

## Tech Tuesday: Building a Digital Defense Against Unwanted Apps

June 1, 2021

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 this is the text "TECH TUESDAY: Unwanted Apps" in white, bold, sans-serif font. Below this title is a bulleted list of four items in white text. 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: Unwanted Apps**

- Delete all unused apps from your devices.
- Ask: do I really want this app to have access to my data & accounts? If not, click “deny.”
- Go into your social media accounts & check the permissions/access you have given it to other apps and sites. Purge those you no longer want.
- Report scams to [www.ic3.gov](http://www.ic3.gov).

 **FBI** FEDERAL BUREAU OF INVESTIGATION

**Portland Field Office**

Welcome to the Oregon FBI’s Tech Tuesday segment. Today: Building a digital defense against unwanted apps!

Did you forget your password again? You know you are supposed to create complex and unique passwords for everything, which makes it really difficult to remember what they all are. Luckily, more and more sites are offering you the chance to log in with your Facebook or Google or other digital account. Seems easy, right?

It is definitely easier to collect and become registered on more and more websites and apps if you go this route – but our friends at the FTC have a warning for you. This kind of open access can leave you vulnerable to cyberattacks, phishing, and scams.

When you use social media accounts to sign up for apps or websites, you may give the app or website permission to do things on your behalf, like post to your social media page. You’re also possibly saying it’s

OK to access information like your name, birthdate, location, contacts, and even your messages. Over time, you may even forget which apps or sites have these permissions.

Here's how to keep yourself safe:

Start by asking yourself – does this site or app really need my info? Pay attention to what kind of details and access it is asking for. If you are uncomfortable allowing access, click “deny” or “disagree” when it asks for permissions. This typically stops the registration process.

Purge your permissions list. Go to the settings on your social media site and follow the instructions that lead you to the list of sites and apps to which you are granting access. Follow the instructions that tell you how to remove those apps or sites.

Delete all apps from your devices that you are not using.

Keep up the good work! Check your accounts every few months to see what kinds of permissions your programs or apps have.

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](http://www.ic3.gov) or call your FBI local office.