# Don’t Be Hacker Bait: Do This One-Hour Security Drill

## 5 Steps to make your digital self less attractive to hackers, phishers and overly aggressive marketers

Updated Feb. 11, 2016 11:00 a.m. ET

Ask a hacker if your digital security is at risk, and the answer is always yes. You could hide in a mountain bunker lined with tin foil and twigs, and somebody still might drain your bank account.

It’s no reason to feel helpless. You can make yourself less of an easy target for hackers, money-hunting phishers and overly aggressive marketers by bolstering your security and data privacy. I’ll show you how to do it in an hour or less.

The answer isn’t the antivirus software we were all trained to run on our PCs. That can be useful to identify problems, and now antivirus is built into Microsoft Windows 10. But viruses don’t spread the ways they used to—and the bad guys change their strategies so quickly, traditional antivirus can’t keep up.

The foundation of smartphone and laptop safety is software updates, smarter passwords and more defensive Web browsers. Then it comes down to learning a few new digital habits to avoid being duped by criminals who exploit our own good natures.

If you suspect your computer is already in trouble because it’s slow or keeps flashing shady-looking offers, your first step should be to check for malware, damaging software you might have unwittingly picked up on the Web. I recommend downloading the free MalwareBytes, which does a great job of finding and removing worms, Trojans and other nasty stuff on Macs and PCs.

Then dedicate an hour, and work your way through this checklist, starting at the top. Even if you only get through a few areas, you’re less likely to be hacker bait.

Why it matters: Software changes constantly now, which can be annoying—but helps address new vulnerabilities. The golden rule of security is that if you install something, you have to stay on top of it.

Quick fix: Update your phone and computer OS, then move on to your apps. If you browse the Web with Chrome or Firefox, make sure they update automatically in Settings.

Updating software can be either fast or tedious depending on when you last did it. (Before a major update, it’s also a good idea to backup your device.)

On iPhone or iPad: Plug in your device and connect to Wi-Fi. Tap Settings, then General, then Software Update. To update apps, tap the App Store app, then Updates in the bottom right corner. To turn on auto updates, select Settings, then iTunes & App Stores, and then toggle Updates to on.

Using a screen lock or fingerprint on an iPhone makes sure its contents are encrypted. *PHOTO: ISTOCK*

On Android: Every handset maker handles updates slightly differently, but look for Settings, and then System Updates. To update apps, go to the Google Play Store app, then My apps, then Updates. To turn on auto updates, inside the Google Play Store app, select Settings, then Auto-update apps.

On Mac OS X: Open the App Store, and select updates in the toolbar. To turn on auto updates, select System Preferences, then App Store, and check Automatically check for updates.

On Windows 10: Select Settings, then Update & security, then Windows Update. Be sure Windows Defender is turned on, unless you have a better third-party antivirus program.

Deeper dive: Update the software that runs your Wi-Fi router, an often-overlooked back door for hackers, either with its app or by pointing a Web browser to its setup page. Know what I'd do? Just buy a new router—they keep getting faster and easier to manage.

If you have smart home cameras, locks or thermostats, you've taken on extra risk. So confirm they're running the latest software, usually by checking their control apps.

If you want to make sure all the third-party software on your computer is also up to date, Flexera Software's free and rather handy Personal Software Inspector can scan a Windows computer.

2. Fix your passwords

Why it matters: A good password is truly all that stands between you and a hacker. Using passwords the right way can contain the threat when sites get compromised, and keep out snoopers closer to home too.

Quick fix: Go to your most-used Internet services and turn on what's called two-factor authentication. This way, they ask you for additional information when you log in, and notify you if someone else is trying to access your account. Start with the big five: Apple ID, Google, Facebook **FB -0.07 %** (called "login approvals"), Microsoft and Twitter **TWTR 8.46 %** (called "login verification"). Some banks also offer this feature.

Deeper dive: To maximize safety, use a different password on every site—so if one company is compromised, a hacker can't use your stolen password somewhere else. The best passwords are long, random strings of numbers and letters that our overstuffed noggins can't usually remember on their own.

I strongly recommend using a password manager such as Dashlane or 1Password to collect and keep these passwords in sync across all of your devices. (It'll even let you print them all out, if you so wish.) This takes a little extra setup but will save you time in the long run.

3. Encrypt your drives

Why it matters: If you lose your phone or laptop, criminals or even governments could access valuable information. Encryption makes it much harder to retrieve anything without your permission.

Quick fix: Add a password or fingerprint screen lock to your iPhone or Android phone. That makes sure iPhones and newer Android phones are encrypted. On older Android phones, you have to turn on encryption separately.

Deeper dive: Password-protect and encrypt your computer. The Mac's OS X and Windows 10 both have it built in, though you have to turn it on separately. If you get an external drive, even for backup, use a disk utility to encrypt that, too.

4. Bolster your browser privacy

Why it matters: The browser is the No. 1 venue snoopers and aggressive marketers use to exploit you. But there are ways to keep them at bay.

Quick fix: Start with a clean sweep of everything in your browser—sometimes called "clear browsing data" or "remove website data." Doing this will delete passwords saved in the browser (which isn't a safe place to store them), and may require you to re-login to some sites that previously remembered you.

While we're focused on security, this checkup provides a good chance to shake off some unwanted marketers: Activate Do Not Track in the settings for your browser and install a browser extension like Ghostery, Disconnect or EFF's Privacy Badger to block spying ads and trackers.

Deeper dive: Disable Adobe Flash in your browser; it is one of the most common means of transmitting malware.

To further escape tracking by the ad industry and companies like Facebook, go to aboutads.info/choices and request an opt out from more than 120 participating companies.

5. Conduct an app census

Why it matters: The rise of the app economy means more businesses are watching where you're going and what you're doing every minute of the day—which is both a privacy and a security concern.

Quick fix: On your phone, check to see which apps have access to your location and other data. Turn off access or delete any you don't really use. (Bonus: This will save you battery life!)

On iPhone: Go to Settings, then Privacy, and be sure to check Location Services, Contacts and Health.

On Android: To review permissions based on category such as location in the latest Android 6 (Marshmallow), go to Settings, then Apps or Application Manager, and tap the gear icon and App permissions. On Android 5 (Lollipop), you have to check the permissions of each app individually.

Deeper dive: Inspect your Facebook apps, and clear out ones you don't care about—many have your personal info. When I checked, I had 210, including one called "How hipster are you?"

Perform the Google and Facebook security checkups on your accounts from any Web browser. You might be surprised how many different devices you're still logged in on.

Healthy Habits

The biggest security risk to our computers may be ourselves. Today's hackers try to trick us into giving them access to our computers. "People need to think before they click," says Stu Sjouwerman, founder of KnowBe4, which trains corporations to avoid attacks.

Be on alert for phishing schemes, which can easily impersonate a friend or family member. Don't click on links or open attachments in emails you weren't expecting. And ask people who sent them, "Is this really you?"

Use secure websites—marked by "https" at the front—particularly any time you enter payment info. You can force your browser to use it by installing HTTPS Everywhere.

When you're on a public network, consider using a VPN—HotSpot Shield for Windows and Android, Cloak for iPhone and Mac users.