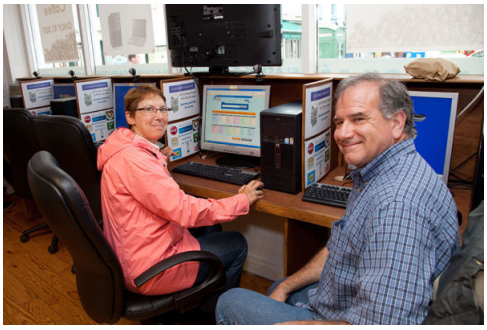
Internet Security for Travelers

The joys of widespread Wi-Fi availability come with the responsibility to take some protective precautions.



Take extra care if using a public terminal — if you must log in to any account, use an incognito window, and be absolutely sure you've logged out.

By Rick Steves

While you shouldn't be freaked out about your computer use on the road, travelers who are too careless with their digital information open themselves up to significant hassle and expense. Aim for a middle ground of cautiousness, and protect your personal information by heeding the following tips.

Safety Tips for Traveling with Your Own Device

If you're taking your devices on the road, be aware that gadget theft is an issue in Europe. Not only should you take precautions to protect your devices from thieves, but you should also configure them for maximum security so that if they are stolen, your personal data will stay private.

First, check that you're running the latest version of your device's operating system and security software. Next, consider tightening your security settings. At the very least, make sure your device is password- or passcode-protected so thieves can't access your information if it's stolen. If it's already protected, consider decreasing the time it takes for the screen to lock when not in use — while it's annoying to have to keep entering your code, that's not nearly as annoying as identity theft (and you can relax your security settings once you're home). For an extra layer of security, consider setting passwords on apps that access key info (such as email or Facebook).

Many laptops have a file-sharing option. Though this setting is likely turned off by default, it's a good idea to check that this option is not activated on your computer so that people sharing a Wi-Fi network with you can't access your files (if you're not sure how, do a search for your operating system's name and "turn off file sharing"). Newer versions of Windows have a "Public network" setting (choose this when you first join the network) that automatically configures your computer so that it's less susceptible to invasion.

Once on the road, use only legitimate Wi-Fi hotspots. Ask the hotel or café for the specific name of their network, and make sure you log on to that exact one. Hackers sometimes create bogus hotspots with a similar or vague name (such as "Hotel Europa Free Wi-Fi") that shows up alongside a bunch of authentic networks.

It's better if a network uses a password (especially a hard-to-guess one) rather than being open to the world. If you're not actively using a hotspot, turn off Wi-Fi so that your device is not visible to others.

Safety Tips for Using Public Computers

It's perfectly safe to use a public computer for tasks that don't require you to log in to an account. For instance, checking train schedules, maps, or museum hours doesn't pose a security risk. The danger lies in accessing personal accounts that require you to enter a login and password (such as email, Facebook, or any ecommerce site).

If you're traveling with your own device, try to make that your sole means of accessing your accounts. But if you'll be relying on hotel-lobby computers or Internet cafés, keep in mind that you have no idea who used that computer last — or who will hop on next. Public computers may be loaded with damaging malware, such as key-logger programs that keep track of what you're typing — including passwords.

If you do need to access personal accounts on a public computer, make sure that the Web browser you use doesn't store your login information. If you have the option of opening an "incognito" or "private" browser window, use it. When you sign in to any site, look for ways to ensure that the browser forgets your user name and password after you log out: For instance, you should click the box for "public or shared computer" or unclick any box that says "stay signed in" or "remember me." It's also a good idea to clear the Internet browser's cache, history, and cookies after you're done, so fewer artifacts of your surfing session remain — especially if you've accessed sensitive information (under the browser's "Options" or "Preferences" settings, look for a "Privacy" or "Security" category).

Finally, consider setting up two-step verification for your most important accounts. This requires you to enter not just a password but a second code whenever you log in using an unfamiliar computer (available with many Web-based email and social-networking sites).

Accessing Personal Information Online

While you're away, you may be tempted to check your online banking or credit-card statements, or to take care of other personal-finance chores. Internet security experts advise against accessing these sites entirely while traveling.

Definitely refrain from logging in to personal financial sites on a public computer. But even if you're using your own mobile device at a password-protected hotspot, any hacker who's logged on to the same network may be able to see what you're up to (chances are remote — but it's possible). If you need to access banking information, it's best to do so on a hard-wired connection (i.e., using an Ethernet cable in your hotel room). Otherwise, try to log in via a cellular network, which is safer than any Wi-Fi connection.

Even if you avoid accessing bank accounts during your trip, you may still need to enter your credit-card information online, such as for booking museum or theater tickets). If so, make sure that the site is secure. Most browsers display a little padlock icon to indicate this; also check that the page's URL begins with *https*instead of *http*. Never send a credit-card number (or any other sensitive information) over a website that doesn't begin with *https*.

For other accounts, such as email, consider upping your security settings while you're on your trip (for

example, see Facebook's "extra security features" page).

Savvy password habits are also critical. Above all, don't use individual dictionary words, don't reuse passwords (or even similar passwords) across different sites (a password-manager program really helps), and think in terms of using a "passphrase" — the longer your password, the better. Take a few minutes to read up online for up-to-date password advice (such as this article, and this list of the top 25 worst passwords).

It's also important to be careful if emailing personal information. Don't send your credit-card number in one email message. It's better to call or fax. Some people send their credit-card number in two halves, via two separate email messages. For extra security, a few banks, such as Citi and Bank of America, allow their customers to create virtual account numbers, which are one-time or short-term numbers linked to their regular credit card.

Resources for Staying Connected

- **Country Calling Codes** Dialing how-tos
- **HowtoCallAbroad.com** Dialing how-tos
- **This site's Tech Tips Forum** Tips from my readers

Apps

- **Skype** Internet-based video and voice calls for most devices (and any computer it's installed on)
- **Google+ Hangouts** Internet-based video, voice, and messaging for Android and iOS devices (and through any computer's browser)
- **FaceTime** Internet-based video and voice calls between iOS devices
- **Viber** Video, voice, and messaging for mobile devices (and any computer it's installed on)
- **iMessage** Internet-based messaging between iOS devices (and Macs)
- **WhatsApp** Internet-based messaging between phones