

Tech Tuesday: Building a Digital Defense Against Data Mining Memes

October 26, 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 the seal and background is the text "TECH TUESDAY: Data Mining Memes" in bold white letters. Below this title is a bulleted list of four items in white text. At the bottom left is the FBI logo and the text "FBI FEDERAL BUREAU OF INVESTIGATION". At the bottom right is the text "Portland Field Office" in white.

TECH TUESDAY: Data Mining Memes

- Use an authenticator app to generate a one-time code to confirm that it's you when logging into a device, website, or service.
- Use highest security settings on devices & accounts.
- Don't respond to memes asking for info!
- Report online crimes 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 against social media mining scams.

Have you seen one of those fun questions on your social media feed? How old would you be if the digits in your age were flipped? What was your first car? What street did you grow up on?

Well the first question obviously gives your age. A quick review of your feed will tell the scammer when your birthday is thanks to those generous friends who wished you well on your special day! Now, he knows your exact DOB... an important piece of personally identifiable info. The other questions can give a scammer the answer to your password reset challenge questions that you set up on your credit cards or bank account or, maybe, even your kids' school portal.

Here's another good, but troubling, meme: the last three digits of your phone number will tell you when you will enter heaven or what you need to be happy. Just kindly type your response into the comment box, and you will get your answer!

Of course, it's still pretty easy to guess at a person's area code based on where they live – and sometimes even their prefix. At that point, the scammer has nine of the ten digits he needs to nail down your number. Assuming you even locked down your phone and billing account, he just usually needs a PIN to gain full access. He can port your number to another phone, and just like that he can start re-setting all of your passwords for all of your other accounts.

Data mining can be automated...and profitable. How do you protect yourself?

Use an authenticator app to generate a one-time code that you use to confirm that it's you logging into a device, website, or service.

Make sure you are using the highest security settings possible on your devices and on all your accounts.

Use multi-factor authentication whenever possible. That includes something you know (such as a passphrase or PIN), something you have (such as a token or smart card) and something you are (such as a fingerprint).

Don't respond to social media memes asking for info!

If you are the victim of an online scam, 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.