

Common Sense on Online Security

What's the Issue?

Technology makes it very 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 kids' safety as well as the security of the information stored on their digital devices. Otherwise, kids can expose themselves and their families to digital threats such as computer viruses, data and identity theft, and hacking.

To understand digital safety and security, you'll need to learn perhaps some unfamiliar words: *phishing*, *malware*, *spyware*, *spam*, and yes, even *junk*. These refer to greedy little programs that 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 help block them, but one of the most important defenses against these threats is teaching kids to treat their devices and information as the truly valuable things they are.

Why Does It Matter?

If kids don't protect their personal information, there are many potential risks: damage to the hardware, identity theft, and financial loss. But children may not realize they are putting their information in jeopardy, because the warning signs aren't always obvious. For instance, another child 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. Older elementary kids might be asked to provide personal identity information, such as a home phone number, address, date of birth, or your Social Security number, by a thief posing as someone else, all of which opens up the family to the risk of identity theft. Just like in real life, kids online have to know who to trust with information.

common sense says

Help your child master the fine art of password creation. Teach them:

- **Not to use passwords that are easy to guess, such as their nickname or their pet's name.**
- **Not to use any private identity information in their password.** Identity thieves can use this information to pretend to be them.
- **Not to use a word in the dictionary as a password.** Hackers use programs that will try every word in the dictionary to guess passwords.
- **To use combinations of letters, numbers, and symbols.** These are harder to crack than regular words because there are more combinations to try.

Teach your kids to be careful with what they download. Let them know not to download free games or videos to their computer. These programs often come with spyware and viruses that will land the computer in the shop – and them in hot water. In the end, what seemed like free software often comes at a cost.

Let your kids know how to identify and deal with spam. Teach them that spam is Internet junk mail. This mail should not be opened, because if they do, they will just receive more of it. The best strategy is not to open email from addresses they don't recognize.