



# Hacked Email Account

## *Recovering from a Hacked Email Account*

Email accounts are a primary target for cyber criminals because they contain sensitive information and are often the key to resetting passwords for other services such as banking, social media, work systems, healthcare portals, and shopping accounts.

When an email account is compromised, attackers may:

- Read private messages
- Send emails pretending to be you
- Reset passwords on other accounts
- Access documents, photos, and contacts
- Set up rules to hide their activity

When your email is hacked, time matters. Acting quickly can prevent wider damage.

Signs Your Email Account Has Been Hacked:

- Emails were sent that you didn't write
- Password no longer works or recovery details changed
- Login alerts from unfamiliar locations or devices
- Missing emails or emails marked as "read"
- Automatic replies or forwarding you didn't set up
- Friends report receiving suspicious messages from you

## Hacked Email Account – Do This First

### Act Quickly

If you suspect your email has been compromised:

- Stop using the affected email account
- Do not click links or reply to suspicious emails
- Use a different, trusted device if possible for recovery

### Secure the Account

If you can still access the account:

- Change the email password immediately
- Turn on MFA or passkeys after changing the password.
- Log out of all active sessions (look for "sign out of all devices")
- Update:
  - Recovery email
  - Recovery phone number





- Review and remove:
  - Unknown email rules
  - Automatic forwarding
  - Unrecognized devices or app connections

If you cannot access the account:

- Use the provider's account recovery process immediately
- Provide accurate information only; beware of paid recovery services that are not the email provider
- Avoid search-ad recovery services and social-media accounts claiming they can recover email for a fee
- Follow the official provider's steps

## Check for Wider Account Compromise

Because email is often the gateway to other accounts:

- From a secure device, change passwords for any additional accounts you suspect are compromised such as:
  - Banking and financial accounts
  - Social media
  - Shopping accounts
  - Work or school systems
- Watch for password reset emails you didn't request

## Preserve Evidence (If Needed)

Before deleting suspicious messages:

- Screenshot:
  - Login alerts
  - Password reset notices
  - Messages sent without your consent
- Record:
  - Dates and times
  - Locations shown in alerts
  - Any financial or personal impact
  - Export email headers for suspicious messages if your provider allows it; headers can help investigations

This is important if you need professional IT help or law enforcement assistance.

## Notify Contacts and Organizations

### Warn Your Contacts

- Send a brief warning message once your account is secured
- Advise contacts not to click links or send money





- This helps stop scams spreading further

## Notify Impacted Organizations

If your email was used to access:

- Work systems
- School accounts
- Healthcare portals
- Financial services

Notify those organizations immediately so they can monitor and secure access.

## If You Believe the Hack Is Part of a Larger Crime

### Report the Incident (If Appropriate)

Report the incident if:

- Money was stolen
- Identity theft occurred
- Extortion or blackmail followed
- Multiple accounts were compromised

Your report can help investigators spot patterns and warn others.

- National Reporting
  - FBI Internet Crime Complaint Center (IC3)  
<https://www.ic3.gov>
- 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 Securing the Account

- Monitor email activity closely for several weeks
- Review sent mail and rules daily
- Watch financial statements and account alerts
- Consider credit monitoring if personal data may have been exposed





## How to Reduce the Risk of Email Account Takeover

- Be cautious with unexpected login alerts or password reset emails
- Avoid clicking links in urgent or threatening messages
- Verify requests for money or sensitive information using another method
- Treat your email account as the master key to your digital life
- Use a password manager and a unique password for email
- Ask for help early, delays increase damage

