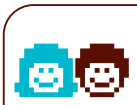
TO DO LIST

home computer for two

Merging hard drives? Follow our tips before logging on à deux. By Paula Kashtan

You may not realize it at first, but sharing a computer with your mate can be even trickier than sharing a bathroom—and present even more privacy issues. You're linking tons of personal information, funds, finances, and important files. That's why you need to create boundaries and form smart habits together (yep, just like keeping the door to the loo shut). Here's how to technologically merge while still protecting yourselves.



Multiple Accounts

CREATE SEPARATE LOG-ONS Keeping multiple accounts isn't about being sneaky. It's an easy way to keep your work lives separate and compartmentalize information that your spouse could accidentally delete. (And yes, password protection is within marital rights.)

MAKE SHARED FOLDERS Got files you both need to access, such as household bills or e-tickets for Thanksgiving? Create a shared folder, which can be accessed and updated from both of your accounts.

ALWAYS LOG OFF Separate accounts mean separate browsers—your cookies, boomarks, and history won't show up on your spouse's screen. Go ahead and use your home computer to plan a surprise vacation or buy birthday concert tickets. As long as you log off, your tracks will be covered.

anti-spyware pick **WebRoot Spy Sweeper 5.5 (*$30*, WebRoot.com). The easiest anti-spyware software to use boasts very high detection rates with free updates and tech support.**
antivirus pick **BitDefender v10 (*$30*, BitDefender.com). With the top virus protection, there's little to take care of after installation, and it comes at a superlow price.**

Antivirus, Anti-spyware, + Firewalls

PRACTICE SAFE SURFING A couple things that separate accounts don't necessarily keep separate: viruses and spyware. These malicious programs can travel from one account to the other, which means your spouse's accidental download could destroy all your files (grrr). It's definitely essential that you both understand and practice safe surfing.

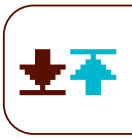
KNOW THE DIFFERENCE The three most common types of malicious programs to look out for are viruses, worms, and Trojan horses, which travel from one account to another.

Viruses and worms are similar in the sense that they both replicate themselves—the key difference is how. A virus needs human action to duplicate—it is imbedded into a program or file, which spreads the virus when you open it. A worm can reproduce itself—so it spreads wider and faster.

Unlike the others, a Trojan cannot copy itself. It's a nasty program disguised as legitimate software that you voluntarily download, allowing other malicious programs access to your computer.

INSTALL AND UPDATE ANTIVIRUS AND ANTI-SPYWARE PROGRAMS About 10 percent of all sites contain potentially damaging software—so it's easy to inadvertently become infected. To stay safe, you *both* need to install antivirus and anti-spyware software, and remember to update whenever prompted. Depending on your security system, updates may not transfer from one account to the other. So if one of you forgets, you both may be vulnerable.

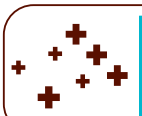
USE A FIREWALL This will notify you whenever programs on your computer want to access the Internet, or when Internet systems or users want to establish a connection with you. These also require consistent updating to "patch" your system to correct vulnerabilities.



Uploading + Downloading

KNOW THE LAW Having separate log-ons does not mean separate Internet accounts. For example, uploading or downloading movies and music could be illegal (stuff in the public domain is fine; *Pirates of the Caribbean*, not so much) and since it all goes through the same Internet account, law enforcement doesn't always know who's responsible. Also keep in mind that uploading files is typically more troublesome than downloading.

SET GROUND RULES We can't tell you what's okay and what isn't, but be sure the two of you agree. Don't be caught off-guard when someone in uniform comes looking for you—especially for something your other half did!



Cookies + Crumbs

UNDERSTAND COOKIES Every time you visit a website that uses them, you leave cookie "crumbs"—small files that track and store personal info and activity—behind. Ever been given a surprisingly accurate book or movie recommendation online and wondered where it came from? That's thanks to a cookie.

SET SECURITY HIGH "Crumbs" of movie or clothing preferences are pretty harmless, but cookies (an ID placed on your computer by a website) that store credit card info are much more dangerous. If your card info is stored on a cookie, it's possible for another site to access it without your authorization.

Avoid this by changing your browser's cookie setting (usually found in the privacy preferences) at the highest security—this blocks cookies that don't have a compact privacy policy and that personally identify you.

CLEAN YOUR CRUMBS You always have the option to see what cookies and other temporary Internet files are stored on your computer (again, you can locate this within your privacy setting), as well as the ability to delete any that hold important information you don't want stored. By performing regular antivirus and anti-spyware scans as a team, you and your partner will be able to identify and delete any cookies that could be potential security risks to your system.

online buying

use secure connections Now that you're sharing finances, it's especially important to take fundamental safety measures—a bad move on one spouse's part could cost you both a bundle. Only enter credit card information when you're on a secure connection. This means the info exchanged during the session is encrypted and can travel without risk of interception.

look for the lock Seeing this small icon means your connection is secure. It's located in different places (depending on your browser and edition) but it's usually in a corner or the URL bar. By the way, whether or not you have a secure connection has nothing to do with vulnerability to viruses and infections. When that box pops up to warn you that you're leaving a secure connection or entering an insecure one, there's really no need to worry unless you're entering private information.

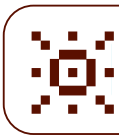
don't save important info You don't need to rely entirely on cookie security settings to keep you safe. Agree with your spouse that—even if it will speed up your online purchases—neither of you will save credit card info, bank account passwords, and the like on a website. Make it a habit to hit "not now" when that pop-up asks if you'd like to store this information or remember your password. This will keep other websites from accessing it.

Online Banking

REALIZE THE RISK With online banking, you need to be very careful. If you inadvertently download a keyboard logger (one common type of spyware), the system can record your keystrokes—meaning, an account username and password—and automatically email your account details to the spyware owner. Sound a little far-fetched? About a million banking customers have experienced some online theft. And remember—this can easily happen behind the scenes, without you noticing until your next bank statement comes.

MAINTAIN TWO BANK ACCOUNTS One should include the online bill-pay function; the other should be where you keep all your money. When you need to pay bills, hit the ATM—where both accounts are accessible—and transfer the exact amount you need into your online account. This way, only that small part is vulnerable and only until you pay the bills.

DON'T USE WIRELESS Use only DSL or cable modem connections. Even with an encryption key, wireless networks are never truly secure—it's easy for someone who knows what they're doing to hack in. You're even vulnerable on a personal wireless connection, if the network extends beyond your home.



Signing Out + Turning Off

SHUT DOWN OR YANK OUT With both DSL and wireless, you're connected to the Internet—and open to malicious programs—as long as your computer is on and the modem or router is plugged in. Even logging out doesn't eliminate the risk; there's technology that has the ability to remotely force your computer to log in and download files. So always remember to shut down when you aren't using it or unplug your modem or router when you aren't online. **[n]**

click
Keep tabs on all your online log-ins and passwords at TheNest.com/accounts

Nestpert: Andrew Colarik PhD, cyber security expert and author of *The Home Executive's Guide to Computer Security.*

nesties sound off!

A few months ago, we found a virus on DH's laptop. It copied his keystrokes, and at the same time his online bank account was locked because of someone trying to log in unsuccessfully.

MDTB

I recommend using Firefox to anyone. It will keep out spyware and viruses better than any other browser.

BUNNYGRRL

We got a letter from our DSL provider saying SPAM was sent from our IP address—which someone stole! We had a Trojan horse and now our computer is on security lockdown.

NESTROSIE