FTC Fact Sheet—Identify Yourself

You might have heard about identity theft: it's what can happen when a thief gets enough of someone's information to commit fraud. Why should people care about it? Because recovering a stolen identity can be a time-consuming and expensive process.

Imagine that someone pretends to be you: they use your name; they even convince businesses that they're you and they open a credit card in your name, get a cell phone in your name, or buy things using checks or a credit card that have your name on them.

ID thieves can be creative about getting your information. There are some low-tech ways they get it: sometimes they steal garbage, going through it to find personal information, or they steal mail. Of course, it's illegal to steal mail—and to steal your identity.

There are high-tech ways, too: ID thieves might put software onto your computer without you knowing it—it can happen when you open an email attachment, click on a pop-up ad, or download some music files, for example. The software, called spyware or badware, lets a thief see everything on your computer, track where you go, and record everything you type on your computer.

Unfortunately, even if you're really careful with your personal information, thieves can still get people's personal information. Sometimes, they hack into computer systems at stores or schools, hospitals or businesses. They look for personal information to use or sell to other thieves.

It's pretty easy for you and your family to make it harder for a thief to steal your identity. You can start with the low-tech defenses: being careful with your mail and garbage. If your family doesn't have a shredder, you might want to get one. Tell your parents to shred anything that has personal information on it before they throw it away.

And be sure to take care with your purse, your wallet, or your backpack. It's especially important not to carry your Social Security card with you. Keep it in a safe, locked place at home.

Practice some routine higher-tech defensive plays, too: protect your computer by installing and turning on an up-to-date firewall along with anti-spyware and anti-virus software. Once you're online, be careful with your personal information. Some sites might ask for a credit card number—maybe for something you're buying, maybe as proof of age. Ask yourself if they really need that number. If your answer is yes, stop and check. Before you type in your number, look for the closed lock icon in the lower right-hand corner of the screen, and look for the URL that starts with https://. These are two ways to tell if a site is secure.

When you get email or pop-ups on your computer, don't respond automatically. Emails that ask you to reply or click a link to "update your account" or "avoid cancellation" could be thieves trying to trick you into giving them your personal information. It's a technique called "phishing," because the thieves are fishing for your information. Pop-ups for free downloads or screensavers could be

spyware in disguise; clicking them could let someone see what you do and where you go online. Stop and think before you click—it could help keep your information private, and keep spyware off your computer.

www.ftc.gov