

---

# Common Sense on Online Security

---

## Staying safe and secure in a digital world

Technology makes it so easy for kids to connect and share things with friends and family no matter where they are. But these connections can come with a huge cost if kids aren't careful. Learning to protect personal identity information, creating strong passwords, and being cautious when downloading programs and files are crucial to the safety and security of the digital devices kids use, as well as the information those devices store. Otherwise, kids can expose themselves and their families to digital threats like computer viruses, data and identity theft, and hacking.

---

### Some facts

A 2009 Consumer Reports survey found that nearly 2 million households suffered ID theft in the previous year

In 2009 McAfee Labs found that the number-one piece of malware detected around the world infected more than 27 million files in the course of 30 days

52 percent of teens have given out personal information online to someone they don't know offline, according to a 2008 study by McAfee and Harris Interactive

---

## What is digital safety?

To understand digital safety and security, you'll need to learn some new words: phishing, malware, spyware, spam, and yes, even junk. These greedy little programs attach themselves to respectable-looking software — for example, a downloadable game that looks really cool — and then wreak havoc once installed on your computer. Security programs can block them, but one of the most important weapons is teaching kids to treat their devices and information as the truly valuable things they are.

## Why it matters

If kids don't protect their personal information, there are many potential risks: damage to the hardware, identity theft, or financial loss. But children may not realize they are putting their information in jeopardy, because the warning signs aren't always obvious.

A friend might ask for your child's computer password to play a game, and then access your child's private email account. Or your child might use a file-sharing program that passes along a virus to your computer. To participate in an online contest, your tween might be asked to provide personal identity information such as a home phone number, address, date of birth, or your Social Security number, all of which opens up the family to the risk of identity theft. Just like in real life, kids have to know who to trust with information. It's as true in the digital world as the real world.

## Parent tips for all kids

Remind your children to follow these important security tips.

- » **Master the fine art of password creation.** It can actually be fun to develop really good passwords. (See more details on how to do this below.) Strong passwords are a key defense against unauthorized access to your information, as well as identify theft.
- » **Know the difference between information worth sharing and private information.** There are many ways you can share your ideas and creativity online, but personal information should remain private. Never input personal identity information such as phone numbers, addresses, or your date of birth in order to download something. And never, ever give Social Security numbers or credit card information.
- » **Be very careful with what you download.** Don't download free games or videos to your computer. These programs often come with spyware and viruses that will land your computer in the shop — and you in hot water.

## Password protection

- » **Protect yourself — and your stuff — with strong passwords that safeguard your digital data.** Use these tips to help you do it:
- » **Don't use passwords that are easy to guess — such as your nickname or your pet's name.** People who know you well can guess these kinds of passwords.
- » **Don't use any private identity information in your password.** Identity thieves can use this information to pretend to be you.
- » **Don't use a word in the dictionary as a password.** Hackers use programs that will try every word in the dictionary to guess passwords.
- » **Do use combinations of letters, numbers, and symbols.** These are harder to crack than regular words because there are more combinations to try.