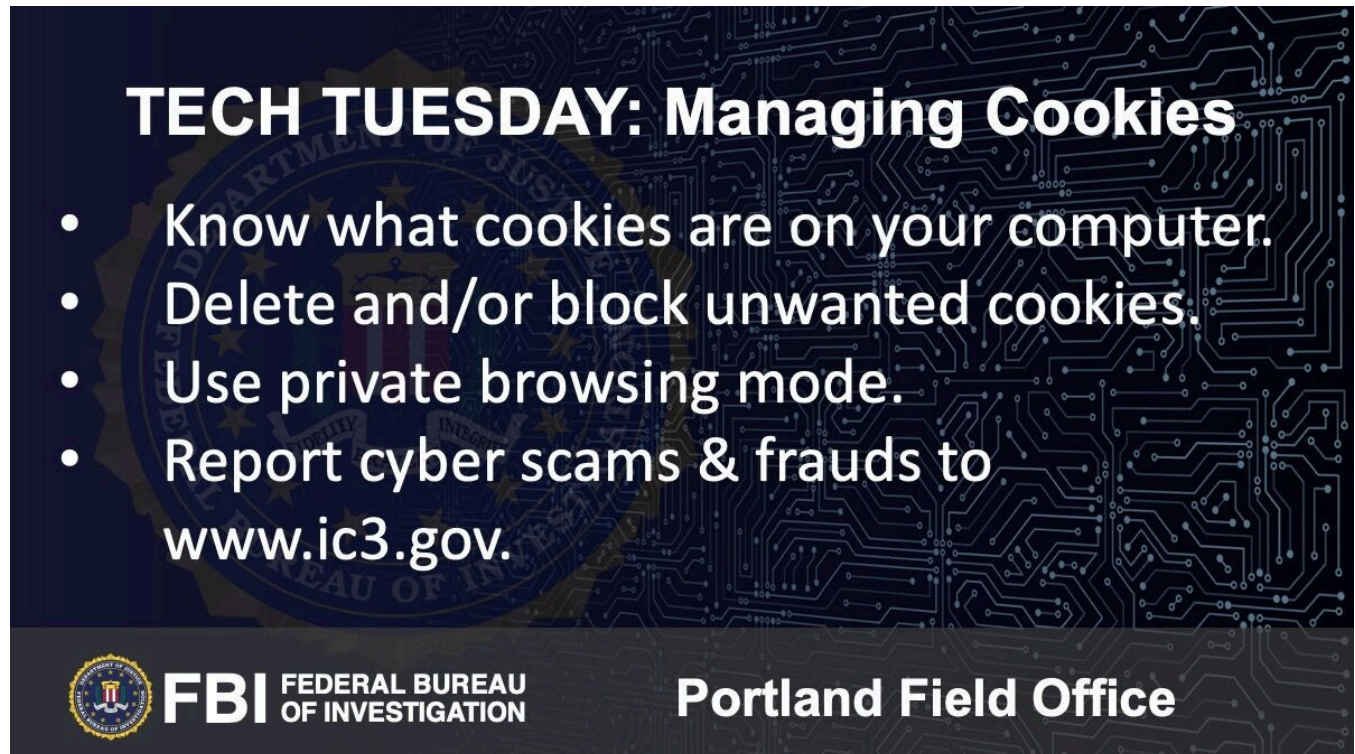


Tech Tuesday: Building a Digital Defense Against Cookies

January 25, 2022

A graphic with a dark blue background featuring a circuit board pattern. In the center is a large, faint circular seal of the Federal Bureau of Investigation. Overlaid on the seal is the text "TECH TUESDAY: Managing Cookies" in white, bold, sans-serif font. Below this title is a bulleted list of four items in white text: "Know what cookies are on your computer.", "Delete and/or block unwanted cookies.", "Use private browsing mode.", and "Report cyber scams & frauds to www.ic3.gov." At the bottom left is the FBI logo (a circular seal) followed by the text "FBI FEDERAL BUREAU OF INVESTIGATION" in white. At the bottom right is the text "Portland Field Office" in white.

TECH TUESDAY: Managing Cookies

- Know what cookies are on your computer.
- Delete and/or block unwanted cookies.
- Use private browsing mode.
- Report cyber scams & frauds to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

This week marks Data Privacy Week – a national and international effort to teach consumers and businesses how to better manage personal information and keep it secure. In honor of that - today's Tech Tuesday focuses on privacy matters related to internet tracking.

Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense by cracking the cookie code.

Unfortunately, we are not talking about chocolate chip or even snickerdoodle varieties. We are talking about the kind of cookie that follows you around the internet.

Our partners at the Federal Trade Commission explain it well:

When you visit a website, that site might place a file called a [cookie](#) on your browser. Websites use cookies to customize your browsing experience. When a website you visit places a cookie on your browser, that's

a first-party cookie. Examples include:

A news website shows local weather and stories about topics you're interested in.

A website remembers your username or items you left in your shopping cart.

The websites you visit often allow other companies to place cookies as well — for example, to deliver ads targeted to you. These are **third-party cookies**. Here's an example of a third-party cookie:

An advertising company places a cookie and sees that you visited a website about running. It then shows you an ad for running shoes when you visit other sites.

Ready to go on a cookie diet? You can choose to have more privacy when you go online by adjusting the privacy settings on the browsers you use. These settings let you do things like:

see what cookies are on your computer and delete them

decide what type of cookies you want to allow, including tailoring those settings by website

turn on private browsing mode

If you clear your cookies instead of blocking them, they'll be set again when you browse, so you may need to clear them from time to time.

This [FTC webpage](#) walks you through how to make changes on some of the most common browsers.

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.