

YOUR EMAIL IS THE MASTER KEY

A plain-English guide to protecting the account that can reset almost everything else.

Why your email matters

Your email is connected to password resets, banking alerts, shopping accounts, social media, cloud storage, and much more. If someone gets into it, they may be able to take over other accounts one after another.

Do These 3 Things First

1. Use a strong, unique password

Do not reuse your email password anywhere else. Make it long, hard to guess, and different from every other account.

2. Turn on two-factor authentication

Use an authenticator app or security key when available. A text-message code is still better than using only a password.

3. Check your recovery information

Make sure the backup email address and phone number belong to you and are still current. Remove anything you do not recognize.

Never share a verification code

A bank, email provider, government agency, or technology company should not call or message you and ask you to read back a login or two-factor code. That code is for you. Anyone asking for it may be trying to get into your account.

CHECK WHAT IS CONNECTED

Attackers do not always change your password. Sometimes they quietly leave a door open.

Review These 3 Areas

4. Review signed-in devices

Look for phones, computers, tablets, browsers, or locations you do not recognize. Sign them out immediately.

5. Check forwarding and mail rules

Look for unfamiliar forwarding addresses, filters, inbox rules, blocked senders, and automatic replies. Attackers may hide security alerts or forward copies of your messages.

6. Review connected apps

Remove apps and services you no longer use, especially anything that can read, send, delete, or manage your email.

Warning Signs

- You receive a password reset or login alert you did not request.
- Messages appear in Sent, Trash, Spam, or Archive that you did not create.
- Friends receive strange messages from your account.
- Your recovery phone number or backup email address has changed.
- You are suddenly signed out, or your password no longer works.

Simple habit

Review your email security settings every few months. Five minutes now is much easier than trying to recover ten accounts later.

IF YOUR EMAIL WAS HACKED

Move quickly, but do not panic. Use a trusted device and work through the steps in order.

Immediate Response Checklist

- Change the email password from a device you trust.
- Turn on two-factor authentication, or reset it if it was already enabled.
- Sign out of all other devices and sessions.
- Check recovery email addresses, phone numbers, and security questions.
- Delete unfamiliar forwarding addresses, inbox rules, filters, and automatic replies.
- Remove unknown connected apps, browser extensions, and account permissions.
- Check Sent, Trash, Spam, Archive, and Deleted folders for activity you did not create.
- Change passwords on important accounts that use this email for password resets.
- Contact your email provider if you cannot regain control.

Protect the Most Important Connected Accounts

Banking and credit cards: Review transactions, alerts, contact information, and login history. Call the number on the back of the card if anything looks wrong.

Apple, Google, or Microsoft: Review devices, recovery settings, cloud storage, purchases, and account permissions.

Social media: Change passwords, sign out other sessions, and check whether posts or messages were sent without you.

Shopping and delivery accounts: Review saved payment methods, addresses, orders, gift cards, and account changes.

Final reminder

Treat your email like the front door to your digital life. Use a unique password, turn on two-factor authentication, keep recovery information current, and review account activity regularly. Your email should never be the easiest door to open.