8 Keys to Internet Security

I recommend Avast Antivirus as a decent free antivirus program. Others have recommended different programs, and that's fine – in the end, I don't think there's much meaningful difference between the various antivirus programs, at least in terms of security.

Much more important than which antivirus program you use (or anti-spyware, or firewall, or any security software), or even if you use one at all, are the practices that make up your online behavior. People who do risky stuff on the Internet will get a virus, sooner or later, *regardless* of how good their security software is. On the other hand, many security experts don't use any antivirus software and still manage to avoid viruses.

I don't recommend that you follow in the footsteps of the security experts – the nature of their calling demands a kind of paranoia that few of us can maintain. I recommend a solid package of security software (I run Cloud Antivirus and Windows Defender) but only as a safety net – something to pick up the slack when we make mistakes, not a first line of defense.

The thing with security, online or anywhere else, is that it's always a trade-off between protection and convenience. I can tell you how to absolutely avoid any risk of computer virus, spyware, or Trojan: stay offline and never install anything or use any removable storage media. That's 100% perfect protection, but it would severely hinder your computer usage. It's like securing a house: You could build a door-less, window-less titanium-sheathed reinforced-concrete bunker around your house and be absolutely sure burglars couldn't get in, but you probably wouldn't want to live there.

The tips below are sufficient to account for all but the most determined attacks against your computer. No amount of software or behavioral change can protect you from every possible attack (if the NSA wants to get on your PC, they are probably going to do so) but you can protect yourself from virtually all of the attacks you're *likely* to face online.

I owe thanks for most of these tips to Leo Laporte and Steve Gibson, hosts of the TWiT netcast Security Now. If you're interested in computer security at a very deep level, this weekly show is your ticket, and I heartily recommend it!

1. Use a router.

The very nature of the way routers works acts as an effective hardware firewall, preventing access to computers on your home network from outside the network. Put simply, when you request something from the Internet – say, you click a link, check your email, or enter a URL – the router notes which computer on its network the request came from so it can send the reply to the proper recipient. If a would be intruder attempts to enter your network, the router checks its list of outgoing requests and, if none is found correlating to the attackers' IP address, it ignores it. It basically doesn't know which computer to send it to, so it throws it out.

If you simply cannot use a hardware router, make sure your operating system's firewall is turned on. This is almost, but not entirely, as good.

2. Do not open email attachments.

I know, who doesn't want to see pictures of Anna Kournikova naked, right? Email attachments are a major vector for infecting computers, because it's so easy to fake the sender so the email looks like it came from someone you know, and everybody loves opening attachments from people they know. It could be a funny picture of penguins, after all. But bottom line, don't open attachments. If your email client automatically opens or previews them, turn that feature off. Even if it's from your mom, and even if your mom says she opened it and it's fine, still don't open it. (By the way, next time you're at mom's, reinstall Windows. She's got tons of viruses now.)

Now, I know that sometimes you have to open attachments, so here's a simple test to know when it is most likely safe to open an attachment:

1. You know that the email is from the person it says it's from. That usually means that either they said they were sending it, or they've written a note that only they could have written.
2. You are expecting an attachment from that person.
3. You know the person who created the file.
4. There is a compelling reason to open the attachment. I'm sorry, ma, but a good laugh isn't enough to get me to risk my computer's security.

If you can't be absolutely, 100% sure on all these counts, trash it.

3. Do not download bittorrent files.

That sucks, I know, but since you're never absolutely sure where the file comes from, where it's been, or who might have altered it, bittorrent is risky. Downloading a Linux distribution from Ubuntu is probably ok; downloading it from Pirate's Bay is a bit dodgy. Downloading Oscar screeners of movies that haven't been released yet is super-duper dodgy. It's a real shame to have to forego sticking it to The Man because of practical concerns, but you're taking a big risk downloading an unknown file from an unknown person about whom the only thing you know is that they don't feel any compunctions about breaking the law.

4. Do not download warez, porn, or other dubious files.

First they came for my bittorrents, then they came for my porn! It just gets worse and worse, doesn't it. But really, think about it – people who distribute illegal copies of illegally hacked software a) are demonstrated lawbreakers, b) are familiar with programming code, and c) had access to the code you're expecting to install on your computer. As for porn, while I'm sure there are plenty of Good Samaritans out there who distribute free pornography simply out of a desire for greater happiness in the world, some small number of them do it for financial gain. If they're giving you free porn, they must be making money off you another way, and one of the easiest is to install a bunch of malware on your computer, run whatever code they want on it, and then sell the use of your computer to spammers, phishers, and other unsavory sorts. You want to know how bad these guys are? They don't even care if they give pornography a bad name!

5. Do not download *anything* from sites you're unfamiliar with.

Again, if you're intending to install something you've downloaded onto your computer, you have to know that only people you trust have had access to it. Adobe, Microsoft, and other software manufacturers are generally trustworthy, as are sites like C|net's Download.com. "Bob's Free Software I Like a Whole Bunch" might not be quite as safe a bet.

6. Turn off Flash, Javascript, and other browser plugins.

Flash ads have been used to install viruses. So has Javascript code. You don't have to do anything to get infected this way; you just visit a site with the malicious code on it and *bam*, you're infected. Because of that, hardcore security folks turn off Javascript and either block or never install Flash. Personally, I think it limits the usefulness of the Internet too much; I've decided to risk running Javascript, and use the FlashBlock plugin in Firefox so I can select which Flash objects on a page I want to run (allowing me, for instance, to watch YouTube videos while preventing Flash ads on the same page from loading).

7. Do not click links in email.

It’s very easy to hide the real destination of links sent in email by using HTML where the text reads “www.perfectlysafesiteyouknowandtrust.com” but the actual URL is “www.reallybadsiterunbymeanpeoplewithnofriends.net”. This is how phishing scams work – you think you’re going to PayPal or your bank, but really you’re going to a page designed to look just like your bank’s login page but hosted on the mean people’s server. Also, bad guys often put unique tracking IDs into links, so that they know exactly who clicked on a link – which means that they know which email addresses out of the millions they sent spam to are valid, which makes them worth more money to other spammers. Um, yay?

7a. Do not click shortened URLs.

I don’t like this one, because I like Twitter and you lose a lot of functionality if you don’t use a service like bit.ly or is.gd to shorten URLs, but these links are scary. When you hover your mouse over a link, the URL appears in the email or browser’s status bar, meaning you can verify that the link heads to where it says it does. When you do the same with a shortened URL, it just says the shortened URL. There are Firefox extensions like UnTiny that will reveal the true destination of shortened URLs, and some Twitter clients do as well, but until a universal solution is standardized, these URLs remain a bit scary, security-wise.

8. Install all security updates.

Unless you’re a multi-national mega-corporation running oodles of mission-critical custom-designed software, you need to install security updates as quickly as possible upon release. If remembering to do this isn’t something you think you’d be likely to do, set your computer to automatically download and install updates. Increasingly, we’re seeing “0-day” exploits – viruses and trojans written to make use of security flaws before those flaws are corrected by – or, in some cases, even known to – manufacturers. Keeping up-to-date is essential to keep even marginally safe.

I know that, the world being what it is, someone will be thinking right about now, “Hey, why don’t you just switch to Mac OS X or Linux?” It’s true, those operating systems get far fewer viruses and other problems than Windows PCs, but most experts seem to agree that this is at least in part because there are so many Windows PCs and so few Mac and Linux PCs. (There are plenty of Linux servers, but those are under professional supervision, which goes a long way towards making up for any security weaknesses Linux has.) Bad guys program for the system that allows the greatest spread of their malware, and right now, that’s Windows.

But if you’re still not convinced, I’ve got an even better idea for you. Both Mac OS X and Linux have demonstrated security vulnerabilities, and as they become more common are likely to become targets for hackers. So they’re not really safe bets. Instead, try BeOS! It may be riddled with security holes and only run on Pentium 4 and earlier PCs, but I can guarantee you, *nobody* is writing viruses for it!

For everyone else, whether you use Windows, Mac, or Linux, make sure to follow the rules above and, chances are, you’ll be just fine.