by Pat Regnier and Jeanne Sahadi
photo illustrations by Viktor Koen

THE COMPLETE LAYMAN'S GUIDE to Cyber Safety

ID theft, pretexting, security holes in browsers, targeted Web advertising, the kids' MySpace profiles, the company's monitoring software, phishing, spyware, Wi-Fi break-ins. CAN'T A PERSON GET A LITTLE PRIVACY HERE?

Sure you can. You can spend hundreds of dollars a year on credit monitoring and security software, and maybe even pay to go to a privacy seminar. But you don't really need all that. By learning a little, spending a little and applying a lot of old-fashioned common sense to new situations—from social-networking sites to the local coffee shop's wireless network—you'll do a fine job of keeping yourself and your family safe from the guys trying to peer through the blinds. This guide will get you started. Don't keep what you learn here a secret. »

Defend Your (Virtual) Home

Some pretty bad folks are trying to break into your computer all the time. But you can make it a lot harder for them.

The Threat

It may seem melodramatic, but the truth is, hackers across the globe—or maybe across the street—are working 24/7 to find ways to steal your passwords, take control of your computer or turn your hard drive into a whirring pile of scrap metal. Visit the wrong site or download the wrong file, and your PC could end up with spyware that tracks your surfing or adware that chokes your Internet connection. Meanwhile, since nearly everything you do on a computer leaves a trace somewhere, your privacy is at the mercy of companies that hold the data. Maybe they'll hand it over to the government someday. Or they'll just be careless with it, leaving you exposed to ID thieves.

Unless you are permanently logging off, though, you can't eliminate these risks. You can only learn how to manage them. But in that sense, your life online is no different than your life offline. "Why doesn't your house get robbed every day? Because you weren't targeted," says Thomas Longstaff, a computer security expert at Carnegie Mellon University. So take some simple steps to make yourself a less appealing target and to help you recover more easily if you do get hit.

The Fix

Keep your computer up to date. Hackers are constantly searching for flaws in your operating system, especially if you run Windows. So update your most critical software regularly. You can do this automatically. Check your settings (under Control Panel in Windows and System Preferences on Macs) to make sure automatic updates are on.

Use security software... At a minimum, on Windows machines you must have antivirus, anti-spyware and firewall software. The antivirus/anti-spyware programs from Symantec and McAfee cost $40 for a year. Your Internet service provider may supply free software—compare it with the paid stuff by downloading a free trial. A firewall blocks outside computers from getting access to your machine. The latest versions of Windows and Mac OS X have optional basic firewalls. But Windows users should use a third-party firewall. ZoneAlarm is a free download available at zonelabs.com. Firewalls also come bundled with all-in-one Internet-security suites, which range in price from $50 to $70.

...but don't depend on it. "You catch the low-hanging fruit with antivirus software," says Jeff Moss of Black Hat, a security consultant. The biggest threat you face is the new hacker tactic that your security program doesn't know about yet. So you must develop Internet street smarts. Unless you have good reason to believe otherwise, assume that any attachment to an e-mail or any free download offered on a website contains a dangerous program. That goes triple for e-mails from strangers and for websites you've never heard of.

A University of Washington study found that one in 25 sites contained intrusive software, ranging from adware to really scary stuff that lets someone see what you type. Many of the most dangerous sites entice users who are looking for something for nothing, such as games, illegal music downloads or screen savers.

Take away your PC's superpowers. Both Macs and Windows PCs allow you to set up accounts for different users and give each user a different level of privileges to alter the machine, such as by adding software. Chances are, you've got administrator rights. This makes using your computer a bit easier, but it makes you more vulnerable, warns Mike Reiter, technical director at Carnegie Mellon's CyLab. Say you come across a malicious piece of software. If it launches when you're in admin mode, it could wipe out your hard drive. Work on an account with limited privileges, and the bad code may not be a threat. Use your admin account only to install software or perform maintenance chores.

Get a router and lock it down. Almost any $30 Wi-Fi router beefs up your security by acting as another firewall between your computer and everybody

else on the Internet. But that doesn't do you much good if you then leave your wireless connection open to your neighbor or anyone driving down your street. If you have unencrypted Wi-Fi, anybody can hop on to your network and use your bandwidth—or watch what you do or even break into your computer. To foil them, set your router to encrypt your data, advises Stu Elefant of McAfee. You usually have two choices: WEP or WPA. Choose WPA. It's tougher to break.

Be careful at the coffee shop. A lot of places offer free laptop Wi-Fi access. But if it's easy for you to log on, it's easy for the guy sipping a latte at the next table to spy on you, says Devin Akin of the CWNP Program, a wireless-security training firm. Make sure your computer is set not to share files with a network, and avoid typing in passwords or sensitive data, especially if you're on an unsecured Web page (one that doesn't start "https"). No matter what, don't do your banking in a public spot. If you have a POP-based e-mail program, use a secure SSL connection—and if that's all alphabet soup to you, lay off e-mail and get that scone to go.

Get smart—and get real—about passwords. Use different passwords for your sensitive accounts. A strong password is long, combines letters and numbers and is not a dictionary word, name or anything someone who knows a bit about you could guess. Microsoft has a neat tool that tests password strength (microsoft.com/protect). Unfortunately, such a password is devilishly hard to remember. That's why security guru Bruce Schneier of Counterpane Internet Security recommends doing what you've always been warned not to do: Write your passwords down. "Human beings are very good at securing little pieces of paper," says Schneier. "We've been doing it a long time."

Know how your computer watches you. As you wander the Web, your browser can record every site you visit. You may be collecting "cookies" loaded onto your computer by the sites you visit, as well as storing copies of those sites in your cache file and leaving a history log easily accessible to anyone else who looks at your browser. The new Internet Explorer and Firefox have one- or two-click functions under Tools that clear your browsing history.

Shred or smash. Little bits of personal information can linger on your hard drive even if you think you deleted them. Before you throw or give away an old computer, wipe your hard drive clean with software that meets Department of Defense standards for data destruction. Disk wipers go for about $30, or you can download the free Darik's Boot and Nuke at dban.sourceforge.net. Alternatively, you can remove your hard drive and apply a sledgehammer ($30) while, of course, wearing your safety glasses ($10).

SENSIBLE STEP

For the slightly paranoid

› Don't assume you are anonymous online. Websites can keep surprisingly detailed records about their visitors, and your digital footprints might, in theory, be traced to you. AOL (a unit of MONEY's parent company) recently exposed some customers' Web searches to public view, providing clues to their identities. That's why the Electronic Frontier Foundation recommends that you avoid entering personal information like your name or Social Security number into a search engine on your own PC, and that you not use search engines run by your ISP or e-mail provider.

Hackers Really Are Everywhere...

and they'll take over an unprotected PC in no time.

4%
Websites that contain spyware

240 seconds
Time for an unguarded PC to be taken over by a hacker

8,177
Daily break-in attempts on that PC

NOTE: Attack statistics are for a Windows machine without the latest updates and no firewall.
SOURCES: "A Crawler-based Study of Spyware on the Web" by A. Moshchuk *et al.*; Avantgarde/*USA Today* test of unprotected PCs.

Thwart the ID Thieves

You can spend big bucks and drive yourself nuts listening to the hype. Or you can take a few sensible precautions.

The Threat

There's no surefire way to stop ID theft because so much of your information is already out there. More than 93 million personal data records have been lost or stolen since February 2005. That's on top of the tens of millions of records bought and sold annually by credit issuers, insurers, government agencies, data brokers and, of course, identity thieves. Your info is easily accessible to hackers and company insiders who can profit by selling it on an online black market that didn't even exist five years ago, says Dan Clements, CEO of CardCops, which monitors the online trade in stolen information.

And a little data, especially your credit-card information combined with your Social Security number, goes a long way. Thieves can open accounts and borrow money in your name or even establish a new life as you, complete with job, home and claims on your Social Security benefits.

But here's the thing: The most common form of ID theft, charging purchases on your credit card, costs you nothing and is almost always easy to fix. New-account fraud, which is more problematic, affected a mere 1.5% of adult Americans last year. The really scary stuff—someone living your life—hardly ever happens. "It's possible, but there's no reason to lose sleep over it," says Jay Foley, co-executive director of the nonprofit Identity Theft Resource Center.

The Fix

Most "identity theft protection services" are a waste of money. Even the best are limited in what they can do. Credit monitoring services, for example, can neither tell you if someone is using your Social Security number to get a driver's license nor prevent ID theft. They just alert you sometime after the crime occurs, says Avivah Litan, a security and privacy analyst at Gartner.

MONEY asked seven identity theft experts what they do to protect themselves. After all, these folks know how to separate the hype from the reality. Their most important steps:

Get three free credit reports a year. You're entitled to a free credit report once a year from each of the major credit bureaus. Order one every four months by going to annualcreditreport.com or calling 877-322-8228. You can get another set of free reports if you call any one of the major bureaus and request that it place a 90-day fraud alert on your file. The alert tells lenders that are checking your report that they must call you before they extend credit in your name.

Monitor online banking and brokerage accounts a few times a week. Then check your credit-card statement every month. For example, if you see a $1 debit-card charge from the Red Cross, that could indicate a thief is testing your debit-card information, Clements says.

Use cash or a credit card, not a debit card, when practical. Neither cash nor a credit card leaves any trace of your bank account information. And making more charges on your credit card isn't likely to increase your risk of ID theft since your card info is already recorded every place you do business.

Opt out. Tell banks, insurance companies and brokerages that you don't want your financial information and credit status shared with anyone. Companies must send you opt-out privacy notices, which offer a toll-free number to call or an address where you can send a written request. Also, call the three major credit bureaus' toll-free line (888-567-

Meet the Digital Me

I am definitely not this cool.

GOOGLE "PAT REGNIER" OR "PATRICK REGNIER" and you'll learn that I'm a journalist who has written for MONEY and *Time*. And that I'm a convicted killer now in a federal pen, an expert on bossa nova and elective colon surgery, a Chihuahua breeder and (I wish) a guitarist (at right) for a Canadian heavy-metal band named Endyium.

Chances are, anybody doing an online check on me will conclude that I can't be all of those people. I hope. Fact is, we're all taking our chances that the folks who see the digital profiles being built on us will be able to sort out what's true, what's false and what's just a case of mistaken identity. And it's not just a Google thing. Companies routinely run background checks on potential new hires, tapping into huge public-records databases maintained by private companies that have little accountability to you.

You can't do much to control this. But forewarned is forearmed: If you know there's something bad or misleading in your digital profile, you'll at least have a chance to explain it to people before they see it. That's why Pam Dixon of the World Privacy Forum recommends checking your name in search engines including Google, Yahoo and ZoomInfo, especially before applying for a job (but maybe not on your own computer; see page 123). With the big private databases, you'll likely have to pay to peek. I shelled out $80 for MyPublicInfo.com to run a search of the databases the company says employers are most likely to see. None had mixed me up with the killer, a fellow New Yorker. But how can I be sure another database somewhere doesn't make this mistake? Right now, I don't think I can. Which is why there ought to be a law (see page 127).

The Price of Fraud

$6,771

Average amount fraudulently charged by credit-card thieves

5 hours

Average time victim spends getting the charges erased

SOURCE: Javelin Strategy and Research 2006 Identity Theft and Fraud Survey.

8688) to opt out of prescreened offers of credit and insurance.

Don't share. Leave your Social Security card at home, and don't offer your number to anyone unless it's for tax, employment or credit purposes (including the opt-out option described above). Shred financial documents you no longer need. And lock your mailbox.

Don't fall for phishers. Ignore phone or e-mail solicitations or "security checks" from institutions you do business with unless you initiated the exchange. Your bank isn't sending you an e-mail asking for your account number. That's a crook hoping you volunteer information that he can make a buck on by ripping you off directly or by selling your data. Don't open suspicious-looking e-mails.

SENSIBLE STEP

For the slightly paranoid

Guard against pretexting. If you are worried that an employer, an ex or a debt collector might try to get records of your financial or phone accounts, tell companies to use a randomly assigned number as an identifier for you, not your Social Security number, or to require three to four identifiers. Also, create online versions of those accounts right away so that someone else pretending to be you won't be able to do it. Use complicated passwords. For more on passwords, see page 123.

Hide from the Boss (in a Good Way)

Work is a no-privacy zone. Understand that and you can save yourself embarrassment. Or worse.

The Threat

There are few bright lines dividing your private life from work these days. Who hasn't done something like this?

- While on a business trip, you use a company laptop to log on and pay bills, including one to your therapist.
- At lunch, you e-mail a friend from your Yahoo account saying that you are thinking of talking to HR about your manager.
- You check work e-mails from your computer at home, send off a memo, then click to a couple of job-site listings a colleague mentioned to you.

All of these could be big mistakes. You may think what you're doing is private, but when you do it at work, on company equipment or even on your own computer (if it's connected to a company network), it's not. Thanks to an ever-growing list of technologies that monitor productivity and ferret out undesirable behavior such as employees leaking company secrets, your employer can learn a lot about you. Not all companies monitor extensively. But absent a contract or stated policy to the contrary, assume that your employer can log every phone number you call, every keystroke you type and every website you visit on its equipment. And that it can put GPS trackers in company cell phones and cars and check out what you do on your home computer if you're using VPN software to get on the company's network.

And assume that your boss can fire you if he doesn't like what he learns. Maybe

that won't be the explicit reason; maybe it will. "You don't know what your company's threshold is," says former HR executive Cynthia Shapiro, author of *Corporate Confidential*. Either way, in most states you'll have few if any legal protections if you work in the private sector.

The Fix

You can't live your life like a character in an Orwell novel. Everyone does some personal things on company time, and who doesn't gripe about the boss once in a while? Most companies aren't likely to turn their high-tech version of *I Spy* into a nasty game of Gotcha unless you give them a really good reason—or they're really dreadful places to work. Still, if you value your job, make sure your private life doesn't undermine your professional one.

Respond to inappropriate e-mails immediately. If friends send you an offensive joke or photo at work, "a lack of response can be construed as agreement," Shapiro says. So write back quickly on company e-mail letting them know it's inappropriate and not to do it again.

Don't do, say or write anything at work that you don't want your employer to know about. Job hunting, discussing a medical issue or looking for the nearest AA meeting are good examples of what to avoid, even if you're using your personal e-mail account at work or making calls at lunch, says Frederick Lane, author of *The Naked Employee: How Technology Is Compromising Workplace Privacy*. And if you're really stewed about the boss and eager to undermine him, keep a lid on it. That also goes for outside the office: Blogging about the job may be therapeutic, but if your posts are traced back to you and the company doesn't like what you're saying...

Disconnect from company technology. If you're using your own computer to work remotely, log off the company network once you're done, says Nancy Flynn, executive director of the ePolicy Institute. Road warriors: Don't conduct serious personal business on a company laptop. It may feel like you're surgically attached to the damn thing, but it belongs to the firm, and the IT guys can learn what you've done on it.

SENSIBLE STEP

For the slightly paranoid

› **Guard against the office busybody.** Ask for a glare and privacy guard for your computer screen. If you're stepping away from your desk, log off, which will close your files. You'll need a password to reopen them. Clear your browsing history and empty your cache of stored pages. (See page 123 if you're unsure how to do this.) Avoid faxing or copying personal documents. It's too easy to get distracted and leave a stray paper lying around. Need to make an important call? Take a walk and use your cell phone.

They're Watching You

Your employer would prefer you not goof off, sure. But the real worry is you might hurt its business. So companies are keeping an eye on workers.

76% monitor employees' website connections.

26% have fired employees for e-mail misuse.

13% retain IM business records.

SOURCE: American Management Association with the ePolicy Institute, July 2006 e-mail/IM/blog survey of 416 companies.

Keep Your Kids Safe

Your parents worried that you watched too much TV. They never had to deal with IMs and MySpace.

The Threat

Chances are, your child will spend most of his Net time instant messaging with the same kids he sees all day in school, doing homework, playing video games or finding other fans of his favorite obscure band. But creeps are out there, and it's not just predators who want to use the Internet to get to know your kid. It's marketers too.

The Fix

Consider a Web filter. Parental control software such as CyberPatrol ($40 for 12 months of updates), Cybersitter (a one-time payment of $40) and Safe Eyes ($50 for 12 months) can help you control what your kids see and do online, filtering out objectionable content and letting you block sites of your choosing. But parental control software often comes bundled with Internet-security software suites or may be provided by your ISP. The new version of Windows due out early next year will also have filtering features. Whichever filter you pick, it will miss some bad stuff and screen out some good stuff, so get a trial download and spend some time surfing with it to see if it works for your family.

Teach your kid to value privacy. Even young children can grasp the basics of privacy. "Start by asking your child if there are things he wouldn't mind Mom or Dad knowing but wouldn't want the kid down the street to know," suggests privacy lawyer Parry Aftab, executive director of WiredSafety.org. Your kids should understand that the Web is a very public place. That rude and crude blog

that your daughter thinks only her friends read could come back to haunt her. "Two years later, search engines have a way of picking up these things," says Hemanshu Nigam, chief security officer of MySpace, the popular social-networking site where kids can set up Web pages and connect with other users.

Set firm family Web rules. These five are a good place to start.

1) You need my permission before entering personal info into a website.

2) Don't answer an e-mail or an instant message from a stranger or arrange to see anyone you first met online.

3) Don't lie about your age on any website, especially networking sites such as MySpace. (That's assuming you allow your kids to use these services. Check them out carefully before you do.)

4) Don't share information on a social-networking site that makes it easy for someone to find you in the real world.

5) Be careful with your photo. "When kids are posting photos of themselves, they are certainly increasing the chance that someone will try to contact them," says Michelle Collins of the National Center for Missing and Exploited Children (missingkids.com). While you may decide that older teens can handle this risk, they should know that sexually suggestive photos and pictures that could be taken out of context are dangerous even when just shared with friends. "Get them to realize that everyone has a forward button," says Collins.

Check in. You're asking your kid to make a lot of careful decisions. He deserves some help. Ask him to show you his Web pages, blogs or profiles at networking sites. Collins suggests going through instant-messaging buddy lists and asking who each person is. If your child resists this kind of attention, remind him who pays the broadband bill.

Treat your PC like a TV. Yes, the Internet is a great tool for homework and research. But it's also an entertainment device and a very powerful tool for advertisers. Teenagers are legally fair game for all the forms of Web-use tracking and profiling that allow advertisers to target them based on their interests, obsessions and anxieties, says Kathryn Montgomery, an expert on children and media at American University. Putting time limits on Web use will give your children mental and emotional breathing space. Keep the computer in the family room or living room. If you have a teenager who needs to write school reports in the quiet of her own room, buy a second computer with a good word processor but no Internet connection. Perfectly workable used laptops and old Macs are available for $100 or less on eBay. (Don't worry, your kid can help you with that.)

SENSIBLE STEP

For the slightly paranoid

› **You can spy on them if you need to.** Some Web-filtering software can keep logs of the Internet traffic on your computer; dedicated monitoring programs that capture what your kid does online range in price from $30 to $100. What you'll choose depends on how much spying you want to do and whether you want a program that runs without your child's knowledge (to compare software, go to kids.getnetwise.org/tools). **$**

There Oughta Be a Law

ALL THE TIPS in this story can help prevent you from becoming overexposed, but they aren't enough. It's time for privacy law to catch up with technology. Computers are recording more and more about us, and corporate networks may be saving the data essentially forever, says security expert Bruce Schneier. "The data about you isn't owned by you," says Schneier. That makes it harder for you to control.

George Washington University law professor Daniel Solove recommends four ways that lawmakers could give a little control back to you:

1) **Let you "freeze" your credit whenever you want,** making it impossible for any lender to call up a credit report. Some states do this now.

2) **Set minimum fines,** enforced by states, for companies that lose control of sensitive data.

3) **Make companies that keep big databases on you register with the Federal Trade Commission,** so you can contact them and see what's in your file.

4) **Set strict rules for government access to the information you store on the Internet,** such as Web-based e-mail or files created on sites like Google Docs, so that it's as safe from arbitrary searches as what's in your file cabinet at home.

FEEDBACK: *pregnier@moneymail.com*