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.

NATIONAL CYBERSECURITY ALLIANCE

STOP | THINK | CONNECT

StaySafeOnline.org

Tips and Advice

IF YOU BECOME A VICTIM OF CYBERCRIME

The Realities of Cybercrime

Cybercrime in all its many forms (e.g., online identity theft, financial fraud, stalking, bullying, hacking, e-mail spoofing, information piracy and forgery, intellectual property crime, and more) can, at best, wreak havoc in victims' lives through major inconvenience and annoyance. At worst, cybercrime can lead to financial ruin and potentially threaten a victim's reputation and personal safety.

One of the best ways to learn how to prevent cybercrime is to check out **STOP. THINK. CONNECT.** at **stopthinkconnect.org/tips-and-advice/.**

SHOULD I REPORT CYBERCRIME?

Cybercrime can be particularly difficult to investigate and prosecute because it often crosses legal jurisdictions and even international boundaries.

Who to contact:

Local law enforcement. Even if you have been the target of a multijurisdictional cybercrime, your local law enforcement agency has an obligation to assist you, take a formal report, and make referrals to other agencies.

IC3. The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. Complaints may be filed online at www.ic3.gov/default.aspx.

Federal Trade Commission. The FTC does not resolve individual consumer complaints, but does operate the Consumer Sentinel, a database that is used by civil and criminal law enforcement authorities worldwide. File your complaint at www.ftccomplaintassistant.gov/FTC_Wizard.aspx?Lang=en.

Your Local Victim Service Provider. Most communities in the United States have victim advocates ready to help following a crime. Find local victims service providers here: ovc.ncjrs.gov/findvictimservices/search.asp

COLLECT AND KEEP EVIDENCE

It's important to keep any evidence you may have related to your complaint. Evidence may include the following:

- Canceled checks
- Certified or other mail receipts
- Chatroom or newsgroup text
- Credit card receipts
- Envelopes (if you received items via FedEx, UPS, or U.S. Mail)
- Facsimiles
- Log files, if available, with date, time and time zone
- Messages from Facebook, Twitter or other social networking sites
- Money order receipts
- Pamphlets or brochures
- Phone bills
- Printed or preferably electronic copies of emails (if printed, include full email header information)
- Printed or preferably electronic copies of web pages
- Wire receipts

TIPS FOR SPECIFIC TYPES OF CYBERCRIME

Here are useful tips to follow for some specific types of cybercrimes:

In cases of identity theft:

Make sure you change your passwords for all online accounts. Make it long, strong and unique, with a mix of upper and lowercase letters, numbers and symbols.

Close any unauthorized or compromised credit or charge accounts. Inform the companies that someone may be using your identity, and find out if there have been any unauthorized transactions.

Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft.

File a report with your local law enforcement agency. You will need to provide a copy of the law enforcement report to your banks, creditors, other businesses, credit bureaus, etc.

If your personal information has been stolen through a corporate data breach, you will likely be contacted by the business or agency whose data was compromised with additional instructions, as appropriate.

If stolen money or identity is involved, contact one of the three credit bureaus to report the crime (Equifax at 1-800-525-6285, Experian at 1-888-397-3742, or TransUnion at 1-800-680-7289). Request that the credit bureau place a fraud alert on your credit report to prevent any further fraudulent activity from occurring. As soon as one of the bureaus issues a fraud alert, the other two bureaus are automatically notified.

For additional resources, visit the Identity Theft Resource Center at www.idtheftcenter.org or the Federal Trade Commission at www.ftc.gov/bcp/edu/microsites/idtheft/tools.html.

In cases of Social Security fraud:

If you believe someone is using your social security number for employment purposes or to fraudulently receive Social Security benefits, contact the Social Security Administration's fraud hotline at 1-800-269-0271. Request a copy of your social security statement to verify its accuracy.

For additional resources, visit the Social Security Administration at oig.ssa.gov/report-fraud-waste-or-abuse.

In cases of online stalking:

In cases where the offender is known, send the stalker a clear written warning saying the contact is unwanted and asking that the perpetrator cease sending communications of any kind.

Save copies of all communication from the stalker (e.g., emails, threatening messages, messages via social media) and document each contact, including dates, times and additional circumstances, when appropriate.

File a complaint with the stalker's Internet Service Provider (ISP) and yours. Many ISPs offer tools that filter or block communications from specific individuals.

Own your online presence. Set security and privacy settings on social networks and other services to your comfort level of sharing.

Consider changing your email address and ISP; use encryption software or privacy protection programs on your computer and mobile devices. (Consult with law enforcement before changing your email account.)