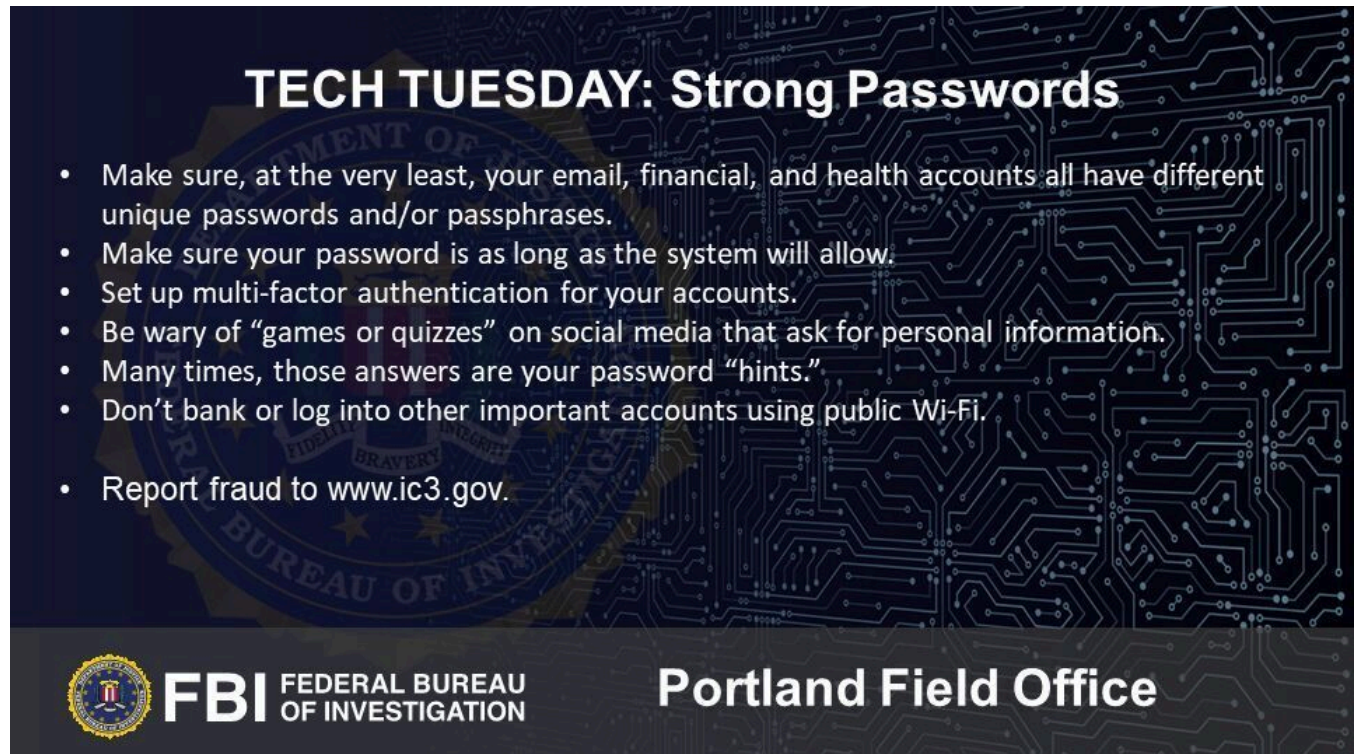


Tech Tuesday: Building a digital defense with strong passwords and account protection

May 4, 2022

A graphic with a dark blue background featuring a circuit board pattern. On the left is the FBI seal. The text "TECH TUESDAY: Strong Passwords" is at the top in white. Below it is a bulleted list of password tips. At the bottom left is the FBI logo and text, and at the bottom right is "Portland Field Office" in white.

TECH TUESDAY: Strong Passwords

- Make sure, at the very least, your email, financial, and health accounts all have different unique passwords and/or passphrases.
- Make sure your password is as long as the system will allow.
- Set up multi-factor authentication for your accounts.
- Be wary of “games or quizzes” on social media that ask for personal information.
- Many times, those answers are your password “hints.”
- Don’t bank or log into other important accounts using public Wi-Fi.
- Report fraud to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

In honor of World Password Day on Thursday, May 5, 2022, the FBI is encouraging the public to strengthen their passwords/phrases and account protection.

Passwords are used for everything; we use them for our phones, computers, email, even financial information. Unfortunately, many people use the same simple passwords, like 1234 or Password1, for multiple accounts. Simple passwords, even those with special characters, are easier for someone to crack.

Recent guidance from the National Institute of Standards and Technology (NIST) advises that password length is much more important than password complexity. Instead of using short complex passwords, use passphrases that combine multiple words and are longer than 15 characters. For example, TechTuesday2022Strengthen!

Strong passphrases can also help protect against personal data breaches.

According to the FBI’s Internet Crime Complaint Center (IC3), a personal data breach is defined as a leak/spill of personal data which is released from a secure location to an untrusted environment. Also, a

security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

It's important to note that scammers obtain people's information in many ways. Sometimes a victim will unintentionally give the scammer their passwords, other times, the criminal is able to crack the code.

The following tips may help protect you and your information from a breach:

Make sure, at the very least, your email, financial, and health accounts all have different unique passwords and/or passphrases.

Make sure your password is as long as the system will allow.

Set up multi-factor authentication for your accounts.

Be wary of "games or quizzes" on social media that ask for personal information.

Many times those answers are actually your password "hints"

Don't bank or log into other important accounts using public Wi-Fi.

If you believe are a victim of an online scam, 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.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-strong-passphrases-and-account-protection>