

Tech Tuesday: Building a Digital Defense Against Hacked Email Accounts

March 24, 2022

A graphic with a dark blue background featuring a circuit board pattern. In the center, the text "TECH TUESDAY: Hacked Email Accounts" is written in white. Below this, a list of five bullet points provides security advice. 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: Hacked Email Accounts

- Update your security software, run a scan, and delete any possible malware on your devices.
- Check the “rules” setting on your account to ensure that it is not set up to forward emails automatically to someone else’s address.
- Check trash folder for what the hacker may have done then deleted.
- Don’t let your web browser remember your passwords.
- 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 email accounts.

Last week we talked about bad actors gaining access to your social media accounts. For those using email, though, the danger can be just as great.

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

- You can’t log into your account.
- Your “sent” folder has messages you didn’t send or has been emptied all together.
- Friends or family report getting messages from you that include strange links or attachments.
- You know that your information has been compromised via a data breach, malware infection or a lost device.

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 and set up multi-factor authentication.
- If you can't access your account, check with the email provider to see what steps you must take to reclaim your account.
- Check the "rules" setting on your account to ensure that it is not set up to forward emails automatically to someone else's address.
- Check your trash folder for any hints as to what the hacker may have done then deleted.
- Don't use public WiFi.
- Don't let your web browser remember your passwords.
- Finally, never give your personal information – including login credentials and passwords – to people who contact you unsolicited. Make sure *you* are the one initiating any important contacts when dealing with your bank, health care provider, or other business.

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.