

Tech Tuesday: Building a Digital Defense with Privacy Controls

February 1, 2022

A graphic with a dark blue background featuring a circuit board pattern. On the left, there is a faint, large circular seal of the Federal Bureau of Investigation. The text is in white. At the top, it says 'TECH TUESDAY: Privacy Settings'. Below that is a bulleted list of four items. At the bottom left is the FBI logo and text, and at the bottom right is the text 'Portland Field Office'.

TECH TUESDAY: Privacy Settings

- Check settings on all devices & all browsers.
- Consider turning off location sharing & ad personalization.
- Know what apps & “advertising identifiers” are tracking you, and consider restricting access.
- Report cyber scams & frauds to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Last week, the United States and international partners recognized Data Privacy Week. This week, we continue education efforts with an FBI Oregon Tech Tuesday report on protecting your personal information.

Welcome to the Oregon FBI’s Tech Tuesday segment. Today: Building a digital defense by keeping track of who is tracking you.

Last week we talked about how “cookies” can follow you around the internet. This week, we will discuss other ways big business finds its way into your personal business.

As our partners at the [www.FTC.gov] **Federal Trade Commission** explain:

When you use an app on your smartphone, advertisers may use a unique identifier generated by your smartphone to track you.

Or they may use a technique called device fingerprinting. Device fingerprinting uses your browser's unique configurations and settings to track your activity.

Companies may also use techniques to connect your identity to the different devices you use to go online — say, your laptop and your smartphone — and then tailor ads to you across all your devices.

You can't completely get rid of targeted ads, but you can take some control by modifying your privacy settings. Remember, the steps you take on one device (such as your laptop) usually do not carry over to your other devices (such as your mobile phone). And, if you use more than one browser, the changes you make to one browser don't affect the others. Bottom line: remember to check all your devices and browsers.

This **FTC webpage** walks you through how to make changes on some of the most common browsers.

When it comes to your cell phone, you will need to dig into the privacy settings. Here are some options that you may find on your phone:

- **Reset advertising identifiers:** Under the “advertising” section of your phone’s privacy settings, you may find an option to reset advertising identifiers. If you reset, your device will generate a new identifier. Any data associated with your previous advertising identifier will not be linked to your new identifier... but tracking will start fresh with your new identifier.
- **Tracking control:** As you use an app, you may see a notice asking if you want to allow the app to track your activity. If you decline, the app can't access your device's advertising identifier.
- **Location controls:** Many companies track where you (and your phone) are to send you ads based on your location. Check your “location services” setting to limit how much you share.
- **Ad personalization:** In the “advertising” section of your privacy settings, there may be a “Personalized Ads” or “Ad Personalization” control. If you turn off personalized ads, your phone will stop using your info to show you targeted ads.

Remember, it is up to you to secure your privacy across every device you use.

If you are the victim of an online fraud, you should report the incident to the FBI's Internet Crime Complaint Center at [www.ic3.gov]**www.ic3.gov** or call your FBI local office.