

# SECURING KEY ACCOUNTS AND DEVICES

## Parental Control

Parental controls are available on most internet-enabled devices like computers, smartphones, tablets and gaming systems. When enabling parental controls, use age-appropriate settings to filter, monitor and block your child's activities.

As a parent, you'll likely want to allow your children to use technology for communications, learning and more. You're also going to want to be sure that your children use the internet safely and securely. Parental controls are a great way to be proactive about your child's online safety and activities.

**OnGuardOnline.gov** gives a breakdown of different types of parental controls:

- **Filtering and blocking** limit access to specific websites, words or images.
- **Blocking outgoing content** prevents your children from sharing personal information online and via email.
- **Limiting time** allows parents to set time limits for how long their children are online and the time of day they can access the internet.
- **Monitoring tools** alert parents to their children's online activity without blocking access and can be used with or without the child's knowledge. Some software can record which websites a child has visited. Other programs display warning messages when children visit certain websites.

**Mobile phone service providers** have different options for controlling privacy and usage, filtering content and location and monitoring settings.

- **Usage controls:** Most companies will allow parents to turn off features, such as downloading videos or images, text messaging and accessing the internet. These controls can also be used to limit the number of calls or texts and set time restrictions.
- **Content filtering:** These controls can block certain websites to allow for safer mobile browsing. Some filters can also limit videos and other multimedia.
- **Location and monitoring settings:** These controls allow parents to track their children's whereabouts using GPS systems that are built into mobile devices.

**Protect yourself with these STOP. THINK. CONNECT.™ tips:**

- **Secure your phone:** Use a strong passcode to lock your phone.
- **Think before you app:** Review the privacy policy and understand what data (e.g., location, access to your social networks) an app can access on your device before you download.
- **Only give your mobile number out to people you know and trust,** and never give anyone else's number out without their permission.
- **Consider disabling the geotagging feature on your phone.**
- **Know how to cell block others:** Using caller ID, you can block all incoming calls or block individual names and numbers.
- **Use caution when meeting face to face with someone who you only know through text messaging:** Even though texting is often the next step after online chatting, it is not necessarily safer.

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