The Federal Trade Commission Response to Technology Misuse and Abuse
The Stalking Resource Center is a program of the National Center for Victims of Crime. The mission of the Stalking Resource Center is to enhance the ability of professionals, organizations, and systems to effectively respond to stalking.

The Stalking Resource Center provides training, technical assistance, and resource materials for professionals working with and responding to stalking victims and offenders.

Moderator: Rebecca Dreke, Deputy Director
rdreke@ncvc.org
Presenters

- **Jacqueline Connor** is an attorney in the Division of Privacy and Identity Protection at the Federal Trade Commission in Washington, D.C. She investigates and litigates violations of U.S. laws enforced by the Commission that govern the privacy and security of consumer information.

- **Lisa Weintraub Schifferle** is an attorney in the Federal Trade Commission’s Division of Consumer & Business Education. At the FTC, she regularly trains advocates across the country on identity theft, scams, privacy and technology.
Online Safety for Domestic Violence & Stalking Victims

FTC Presentation for the Stalking Resource Center
April 29, 2015
What We’ll Cover

- The FTC’s role in stopping misuse of technology
  - Consumer & business education
  - Complaint gathering
  - Law enforcement
  - Policy recommendations

- Tools Stalkers Use

- Online Safety Tips
  - Computers
  - Mobile Phones

- Resources
FTC’s Role

- Consumer & business education
- Complaint gathering
- Law enforcement
Consumer Education

OnGuard Online

Net Cetera

Living Life Online
Cyberbullying: What You Can Do

August 1, 2012
by Aditi Jhaveri
Consumer Education Specialist, FTC

These days, bullying doesn’t just happen in the schoolyard. Bullying has followed kids into cyberspace as they spend more time online and on their phones. Cyberbullying happens when kids bully each other through emails, text messages, online... Read More

Learn more about the Net Cetera Outreach Toolkit

Avoid Scams
- Phishing
- Online Dating Scams

Protect Kids Online
- Child Identity Theft
- Kids, Parents, and Video Games

Stay Connected
- Get Email Updates
- Blog Feed
- Facebook
Net Cetera Outreach Toolkit

- Net Cetera – guide for parents
- Heads Up – booklet for teens
- Presentations tools
  - Videos
  - PowerPoint presentation
  - Spread the Word – community outreach guide
Contents

- About the FTC
- You in the World
- Your Life Online
- Sharing Well With Others
- Sexting
- Minding Your Manners
- Cyberbullying
- Looking Both Ways
- Meet Shock... Bill Shock
- Go Ahead – Be Critical
- Ad it Up
- Try it Out
- Now it's Your Turn

Ftc.gov/LivingLifeOnline
Tips like mobile app security:

• Take stock of data you collect and retain
• Use transit encryption on usernames, passwords and other important data
• Consider protecting data you store on a user’s device
Complaint gathering

- File complaints at ftc.gov/complaint
- Federal government’s centralized database of identity theft & fraud victim complaints
- Contents
  - victim contact information
  - suspect information: name, address, phone, relationship to the victim
  - description of crime, details
  - police report number, department name, contact information
Many law enforcement actions affect online safety for domestic violence & stalking victims, including:

- RemoteSpy (2010)
- DesignerWare (2013)
- TRENDSnet (2014)
RemoteSpy

Keylogger spyware was used to secretly monitor unsuspecting consumers’ computers

• Spyware was disguised as innocuous email attachment

• When consumer clicked on attachment, the keylogger spyware was silently installed on computer

• Spyware was able to:
  ▪ Record every keystroke typed on computer (including passwords)
  ▪ Capture images of the computer screen
  ▪ Record web sites visited

Outcome: among other things, defendants cannot provide purchasers of program with means to disguise the product as an innocent file or email attachment
Software design company that licensed software to rent-to-own stores that enabled stores to track and recover rented computers

Software also had add-on program known as “Detective Mode,” which when activated could:

- Log key strokes
- Capture screen shots
- Take photographs using computer’s webcam
- Presented fake software program registration screen that tricked consumers into providing personal contact information
Features of software program used without notice to, or consent from, the consumers renting the computers

Outcome:

- Banned from using monitoring software like Detective Mode
- Prohibited use of geolocation tracking without consumer consent and notice
- Seven rent-to-own companies also charged with breaking the law, including:
Company markets video cameras designed to allow consumers to monitor their homes remotely

Problem: lax security practices led to hundreds of consumers’ private camera feeds being made public on the Internet

Outcome: among other things, required to establish information security program to protect the security, confidentiality, or integrity of information
Policy recommendations

Congressional testimony
- June 2014 – Bureau Director Jessica Rich testified before Senate
  - Privacy concerns regarding consumers’ geolocation information
  - Endorsed legislation that protects consumers’ sensitive geolocation information

Workshops
- February 2014 - Mobile Device Tracking

Staff Reports
- January 2015 – Internet of Things: Privacy & Security in a Connected World
Technologies Stalkers Misuse

Cyberbullying
Geo-location tracking
Stalkers can:

- Install spyware to hack into a victim’s email
- Use Bluetooth or GPS to track a victim’s location via phone, tablet or other Bluetooth/GPS enabled device
- Covertly turn on a device’s camera or microphone to watch and listen to the victim
Stalking mobile applications

- Various apps, not sold on iTunes or Google Play app stores
- Usually need physical access to mobile phone to install
- These stalking applications have various capabilities, including:
  - Listen to & record phone conversations
  - Read texts and emails
  - Geolocation
  - Listen to ambient sounds
- StealthGenie & DOJ law enforcement
Online Safety Tips
Online Safety Tips for Victims of Domestic Violence and Stalking

Tip #1: Use strong passwords and change them frequently.

• Strong passwords have a combination of letters, numbers and special characters.

• Have passwords on phone, computer and all online accounts.

• Keep passwords private.
Online Safety Tips for Victims of Domestic Violence and Stalking

Tip #2: If a victim believes someone may be monitoring them, encourage them to use a safer computer – one that the abuser has not/does not have access to.

- It’s especially important to use a safer computer if victim is researching an escape plan, new jobs or a place to live.

- Change usernames and passwords of online accounts on the safer computer.

- Do not log into those accounts on any computer that may be being monitored.
Cyberbullying

Harassment that happens online

Best to not respond:

• Encourage victims to connect with an advocate to discuss situation

• Encourage victims to save the evidence of the cyberbullying (i.e., take screen shots, print the messages, etc.)

• Block the bully/stalker online – remove from friends list

• Have any bogus profiles taken down – contact company that runs site
**Hacked email?**

- Update system & delete malware
- Change passwords
- Check advice with email provider or social networking site
- Check account settings for unfamiliar activity or links
Malware?

- Be very cautious about shopping and banking online
- Update your security software
- Use trusted tech support, if needed (but beware of tech support scams)
Mobile Phones

Think about privacy and safety
- Password-protect phones
- Beware of photo- and video-sharing

Filters on home computers don’t apply on phones
- Risks with social networking on phone
Choose the right options and features for your phone

- Consider non-smartphones

Find out about location-based services

- Is your phone GPS-enabled?
- Consider turning off Bluetooth when not using

When disposing of phone, ways to do so safely:

- Think about whether you want to keep your phone to preserve evidence of abuse
- If you get rid of your phone, remove the SIM card and all personal information
Mobile Safety Tips for Victims of Domestic Violence and Stalking

Tip #1: Know where your phone is at all times.
- Malware, spyware and tracking apps can be installed in just a few minutes.

Tip #2: Check your phone’s settings.
- Bluetooth and GPS can be used to track you.
- A victim advocate can help strategize a specific tech safety plan for your situation.
Tip #3: If you’re not sure if your phone is being monitored, look for:

- Patterns or behaviors
  - What does the person know?
  - Does the person have access to your wireless carrier’s account?
- Do they seem to know your location?
  - Check whether locate my phone features are on
  - Ask friends or family not to mention your location on social media
- Do you notice unusual activity on your phone?
  - Look for excessive battery drain or a spike in data usage
Mobile Safety Tips for Victims of Domestic Violence and Stalking

Tip #4: If you think your phone is being monitored, consider purchasing a new phone.

• The safest thing is to get a new phone with an account that the abuser does not have access to.
• Remember to put a password on your new phone, then disable Bluetooth and GPS.
• Consult House of Ruth, Verizon Hopeline, Safe Link Wireless, or other entities with free phones for domestic violence victims
FTC Resources

- Visit OnGuardOnline.gov/netcetera
- Order free copies: http://bulkorder.ftc.gov
- File a complaint at www.ftc.gov/complaint
Other Resources

- If in danger right now, call 911
- National Domestic Violence Hotline at 1-800-799-SAFE
- The Stalking Resource Center at the National Center for Victims of Crime:
  - www.victimsofcrime.org/src
  - 202-467-8700
Questions?

Lisa Schifferle
• lschifferle@ftc.gov

Jacqueline Connor
• jconnor@ftc.gov
Upcoming webinar:

**Media Literacy and the Social Normalization of Stalking**

- **Thursday, May 14, 2015**
- **2:00 p.m. - 3:30 p.m. ET**
- Stalking is a crime that is frequently minimized and misunderstood, in part because it is a behavior that is socially normalized. Media plays a critical role in shaping our understanding of stalking, and other forms of violence. Media literacy is a tool that we can all use to better deconstruct media and deconstruct the culture at large as we work towards building more effective violence response and prevention methods.