Computers can be enormous timesavers and powerful financial tools. Using budget tracking software, paying bills online and buying items more cheaply from wholesale or auction sites can make a lot of sense.

Secure your ID on your PC

1. Using passwords and profiles
2. Getting your guard up
3. Upping the anti with software
4. Running scans to stay current
5. Taking wireless precautions
6. Pumping up passwords
7. Doubting downloads
8. Avoiding public computers
9. Watching smart phones and PDAs
10. Scrubbing files

But before you load up your computer with sensitive information about yourself, you'll want to take the necessary steps to ensure your personal finances stay personal. Here's how to keep your computer on lockdown and off limits to identity thieves.

1. **Use passwords for protection**

You wouldn't leave sensitive documents laying out for prying eyes; likewise, you need to put away the information stored on your computer in a safe place: locked behind a password in your own user account.

Even if you are a true Luddite and never intend to go online, you'll still want to password protect your computer. That's because if you have a snoopy houseguest or if a thief picks up your laptop, they could get at your information as you sleep if it's not password protected.

Set up a separate user account for others to surf on so you keep your sensitive information private.

**HOW TO:** For Windows-based machines, go into the control panel, choose user accounts and follow the instructions. Mac users must create a password upon using the computer for the first time and they can change their password settings by going into system preferences. There they can disable automatic login. (If you get stuck, ask a trusted techie for assistance. That goes for all these tips.)
2. Get your guard up

Before merging with the information superhighway, you're going to want to make sure that all the existing security settings your computer comes with are turned on. If you want to go out and buy added protection later, that's great. Just make sure you have basic protection enabled before going online.

First, fire up the **firewall**. Your computer should come with a firewall, or perhaps a software package came bundled with your purchase that includes a firewall. It's basically a set of programs that work together to enforce the safety rules you outline when you choose a security level. The firewall is the gatekeeper for Internet activity.

The default setting is usually on, but you'll want to verify that it's on if you don't see the firewall icon when you turn on the computer.

Go into the control panel to find the security settings, says Jennifer Leach, a consumer education specialist with the Federal Trade Commission.

The higher you set your security, the more you are going to screen out, dangerous and harmless. According to Leach, medium to medium-high is fine for most people.

"If you're extremely cautious and you want to set it high, your friends might start telling you you're not getting their e-mails or you might see Web pages aren't loading. I think if you set them pretty low, a lot of stuff's going to creep through," she says.

3. Up the 'anti' with software

Next, up the anti -- **antivirus** and **antispyware**. These can be packaged separately or together. Spyware is software installed surreptitiously by outsiders on your computer that stealthily collects information as you navigate the Internet. Only some spyware is actually malicious; the spyware that marketers use is sometimes called **adware**. **Viruses** are pervasive and pernicious. More than 90 percent of all viral attacks go after the consumer, according to David Miner, senior director of Financial Services Industry Solutions at Symantec. "One out of every 233 e-mails that comes in is going to carry some kind of malicious code. With odds like that stacked against you, you can't afford to go out without protection."

Immediately download or activate antivirus and antispyware software, he advises.

"Often the way computers are sold these days, it comes bundled with software with a free 30- or 90-day trial. If you don't already have other antivirus software, you should click it on -- you can shop during the free trial period, but you should make sure that you have something running before you start surfing the Web," says Dan Salsburg, assistant director in the Division of Marketing Practices at OnGuard Online.

"If your computer doesn't come with anything, you can try free shareware while you are deciding. Look to something like Zone Alarm, Ad-Aware, or Spybot Search & Destroy," suggests Miner.

4. Run scans to stay current

Unlike fashion, keeping up with computer security trends is easy. Just set automatic updates and let them run.

"Having the best security system in the world doesn't do you any good unless you keep it current," Miner says.

From the time the computer is boxed until you bring it home and plug it in, a lot can change: Either new threats arise or security flaws are detected in the software, so it is important to get the updates immediately.

"New attacks are being created daily," warns Miner. Set your protection updates to run regularly: daily is best. Then run your full system scans regularly against viruses and spyware."
5. Take wireless precautions

Even if you're a giving person, you can't afford to share your wireless connection with the neighbors. Letting people piggyback on your connection sucks up bandwidth, slowing you down. Worse: They could potentially see everything on your computer.

"It's been my experience that most people will connect in an insecure manner and end up exposing most of the information that is on their drive," says David Marcus, security research and communications manager at McAfee. "You don't want just anyone to connect to your documents folder if it has all your passwords on it."

If you don't turn on wireless encryption, a neighbor who's only halfway computer savvy could easily put something on your PC that would track your keystrokes, warns Mark Sunner, chief security analyst at MessageLabs. This means that even if you're logging onto a secure site, they would be able to record the keystrokes and go back and log in later.

It's very tempting to buy a wireless router, plug it in and be up and running within a matter of minutes, but realize that by default the firewall component of that router might not be on. Encryption is almost certainly not on, says Sunner.

HOW TO: The typical wireless router will have local area network, or LAN, ports in which you plug in wires connecting to your computer. That's how you can initially install your updates to the wireless software.

1. Encrypt. Usually the router will come with a CD that has installation software and the installation software should have a tab on it for security and should show you how to set up encryption. You may be able to choose from various types of encryption. If so, choose WPA, or its newer variant, WPA2, as they're considered more secure than the older WEP encryption.

2. Always rename your connection from the default name. Your connection is called the service set identifier, or SSID, which is the name of a local wireless area network. It's a case-sensitive string of text with up to 32 characters. You want to call it something that won't identify you, because this is what anyone in the area can see.

3. Choose a strong passphrase to password-protect your router. Don't worry about having to remember this long string of characters. You'll log in from your computer with something shorter. But do keep the passphrase in a secure place that you won't forget about.

"It takes a few extra minutes to set it up upfront when you do it, but it ensures that rogues are not going to connect to your wireless network without you knowing about it," Marcus says.

6. Pump up password protocol

We're constantly called upon to create passwords. How many do we repeat or name something ridiculously easy to guess? "You'd be amazed at the number of people who actually use the word 'password' as their password," PayPal spokeswoman Sara Gorman says.

Here are some rules for creating better passwords:

Don't make it personal: Passwords shouldn't be words from the dictionary, spouses' names, birthdays, Social Security numbers, things that people think are clever because they won't have to write them down. Once a thief gets that fundamental information, it's easier to figure out personal passwords.

Don't recycle: A lot of people will end up reusing a lot of the same username and password combinations, so oftentimes a hacker will gather in that information and use it successfully on other sites.
Test your strength: Miner says that Norton 360, for example, offers a password safe -- software downloaded to your home computer -- that also checks password strength for you. If you keep passwords in an encrypted vault, you don’t have to worry about making it easy to remember either. And, by encrypting the list, you solve the physical security problem of written lists.

Good passwords should be composed of a combination of letters and numbers, suggests Miner.

7. Attachments and downloads

If you’ve ever looked at spam and wondered how anyone could be fooled by the atrocious grammar and ridiculous promises, perhaps next time the joke will be on you. The messages are getting more polished and more targeted.

MessageLabs has seen a sharp increase over the last four years of targeted Trojans. These programs lurk inside something that appears innocuous, such as a Word document or spreadsheet. When that document is activated, the Trojan gets to work, perhaps shipping information out of the My Documents file. "These usually get sent to a single individual, so they rarely get on the radar of the broader security community," Sunner says.

"Never open or execute any e-mail attachment if you don’t know the person," suggests Miner. "Consumers think that they can recognize a spam attack, but the attacks are becoming very regionalized and they look just like something you might expect to get from somebody. You shouldn't view, open, or even execute e-mail attachments unless you know the source, it's expected and you know the purpose of it."

Sometimes your friends are the unwitting messengers of malicious code. Even forwarded messages that legitimately come from friends might shuttle recipients to a dangerous URL where, as Miner illustrates, there's a list of "20 ways to take your 30-year marriage and make it go to 60" and, while you're reading it, in the background a piece of code is slipped on your computer that will start taking information.

Tip: If you enjoy sharing jokes or feel-good messages that are sent to you, copy the information into the body of a new e-mail message rather than forwarding the attachment. Learn more about surfing safely online.

8. Avoid going public

Public cafes are great for surfing, but you really need to recognize the risk of inputting confidential information. There's not much you can do to improve information safety at a public computer. You're at greater risk because you're dependent upon a third party for security.

"Someone else who came in before me might have put in a flash stick that is gathering information," says Miner.

"I would seriously consider if you want to use a shared computer that remotely relates to confidential or identity information," Marcus says, "simply because you don't know if it's got a keyword logger or if all the tracking is turned on on that machine.

"It's a large risk that people really need to weigh. If there's no other access available and there's no other way of getting it done, you take the risk. But if it can wait until you can get home, it might behoove you to wait."

9. Watch your phones and PDAs

Remember, smart phones and PDAs are computers too, which raises two real risks: software security breaches and physical security breaches, such as when you lose the phone. Luckily, consumers can proactively find solutions to keep cell phones safe, just as on home computers.

You should always password lock your phone in case it goes MIA. That will make it harder for a thief to get at your information. Then, call your operator to have the phone locked, if possible, or your subscription canceled.
Threats to mobile software are growing, so it's important to protect yourself by downloading security software to your smart phone or PDA. Traditionally, crackers, the nickname for criminal hackers, haven't been much of a threat to cell phones because older models were essentially dumb boxes, but now the devices are getting smart -- and so are thieves.

"Nowadays, we are carrying around what is essentially a mini-PC that also happens to be a phone," says Sunner. "Because it is that much smarter, it of course is that much more open to abuse. I think, from that perspective, all the same paranoia I would use with my PC, I would apply to my phone as well."

If you're going to engage in mobile banking, even though banks are trying to protect their customers on their end, you should have some sort of mobile security just as you have on your home computer, says Miner.

"The average consumer trusts their device. But as soon as you start putting confidential information -- passwords, identifiers -- that you're then going to send to the bank, that now becomes information either on your cell phone, at risk, or over the air, at risk," he says.

"People should know that what's sent over to them can be pulled out of the air," says Leach. "PDAs should never be used to send Social Security numbers or financial information. Same with cell phones, actually. I hear people all the time in public giving things, that first of all, anyone could overhear, but also that anyone with that kind of scanner could pull out of the air."

Be aware of the kinds of information you send over a PDA because it might not have the kinds of protections that you think it does. When in doubt, get to a landline or a secure computer.

**10. Clean up after yourself**

Before selling or recycling your old computer, wipe the system with a file scrubber. Simply deleting files and emptying the trash bin doesn't mean they can't be recovered by anyone motivated to uncover them.

Free versions of file scrubbers, also called disk wipes or data scrubbers, can be found by doing a quick online search.