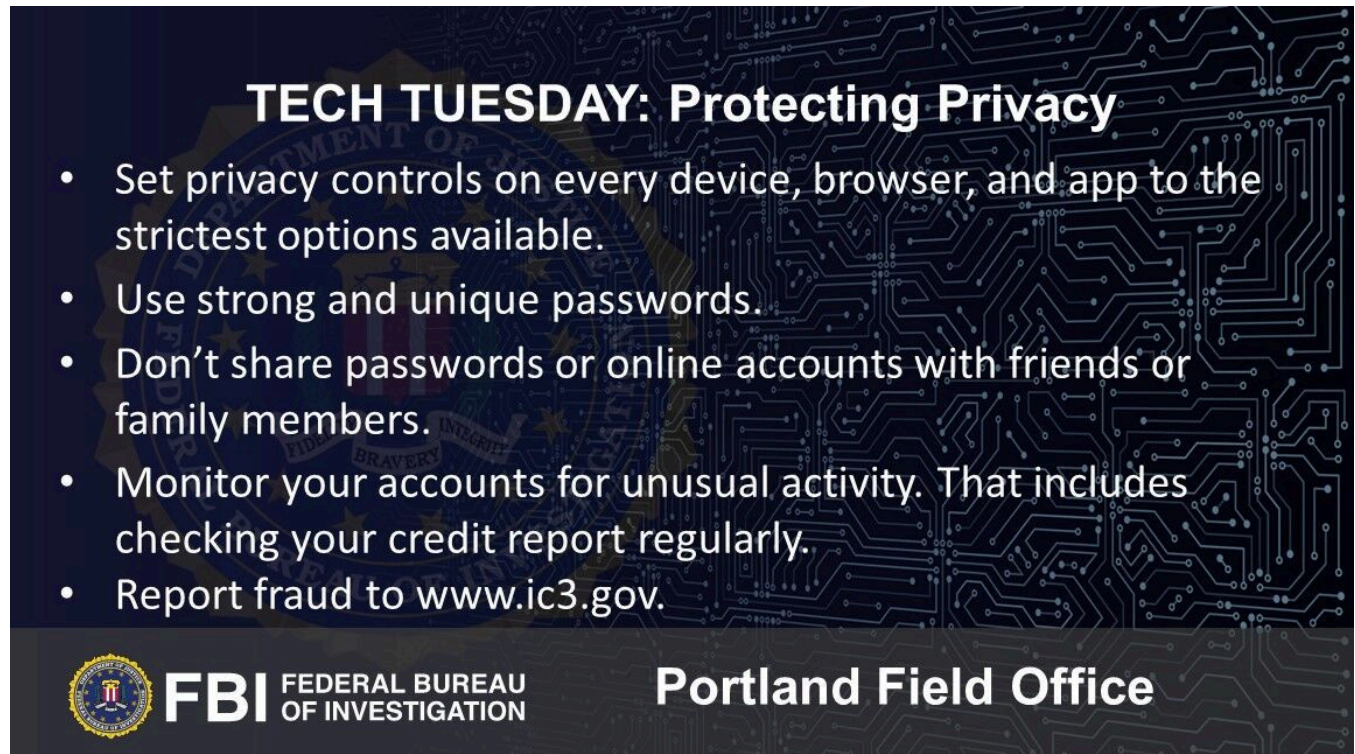


Tech Tuesday: Building a Digital Defense with Privacy Protections

March 30, 2022

A graphic with a dark blue background featuring a circuit board pattern. In the center, the text "TECH TUESDAY: Protecting Privacy" is displayed in white. Below this, a list of five bullet points provides privacy tips. At the bottom left is the FBI seal and the text "FBI FEDERAL BUREAU OF INVESTIGATION". At the bottom right is the text "Portland Field Office".

TECH TUESDAY: Protecting Privacy

- Set privacy controls on every device, browser, and app to the strictest options available.
- Use strong and unique passwords.
- Don't share passwords or online accounts with friends or family members.
- Monitor your accounts for unusual activity. That includes checking your credit report regularly.
- Report fraud to 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 with privacy protections.

We talk all the time about keeping private information, well, private. You know it makes sense... but do you really know how to do it?

Let's start with a discussion of the different buckets of data we need to address.

There's the personal bucket of data – which includes:

- Name
- Birth date
- Work, education, and address history
- Friends and family
- Likes and interests

There's the financial bucket, which includes:

- Credit cards
- Bank accounts
- Digital wallets
- Online payment
- Purchase history

There's the biometric bucket, which includes:

- Face recognition
- Voice recognition
- Fitness data tracker info
- Device authentication tools
- DNA analysis

Finally, there's the behavioral bucket of data, which includes:

- Browsing history
- Social media activity
- Relationships
- Interactions with devices and sensors
- Location tracking

More than ever, each piece of data is important. Taken together, even just a few pieces of data can give a business or a bad guy the keys to your kingdom. Ever wonder why a search for a product on one device leads to ads for a competitor's product on another? Many companies legally buy and sell customer data to track your purchases.

Remember that terms of service agreement you just clicked on when you downloaded that last app? You just gave some unknown company in some unknown country the right to peek into your digital life whenever it wants to.

And then, there are the bad guys. Your data can also mean big bucks for cyber criminals who sell your PII on the dark web for anywhere from a dollar to a thousand bucks or more.

It's almost impossible to live in our modern world without sharing personal data, but at least be smart about it.

- Set privacy controls on every device, browser, and app to the strictest options available.
- Use strong and unique passwords for each of your accounts or considering using a passphrase that is long and more difficult to break.
- Don't share passwords or online accounts with friends or family members.

- Monitor your accounts for unusual activity. That includes checking your credit report regularly. You are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting companies. During the pandemic, the credit reporting agencies are allowing weekly access. Order online from [annualcreditreport.com](https://www.annualcreditreport.com) or call 1-877-322-8228. You will need to provide your name, address, social security number, and date of birth to verify your identity.

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 or call your FBI local office.

###

Sources: https://www.odni.gov/files/NCSC/documents/campaign/DoD_IAPM_Guide_March_2021.pdf
and <https://www.annualcreditreport.com/index.action>