File a report with local law enforcement or contact your local prosecutor's office to see what charges, if any, can be pursued. Stalking is illegal in all 50 states and the District of Columbia.

For additional resources, visit the Stalking Resource Center at www.ncvc.org/src.

In cases of cyberbullying:

- Tell a trusted adult about what's going on.
- Save any of the related emails, texts, or messages as evidence.
- Keep a record of incidents.
- Report the incident to the website's administrator; many websites including Facebook and YouTube encourage users to report incidents of cyberbullying.
- Block the person on social networks and in email.
- Avoid escalating the situation: Responding with hostility is likely to provoke a bully. Depending on the circumstances, consider ignoring the issue. If you or your child receives unwanted email messages, consider changing your email address.

For more information, visit www.stopcyberbullying.org and www.ncpc.org/cyberbullying.

HOW DID THIS HAPPEN TO ME?

A Word about Malware.

Avoid malware with the following tips from the STOP. THINK. CONNECT. campaign:

- Keep a clean machine by making sure your security software, operating system and web browser are up to date.
- When in doubt throw it out. Don't click on any links or open attachments unless you trust the source.
- Make your passwords long and strong and unique. Combine capital and lowercase letters with numbers and symbols to create a more secure password. Use a different password for each account.
- Back up your data regularly.
- Protect all devices that connect to the Internet. Smartphones, gaming systems, and other web-enabled devices also need protection.

OTHER RESOURCES OR FILE A COMPLAINT:

- Anti-Phishing Working Group (reportphishing@antiphishing.org)
- Better Business Bureau (investigates disagreements between businesses and customers; www.bbb.org/consumer-complaints/file-a-complaint/get-started)
- CyberTipLine, operated by the National Center for Missing & Exploited Children (investigates cases of online sexual exploitation of children; 1-800-843-5678 or www.cybertipline.com)
- Electronic Crimes Task Forces and Working Groups (www.secretservice.gov/ectf.shtml)
- The Secret Service (investigates fraudulent use of currency; www.secretservice.gov/field_offices.shtml)
- StopFraud.Gov Victims of Fraud Resources (www.stopfraud.gov/victims.html)
- U.S. Computer Emergency Readiness Team (www.us-cert.gov)
- U.S. Department of Justice (www.justice.gov/criminal/cybercrime)
- U.S. Postal Inspection Service (investigates fraudulent on-line auctions and other cases involving the mail; postalinspectors.uspis.gov/contactus/filecomplaint.aspx)
- Your State Attorney General (the National Association of Attorneys General keeps a current contact list at www.naag.org/current-attorneys-general.php)

The National Cyber Security Alliance would like to thank the National Sheriffs' Association and International Association of Chiefs of Police for their assistance in creating this resource.

Tips and Advice

IF YOU BECOME A VICTIM OF CYBERCRIME