Take Ctrl

A resource guide on online safety for all ages.

You Have the Power … Know How to Use It, Inc.

Our Mission: To empower those victimized by violent crime through education, advocacy, and understanding.

Last updated November 2019

Take Ctrl

A resource guide on online safety for all ages.

You Have the Power … Know How to Use It, Inc.

Our Mission: To empower those victimized by violent crime through education, advocacy, and understanding.

Last updated November 2019

Table of Contents

You Have the Power thanks Selah Russell and Selvia Wagih, our 2019 Opportunity NOW interns, for their research and insights on this resource guide. Find out more about Opportunity NOW and its youth employment possibilities at https://www.nashville.gov/Mayors-Office/Opportunity-NOW.aspx

Updated November 2019

Message from Our Founder

You Have the Power…Know How to Use it, Inc., was founded in Nashville TN in 1993. Our mission is to empower, support and advocate for those victimized by crime.

The Internet has revolutionized the way people communicate, the way they learn, the way they do business—almost every aspect of our lives. This includes the way they fight, the way they harass and exclude others, and the way they commit crimes.

Cyberbullying and online harassment can cause just as much damage as its real-world equivalent. Online searches for seemingly innocent content can bring up pornography and other unwanted or damaging material. Malicious websites and software can endanger your finances and safety without you even knowing it. And online fraud is a multi-billion dollar business.

Isolating yourself from the Internet is not an option in the 21st century. But there are some simple steps you and your family can take to reduce your chances of being a victim.

We hope you find helpful information in this guide. For more information on this topic or about our organization, please contact us at (615) 292-7027 or our website at www.yhtp.org.

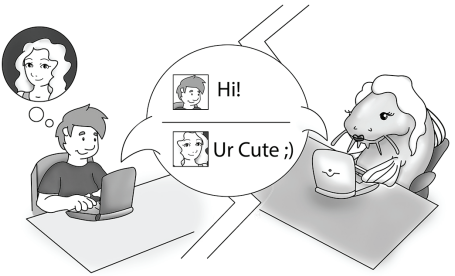
Thank you,

Andrea Conte
Founder, You Have the Power

Basic Rules of Internet Safety

Be careful what you post.
This may be the most important rule of the Internet and the one that causes the most problems when broken. Anything you post could stay online forever. Even if you delete the original, someone else might make a copy and post it. Once that embarrassing remark or picture is out there, it can go "viral" and become unstoppable. A good rule to follow: don't put anything online that you wouldn't want your mom or your boss to see.

Be careful who you meet online.
People you meet online are not always who they claim to be. Indeed, they may not even be real. Fake social media profiles are a popular way for hackers to fish for information or establish an opening for harassment and cyberbullying attempts. When meeting your online friends IRL ("in real life") for the first time, agree to meet in person and, until then, avoid giving out any sensitive information.



"Catfishing" is drawing someone into a relationship using a fake persona. This tactic has been used in both cyberbullying and romance scams, both of which are discussed on pages 6-8 (15). (Illustration by Kelly Gillit for the *Flare*, the student newspaper of Kilgore College.)

Limit the amount of personal information you give out. Not everyone needs to know your relationship status, your home address, or what you did last Saturday night. Make sure publicly accessible sites show the best possible version of you, and the minimum amount of information they need to contact you.

Keep your privacy settings on.
This applies to both your email and your social media (even if they can be hard to find sometimes). Activating your privacy settings keeps hackers from obtaining your personal information. They can also prevent marketers from contacting you with unwanted spam and advertising.

Basic Rules of Internet Safety (continued)

Make sure your Internet connection is secure.

When you use public Wi-Fi or go online in a public place, your Internet security is only as good as the place where you're connecting. Avoid using public Internet to access sites where you enter passwords, banking info, etc. You might want to go one step further and use a virtual private network, or VPN, to keep anyone else from accessing your data.

Make online purchases from secure sites.

On a related note, your security while shopping online is only as good as the site where you're shopping. Only buy from sites with secure, encrypted connections. You can identify these by looking for an address that starts with **https:** (the S stands for secure) rather than simply **http:** They may have a padlock icon next to the address bar. Buying from insecure sites could put your credit card or bank account in the hands of cybercriminals.

Most Internet browsers will notify users if a site is attempting to collect login or credit card information but is not an HTTPS page. Above are examples from Firefox and Chrome, the two most common browsers in the US. (18)

Use stronger and better passwords.

Passwords that are easy for you to remember are easy for someone else to guess. Avoid using simple passwords like "password", your birthday, your pet's or children's names, or numbers and letters in sequence (example: "abcdef" or "123456"). A password 15 characters long that mixes letters, numbers, and special characters will stump most hackers. And password manager software can help you to manage multiple passwords so that you don't forget them.

Be careful what you download.

A primary tool of hackers and cybercriminals is malware—programs or apps that steal your information, pull up unwanted ads, or (in the case of ransomware) hijack your system until you pay up. Any kind of

(continued on page 6)

Basic Rules of Internet Safety (continued)

program could be malware, but you can reduce your chances by only downloading files, programs, and apps from sites you trust.

Practice safe browsing.

The less respectable areas of the Internet (i.e., porn sites and illegal download sites) present opportunities for virus/malware infections or exposing personal data. Criminals know people let down their guard when searching for or purchasing questionable material. Avoid these sites and you avoid the risk.

Keep your antivirus program up to date.

Internet security software cannot protect you from every threat, but it will detect and remove most malware—if it's the current version, designed to handle the latest threats. Keeping your operating system and antivirus programs current gives you an extra level of security that could make the difference.

These guidelines were adapted from Kaspersky. 2019. "Top 10 Internet Safety Rules & What Not to Do Online." Accessed June 10, 2019. https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online

Signs of an online dating SCAM

Professes love quickly.

Claims to be from the U.S., but is overseas for business or military service.

Asks for money, and lures you off the dating site.

Claims to need money for emergencies, hospital bills, or travel.

Plans to visit, but can't because of an emergency.

Source: ftc.gov/imposters

Victoria (Australia) Advocate

Cyberbullying: An Introduction

Cyberbullying is essentially the same as "regular" bullying, only involving computers, cell phones, or other devices. It can involve unwanted and hostile emails and messages, harassment over social media, the upload and posting of hurtful content online, etc. The basic principle is the same: deliberately and repeatedly hurting people.

What happens online doesn't always stay there. A 2013 research study found that 25% of teens who experienced cyberbullying ended up in a face-to-face confrontation with someone stemming from the abuse. 13% were concerned about going to school the next day after it happened. 8% ended up in a physical fight with someone because of something that occurred on a social network site. (7)

Cyberbullying presents just as much potential for violence as bullying in-person. And while it's often considered something that happens between kids and teenagers, anyone who uses the Internet is vulnerable to online harassment. Both adults and kids need to know how to respond.

Cyberbullying: An Introduction

Most cyberbullying falls into one of these five categories (1):

Harassment: the bully sends offensive and malicious messages to an individual or a group, often multiple times. Cyberstalking is one form of harassment that involves continual threatening and rude messages. It can either lead to real-world stalking, or it can be part of stalking behavior that is already happening.

Flaming: online fights via email, instant messaging, or chat rooms. In the course of the fight, people may direct harsh language or images at a specific person.

Exclusion: intentionally singling out and leaving a person out from an online group such as chats and sites. The group may then leave hostile messages or otherwise harass the person they singled out.

Outing: a bully shares personal and private information, pictures, or videos about someone publicly. Taking and sharing pictures of others without their consent can lead to potential felony charges, and social media sites increasingly taking precautions to prevent this kind of abuse.

Masquerading: a bully creates a fake identity to harass someone anonymously. In addition to creating a fake identity, the bully can impersonate someone else to send malicious messages to the victim. This may include “catfishing”—drawing someone into a relationship using a fake persona—which has been used in both cyberbullying and romance scams (15).

Cyberbullying: Facts and Figures

- Nearly half of young people (47%) have received intimidating, threatening, or hateful messages online. (2)
- Teens are most likely to experience cyberbullying on Instagram, Facebook, and Snapchat. While YouTube is the most popular online platform, its use in cyberbullying is relatively rare. (3)
- A 2016 report from the Cyberbullying Research Center indicates that 34% of teens between 12 and 17 have been victims of cyberbullying in their lifetime. About 12% admitted to bullying other people online. (4)
- A U.S. Department of Education study found that 21% of girls and 7% of boys in middle and high school reported being bullied online or by text message in the 2016-17 school year. This is up from 2014-15 when 16% of girls and 6% of boys reported cyberbullying. (14)
- Only 60% of teens who experience online harassment tell an adult. (5)
- Females are more likely to experience cyberbullying than males, likely due to more involvement on social media. (6)
- Victims of cyberbullying are most likely to be targeted because of their appearance, or their perceived intelligence/school performance (either high or low). (5)

AdobeStock

Cyberbullying: The Warning Signs

A child may be a victim if they:

- unexpectedly stop using their devices
- appear nervous or upset while online
- seem uneasy about going to school or even outside
- avoid talking about what they are doing online
- become unusually secretive, especially about their online activity
- avoid or try to get out of going to school
- appear angry, depressed, or frustrated after going online (including gaming sessions)
- experience changes in eating or sleeping patterns
- seem depressed in general or even suicidal

A child may be a cyberbully if they:

- are constantly online, even at night, and get upset if they aren't allowed to use their devices
- quickly switch screens or hide their devices when an adult is nearby
- laugh excessively while using their devices but won't show anyone else what is so funny
- use multiple accounts or one that does not belong to them
- seem overly conceited about their technical skills and abilities
- avoid talking about what they are doing online
- seem overly concerned with popularity or their status in a particular friend-group
- experience increased behavioral or disciplinary issues, possibly including violence or hanging out with "the wrong crowd"
- demonstrate increasing insensitivity or callousness towards other people (8)

Cyberbullying: What Can You Do?

NOTE: if you or someone you know is in immediate danger, call 911 or your local police department.

There are easy things you can do to prevent your child from being bullied online. These tips are not only useful for preventing cyberbullying… they can also prevent targeting by online predators.

- Spend time with your kids online, but make it fun! Get them to teach you the latest technology.
- "If you wouldn't say it 'IRL', don't say it online."
- Teach your children never to post their information like phone numbers, addresses, or locations on their socials.
- If your child meets someone on the Internet and wants to meet them IRL, insist on meeting them too.
- Make sure you approve any picture of themselves your child posts online… and teach them that it's never okay to post inappropriate pictures of anyone.
- Teach your children not to acknowledge rude texts and messages… but to tell you if they turn threatening.
- Encourage your child to delete/block people who keep bothering them or post inappropriate things.
- You are the only other person who should know your kid's passwords and how to unlock their phone.
- Don't allow your kids to install anything on their computer or phone without your approval.
- Find out about the privacy settings about the social media apps your kids use.
- Encourage your child to come to you if anything happens to them online that makes them uncomfortable. (11)

Cyberbullying: What Can You Do?

If cyberbullying does occur:

- Block the users participating in the bullying—keep in mind they may have multiple accounts.
- Document everything that was said or that happened. Take screenshots and make printouts if possible.
- If the bullying is coming from classmates, talk with school counselors or principals about the problem. Avoid confronting the bully or the bully's parents.
- Guide your child through the process of fixing the problem so they learn how to respond in the future.

If you discover your child is a cyberbully, simply taking away or restricting access to their devices may not be the answer.

- Figure out what needs to change, and who needs to be involved. Your child's actions may have affected multiple people, or they may have been part of a larger clique that harassed others. Depending on what they did, you may need to get a counselor or an attorney.
- Find out what they did and why they did it. Have them show you any evidence if it exists. Were they just going along with the group? Were they getting back at someone else? Were they taking out their stress on an innocent victim? Or did they just think it was funny? Explain how their actions could have affected other people as well as them personally. Try not to get too angry, however. They may shut down and stop talking, or it may turn into a fight that resolves nothing.
- Show them that actions have consequences. This could include blocking access or taking away devices, installing parental controls, or turning off their cell phone's data and texting capabilities. Make them remove any damaging messages or other content and have their friends do the same. Have your child make a sincere apology if possible. (This may be in addition to any other consequences mandated by the child's school or by law enforcement.) Watch out for any signs of retaliation by or against your child and respond accordingly. (12)

ONLINE PREDATORS

The Internet can be a haven for sexual predators who exploit children, gaining their trust so they can trick or blackmail the child into sexual acts. They use the anonymity of the Internet to their advantage since they can pretend to be whoever they want. Usually, the perpetrators are men, but sexual predators can be anyone, regardless of sex, race, or sexual orientation. They target both boys and girls of all ages.

Online predators look for emotionally vulnerable children. They take advantage of children with problems at school or home to connect with them, building a one-sided friendship. Predators watch the child's online profiles carefully to see if the child reveals any information accidentally, like email addresses, home addresses, or phone numbers.

Once a predator establishes a relationship, they may send gifts (especially things the parents won't buy them), pornographic pictures via chat or email, or a cell phone so calls or texts will not show up on a phone bill that parents will see. These items are bait used to trap the victim. If the victim tries to break things off, predators may threaten to tell their parents what they have been doing online or about the gifts… scaring the victim into continuing the relationship.

"Sextortion" takes this to a new level if the predator can hack into their device and steal material or information, track down information about them from their assorted accounts, or coerce them into sending nude images or disrobe on a live webcam session. In return for not exposing the victim , the predator will demand money, additional material, or even sex (10). The predator might even threaten them or their family (17).

More information about child sexual abuse—both online predators and the IRL variety—is available in You Have the Power's *Our Children* resource guide.

Many of the same guidelines for preventing cyberbullying (see page 9) can also keep your child safe from predators online. Here are some others:

"YAPPY"

A popular acronym outlining the information you shouldn't share with strangers on the Internet:

Your full name
Address (home, school, or e-mail)
Phone number
Passwords
Your plans

Remember:
"Don't yap about your YAPPY online!"

- Teach your child not to give out personal information online ("YAPPY" makes a good framework).
- Instruct your child to not post or send photos of themselves, their house, their room, their family, their friends, etc., to an online "friend" they do not know.
- Encourage your children to use different usernames for different sites and platforms. Online predators often search for kids' usernames to find their other online profiles and additional information about them.
- Tell your child to not phone someone they met online. If the new online friend has caller ID, the "friend" will find out where the child is and how to contact them.
- Remind your child that people on the Internet can pretend to be someone else. If their new friend likes everything the child does and says, takes the position the child is always right and is unusually supportive and available, be suspicious. If they encourage the child to keep their chats a secret from parents, watch out. Child sexual abusers quickly key in on conflict or inattention between child and parent and move in to fill that vacuum.
- If you think your child is communicating with a sexual predator online, talk openly with your child about the dangers of sexual abuse. Review what is on your child's computer. Use caller ID to determine who keeps calling your child if they get calls from people you don't know. Block any incoming calls where the caller is not identified.
- Assure your child that even if they became involved with a predator, **it's not their fault.** The child is the victim. The other adult is the one to blame.

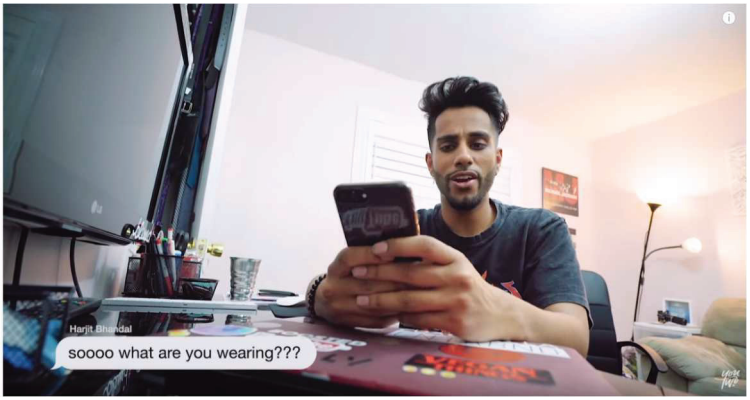
Sexting

Why would someone, especially a child or teenager, send a revealing and potentially embarrassing photo of themselves? Maybe it's meant as a joke, an attempt at seduction, or proof of commitment to a romantic interest they don't want to lose. And certain apps out there make it especially easy (see the back page of this booklet).

Studies have found that teens and pre-teens who sext are more likely to use drugs and alcohol, more likely to have multiple partners, and less likely to use protection. But perhaps the more immediate problem is that once kids hit "send" on that picture, they no longer control where it goes. Anyone can save, copy, and post the image somewhere else.

Even on a platform like Snapchat where images are supposedly temporary, people can still save the pictures for later. Recent leaks of celebrities' photos show that even if you have your photos saved somewhere private, they can still get out.

Both the sender and the receiver of these photos may be subject to bullying, harassment, or sextortion (see page 13). Depending on the ages of the people involved, either party might face criminal charges.



"Sexting Gone Wrong" offers a funny but fairly accurate portrayal of what can happen if you let someone pressure you into sexting. Watch what happens at https://youtu.be/P3K__tVKWRU

Sexting (continued)

Statistics on Sexting

- 48% of teenagers have received a sext (a sexually suggestive message or image). 39% of teens have sent them.
- 86% of teens who send these messages have never been caught by a parent or other authority figure.
- Boys and girls are equally likely to send sexually related texts and images.
- 17% of teens who received a sext-related image shared it with someone else, either forwarding it to them or showing it to them on their phone. 9% of sext recipients shared the images with more than one person.
- 22% of girls and 18% of boys have sexted nude or semi-nude photos of themselves.
- Teens are most likely to sext current, potential, or former romantic interests--boyfriends, girlfriends, crushes, or exes. Fortunately, very few are willing to sext someone they don't know personally.

Self-reported data by teens collected by uKnowKids, an online/mobile parental control software company, which in turn obtained the data from PCs n Dreams, the American Osteopathic Association, Enough is Enough, and the Pew Charitable Trusts.

When is an Eggplant Not an Eggplant?

People who sext, including teens, often use otherwise innocent emojis and code phrases to bully or harass others, or in the course of sexting.

Parentology offers a helpful guide to decoding secret codes you might find in your child's e-mails or texts.

https://parentology.com/40-teen-texting-codes

The tips we've offered regarding cyberbullying and online predators (see pages 11 and 14) can help parents address underage sexting before it becomes a problem--teaching them not to post inappropriate images of themselves or others. Here are some others (16):

- **Acknowledge the problem of peer pressure.** Boys may pressure each other to have girls send them explicit photos. Girls might feel like they have to send nudes because their girlfriends already do it. And again, some people may feel like they have to send photos to keep the other person interested so they won't get dumped.
- **Explain the potential consequences.** Even if your child completely trusts the other person, what if they (the sender or recipient) lose their phone? What if someone goes through their phone and they see the photo? What if someone's phone gets hacked? What if the relationship falls apart and the recipient posts it as "revenge porn" or blackmails them with it?
- **Teach your child how to say no.** Have them explain to other people that they don't want inappropriate photos getting out, even by accident. They have control over their image and how other people see them. If the person asking for photos won't accept that, it suggests a larger problem with the whole relationship.
- **"I'll show you mine if you show me yours" might be a trap.** The recipient could always send someone else's photo instead of their own.
- **Don't let your child become part of the problem.** If they get an inappropriate photo of someone else, they should delete it instead of saving it or forwarding it.
- **If your child does send someone an ill-advised photo, focus on damage control first and punishment later.** Get them to contact the recipient as soon as possible to have them delete it. If they refuse, you have several alternatives. Depending on the situation, you may be able to get help from your child's school, your local police, or even the National Center for Missing and Exploited Children (http://www.missingkids.com). You may be disappointed and angry with your child, but right now they need your support.

MALWARE

Malware is any software designed to damage a computer, client, server or network. It can take any number of forms, from simple viruses and adware to more complicated and dangerous ones like ransomware (see page 6) and keyloggers that transmit keyboard activity (including typed logins and passwords).

Any computer could be affected by malware, no matter how current the antivirus software, whether it's a desktop computer or a mobile phone, what kind or brand of computer it is, what it's used for, or what sites you visit.

Some common signs of a malware infection:

- Freezing, crashing, or restarting constantly
- Sudden loss of Internet access
- Pop-ups or strange warnings
- Unfamiliar error messages
- Slow and unresponsive performance, especially while booting up
- Lack of hard drive space
- Anti-virus or other programs disabled without your permission
- Odd programs showing up in the system tray or the list of installed programs—especially ones you don't remember installing
- Sudden change in your Internet browser home page or default search engine
- Programs turning on and activating without you doing anything
- Sudden increases in data usage
- Unexplained charges on your cell phone bill (caused by malware that makes calls and texts on its own)
- Laptops or cell phone battery charges that run down for no good reason
- People on your contacts list reporting strange calls and texts from your phone
- Devices overheating without heavy use

Malware can be annoying, even scary… but it is not the end of the world if you are infected. There are plenty of legitimate antivirus and antimalware programs available online or retail. (Make sure to install one that's recommended by a source you trust.) Install it and run a scan—it will search out, quarantine, and allow you to delete any malware on your device.

Once the device is clean and secure, make sure to change your passwords… not just for your computer or phone, but for your email, social media, bank site—any website you've used on that device.

Thinkstock

(Be advised that fixing an infected iPhone is harder since Apple does not allow scans of an iPhone's system or other files. You will probably need to wipe your phone entirely with a system reset, then install a security software program compatible with iOS.)

Some steps you can take to prevent a malware infection (9):

- Avoid websites with odd domain names (something besides .com, .org, .edu, or .biz).
- Keep your operating system, browsers, and plug-ins up to date.
- Don't click on pop-up ads while browsing the Internet, especially if they don't look like they're associated with the site you're using.
- Avoid downloading software from peer-to-peer file transfer networks or any site you don't entirely trust. Check the reviews and ratings first.
- Don't click on strange links or attachments in emails, texts, or other messages, even if they come from people you know.
- Back up any important files on a USB drive or online storage so you don't lose them if you get hacked (or if you lose or break your device!)

INTERNET FRAUD

Internet fraud can affect anyone, young or old. And it is increasingly becoming con artists' preferred way of working. A 2019 joint study by the Better Business Bureau, the Financial Industry Regulatory Authority and the Stanford Center on Longevity found that consumers are now more likely to become victims on social media and online marketplaces than over the phone (19).

The true extent of Internet fraud is hard to guess—one study found that only 14 percent of victims reported being a victim of a scam because they were embarrassed, felt it was pointless, or didn't know where to make the report. (14)

The most common type of online scam involves "phishing"--sending a spam email that looks like it came from a trusted source like a bank, a credit card company, a favorite charity. These emails ask recipients to verify their information... and in the process, hand over personal information like credit card and Social Security numbers.

Internet scammers may call or email you asking you to access the computer remotely to fix a supposed problem. Never allow this unless you are working with a trusted technician you have personally contacted to fix a known problem with your computer.

Do not click on emails or links from unrecognized senders. Some scammers create email addresses that are similar to name brand companies. You may consider opting out of commercial email lists altogether.

When shopping online, consider using a credit card instead of a debit card. If your payment information is compromised, the scammer will not be able to drain the full bank account. Debit card fraud protections are usually not as strong as those for credit cards. Make sure to check your bank account after an online purchase and report any strange activity.

Protections against Internet fraud are available on both the state and federal level:

123rf.com

- You can contact the Tennessee Secretary of State's Division of Charitable Solicitations at (615) 741-2555 to verify the legitimacy of a charity. You can also check tnsos.org/charitable/CharitableOrgReports.php to obtain financial reports on charities in the state of Tennessee.
- Additionally, the Tennessee Department of Commerce and Insurance's Division of Consumer Affairs (www.tn.gov/commerce/consumer-affairs.html) protects consumers and businesses from fraud. Check the site for updated consumer resources and news about trending con games.
- The Children's Online Privacy Protection Act (COPPA) requires websites to obtain parental consent for the collection or use of any personal information of users under the age of 13. COPPA was passed in response to the rapid growth of online marketing techniques targeting children. You can report any suspected violations of COPPA to the Federal Trade Commission (FTC) at www.ftc.gov.

The most important part of reporting a scam is going to the right agency:

- For stolen property, contact your local police department.
- For compromised credit or debit card information, talk to the banks or company that issued the card.
- For most scams involving goods and services (nonexistent vacation properties, fake employment agencies, etc), contact the Division of Consumer Affairs listed above. You can also report the scammer to the Better Business Bureau (bbb.org) or the FBI's Internet Crime Complaint Center, known as IC3 (www.ic3.gov).
- If your identity has been stolen, consult identitytheft.gov to find out what you need to do to minimize the damage.

Internet Fraud (continued)

Other resources:

- The FTC offers a wealth of fraud resources at its website (see page 16).
- The Financial Industry Regulatory Authority (finra.org) offers a useful listing of groups that specialize in investment fraud and ways to get your money back. Its online guide "A Recovery Checklist for Victims of Investment Fraud" (available via the website search function) offers some useful first steps.
- The AARP Fraud Watch Network also has a hotline available to anyone, not just older adults: (877) 908-3360. Hotline volunteers can guide you through the next steps. Its website (www.aarp.org/money/scams-fraud) has information and resources on all kinds of fraud, from charity scams to cryptocurrency fraud.

Perhaps the most important thing you can do for yourself is to look after your emotional recovery. State and federal law enforcement are not always successful in tracking down online scammers or helping people get their money back--although reporting the crime helps these agencies discover patterns of abuse that can take down entire companies or industries.

You may feel stupid or ashamed for falling for the scam, and you may hear that from other people. And you may feel like you can't trust anyone ever again, online or IRL. But rather than torturing yourself with blame, you should focus on figuring out how to repair the damage done--the very act of taking action can make you feel a little better--and searching out supportive people who can restore your trust in others. (13)

Works Cited

1. End to Cyberbullying, Inc. "5 Different Types of Cyberbullying." Accessed June 11, 2019. https://www.endcyberbullying.org/5-different-types-of-cyberbullying
2. The Children's Society and YoungMinds. "Safety Net: Cyberbullying's Impact on Young People's Mental Health: Inquiry Report." London: The Children's Society, 2018. Accessed June 11, 2018. https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf
3. Ditch the Label. "The Annual Bullying Survey 2017." Brighton, UK: Ditch the Label, 2017. Accessed June 11, 2018. https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf
4. Patchin, Justin W. "2016 Cyberbullying Data," last modified November 26, 2016, https://cyberbullying.org/2016-cyberbullying-data
5. Cox. "2014 Teen Internet Safety Survey," accessed June 12, 2019, https://www.cox.com/content/dam/cox/aboutus/documents/tween-internet-safety-survey.pdf
6. Patchin, Justin W. "2015 Cyberbullying Data," last modified May 1, 2015, https://cyberbullying.org/2015-data
7. Zweig, Janine M., et al. "Technology, Teen Dating Violence and Abuse, and Bullying." Washington, DC: Urban Institute, 2013. https://www.ncjrs.gov/pdffiles1/nij/grants/243296.pdf
8. Hinduja, Sameer, and Justin W. Patchin. "Cyberbullying Warning Signs". Cyberbullying Research Center, 2018. Accessed June 13, 2019: https://cyberbullying.org/cyberbullying-warning-signs.pdf
9. Malwarebytes. "Malware," accessed June 17, 2019, https://www.malwarebytes.com/malware/
10. Family Safe Computers. "Online Predators," accessed June 19, 2018, http://familysafecomputers.org/predators.htm
11. “Tip Sheets.” Netsmartz.org. Accessed February 28, 2019, https://www.netsmartz.org/TipSheets. Also see “The Parent’s Guide to Cyberbullying.” Connectsafely.org. Accessed February 28, 2019; https://www.connectsafely.org/cyberbullying/
12. Webroot. "My Child is a Cyberbully, What Do I Do?" accessed July 1, 2019, https://www.webroot.com/us/en/resources/tips-articles/my-child-is-a-cyberbully-what-do-i-do
13. Glennon, Lorraine. "What to Do If You've Been a Victim of Scams or Fraud." Consumer Reports, last modified May 1, 2018, https://www.consumerreports.org/scams-fraud/scam-or-fraud-victim-what-to-do/
14. Ho, Sally. "Girls Are Bearing the Brunt of a Rise in US Cyberbullying." AP News, last modified July 26, 2019, https://apnews.com/96a0dad274244d50b32eea1699bcb3a5
15. Patchin, Justin W. "Catfishing as a Form of Cyberbullying". Cyberbullying Research Center, last updated February 7, 2013; https://cyberbullying.org/catfishing-as-a-form-of-cyberbullying
16. Common Sense Education. "Sexting Handbook", accessed August 14, 2019, https://www.commonsensemedia.org/sites/default/files/uploads/landing_pages/sexting_handbook_ce_1020_1_.pdf
17. Savannah Sellers, “Sextortion: Predators Targeting Kids in Video Game Chatrooms,” TODAY, 5:33., Aug. 22, 2019, https://www.today.com/video/sextortion-predators-targeting-kids-in-video-game-chatrooms-66960453859
18. GoatCloud Communications LLC. "Is Your Website Secure for Visitors?" Last updated February 18, 2017, https://goatcloud.com/2017/02/18/http-v-https-v-chrome-v-firefox-time-for-website-security/
19. DeLiema, Marti, et al. (2019). "Exposed to Scams: What Separates Victims from Non-Victims?" Last updated September 12, 2019, https://www.bbb.org/ExposedtoScams

Apps Parents Should Know

The following section is adapted from material provided by the Sarasota County (Florida) Sheriff's Office. Keep in mind that new apps launch all the time while existing apps rise and fall in popularity.

Not all of the apps listed here are entirely problematic. Some of them legitimately allow young people to build and maintain friendships with classmates, distant friends, or people from other parts of the world.

However, depending on the app in question, your child could chat with ill-advised strangers, send and receive inappropriate content, share personal information (see the "YAPPY" inset on page 14), experience cyberbullying, get false ideas about body image, develop distorted ideas about body image, or be exposed to extreme sociopolitical agendas.

Most of these apps have a minimum age of 13 and over, but kids and teens often lie about their age to access them.

InternetMatters.org (which we also consulted in the development of this list) maintains a list of social media apps made especially for kids. They can help your child learn how to interact with people online so they'll be ready to use the more common platforms later. Check out their list at https://www.internetmatters.org/resources/social-media-networks-made-for-kids

Ask.fm lets users create profiles and send each other questions, all anonymously. The app has a bad reputation for cyberbullying.

Calculator% looks like an unassuming calculator app, but it's designed to hide files, photos, and videos. It's one of several apps under different names that can hide password-protected files.

Badoo, Bumble, MeetMe, and Skout are all dating/social networking app where users can chat, share photos and videos, and/or connect based on location. While all these apps are intended for adults, teens are known to create profiles, lying about their age.

Discord is used to communicate with others while gaming online and streaming live video. It's had problems with harassment inappropriate content, and white supremacist content/recruiting attempts in chats.

Grindr was one of the first dating apps geared towards gay, bi, and trans males. The app lets users meet up using a smart phone's GPS feature, which has been pinpoint and stalk individual users.

HOLLA is a video chat app that lets users meet people all over the world in just seconds. But reviewers say they have been confronted with racial slurs and explicit content.

Hot or Not encourages users to post photos of themselves, let other users rate their profile and pics, and chat with strangers. Naturally, many people use it as a hook-up app.

Instagram is one of the most popular photo-sharing apps. It allows users to edit photos and videos, upload them and share them to other social networking sites.

Kik is an instant messaging mobile app that uses a phone's data plan or Wi-FI to transmit and receive data. Kik has been criticized for inadequate parental control over minors' use of the app.

Live.me promotes itself as a live -broadcasting app for aspiring performers and social media influencers. But the geolocation feature used for sharing videos can be used to find out a broadcaster's exact location. Also, users can earn "coins" to "pay" others for photos and videos.

Snapchat may be one of the most popular apps among teens and young adults. While the app promises users can take a photo/video and it will disappear, new features allow users to view content up to 24 hours. Snapchat also allows users to see your location.

TikTok lets users create and share short lip-sync, comedy, and talent videos. With very limited privacy controls, users are vulnerable to cyberbullying and explicit content.

WhatsApp is a popular messaging app that lets users send texts, photos, and voicemails, and make calls and video chats worldwide. Sadly, it has been implicated in the spreading of fake news, scams, and hoaxes.

Whisper is an anonymous social network that lets users post secrets and confessions by superimposing text on pictures. While it's theoretically anonymous, people can communicate by responding to each other's Whispers or using the chat function.

Notes

Printing made possible with the generous support of

of The Community Foundation
of Middle Tennessee

You Have the Power … Know How to Use it
2401 White Avenue
Nashville, TN 37204
(615) 292-7027

www.yhtp.org

www.facebook.com/youhavethepowerknowhowtouseit/
twitter.com/yhtp1
linkedin.com/company/2766127
pinterest.com/youhavepower
instagram.com/youhavethepower2401