

Tech Tuesday: Building a Digital Defense Against Hacked Social Media Accounts

March 16, 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 and background is the text "TECH TUESDAY: Hacked Social Media Account" in white, bold, sans-serif font. Below this title is a bulleted list of five 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: Hacked Social Media Account

- Update security software, run a scan, and delete any possible malware on your devices.
- If you can access the account, change your password.
- Set up multifactor authentication.
- If you can't access your account, check with the social media platform to reclaim your account.
- 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 against hacked social media accounts.

Facebook, Instagram, TikTok, and Twitter. Social media accounts play an important role in many people's day to day lives... and they are truly a lifeline for small businesses and organizations. When someone hacks your account, the results can be devastating.

According to our partners at the Federal Trade Commission, here are some signs that someone has hacked your social media account:

- You can't log into your account.
- Your account has posts that you didn't make.
- Friends and family are getting messages you didn't send.

If you are worried about your email account's security, here are some steps to take:

- Update your security software, run a scan, and delete any possible malware on your devices.
- If you can get into your account, change your password. Also change any similar passwords on any other accounts. Consider using a passphrase, which is simply a string of unrelated (but easy to remember) words to increase the length of the phrase.
- Use multi-factor authentication which means that you set the account to require any user to use two or more credentials when logging in. For instance, you would need a password plus a PIN or a smart card plus a biometric scan.
- If you can't access your account, check with the social media platform to see what steps you must take to reclaim your account.

Finally, if you are hacked, make sure to let your friends and followers know so they don't also fall victim to your bad luck.

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 local FBI office.

Sources: <https://www.consumer.ftc.gov/articles/how-to-protect-your-privacy-online>