell him off. Soon she became the target of abuse herself. In her interview, Caitlin explains what happened when she tried to deal with the situation alone.
- **Caitlin's Parents.** When Caitlin finally told her parents about the stalker, their emotions ran from anger to panic. This interview follows the family's first attempts to protect their daughter, attempts that could have landed them in legal difficulties of their own.
- **Sgt. Fred Morton.** When Caitlin's family approached Sgt. Fred Morton of the Saint John Police Department, they were distraught. Sgt. Morton mapped out a strategy to protect the victims and their families in the days leading up to the arrest.
- **James McAvity.** As Prosecutor, James McAvity was responsible for bringing Rob to trial. In this interview he explains how he chose his trial strategy.

"Caitlin" is the pseudonym of Katrina Russon, who was stalked for a year. In the spring of 2006, Katrina told her story at a gala benefit organized by the Mounted Police Foundation in Toronto, Canada. Her presentation can be viewed on our website at www.cybercops.net.



Discussion

Caitlin:

- What were Caitlin's reasons for contacting the predator?
- What frightened Caitlin most about the predator's behavior?
- Caitlin waited one year before she told her parents about the stalking? Why?

Caitlin's Parents:

- How did Caitlin's mother react to the news of the stalker? How did her father react?
- How could the parents have handled the situation better?

Caitlin's School:

- What effect did the predator's behavior have on the school?

The Police and Prosecutors:

- Why did the police find it difficult to find the predator?
- What charges could the prosecutor have laid against Rob?
- Did the prosecutor make the best choice?

next steps...

Go to our website, www.cybercops.net. One of the Best Practices describes how the Mirror Image game was delivered at River Valley Middle School close to the location of the original crime.

Students from River Valley Middle School in Grand Bay, New Brunswick, Canada, were the first to participate in the Behind the Headlines discussion. The original police case took place only a few miles from the school.



4. Internet Safety Plans



Internet Safety Plans

Mirror Image is fun to play, but is it an effective Internet safety tool? The question was asked by researchers at the University of Lethbridge. They found that the greatest impact came when students played the game first and read a case history afterward.

During the 2004 school year, researchers conducted an evaluation of the Mirror Image game with 1,000 students from schools in Canada, the United States and Australia. Students filled in an Internet Safety Plan before and after playing Mirror Image. The completed surveys were analyzed to see whether there was a significant increase in safety ideas in three areas.

- There was an increase in the guidelines students had for their personal protection. The most dramatic gains were made in the number of students who realized they should not send photographs of themselves over the Internet.
- The researchers noted an increase in the guidelines for protecting the family computer, as students recognized the importance of using filtering software and controlling webcam use.
- Perhaps the most gratifying result was a significant rise in the number of students who wrote that they would talk to their parents or a police officer if they ran into difficulties on-line.

During 2005, the researchers invited an additional 200 students to play Mirror Image and then read, Behind the Headlines, the story of a teenager who was cyberstalked. The combination of the game and the factual account had an even more pronounced effect on the students.

The full report from the University of Lethbridge, authored by Glen Hutton, can be downloaded from our website, www.cybercops.net.



Mirror Image



PROTECT YOURSELF

1

2

3
