



Hacked Social Media Account

Recovering from a Hacked Social Media Account

Social media accounts are frequent targets for cyber criminals because they provide access to:

- Personal information
- Photos and private messages
- Large networks of trusted contacts
- Business or community audiences

When a social media account is compromised, attackers may:

- Post scams or malicious links as you
- Message friends requesting money or sensitive information
- Lock you out by changing passwords and recovery details
- Use your identity for impersonation or extortion

If your social media account is hacked, acting quickly can prevent widespread harm.

Signs Your Social Media Account Has Been Hacked:

- Posts, stories, or messages you didn't create
- Friends report receiving suspicious messages from you
- Password no longer works
- Profile details or email address changed
- New accounts linked without your permission
- You are locked out unexpectedly

Hacked Social Media Account – Do This First

Act Quickly

- Stop using the compromised account
- Do not engage with messages sent by the attacker
- Use a different, trusted device for recovery if possible

Secure or Recover the Account

If You Can Still Log In:

- Change the account password immediately
- Log out of all active sessions
- Review and remove:
 - Unknown devices
 - Third-party apps
- Check:





- Email address
 - Phone number
 - Username
- Enable additional security features if prompted. Turn on MFA or passkeys if available.

If You Are Locked Out:

- Use the platform's account recovery or "report hacked account" process
- Follow the platform's recovery steps and provide accurate information only
- Be patient, multiple attempts or identity verification may be required

Preserve Evidence

Before deleting or overwriting anything:

- Screenshot:
 - Unauthorized posts or messages
 - Login alerts
 - Profile changes
- Record:
 - Dates and times
 - URLs of posts or profiles
 - Any financial or reputational harm

This evidence may be needed for platform support or law enforcement.

Contain the Damage

Warn Your Contacts

Once access is restored:

- Post or send a clear warning such as, My account was compromised. Do not click recent links or send money/codes.
 - Advise friends not to click links
 - Warn against sending money or codes
 - Remove malicious posts and messages

Check Linked Accounts

Social media accounts are often connected to:

- Email accounts
- Business pages
- Advertising accounts
- Payment methods

Review and secure all linked services immediately.





If the Hack Leads to Fraud, Extortion, or Threats

Report the incident if:

- Money was stolen
- Identity theft occurred
- Blackmail or impersonation followed
- A business or organization account was affected

Your report can help investigators spot patterns and warn others.

- National Reporting
 - FBI Internet Crime Complaint Center (IC3)
<https://www.ic3.gov>
 - Federal Trade Commission (FTC) - report consumer fraud and scams at [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud).
- Ohio Resources
 - Ohio Attorney General – Identity Theft & Cybercrime Help
<https://www.ohioattorneygeneral.gov>
Hotline: 800-282-0515
- Geauga County
 - Geauga County Sheriff's Office
<https://www.geaugasheriff.org>
 - Local police non-emergency line if fraud or threats occurred

Recovery – After Regaining Control

- Monitor the account daily for unusual activity
- Review privacy and security settings
- Check for impersonation or duplicate accounts
- Watch for follow-up phishing attempts

How to Reduce the Risk of Future Social Media Account Takeovers

- Be skeptical of urgent messages asking for help, codes, or money
- Verify unusual requests through a separate communication method
- Avoid clicking links sent through direct messages
- Treat social media accounts as high-value targets
- Ask for help early, waiting increases harm

