Protecting your privacy from Windows 10

Chicago Tribune: Adam Rouse, Lori Andrews

Microsoft expects that a billion people will be using Windows 10 by 2017. But for privacy advocates, receiving a device with Windows 10 this Christmas may be the equivalent of coal landing in your holiday stocking.

Windows 10 is central to delivering the programs you use daily, providing the basic foundation for you to search the Internet, send emails, write documents, create spreadsheets and otherwise function in the digital age.

But Windows 10's default settings invade your privacy and could put you at a higher risk of identity theft and Internet fraud than those in previous versions. Here are some invasive aspects of Windows 10 — and what you can do to protect yourself:

1) Sharing your information with advertisers. Windows creates an advertising ID that's designed to track you as you visit different websites. The aggregated information about you (such as whether you look up the side effects of a medication or shop on discount sites) can be used by companies (such as life insurers) to discriminate against you. Solution: To disable your advertising ID, open the "privacy" settings page and under "general," slide the toggle to "off" under the setting that allows apps to use your advertising ID. Once this setting is off, Windows will not share your advertising ID without your explicit permission.

2) Connecting you to wireless networks that are risky. Windows 10 connects to Wi-Fi hotspots automatically, even if you've never connected to a particular network before. But connecting to open Wi-Fi networks in places like Starbucks or a hotel lobby can let others on the same network access your data and view your unencrypted information by using common software available online for free.

Worse yet, hackers create fake Wi-Fi hotspots linked to a computer that intercepts your messages before they reach the Web. If your device connects to a rogue hotspot, the hacker can view even your seemingly secure transactions such as bank information, passwords, and any other data transmitted between your computer and the websites you visit. Solution: Open the "network and Internet" settings page and then choose "Wi-Fi" and "manage Wi-Fi settings." Then under "connect to suggested hotspots," slide the toggle to "off." Windows will no longer automatically connect you to hotspots, but instead allow you to choose which hotspots you trust enough to connect to.

3) Eavesdropping through your microphone. Cortana is a voice-activated digital assistant included with Windows 10 that can perform functions such as setting an alarm, putting an appointment on a calendar or answering questions like Siri does on an iPhone. To enhance voice recognition and learn your tones and speech patterns, Cortana listens to everything you say in the vicinity of your Windows 10 device. This means the microphone on your Windows 10 device is always on and listening while the device is on, even if you are talking to your doctor about your health or your accountant about your finances. Solution: You can control which apps have access to your device's microphone in the "privacy" settings window. Click on "microphone" and slide the master toggle to "off." If you want to Skype or otherwise use the microphone, slide the toggle to the "on" position for just the app in which you would like to use the microphone. But don't forget to turn the toggle back to "off" when you're finished.

4) Inadequate encryption of OneDrive. Microsoft offers free cloud storage to Windows 10 users, letting anyone with a Microsoft account upload and store documents in Microsoft's cloud. The documents stored in the cloud are encrypted while in transit between your computer and the cloud, but once the documents reach the cloud server, they are stored in an unencrypted state. Thus, if hackers were to attack and gain access to any of Microsoft's cloud servers, they would be able to see all of your stored documents and look through their contents. Solution: Pick a cloud service that encrypts both en route and in the cloud, such as SpiderOak or Tresorit, where you hold the only key to access your information. If you already use a service like Dropbox, you can use SkyCrypt to encrypt data before uploading it to Dropbox.

Once you've completed these steps, you can use your Windows 10 device without gifting your personal information to advertisers and hackers or risking Cortana eavesdropping on your holiday party.

Adam Rouse is a Chicago cyber attorney. Lori Andrews is a law professor at IIT Chicago-Kent College of Law and the author of "I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy."