Keeping Your Family Safe Online

Protecting your family from online threats and the dangers of bad actors can seem overwhelming, but there are some simple steps you can take to improve your security posture. Following these online rules and tips can benefit the entire family.
Contents

Follow Good Digital Hygiene ............................................................................................................ 3
  Basic online safety ................................................................................................................... 4

Simple Steps to Protect Your Children Online .................................................................................. 6
  What you should know about social media ............................................................................... 7
    Risks ................................................................................................................................. 7
    Best practices .................................................................................................................. 8
  Cyberbullying – It’s happening more than you know ................................................................. 9
    Signs your child might be a victim of cyberbullying .......................................................... 9
    Tactics a child might use to cyberbully others .................................................................. 9
    Cyberbullying and online gaming ................................................................................. 10
  The dangers of sexting .......................................................................................................... 11
    Risks ................................................................................................................................. 11
    Best practices .................................................................................................................. 12

Helping Silver Surfers Navigate Online .......................................................................................... 14
  Top elderly scams ................................................................................................................ 15
  What seniors can do to prevent being scammed ................................................................ 15
  What you can do to protect seniors ..................................................................................... 16
  How to report scams and cyber crime ............................................................................... 17

Additional Resources for Keeping Your Family Safe Online ............................................................ 18
Section 1

Follow Good Digital Hygiene
Basic online safety

Use these tips to improve your cyber hygiene

Secure your home network

- Sign up for Cisco OpenDNS Home. Cisco’s classic, free service with customizable filtering and basic protection
- Follow these simple solutions to help keep your home environment secure

Manage your privacy settings
Want to view or change your privacy/security settings, but don’t know where to find them? Refer to these direct links to update your privacy settings on popular devices and online services.

Set up parental controls and filtering
Consider using parental control tools on all accounts to reduce your family members chances of unintendedly landing on a website. Many highly visited sites like YouTube and Netflix have parental controls that you can set so you can prevent unwanted or inappropriate content from being displayed. Follow these instructions to set up filters on YouTube.

Protect your passwords
- Never use the same password on different accounts
- Create strong, unique and complex passwords
- Wherever possible Use 2-Step verification, also known, as 2-Factor authentication or dual-authentication. As students venture back to school, it is more important than ever to secure remote learning. Try Duo, Cisco’s secure 2-Factor Authentication solution. Learn more about Duo and sign-up for free.
Be credit card smart
Review these online shopping guidelines to keep your internet shopping secure.

Use virus protection software
There are a variety of selections on the market such as Talos Intelligence.

Avoid downloading adware
Although online pop-up offers can seem enticing, they often come at a price.

Turn off location services
Many apps have automatic location services. Make sure you are in control of who is trying to locate you. You can find these controls in your settings on your phone.

Back up your data
Data is the most important asset on your computer. Computers can fail, get stolen or destroyed and even be subject to ransomeware. Backing up your data can help prevent you from being powerless over your data and can help protect and restore your data in case something goes wrong. Here are a few best practice suggestions.

- Make three copies of your data
- Store your data using two different media or methods
- Store the backup device that holds your copied files in a safe place
Section 2

Simple Steps to Protect Your Children Online
You play a critical role in protecting your children online

It’s not enough to rely on technological controls to do this for you: kids need cyber-training and support as they develop. For example, you wouldn’t dream of letting a six-year-old child go shopping alone in the local mall in the evening, so apply the same reasoning to online access. Use real-life physical comparisons like this one as a way of sanity-checking possible online risks.

Here’s another example. When your child comes home from school you might ask about his or her day. What did they do? If this same child has been using a tablet to access the internet for two hours, would you ask similar questions? Show the same interest.

Continuing with this hypothetical scenario, if your child came home from school and was very quiet, or not their usual self, would you try to find out why? Be observant of unusual behavior.

What you should know about social media

Risks

- Cyberbullying
- No privacy protection
- Sharing of information with bad actors
- Loss of ownership of your photos, videos etc.
- Identity theft
- Seeing offensive images or messages
- Meeting bad actors in real life whom they’ve met online

One in three young people in 30 countries said they have been a victim of online bullying, with one in five reporting having skipped school due to cyberbullying and violence¹.

¹ UNICEF September 3, 2019
**Best practices**

- Only talk to people you know in real life
- Guard your passwords and don’t share them with anyone
- Do not download files from strangers or unknown sources. A bad download could lead to viruses and/or malware.
- Be aware that people are not always who they claim to be on the internet
- Memorize this “rule of three”:
  1) Never post any personal information online such as phone numbers, addresses, school names, etc.
  2) Never post inappropriate photos online, even if you think the communication is private
  3) Never arrange in-person meetings with someone you meet online, unless your parents have confirmed the person’s identity in advance
- Remember, once you put something on the internet, it is there forever. If you wouldn’t put the information on a sign outside your house, then don’t share it on the internet. And if you wouldn’t show your grandparents, then you probably shouldn’t be sharing with everyone on the internet.
- Do not build relationships with strangers online
- Do not click on suspicious links from unknown people or websites
- Understand that influencers are marketers
  - Many pay for their likes, and are paid by corporations to market to your children and teens

**Resources**

- [Online parent/child agreement](#)
- [Click here](#) for a list of the most commonly used social media apps by children and teens
Cyberbullying

*It’s happening more than you know*

**Signs your child might be a victim of cyberbullying**

Noticeable increase or decrease in device use, including texting.

A child exhibits emotional responses (laughter, anger, upset) to what is happening on their device.

A child starts to avoid social situations, even those that were enjoyed in the past.

A child becomes withdrawn, depressed, or loses interest in people and activities.

A child hides their screen or device when others are near, and/or avoids discussion about what they are doing on their device.

A child shuts down social media accounts or opens new ones.

**Tactics a child might use to cyberbully others**

Posting comments or rumors online about someone online that are mean, hurtful, or embarrassing.

Threatening to hurt someone or telling them to kill themselves.

Pretending to be someone else online in order to solicit or post personal or false information about someone else.

Creating a mean or hurtful webpage about someone.

“Doxing,” an abbreviated form of the word “documents”, is a form of online harassment used to exact revenge and to threaten and destroy the privacy of individuals by making their personal information/documents public, including addresses, Social Security, credit card and phone numbers, links to social media accounts, and other private data.

---


Cyberbullying and online gaming

Risks

Not everyone will be nice
Some gamers might say nasty things or try to bully and upset other players. This can be done by people you know or strangers.

Not everyone will admit their real age, gender or intentions
Individuals with malicious intent often, deliberately pose as being a different age/gender (fake identity) to build relationships with the person they are pursuing. This happens for many reasons, i.e., to gain the other person’s trust; or possibly to take advantage of their target.

Some people might use games to try and groom children
Grooming is when someone tries to build a relationship or friendship with a young person to trick or pressure them into doing something sexual or otherwise inappropriate.

Some games might have upsetting content
This might include violence, horror, or sex and can be more life-like if you play virtual reality games.

Best practices

Get involved
Play the game with your child or observe when the gaming happens to understand how it works and what your child is exposed to in the game.

Be a nosy parent
Check in periodically with your child about whom they are playing online games with.

Explain cyber-stranger danger
Teach your children about safe online behavior, including not clicking on links from strangers, not sharing personal information, not participating in bullying behavior of other players, and what to do if they observe or experience bullying.

Set boundaries
Establish rules about how much time a child can spend playing video games.

Check game ratings
These inform you whether a game is suitable for younger age groups.

Resources

How to report cyberbullying
What do I do if I think my child is being cyberbullied? Follow these steps.
The dangers of sexting

Sexting is the sending of sexually explicit digital images, videos, text messages, or emails, usually by cell phone. Research finds at least 1 in 7 teens are sexting. Although most of teenagers don’t report sexting, 15 percent of teens say they send sexts and 27 percent receive them. When discussing this subject, you should remember that children can “normalize” some of this behavior, and responsible adults must be on guard to explain that this behavior is not normal and can never be removed from the internet. For instance, an 11-year-old girl tells her friend that a boy has sent her an unsolicited nude selfie, but her friend replies “don’t worry he does that to all new girls, its fine”. They have normalized the behavior, but it is NOT okay, and we need to ensure they know this. For more in-depth information on sexting, visit a newly release report Look At Me, Teens, sexting and risks from the United Kingdom.

Risks

Sexting between an adult and a minor constitutes child pornography and is a felony.

Sexting can lead to sexual bullying.

Sexting can open the door to sexual predators.

Sexting puts teens at risk for blackmail.

Sexts never go away.

Exposure to sexting can ruin a person’s reputation.

Not everyone in real-life is who they portray themselves online.

Sexting can lead to emotional stress – If images fall into the wrong hands, the victim’s mental health can be compromised which can lead to depression, isolation, eating disorders and possible worse consequences such as suicide.

---

5 Source: CBS News
6 Time.com
7 Source: Cyberbullying.org and Internetmatter.org
Best practices

Give your children or teen an out
Children are often peer pressured into sending explicit images online. Help them come up with a strong explanation to tell their friends why they don’t want to send explicit images. Example: Many employers research potential candidates online and finding unwanted information or content could jeopardize the candidate’s chances of obtaining the position.

Share with your children what to do if they receive an explicit text
1) Don’t forward it to anyone
2) Delete the image
3) Report the image (if online) so it can be removed
4) Tell the person not to send images anymore
5) Block their number or account
6) Make a report to your mobile phone company if the images don’t stop

Discuss online risks
Be open and talk to your children about why security awareness is so important. Having discussions about what they view online each time they access the internet builds a routine to help emphasize safety measures and builds trust with your children.

Remind children that no message is truly private
Make sure your kids understand that messages or pictures they send over the internet or on their cell phones are not truly private or anonymous. Make sure they know anyone can—and often will—forward their pictures or messages to others. Ask your child what their boyfriend or girlfriend will do with those pictures if they break up.

Get to know your children’s friends
Know who your children are communicating with online and on their cell phones. Do your best to learn who your kids are spending time with online and on the phone by checking their messaging buddy lists, social networking friends, and mobile device address/contact lists.

Teach your child to unplug occasionally
Consider placing limits on electronic communication. Check out the parental controls offered by your mobile provider. Many mobile carriers offer family plans that allow you to limit the amount and types of text messages your kids can send. Disable attachments on text messages.

Set expectations
Make sure you are clear with your children about what you consider appropriate online and texting behavior.

Resources
- Look At Me, Teens, sexting and risks from the United Kingdom
- Learn more about sexting

Source: Cyberbullying.org and Internetmatter.org
What can you do?

1) **Educate yourself**
   It can be hard to tell your child what to look out for if you're not completely sure yourself. Online threats change all the time, so it pays to follow the news and stay alert to the newest dangers.

2) **Get involved and stay involved**
   Keep your computer in an open area so you can monitor computer activity. Take an interest in where your children are going on the internet.

3) **Establish your own rules**
   Establish clear boundaries with your children about what is and isn’t acceptable when they are online. Draft an age-appropriate online contract so your child knows and agrees to the rules. Install and use parental controls to help enforce these rules.

4) **Keep lines of communication open**
   Have local house rules but plan how you will react to various possible scenarios. Your child might be upset or confused by what has happened, they might feel it’s their fault. Be prepared to handle questions and try not to over-react.

5) **Teach kids that the internet is forever**
   Once the information is out there, whether it is comments, photos, or video, it is there forever. And as the parent or caregiver, remember that you should not overshare information and details of your children! A lot of material has been innocently uploaded by proud parents, without thinking of the ‘internet is forever’ concept.

6) **Keep your child’s privacy private**
   If you are sharing pictures of your children online with family and friends on Facebook or another social media platform you are sharing it with the world. Once their pictures are out there, they are out there for everyone to share.

7) **Be mindful of your circle of friends and family**
   Many times we are told about the stranger dangers in the world, but we need to be mindful that trusted individuals can unfortunately be a harmful source. Be aware of who is befriending your child and teen online.
Section 3

Helping Silver Surfers Navigate Online

Scamming the elderly is a multibillion-dollar business that drains seniors of their retirement funds and government benefits. Bad actors do not discriminate. They take from all regardless of race, rich or poor, healthy or ailing\(^9\). Recent estimates from the United States Department of Justice indicate that elderly people lose about $3 billion to scammers every year. And less conservative estimates project seniors lose up to $36 billion annually\(^10\).

\(^9\) \(^{10}\) agingInPlace
Top elderly scams

Malware
Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Fake sweepstakes or lotteries
A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing often claiming that you have won a large sum of money or prize.

Counterfeit prescription drugs
Counterfeit medication or drug is a medication or pharmaceutical product which is produced and sold with the intent to deceptively represent its origin, authenticity or effectiveness.

These fake medicines may be contaminated or contain the wrong or no active ingredient. Counterfeit drugs are illegal and may be harmful to your health. For more information click here.

Pop-up ads peddling fake anti-aging products
Fake pop-up advertising can include phone numbers to call, reputable brand names you recognize and initiate unsolicited noise while your surfing the internet. Avoid clicking on these ads that open in a separate window, advertise free or heavily discounted products and services, and can potentially enable others to capture your personal information and/or maliciously steal your money.

Sweetheart scams
Online dating is common practice in today’s day and age to find romance. Be cautious of people who appear too good to be true, ask for personal information or request money. Make sure you investigate the dating site before you create a profile.

Fake credit card scams
There are many scammers out there trying to make a quick buck. Many will pose as credit card issuers, suggesting that your personal information needs to be updated for one reason or another all to gain access to your assets. Tip: Never give out personal information over the phone or in an email to people you do not know or have not called yourself.

Employment scams
Job and employment scams trick individuals into handing over their money in return for a “guaranteed” way to make fast money with little effort.

Phony free vacations
Be on the look out for travel scams because they are out there. Before booking your next adventure, check out these 10 red flags that could be a possible travel scam.
What seniors can do to prevent being scammed:

**Manage their transactions**
Never make unusual money transfers without discussing with a friend or relative. Without exception, try to talk to someone first. Criminals will rely on pressuring seniors and will do everything they can to ensure they don’t talk to someone else! For instance, keeping them on the phone and implying urgency.

**Don't give away personal information**
Consult family members and caregivers about potential purchases before going through with them. Never give away information on an impulse unless you are positive it’s to a trusted source, for example, a doctor or company you’ve done business with before.

**Watch for too-good-to-be-true scams**
If a deal on a vacation, prescription drug, or anything else seems too good to be true, it probably is. Research the company offering the deal.

**Don't fall for bad actors**
If someone is trying to sell something to you or get more information out of you, ask for verification about who they represent. If they refuse, walk away or hang up the phone.

**Know that the government will only notify you by mail**
The U.S. government never uses email or website ads to notify you of an infraction or collect personal information from you.
What you can do to protect seniors

Individuals are still the first line of defense for stopping fraud against senior citizens. You can help keep the elderly safe with these actions:

**Be your seniors “safe place”**
Foster a relationship of gentle trust. Seniors may feel reluctant to give up control and therefore, keep secrets about decisions or certain arrangements. Let them know that you are there to offer help, understanding and not to take over or judge. This will hopefully lead to an open dialog that can give you the insight necessary to protect them effectively.

**Regularly call or visit seniors**
Be suspicious if a senior citizen has a new “best friend”, becomes socially isolated, never seems to be available or able to come to the phone, or is hesitant to have contact with others unless a caregiver is present. This could indicate that someone has undue influence on the senior’s behavior and decision-making. Try to encourage your friend to always chat through money ideas and transactions with you first. Telling someone before the transaction will help a lot.

**Block solicitations**
- Opt-out of commercial mail solicitations. You can arrange for a ban of five years at a time with the Direct Marketing Association’s mail preference service
- To eliminate unsolicited offers for credit, go to Opt Out Prescreen
- Tools for controlling mail, email and telephonic direct marketing contacts

**Set up safeguards at the bank**
If you’re concerned about your relative’s financial decision-making, set up a small account at a local bank for them.

**Arrange for limited account oversight**
Ask financial institutions to send statements and alerts to a trusted person who has no direct access to the senior’s accounts, so that person can check for fraud.

**Keep loved ones informed**
Let seniors know they could be scammed on the internet through things like emails and pop-up ads. It is good to remember that if it seem to good to be true, it probably is.

**Check seniors’ bank accounts regularly**
Check your loved one’s bank accounts and retirement accounts often with an eye for odd purchases or withdrawals.

**Visit seniors to discuss their monthly bills and prescriptions**
They may mention a “new” bill or a “cheaper” way to get the prescriptions they need in passing, so follow up on any of those.

**Make sure your loved ones know not to make any impulse online buys**
Pay special attention to a “deal” ending in the next few minutes.

**Be mindful of family and friends**
Although we want to believe that most people have good intentions, it is often family members or friends that will take advantage of ailing seniors.
How to report scams and cyber crime

More than 80 percent of online scams go unreported, partly because people don’t know how or where to report them.

Reporting Resources:

**Banking and Retirement Fraud  (*Contact your bank/retirement facility immediately*)**
Scams of the elderly often involve money coming from bank or retirement accounts. As soon as you discover that you or someone you know has been scammed, notify whomever deals with the account. You might still have a chance to recover money, or it might not have left the account yet.

**Identity Theft**
If you have been a victim of identity theft, report it [here](#).

**Investment Scams**
- **Securities and Exchange Commission (SEC)**
  If you’ve “invested” in an opportunity that you later suspect is a scam, report it to the [SEC](#).

**National Center For Missing and Exploited Children – Cyber Tipline.**

**Online Business/Shopping Scams**
- **Better Business Bureau (BBB)**
  If you suspect a business is scamming you online, report it to the [Better Business Bureau](#).

  A map on their website identifies businesses all over the country that have tried to scam people in person and on the web.

**Phishing and Telemarketing Scams**
- **Federal Trade Commission (FTC)**
  The FTC shares consumer complaints covering a wide range of categories, including online scams, with local, state, federal, and foreign law enforcement partners. It cannot resolve individual complaints, but can give you information on the next steps to take. File a complaint [here](#).

**Social Security Fraud**
- **Social Security Administration (SSA)**
  [The SSA](#) is a great place to report potential scams involving your Social Security number or funds.

**Cyber Crime**
- **The Internet Crime Complaint Center (IC3)**
  IC3 is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. Complaints may be filed online. Keep in mind, you will need to contact your credit card company directly to notify them if you are disputing unauthorized charges on your card or if you suspect that your credit card number has been compromised.

- **Federal Bureau of Investigations (FBI)**
  The [FBI](#) deals with blue- and white-collar crimes and will investigate online scams, especially if money is involved.

**Cyberbullying**
If you suspect that someone is being cyberbullied: Find out how and where to report it [here](#).

**Foreign company complaints**
[ECConsumer.gov](#) accepts complaints about online and related transactions with foreign companies.
Section 4

Additional Resources for keeping your family safe online
Learn more about keeping your family safe online

- Staysafeonline.com
- Download tip sheets, lesson plans and other safety resources
- Cyberbullying, sexting, social networking, and more
- U.S. Federal Trade Commission’s main resource to educate consumers on staying safe and secure online

Cybersecurity and Infrastructure Security Agency (CISA)

Concerned Parent’s Internet Safety Toolbox

Identity Theft Resources

National Do Not Call List - Action: Register your phones

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.

Global Resources:

Children Helpline International

EMEAR NSPCC

EMEAR Secure Internet Centre (SIC)

APJC Go safe online

Homeland Security

UNICEF East Asia – Child Protection in the digital age

UNICEF - End Violence online