To help protect your kids and grandchildren, be sure to set up parental controls on all their electronic devices, including their smartphone, tablet, computer, video game systems, and TVs.

BONUS

3

In this chapter, you'll discover ways to help protect the young people in your life from the potential dangers on the Internet, while still allowing them access to this vast and powerful resource. Topics include:

- ➔ Teaching young people to stay safe online
- ➔ Learning about parental controls offered by smartphones, tablets, computers, video game systems, smart TVs, and cable TV boxes (as well as digital video recorders)
- ➔ Setting online access and usage limits

Protect Your Kids and Grandchildren Online

Children frequently are more tech savvy than their parents and grandparents. Children have grown up with the Internet, touchscreens on their smartphones and tablets, and access to advanced technology when playing their favorite video games. They have no fear of this technology. It surrounds them, and they're exposed to it every day in all aspects of their lives.

When young people have a question, instead of looking up the answer in an encyclopedia or visiting the library, they type their question into a search engine, or ask Siri or another digital assistant that's built into their smart speaker, mobile device, or computer. When they want to interact with friends, they often send a text message (instead of making a phone call) or virtually meet up on whichever social media service is currently popular.

This comfort with cyberspace is good in many ways, but it also has some potential pitfalls.

Understanding the Potential Problem with Young People Having Online Friends

When you ask a young person to talk about their "best friends," they rarely differentiate between the kids they know in real life from their neighborhood, soccer team, or school, versus their online friends, whom they've never met in the real world, but often spend hours per day interacting with when playing video games or using social media.

Although young people see no problem with this lack of differentiation between real life and online friends, adults often and immediately understand the inherent risks associated with interacting with random people online and referring to these people as "friends." After all, "friends" are people you typically trust, open up to, and share information with.

In cyberspace, anyone of any age can create an online persona and pretend to be whomever they want. Young people may know this, but rarely understand the implications.

For example, a 40-year-old man from anywhere in the world can go online, easily pass himself off as a 15-year-old, and freely interact with and mislead young people into revealing personal information about themselves—where they live, their parents, and when their family will be on vacation, thus leaving their home empty.

With even the smallest amount of technical know-how, anyone can participate in a multiplayer video game—via the Internet and a Nintendo Switch, Sony PlayStation, or Microsoft Xbox video game system or computer—and freely interact with your child or grandchild, especially if everyone is using a headset with a built-in microphone to freely communicate during a game.

In other words, anyone who plays an online-based multiplayer game can freely interact with strangers. When what's discussed relates only to the game being played, all is fine. It's when your child or grandchild begins talking to strangers about other topics that their safety and privacy can easily be compromised.

If you've ever watched young people play a video game, concentrating on the challenges at hand, they often are hyper-focused on what's happening on the

game screen. When an adult is posing as a young person and also playing the multiplayer game via the Internet, it's easy to interject seemingly harmless conversational questions, such as: Where are you from? What grade are you in? What's the name of your school? Are your parents home right now? What do your parents do for a living?

Young people who are feeling bored or lonely may go online and play multiplayer games while seeking out people to talk to and share personal details about their lives with—often with no adult supervision.

Because the people in the game are perceived as "friends," and everyone is having a good time playing the same video game, young people rarely censor their responses to questions, even though in real life, they know never to talk to strangers.

Even if you have no understanding of the games your children or grandchildren are playing, you can teach them the difference between real-life friends and online friends. Drill into their young heads that online friends who they've never met may be nice and fun to play games with, but they are still strangers and should be treated as such.

It's important to teach young people never to answer certain types of questions when interacting with people online. Some of the topics they should refuse to discuss with online friends, whom they've never met in real life, include:

- Giving out their first and last name
- Telling people where they live
- Sharing information about what school they attend, what sports teams they play on, and what afterschool activities they participate in
- Sharing their parents' names and what their parents do for a living
- Revealing when their family is going on vacation and where they're going
- Giving a physical description of what they look like, or revealing their age
- Disclosing any usernames and passwords they use on their gaming systems, personal email accounts, school-related accounts, and social media

Young people need to understand that if a stranger is looking to gather information from them, they might not be so obvious about it. Instead of asking, "Where do you go to school?" an online child predator might ask, "What's your teacher's name?" or "What's the name of the football team's mascot at your school?" Using this information, it's easy to go online and track down what school someone attends and potentially what grade they're in.

An online predator looking to obtain information from a child might also ask a trick question to gather information, such as, "I think I know you! Aren't you in Mrs. Smith's class?" A typical answer might be, "No, my teacher's name is Mr. Johnson. I go to…."

In addition to teaching children not to reveal personal information online, it's even more important to instruct them never, under any circumstances, agree to meet with an online friend in person without being accompanied by a parent or grandparent.

Again, after days, weeks, or months of talking and interacting online, an online friend may be perceived as a "best friend," so your child might not hesitate to agree to meet that person in real life. If a child is asked to meet with an online friend, they should know to discuss the interaction with a parent or grandparent immediately. The person they're communicating with usually will be a legitimate kid looking to meet their online friend. But, there's always the chance that the online friend could be an adult predator who is looking to endanger your child.

As an adult, you can still allow children to play online games and interact with other young people on social media, but you should take some steps to ensure their safety, beyond just teaching them to avoid sharing personal information.

These steps include:

- Monitoring your kids' or grandkids' online activities in person—and making sure young children know that you, as a grownup, will be monitoring their activities.
- Paying attention to the online games they are playing. All games have an age-appropriate rating, just like TV shows and movies. Simply by looking at this rating and reading a description of a game, you can easily determine

what age the content is suitable for. Don't allow young people to play games that have an "M" (Mature) rating, especially if it's an online game. In this situation, the people they wind up playing with online will likely be older.

- While watching your kids or grandkids interact online, ask to play the online games with them, or allow them to show off their gaming skills to you as they explain exactly what they're doing and with whom they're doing it. Show interest in their activities and have them teach you about the technology.
- Turning on the parental controls. When you do this, make sure you do not share the parental controls password or PIN with the young people who will be using that equipment, and don't use a password or PIN that they'll easily figure out on their own. Make sure they understand that parental controls are not about punishment—they're about safety.
- Installing optional child monitoring software onto their computers and mobile devices. In addition, almost all browsers provide the option of blocking access to restricted sites, whether it's part of the browser's settings, or if it's something you have to download.
- Obtaining all your child's account usernames and passwords and forbidding them from creating additional accounts without your knowledge. This includes on their computer, smartphone, tablet, gaming system, and on the social media services or online services they're active on.
- Signing in to a young person's online accounts regularly and reviewing their activities.
- Making an effort to understand what games and online services a young person is using and what types of content they're being exposed to. Monitor who they're communicating with and what's being discussed.
- Allowing a young person to have Internet access only in areas of their home where they know an adult can walk in at any time and look over their shoulder to see what they're doing. If a child feels safe in their bedroom, with the door closed, they're more apt to do things online and share information that they shouldn't.

>>>Go Further

UNDERSTAND GAME RATINGS

The Entertainment Software Rating Board (www.esrb.org) has developed a comprehensive rating system for computer and video games based on content and age appropriateness.

- **RP (Rating Pending):** Sometimes seen in a game's advertising before it's released, this means Rating Pending. The game has not yet been rated by the ESRB.
- **EC (Early Childhood):** Means the content is suitable for a preschool audience.
- **E (Everyone):** Refers to content that's suitable for everyone—all age groups.
- **E 10+ (Everyone over the age of 10):** Means that the content is suitable for everyone over the age of 10.
- **T (Teenage):** Means games that are suitable for a teenage (13 and up) audience.
- **M (Mature):** Given to games that contain adult themes, graphic violence, and adult language. These games are not suitable for people younger than age 17.
- **AO (Adults Only):** Means the games should not be played by anyone under the age of 18.

Ratings are offered to provide a guideline for parents, but it's up to the parents to determine what games are suitable. Keep in mind that if you make a big deal out of preventing children and grandchildren from playing an M-rated game, they'll often just go to a friend's house to play it. It's important to set guidelines and expectations for what games they can play.

As a parent or grandparent, set realistic guidelines for what games kids or grandkids can play, where and when they can be played, and how much time they can be played per day. It's up to you whether you use game time as a reward for finishing homework or household chores, or block gameplay as a punishment when a child misbehaves.

It's Not All Good

Immaturity Leads to Unwise Decisions

Although the young people you're close to might be more technologically savvy than you are, they lack maturity. This is what can get them into trouble when they're using the Internet or the latest technologies. So, even if you don't fully understand the technologies they are using, you can still guide and protect them, monitor their activities, and prevent them from making potentially dangerous mistakes—like sharing personal information with strangers or accessing content that's not suitable for them.

Taking Advantage of Parental Controls

Built in to the operating systems of smartphones, tablets, smart TVs, video game systems, cable TV boxes, computers, and computer modems/routers are optional parental controls.

Depending on the device, you can use parental controls to control how much time is spent using a device or to block certain types of inappropriate content. Parental controls can be used to set a daily or weekly time limit for using that technology or to monitor a child's activities.

Regardless of what equipment you're setting up parental controls on, you typically do it by accessing the Settings or Setup menu when using the device. As an adult, you'll be prompted to set up a Parental Controls password or PIN that'll allow you to set, lock down, or unlock the device.

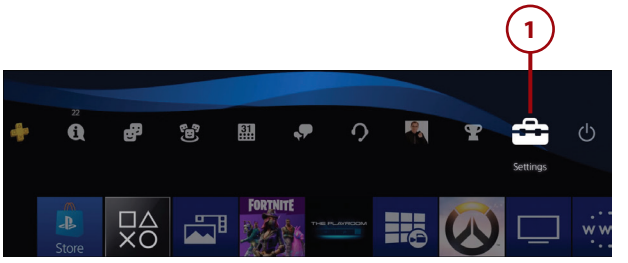
When setting this parental controls password, do not use the same password you use elsewhere, which the young people in your life may already know. And make sure you don't choose a password or PIN that your child will easily be able to figure out.

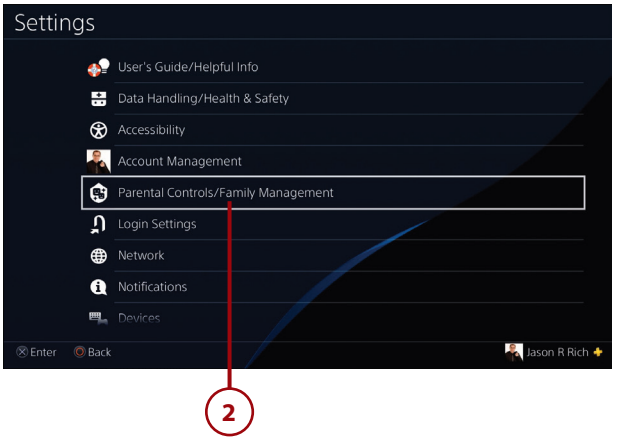
The parental controls offered by each device vary. It's important to invest the time to review each related menu and submenu to develop an understanding of what's offered. You can then adjust the options that you deem important.

Adjust Parental Controls on a Sony PlayStation 4 Video Game System

The Sony PlayStation 4 (PS4) is a popular video game system. Like other gaming systems available, it offers optional parental controls. To turn on and adjust these controls on a PS4 (the steps to follow on other gaming systems are very similar), follow these steps:

1. Connect the gaming system to any HD television set, turn on the gaming system, and select the Settings menu.
2. From the Settings menu, scroll down to the Parental Controls/Family Management option and select it.





Keep Parental Controls Current

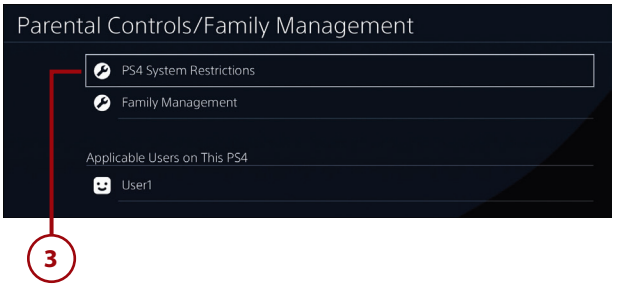
Parental controls need to be set up and turned on only once per device. However, as new operating system or software updates are introduced, new parental control options are sometimes offered. Periodically review the parental control settings to ensure they're up to date and adjusted to a level you are comfortable with and age appropriate for the child you want to protect.

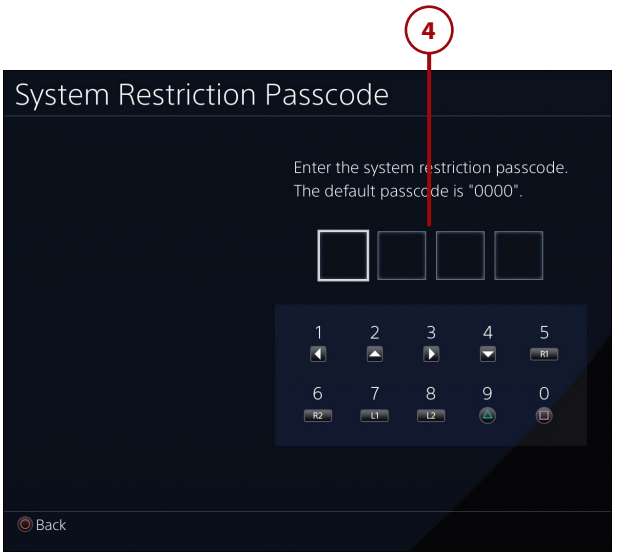
3. Choose to set up system restrictions that apply to all players, to set up individual user accounts for each child, and then to set up individual restrictions based on their respective ages. Start by selecting the PS4 System Restrictions option.

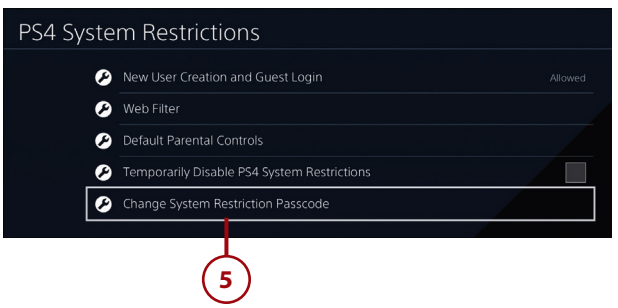
4. When prompted, enter the System Restriction Passcode. This is the code you, as the adult, will use to unlock the system to alter the settings. (Again, choose something your child won't easily figure out.) The default code is 0000, which is what you'll initially use until you change it.

5. From the PS4 System Restrictions menu, scroll down using the controller navigational buttons to move the on-screen cursor. Highlight and select the Change System Restriction Passcode option.

6. Create a new, four-digit passcode. Don't use 0000 or anything similar, and avoid the birthdays of all family members, because this is something a child will easily figure out. Enter the new code, and confirm it. Also, don't forget this password, or you (as the adult) could be locked out of the system in the future. (Not shown.)





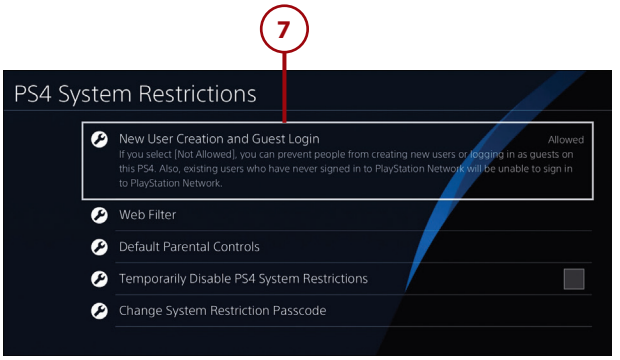


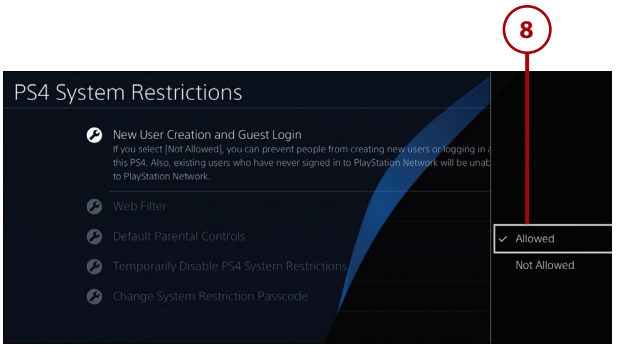
7. Return to the PS4 System Restrictions menu and select the New User Creation and Guest Login option.

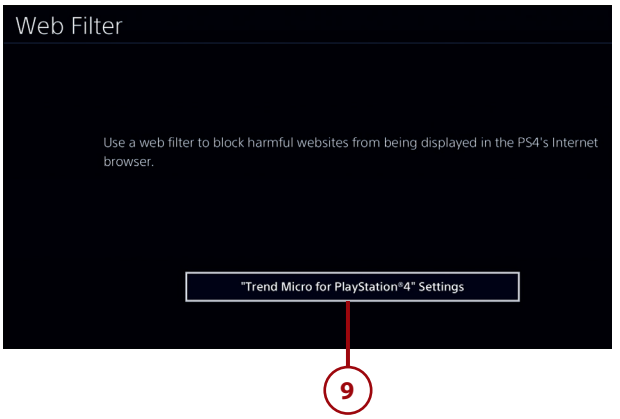
8. Select the Allowed option if you want people (other than yourself) to be able to set up new user accounts or sign in to the system as a Guest user. Select Not Allowed to prevent other people from setting up new accounts or using a Guest account.

9. The PS4, like most gaming systems, has a basic web browser. Select the Web Filter option from the PS4 System Restrictions menu, and then select the "Trend Micro for PlayStation 4" Settings option to download and install a web browser filter (for free) that will prevent inappropriate content from being accessed via the PS4's built-in web browser. Follow the onscreen prompts to find, download, and install the filter.

10. From the PS4 System Restrictions menu, select the Default Parental Controls option to set up or adjust the default parental control options after the feature has been turned on. From this submenu, select the Age Level for Games option. (Not shown.)





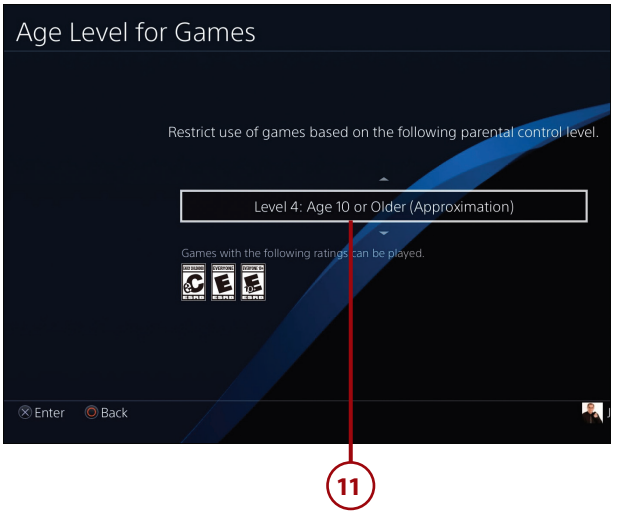


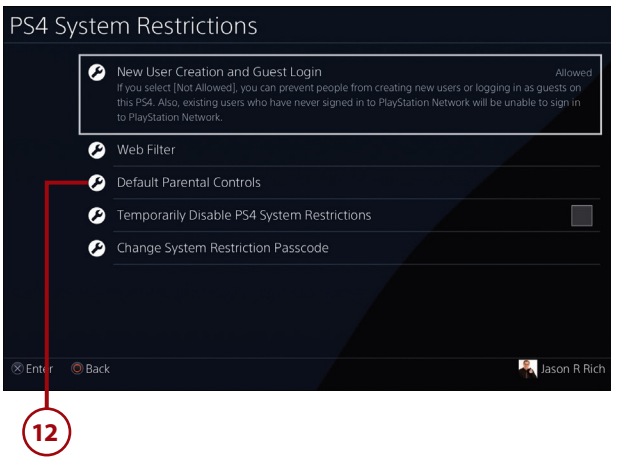
11 You can prevent kids and grandkids from accessing inappropriate content. From the Age Level for Games submenu, choose an age group (and rating level) for your kid or grandkid; for example, you can prevent a 10-year-old from playing an "M" or "AO" rated game.

12 Return to the Default Parental Controls menu and adjust each of the other submenu options to a level you're comfortable with.

13 After reviewing and adjusting each of the submenu options in the PS4 System Restrictions menu, follow the onscreen prompts to save your changes. (Not shown.)

14 Return to the main Settings menu, and determine whether you want to adjust other Settings-related options. Select one menu option at a time to review the submenu options available. When you finish, exit out of Settings. From this point forward, the parental controls and related settings you turned on or adjusted will be active. (Not shown.)





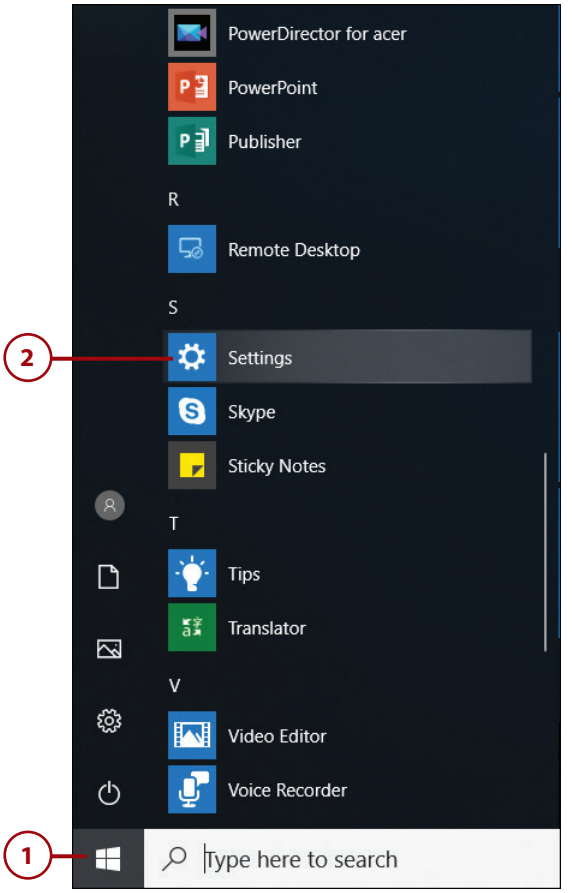
Some games that are installed or played on the various gaming systems might also have their own game-specific parental controls built in to the game. These controls might allow the game to be played, but prevent a child from playing the multiplayer version of the game or from being matched up with strangers.

If you believe there's a need to turn on and use parental controls on your kids' or grandkids' video game system, chances are, you'll also want to adjust similar options on all the other equipment they'll be using. The following section has directions for turning on and adjusting parental controls related to some popular computers, smartphones, and tablets. Remember, you can almost always find the parental controls menu option by accessing a device's Settings, Setup, or System Preferences menu.

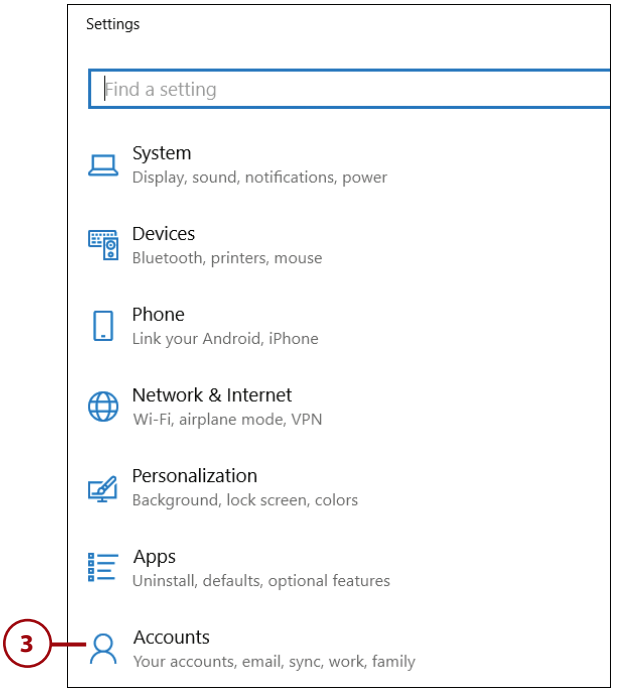
Adjust Parental Controls on a Windows PC

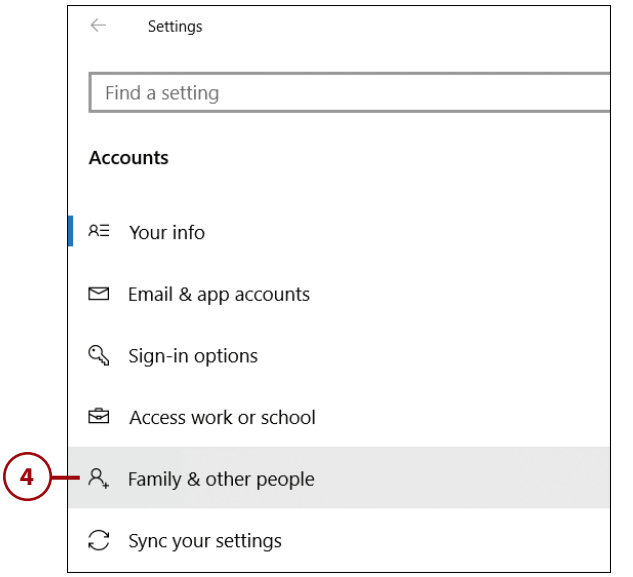
On a Windows PC, to adjust the operating system's built-in parental controls, follow these steps:

1. Click the Windows logo displayed in the lower-left corner of the screen.
2. Scroll down the Applications menu. Click Settings.

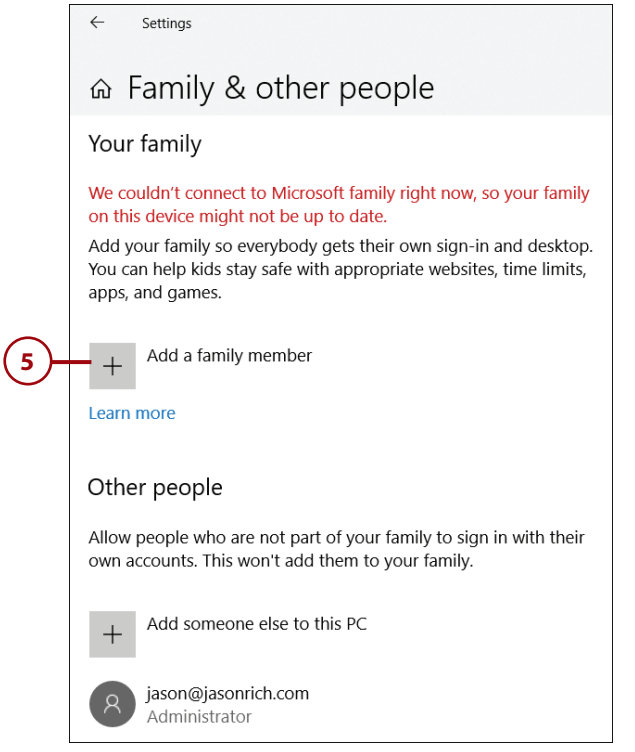


3. Select the Accounts option.
4. Select the Family & Other People option.





5. Select the + Add a Family Member option.
6. For each family member account you set up, follow the onscreen prompts to adjust options for activity reporting, screen time, content restrictions, and online spending. If you're setting up this feature on a notebook computer, for example, you can also turn on a feature that allows you (the parent or grandparent) to track the location of family members using the Find Your Child feature. (Not shown.)



Add More Parental Controls

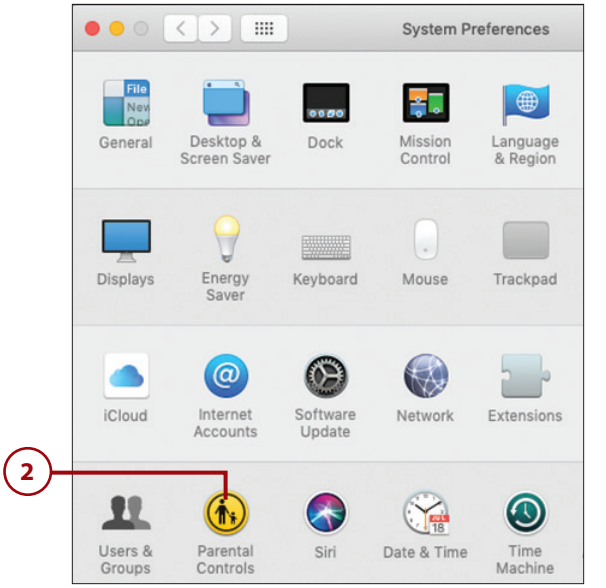
You can purchase and download additional parental control software for any Windows PC, Mac, and mobile device that will give you even more control over what a young person can and can't do when using the equipment. This includes monitoring and protecting their activities on social media.

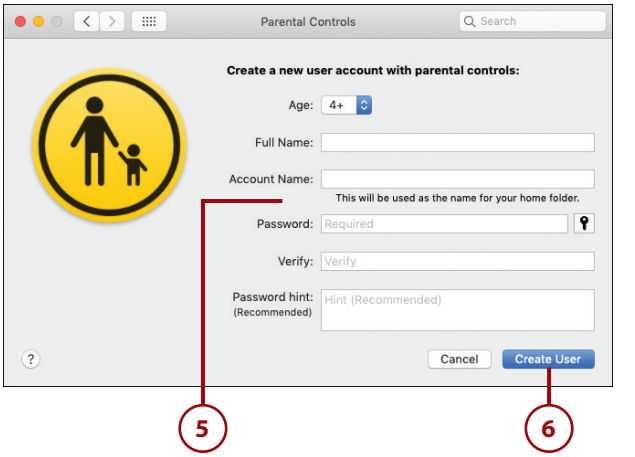
Some of your options include Bark (www.bark.us), FamilyTime (https://familytime.io), Net Nanny (www.netnanny.com/products), Norton Family Premier (https://pr.norton.com/norton-family-premier), and WebSafety (www.websafety.com). A monthly or annual subscription fee applies to use these optional applications.

Adjust Parental Controls on a Mac

On a Mac, to adjust the operating system's built-in parental controls, follow these steps:

1. Launch System Preferences. (Not shown.)
2. Select the Parental Controls option from the System Preferences menu.
3. For each child, one at a time, select the Create a New User Account with Parental Controls option, and click Continue.
4. Type in your own Admin password for the computer. (Not shown.)
5. From the Create a New User Account with Parental Controls screen, fill in each field with information about your child. You'll be prompted to create a password for each child's account. This will be the password he or she will use to log in to the computer. After the kids log in using their account information, the parental control settings you've pre-selected will be active.
6. Click the Create User button.



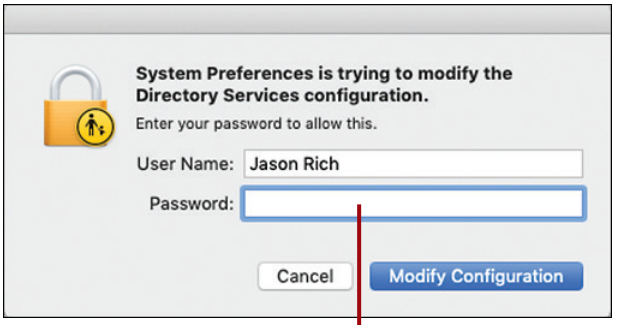


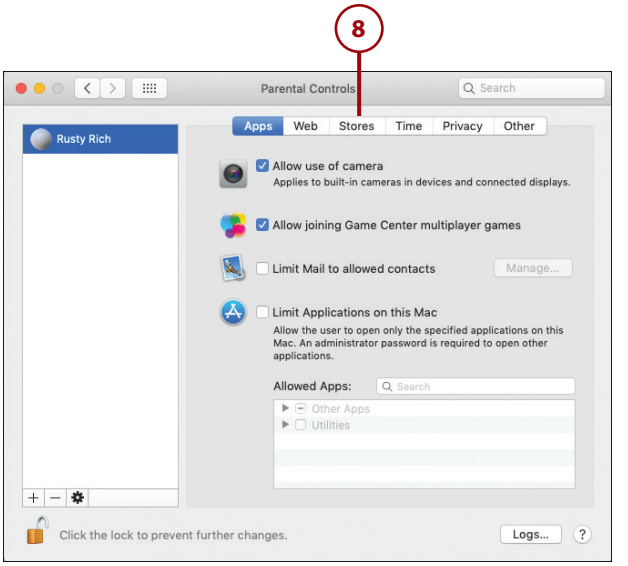
7. Re-enter your Admin password when prompted to create the new account. Click the Modify Configuration button to continue.

8. From the Parental Controls screen, one at a time, click the Apps, Web, Stores, Time, Privacy, and Other tab, and then adjust the options in each submenu for the controls you want to activate.

9. For example, select the Web tab, and then select the Try to Limit Access to Adult Websites option if you want to block adult content, or select the Allow Access to Only These Websites option, if you want your child to only be able to access specific websites that you pre-select. (Not shown.)

10. When you're finished adjusting the various Parental Control options, exit out of System Preferences to save your changes. (Not shown.)

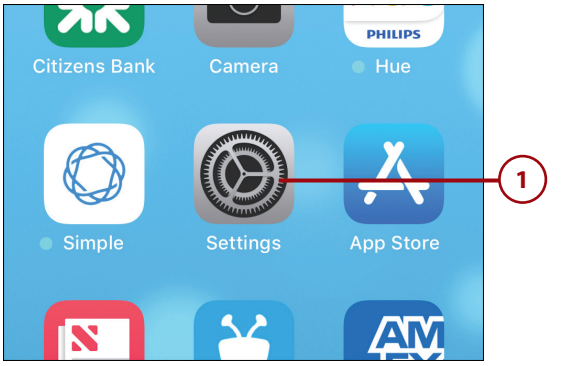


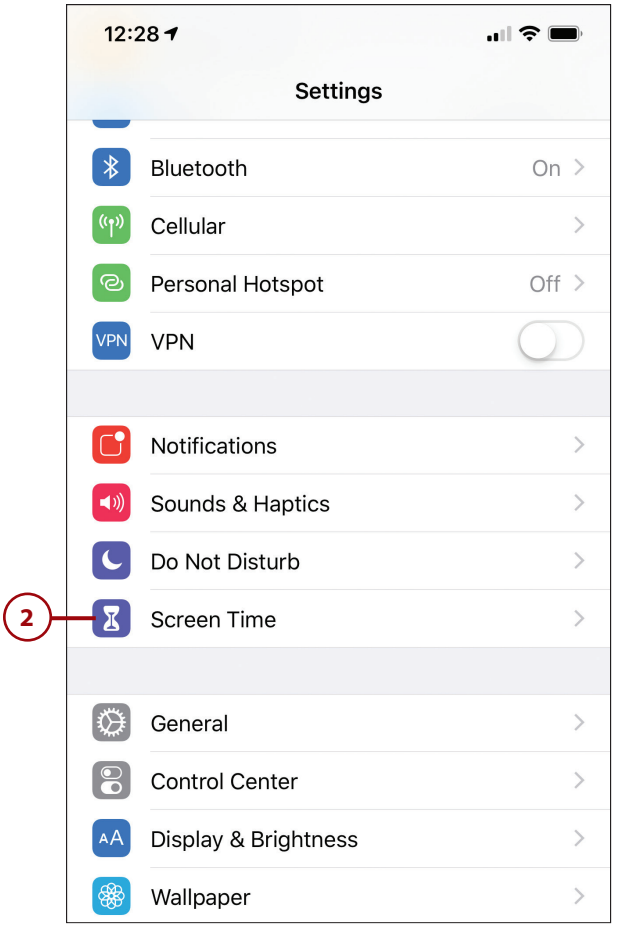


Adjust Parental Controls on an iPhone or iPad

On an Apple iPhone or iPad, to adjust the operating system's built-in parental controls, follow these steps:

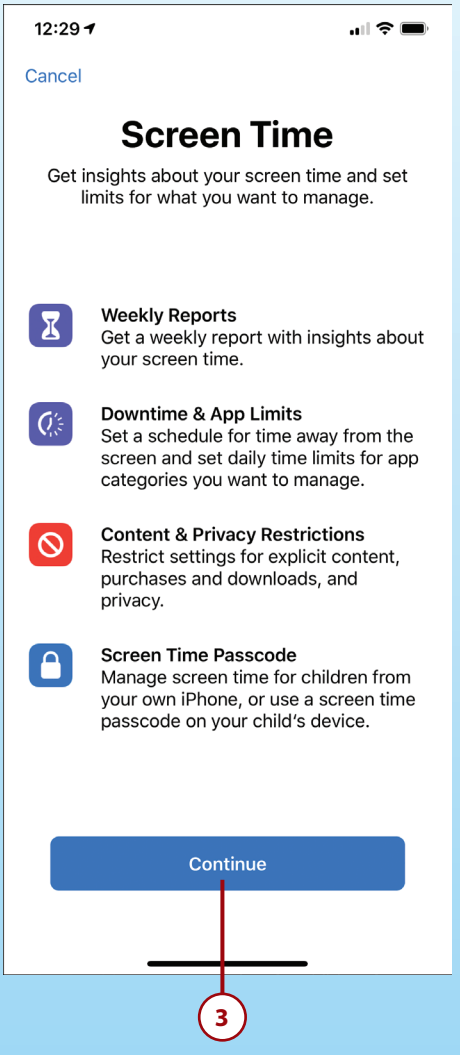
1. From the Home screen, tap Settings.
2. Tap the Screen Time option.

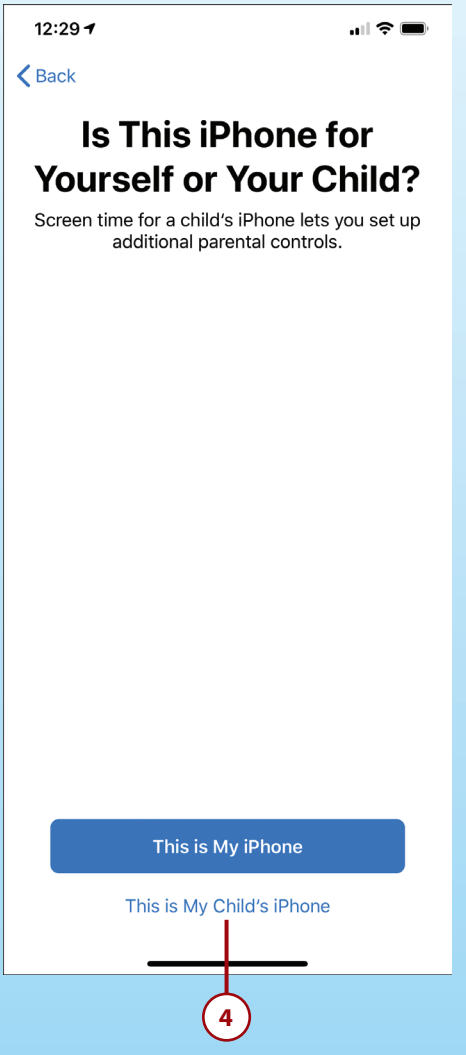




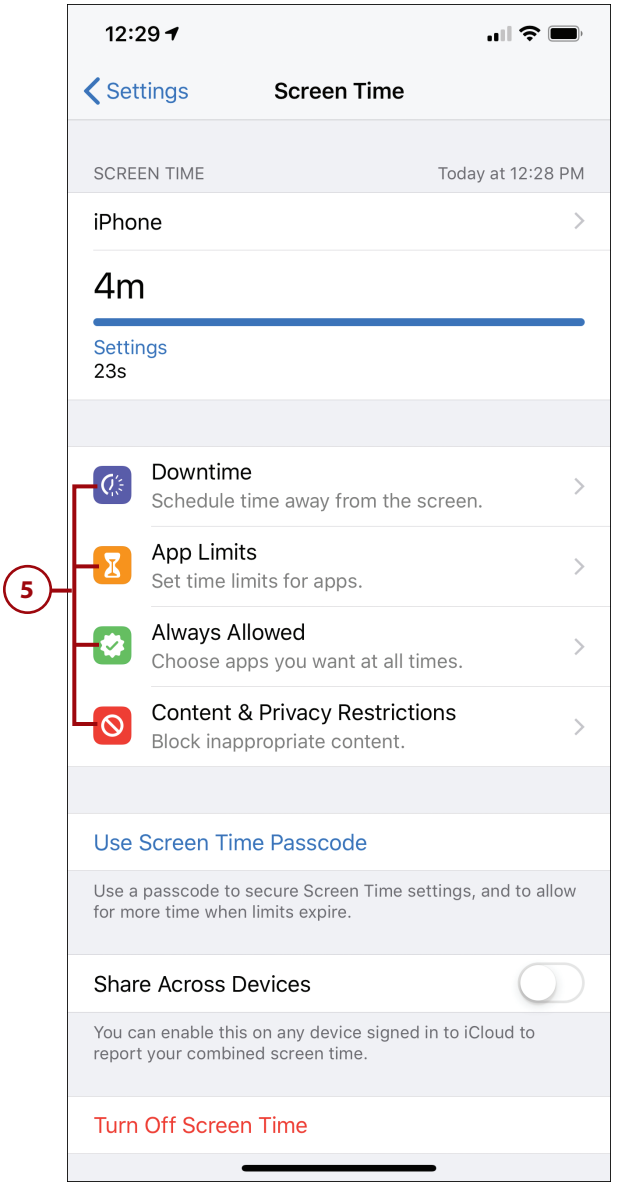
3 On the information screen, tap the Continue button.

4 Select the This is My Child's iPhone (iPad) option.





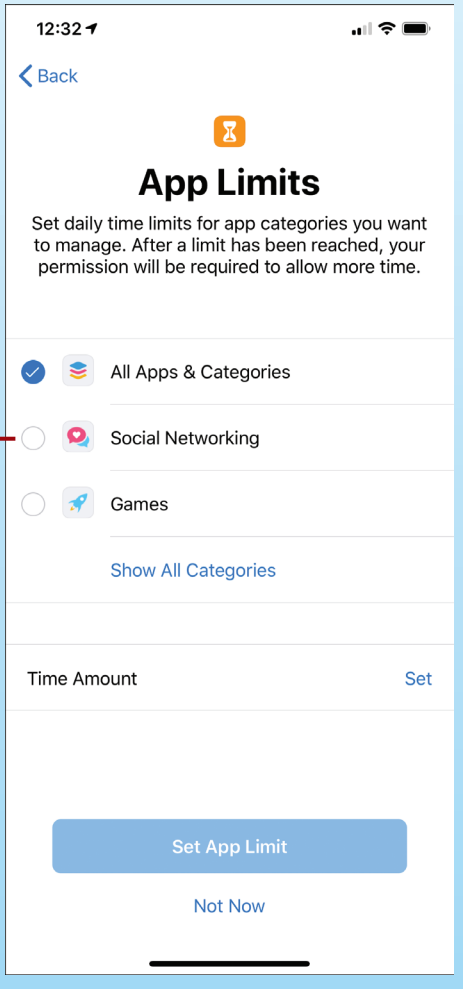
5 From the Screen Time menu, one at a time, tap the Downtime, App Limits, Always Allowed, and Content & Privacy Restrictions options to adjust each of the available submenu settings to a level you're comfortable with based on the age of your child.

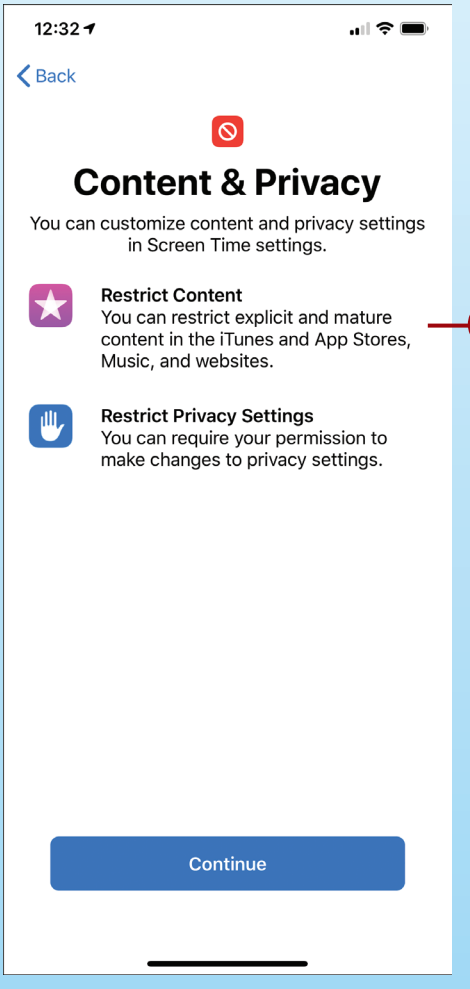


6 From the App Limits menu, you can control which apps, social media services, and games your child will have access to.

7 From the Content & Privacy menu, you can determine the types of content (based on age appropriateness) your child will be able to access.

8 Exit out of Settings to save and activate your changes. When the child signs in to the iPhone or iPad using a passcode, the parental controls you've selected will be active. (Not shown.)





Adjust Parental Controls on an Android-Based Smartphone or Tablet

Many Android-based mobile devices have minimal parental controls built in to the operating system. Using optional third-party apps, however, you can activate a wide range of parental controls at your discretion.

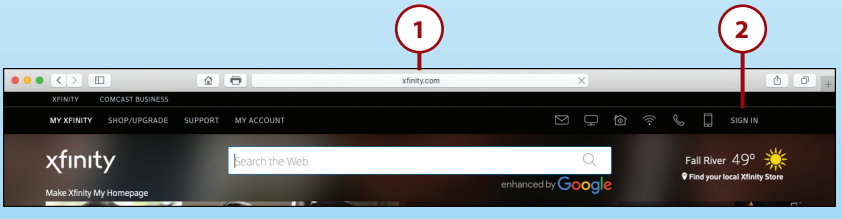
To find, download, and install one of these apps, visit the Google Play Store, and type "parental controls" in the Search field. Some of the popular parental control mobile apps include Kids Place Parental Control, Kids Zone Parental Controls & Child Lock, MMGuardian Parental Control, Norton Family Parental Control, and Screen Time Parental Control.

Adjust Parental Controls for In-Home Internet and TV (Comcast Xfinity Subscribers)

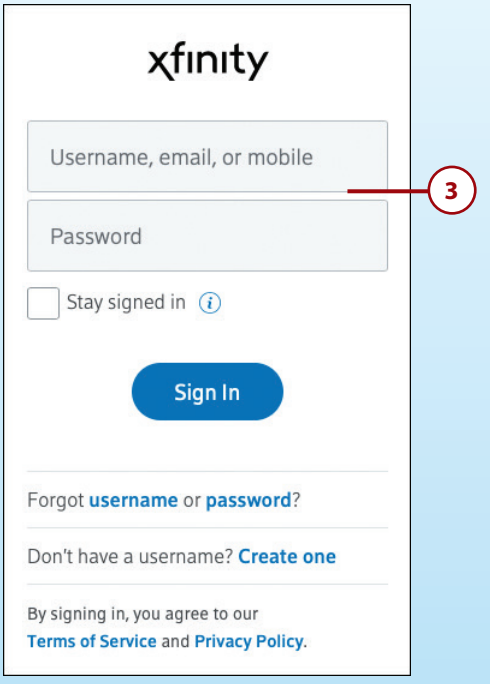
For kids or grandkids to access the Internet from any of their computers, mobile devices, or gaming systems, an Internet connection must be available. If the equipment they're using relies on your in-home wireless network (Wi-Fi), take advantage of the parental controls offered by your Internet service provider to control how much access your kids or grandkids have and what times of day (or night) Internet access is available to them.

All Internet service providers offer similar options. If you're a Comcast/Xfinity Internet service subscriber, you can adjust the parental controls on your home Internet and TV with these steps:

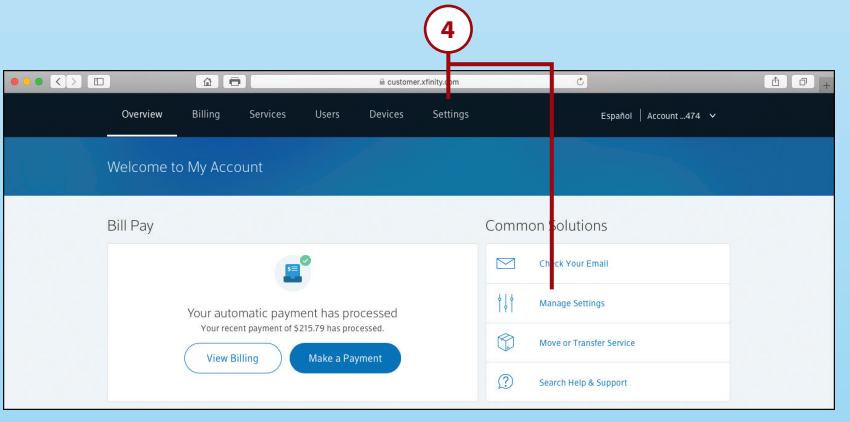
1. Launch your computer's web browser and visit www.xfinity.com.
2. Click the Sign In button in the upper-right corner of the web browser window.



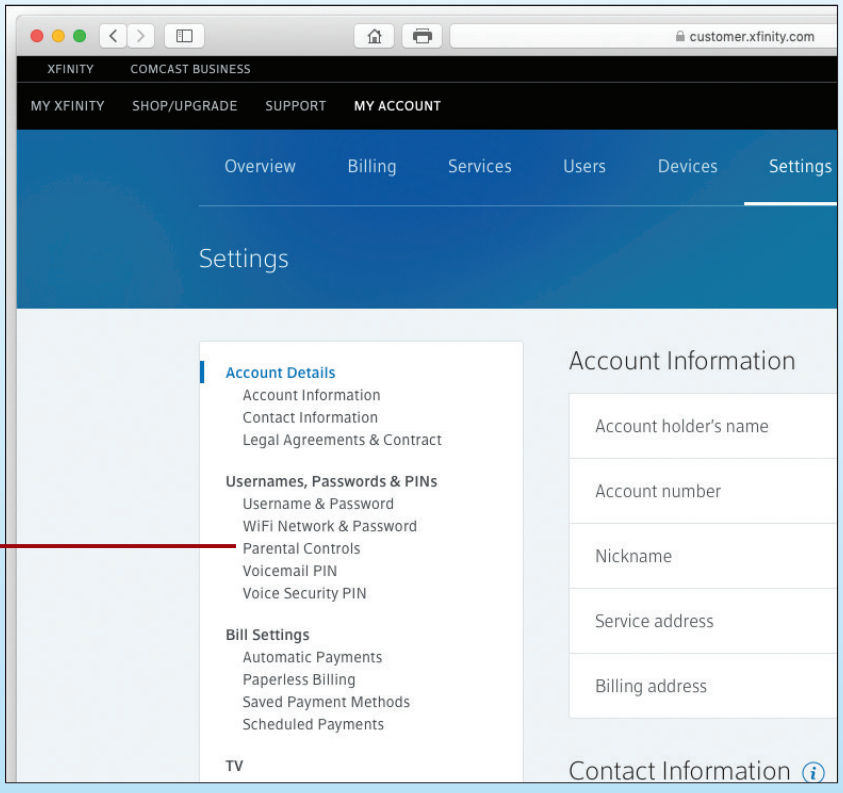
3 Sign in to your account using your username and password.



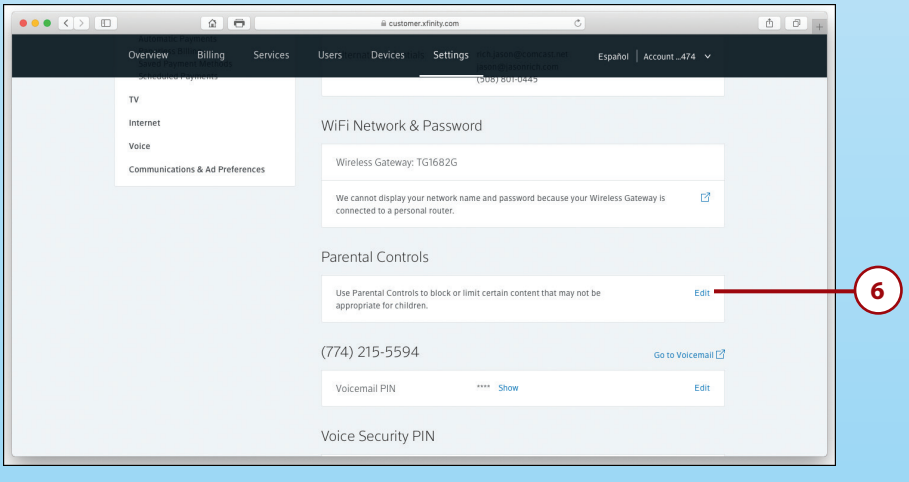
4 From the My Account screen, click the Settings or Manage Settings option.



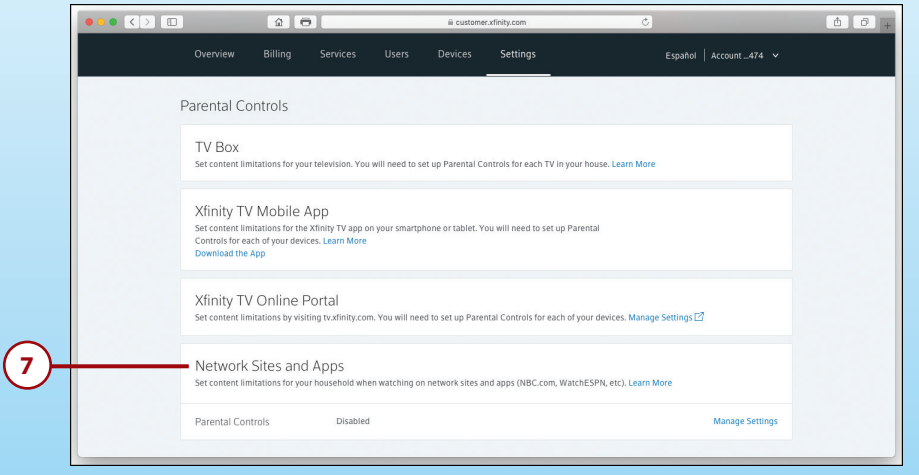
5 From the Settings menu, click the Parental Controls option.



6 Under the Parental Controls heading, click the Edit option.



7 One at a time, click each submenu option and adjust each to a level you're comfortable with, based on the age of your child. As a parent, if you download the free Xfinity TV app, you can also control content your child is exposed to remotely from your own smartphone or tablet.



Taking a Proactive Role in Kids' Online Safety

With basic supervision, and with the help of parental controls, it's relatively easy to determine what the young people in your life are doing online, figure out whether their activities are safe, and prevent them from getting into trouble by interacting with people they shouldn't or accessing inappropriate content.

If you're willing to invest a small amount of time to handle the security and well-being of the young people in your life by monitoring and controlling their online and game-related activities, you'll likely be able to keep them safe, while allowing them to use the Internet as a powerful learning, information gathering, and entertainment-oriented tool.

It's Not All Good

No Solution Is Foolproof

The limitations to parental control tools and the ingenuity of children to get around the tools means none of the tools offer 100 percent protection. For example, even if you add parental controls to your in-home Internet, a child can use the cellular data connection on their smartphone to access the Internet and potentially create a personal Wi-Fi hotspot, with no parental controls, for their other Internet devices.

One solution is to set strict rules for what is and is not permitted, and take away your child's access to their computers or devices for a predetermined time if they break the rules. If the guidelines you set are fair, your kids will likely adhere to them, especially if they know that you'll randomly check all the equipment and online accounts and will not tolerate misuse based on the guidelines and limitations you've set.