

RESPONDING TO IDENTITY THEFT, FRAUD AND CYBERCRIME

Cyber Bullying and Harassment

In cases of cyberbullying:

- If you're a child or teen, tell a trusted adult about what's going on.
- Save any of the related emails, text messages or other correspondence as evidence.
- Keep a record of incidents.
- Report the incident to the website's administrator; many social media platforms and other websites 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. Often, bullies thrive on the reaction of their victims. If you or your child receives unwanted email messages, consider changing your email address. The problem may stop. If you continue to get messages at the new account, you may have a strong case for legal action.
- If the communications become more frequent, the threats more severe, the methods more dangerous and if third-parties (such as hate groups and sexually deviant groups) become involved—the more likely law enforcement needs to be contacted and a legal process initiated.

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. Do this only once, and do not communicate with the stalker again (Ongoing contact usually only encourages the stalker to continue the behavior).
- 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. (You should consult with law enforcement before changing your email account. It can be beneficial to the investigation to continue using the email account so law enforcement can also monitor communication.)
- 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. <http://victimsofcrime.org/our-programs/stalking-resource-center>

Find more information at <https://www.staysafeonline.org>