

Online Predators

Carla Mooney

Issues in the Digital Age

Contents

Introduction	4
Dangers Online	
Chapter One	8
A Real Problem	
Chapter Two	20
Sexual Predators	
Chapter Three	35
Financial Predators	
Chapter Four	50
Cyberbullies	
Chapter Five	63
What Lies Ahead?	
Source Notes	75
Facts About Online Predators	81
Related Organizations	83
For Further Research	87
Index	89
Picture Credits	95
About the Author	96

Introduction

Dangers Online

In 2007 a school resource officer from Birmingham, Alabama, contacted the FBI about a disturbing complaint he had received from one of his high school students. An Internet extortionist was badgering the girl to send nude photos of herself. When FBI agents opened their investigation, they discovered the Internet predator, who went by the username Metascape, had targeted more than 200 young women from several states. After becoming friendly with the women online, Metascape would convince them to send him sexual statements or photos. He then used that material to blackmail the women. In at least 50 cases, Metascape blackmailed his victims into performing graphic sexual acts for him on webcams, which he then used for further blackmail.

A Difficult Case

With the cooperation of law enforcement and victims from several areas, the FBI identified 24-year-old Jonathan Vance from Auburn, Alabama, as the predator. “Tracking him down was complicated. . . . This was really a difficult, unique case,”¹ says Assistant US Attorney Daniel Fortune, who prosecuted the case.

After his arrest, Vance described to FBI investigators some of the methods he used to blackmail the young women and gain control of their Yahoo, Hotmail, Facebook, and MySpace accounts. Sometimes he would contact them through instant messaging and send them a seemingly playful game where he pretended to be a long-lost friend or secret admirer. He told them he would reveal his true identity if they answered 10 questions. He specifically designed the questions to gather intimate and embarrassing personal details about his victims. Sometimes he hacked into a victim’s e-mail or Facebook account, using information such as birth date, school, and hometown that he gathered from public

just absorbed the information in front of them. Instead, they created and added their own information.

At the same time, e-commerce exploded on the Internet. Introduced in the mid-1990s, e-commerce is the buying and selling of products or services over the Internet and other computer networks. According to a 2010 report by investment firm J.P. Morgan, global e-commerce was predicted to reach \$680 billion in 2011.

As online communication and commerce have become more and more a part of daily life, a variety of predators have seen opportunities that never existed before. Hiding behind an anonymous computer screen, people with malicious intent use the Internet every day to find and exploit victims.

Real Risks

While the Internet offers numerous advantages and conveniences, it has opened the door to many real risks. Eager to connect on social networks or shop online, people may let their guard down and share with strangers

information that could be used to hurt them. Sexual predators lurk in chat rooms and social networking sites, looking for potential victims. Financial predators send fake e-mails, hack into computers, or develop elaborate online frauds to access a victim's bank account, credit cards, or Social Security number. Cyberbullies use social networking sites to post humiliating pictures or comments or send threatening texts. "The Internet is a dangerous place and just like we teach our children not to

converse with strangers on the street and not to run red lights when they're driving, we need to teach children about what to look out for online,"⁶ says John Sancin, president of CyberPatrol, a company that develops web-monitoring software.

Some of the Internet's characteristics make people more vulnerable to online predators. Once information or pictures are posted on the Internet, they can be accessed and searched indefinitely. Material found

"Unfortunately, cybercriminals are among the most adept at leveraging these new technologies, and have embraced the Internet to facilitate their criminal behavior."¹⁰

— Linda Criddle, Internet child-safety expert and author.

Please Rob Me

Although social networking sites and location-based apps have made it easy for users to tell friends where they are and what they are doing, sharing personal information online also makes it easier for would-be thieves to plan their next heist. Status posts and pictures tell criminals if a potential victim is on vacation or out for the evening, if they have a dog, and if they own fancy cars or big televisions. In 2009 a group of thieves was arrested near Los Angeles, California, for a series of burglaries targeting celebrities. According to police, the thieves used Internet mapping and gossip sites to case their targets' homes.

A website called PleaseRobMe.com is drawing attention to the risks of sharing locations online. The site has accumulated public posts from location-based services such as Foursquare or Gowalla that allow users to check in to places like restaurants, bars, and stores and then broadcast their location to their online friends. The site allows users to filter the posts by geographic location. According to the founders, the site's goal is to raise awareness and have people think more carefully about unintended consequences when they broadcast their location on the Internet.

online can be forwarded, copied, or pasted anywhere. In addition, every online post is open not only to intended viewers but also to anyone else who happens to be wandering through the online landscape; users never know who is reading or seeing what they post online. A blog update or credit card number intended for a select few could easily be viewed by more than the intended audience. In addition, the ability to connect without seeing or hearing the other person can sometimes cause inhibitions to break down. People are more likely to be uncivil or downright nasty in an anonymous e-mail, blog post, or social media comment than they would be face-to-face.

Related Organizations

Center for Safe and Responsible Internet Use (CSRIU)

474 W. 29th Ave.
Eugene, OR 97405
phone: (541) 556-1145
e-mail: contact@csriu.org
website: www.cyberbully.org

The CSRIU provides consulting services to school districts, administrators, and school attorneys related to Internet use, cyberbullying, and sexting. Its website provides information and resources for students, parents, and educators.

Federal Bureau of Investigation (FBI) Cyber Crime Division

935 Pennsylvania Ave. NW
Washington, DC 20535-0001
phone: (202) 324-3000
website: www.fbi.gov

The FBI's Cyber Crime Division investigates high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber frauds. Agents gather and share information and intelligence with public- and private-sector partners worldwide.

Federal Bureau of Investigation (FBI) Innocent Images National Initiative (IINI)

935 Pennsylvania Ave. NW
Washington, DC 20535-0001
phone: (202) 324-3000
website: www.fbi.gov

The FBI's Innocent Images National Initiative teams FBI agents with local police around the country in proactive task forces that work online undercover to stop online predators.

For Further Research

Books

Martin T. Biegelman, *Identity Theft Handbook: Detection, Prevention, and Security*. Hoboken, NJ: Wiley, 2009.

Thomas A. Jacobs, *Teen Cyberbullying Investigated: Where Do Your Rights End and Consequences Begin?* Minneapolis, MN: Free Spirit, 2010.

Samuel McQuade III, James P. Colt, and Nancy Meyer, *Cyber Bullying: Protecting Kids and Adults from Online Bullies*. Santa Barbara, CA: Praeger, 2009.

Corey Sandler, *Living with the Internet and Online Dangers*. New York: Checkmark, 2010.

Alexis Singer, *Alexis: My True Story of Being Seduced by an Online Predator (Louder than Words)*. Deerfield Beach, FL: HCI Teens, 2010.

Internet Sources

Internet Crime Complaint Center, “2010 Internet Crime Report,” 2011. www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

KidsHealth.org, “Safe Surfing Tips for Teens.” http://kidshealth.org/teen/safety/safebasics/internet_safety.html.

Amanda Lenhart, “Cyberbullying 2010: What the Research Tells Us,” Pew Internet & American Life Project, May 6, 2010. www.pewinternet.org/Presentations/2010/May/Cyberbullying-2010.aspx.

Kathryn Zickuhr, “Generations and Their Gadgets,” Pew Internet & American Life Project, February 3, 2011. www.pewinternet.org/Reports/2011/Generations-and-gadgets.aspx.

Websites

Cyberbullying Research Center (www.cyberbullying.us). The site provides fact sheets, publications, and other research about cyberbullying.

Index

Note: Boldface page numbers indicate illustrations.

- Aftab, Parry, 53, 55, 59
Allen, Ernie, 33
Anderson, Steven, 29
Arpanet, 9
- Bales, Bob, 19
banking, online, 11
 improved safeguards in, 67–68
 Operation Phish Phry targets fraud in, 47–48
 phishing and, 39–40
 prevalence of, 9
Berkman Center for Internet and Society (Harvard University), 33
Betensky, Jason, 25
Beverly, Paul, 68
Blumenthal, Richard, 30
botnets, 49, 69
Brennan, James, 46–47
Briggs, Jason C., 61
Brody, Anita, 57
Brouillard, Becky, 50
Brown, Pamela, 52
Bureau of Justice Assistance, 16
 See also Internet Crime Complaint Center
Bush, George W., 46
Caldwell-Bono, Deborah, 29
Cardona, George S., 44
Carlson, Eric L., 36, 40
car scams, 43
Center for Safe and Responsible Internet Use (CSRIU), 56, 83
Chabinsky, Steven, 66–67
charity scams, 39
chat rooms, use of by online sexual predators, 23–24
Cisco 2010 Annual Security Report, 63–64
Clementi, Tyler, 7
company networks, attacks on, 42–44
Comprehensive Crime Control Act (1984), 46
computer forensics, 68–69
Computer Fraud and Abuse Act (1986), 46
Computer Security Group (University of California at Santa Barbara), 69
Consumer Reports (magazine), 16
Cooper, Roy, 30
Criddle, Linda, 12, 16, 17
Crimes Against Children Research Center (University of New Hampshire), 14, 16
Crouse, Dave, 42