**Top 10 Internet Safety Rules & What Not to Do Online**

A 19-year-old running for public office in New Hampshire found out about the importance of following Internet safety rules the hard way. As [Seacoast Online](http://www.seacoastonline.com/article/20150630/NEWS/150639991) reports, his opponents found images in his social media posts that were sexually suggestive and referenced past drug use. Just like that, his political career crashed and burned upon takeoff. But, unfortunately, he isn't the only one, as careless Internet habits have left others exposed to scams, identity theft and physical harm at the hands of people they met online. With more users accessing the Internet through mobile devices, these risks are changing and growing quickly.

Even though apps loom larger in most people's daily online interactions than traditional websites do, that does not mean that the basic Internet safety rules have changed. Hackers are still on the lookout for personal information they can use to access your credit card and bank information.

Unsafe surfing can also lead to other threats—from embarrassing personal comments or images that, once online, are nearly impossible to erase, to getting mixed up with people you'd rather have had nothing to do with.

Here are the Top 10 Internet safety rules to follow to help you avoid getting into trouble online (and offline).

**1. Keep Personal Information Professional and Limited**

Potential employers or customers don't need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to get in touch with you. You wouldn't hand purely personal information out to strangers individually—don't hand it out to millions of people online.

**2. Keep Your Privacy Settings On**

Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. But you can take charge of your information. As noted by [Lifehacker](http://lifehacker.com/which-browser-is-better-for-privacy-1525895782), both web browsers and mobile operating systems have settings available to protect your privacy online. Major websites like [Facebook](https://www.facebook.com/help/325807937506242/) also have privacy-enhancing settings available. These settings are sometimes (deliberately) hard to find because companies want your personal information for its marketing value. Make sure you have enabled these privacy safeguards, and keep them enabled.

**3. Practice Safe Browsing**

You wouldn't choose to walk through a dangerous neighborhood—don't visit dangerous neighborhoods online. Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it. The Internet's demimonde is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge, you don't even give the hackers a chance.

**4. Make Sure Your Internet Connection is Secure**

When you go online in a public place, for example by using a public Wi-Fi connection, [PCMag](http://www.pcmag.com/slideshow_viewer/0%2C3253%2Cl%3D254312%26a%3D254312%26po%3D1%2C00.asp) notes you have no direct control over its security. Corporate cybersecurity experts worry about "endpoints"—the places where a private network connects to the outside world. Your vulnerable endpoint is your local Internet connection. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you're able to connect to a secure Wi-Fi network) before providing information such as your bank account number.

**5. Be Careful What You Download**

A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. As [PCWorld advises](http://www.pcworld.com/article/243782/five_tips_to_avoid_malware_in_mobile_apps.html), don't download apps that look suspicious or come from a site you don't trust.

**6. Choose Strong Passwords**

Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. And the problem with passwords is that people tend to choose easy ones to remember (such as "password" and "123456"), which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don't forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters.

**7. Make Online Purchases From Secure Sites**

Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections. As [Boston University](http://www.bu.edu/infosec/howtos/how-to-identify-and-protect-yourself-from-an-unsafe-website/)notes, you can identify secure sites by looking for an address that starts with *https:* (the S stands for *secure*) rather than simply *http:* They may also be marked by a padlock icon next to the address bar.

**8. Be Careful What You Post**

The Internet does not have a delete key, as that young candidate in New Hampshire found out. Any comment or image you post online may stay online forever because removing the original (say, from Twitter) does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you hadn't made, or get rid of that embarrassing selfie you took at a party. Don't put anything online that you wouldn't want your mom or a prospective employer to see.

**9. Be Careful Who You Meet Online**

People you meet online are not always who they claim to be. Indeed, they may not even be real. As [InfoWorld](http://www.infoworld.com/article/2991532/security/fake-linkedin-profiles-lure-unsuspecting-users.html) reports, fake social media profiles are a popular way for hackers to cozy up to unwary Web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.

**10. Keep Your Antivirus Program Up To Date**

Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it's to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.