

Consumer Reports WebWatch Cybercrime Prevention Project Fact Sheet #9: Make Sure You ‘Complete Delete’ Your PC Before Recycling or Selling

This is the ninth fact sheet in Consumer Reports WebWatch’s “Look Before You Click” campaign, supported by a grant from the New York State Attorney General’s office, to help educate New York consumers about Internet fraud.

These days, the life cycle of a computer is short. People are often looking to upgrade, buy, sell or recycle. Many people believe that when they dispose of their old computer, the files they’ve erased from their hard drive are gone forever. That’s wrong! For your personal security and safety, you need to make sure you “complete delete” before your computer or hard drive leaves your possession.

This means recycled machines as well. Just as identity thieves hunt garbage dumps and trash cans for information, so do they look for any opportunity to mine unused or junked computers for data. You should buy a paper shredder to dispose of all those credit card offers you get in the mail, and you should data that may be left behind on your computer in the same manner: Cyber-shred it!

Here’s an example why: Consumer Reports recently bought a handful of hard drives on eBay and tried to recover old files by running simple and inexpensive software that anyone can obtain and use. Here’s what the magazine’s testers found: a Microsoft Word tax document that included annual salary information; Quicken files filled with income and expense data; a MySpace account name and password; e-mail from Outlook Express; love letters; photographs; and lists of favorite Web sites. (Don’t worry – the testers later erased all that personal data.) Most of those drives were described by their sellers as either reformatted or wiped clean.

Unfortunately, no recent version of either Microsoft Windows or Mac OS X offers a fast and convenient way to securely erase individual files or an entire hard drive. To securely erase your hard drive in Windows, Microsoft recommends using third-party software.

To securely erase selected files from a Windows computer, use [Eraser](#), which is free. It can wipe out temporary files as well as those moved to the Recycle Bin, and can also erase an entire drive.

You should also consider setting personal passwords for any computer you use at home. In these modern times, when thieves break into homes, they are as likely to steal your laptop or component hard drive as they are to steal jewelry. Remember: Passwords should be as hard to guess as possible. They should have numbers, uppercase letters, and lowercase letters mixed together.