How to Secure Your Main Email Account

A Click Giraffe Guide for Everyday Digital Safety

Your main email account is one of the most important accounts you own.

It is not just a place where you receive messages.

Your email may be connected to:

- Bank accounts
- Credit cards
- Online shopping accounts
- Password resets
- Cloud storage
- Photos and documents
- Social media
- Phone carrier accounts
- Medical portals
- Tax accounts
- Payment apps
- Work or freelance accounts
- Family communication

If someone gets into your email, they may be able to reset passwords, intercept verification messages, hide warning emails, impersonate you, or access sensitive information.

That is why securing your email account should be one of your first digital safety steps.

The Goal

This guide will help you:

- Make your email account harder to break into.
- Review recovery options.
- Turn on multi-factor authentication.
- Check recent sign-in activity.
- Remove suspicious access.
- Protect against password-reset scams.
- Reduce the risk of account takeover.
- Know what to do if something looks wrong.

You do not need to be technical.

Start with the checklist and complete one step at a time.

Quick Start Checklist

Use this checklist first.

[ ] Use a unique password for your email account.
[ ] Turn on multi-factor authentication.
[ ] Review recovery phone numbers.
[ ] Review recovery email addresses.
[ ] Remove old or unknown recovery options.
[ ] Check recent sign-in activity.
[ ] Sign out of devices you do not recognize.
[ ] Review connected apps and third-party access.
[ ] Review mail forwarding rules.
[ ] Review automatic filters or inbox rules.
[ ] Protect your phone and phone carrier account.
[ ] Save backup codes or recovery information safely.
[ ] Never share verification codes with anyone.

If you only have time for two steps, do these first:

1. Use a unique password.
2. Turn on multi-factor authentication.

Step 1: Know Which Email Account Matters Most

Many people have more than one email account.

You may have:

- A Gmail account.
- An Outlook or Hotmail account.
- An iCloud email account.
- A Yahoo account.
- A work email.

- An old email you still use for password resets.

Your main email account is usually the one connected to your most important services.

Find your most important email account

Ask yourself:

[ ] Which email receives bank alerts?
[ ] Which email is used for password resets?
[ ] Which email is connected to my Apple ID, Google account, or Microsoft account?
[ ] Which email is used for shopping accounts?
[ ] Which email is connected to my phone carrier?
[ ] Which email is connected to my password manager?
[ ] Which email would cause the most damage if someone accessed it?

Start with that account.

Step 2: Use a Unique Password

Your email password should not be used anywhere else.

If you reuse your email password on another website and that website is breached, criminals may try the same password on your email account.

Do this

[ ] Make your email password unique.
[ ] Do not reuse it for shopping, banking, social media, or any other service.
[ ] Use a long password.
[ ] Avoid names, birthdays, addresses, pet names, or common phrases.
[ ] Store the password in a reputable password manager.
[ ] Do not store it in a plain note, text message, email draft, or unsecured spreadsheet.

Good password manager options

Reputable password managers include:

- Bitwarden
- Keeper
- 1Password
- Proton Pass

- NordPass
- RoboForm

Choose one you can use consistently.

The best password manager is the one you and your family will actually keep using.

Step 3: Turn On Multi-Factor Authentication

Multi-factor authentication, often called MFA, two-step verification, or two-factor authentication, adds a second step when signing in.

This makes it harder for someone to access your email account even if they know your password.

Common MFA options

- Authenticator app
- Passkey
- Security key
- Text-message code
- Email code
- Backup code

Text-message codes are better than no MFA, but authenticator apps, passkeys, or hardware security keys are usually stronger.

Do this

[ ] Turn on MFA for your main email account.
[ ] Use an authenticator app, passkey, or security key if available.
[ ] Save backup codes in a safe place.
[ ] Make sure recovery options are current.
[ ] Do not share MFA codes with anyone.

Important warning

A verification code is like a temporary key.

If someone asks you to read them a code over the phone, send a code by text, or type a code into a strange website, stop.

They may be trying to log in as you.

Step 4: Review Recovery Options

Recovery options help you get back into your account if you forget your password or get locked out.

But they can also become a weakness if they are old, unknown, or controlled by someone else.

Review these items

[ ] Recovery email address.
[ ] Recovery phone number.
[ ] Trusted phone numbers.
[ ] Backup codes.
[ ] Security questions, if your provider still uses them.
[ ] Recovery key, if enabled.
[ ] Trusted devices.
[ ] Account recovery contacts, if available.

Remove or update

[ ] Old phone numbers you no longer own.
[ ] Old email addresses you no longer check.
[ ] Recovery emails belonging to people you do not fully trust.
[ ] Devices you no longer use.
[ ] Unknown recovery options.
[ ] Weak security questions with guessable answers.

Good recovery rule

Your recovery options should be:

- Current
- Private
- Protected
- Controlled by you
- Accessible in an emergency

Step 5: Check Recent Sign-In Activity

Most major email providers allow you to review recent account activity or recent sign-ins.

This can show where your account was used, what devices signed in, or whether there were suspicious login attempts.

Look for

[ ] Sign-ins from places you do not recognize.
[ ] Devices you do not own.
[ ] Browsers you do not use.
[ ] Failed login attempts.
[ ] Successful logins at strange times.
[ ] Activity from countries or regions you have not visited.
[ ] Security settings changed without your knowledge.

If you see something suspicious

[ ] Change your password immediately from a trusted device.
[ ] Turn on MFA if it is not already enabled.
[ ] Sign out of other sessions if your provider allows it.
[ ] Review recovery options.
[ ] Review forwarding rules and filters.
[ ] Review connected apps.
[ ] Watch for password reset emails or account changes.

Step 6: Sign Out of Unknown Devices

Your email may still be signed in on old phones, tablets, computers, browsers, or shared devices.

Do this

[ ] Review devices connected to your account.
[ ] Sign out of devices you do not recognize.
[ ] Sign out of old phones or computers you no longer use.
[ ] Sign out of shared or public computers.
[ ] Remove lost or stolen devices.
[ ] Change your password if an unknown device had access.

Important

If you sell, donate, recycle, or give away a device, sign out of email and remove the account before letting the device go.

Step 7: Review Connected Apps and Third-Party Access

Some apps and websites may have permission to access parts of your email account or profile.

This can happen when you click “Sign in with Google,” “Sign in with Microsoft,” “Sign in with Apple,” or connect an app to your mailbox.

Look for

[ ] Apps you no longer use.
[ ] Apps you do not recognize.
[ ] Browser extensions with account access.
[ ] Old services connected years ago.
[ ] Apps with permission to read email, contacts, files, or calendar.
[ ] Unknown mail clients or devices.

Do this

[ ] Remove access for apps you do not use.
[ ] Remove apps you do not recognize.
[ ] Keep only services you trust and still need.
[ ] Be careful before granting new access.

Simple rule

If you do not recognize it, do not ignore it.

Review it carefully and remove it if you do not need it.

Step 8: Review Forwarding and Inbox Rules

This step is very important.

If someone accessed your email, they may create forwarding rules or filters to hide messages from you.

For example, they may forward all bank emails to another address or hide password reset alerts in a folder.

Check for

[ ] Email forwarding to unknown addresses.
[ ] Filters that delete messages automatically.
[ ] Filters that archive or hide security alerts.
[ ] Rules that move bank emails to strange folders.
[ ] Rules that mark messages as read.
[ ] Rules you did not create.

Do this

[ ] Remove unknown forwarding addresses.
[ ] Remove suspicious filters.
[ ] Remove suspicious inbox rules.
[ ] Review blocked senders.
[ ] Review automatic replies.
[ ] Check trash, archive, spam, and hidden folders.

Warning sign

If bank alerts, password reset emails, or security notifications are disappearing, check forwarding and inbox rules immediately.

Step 9: Protect Your Phone

Your phone is often connected to your email account.

It may receive MFA codes, password reset links, push notifications, and recovery messages.

Do this

[ ] Use a strong screen lock.
[ ] Avoid easy PINs like 1234, 1111, or your birth year.
[ ] Keep your phone updated.
[ ] Turn on Find My iPhone or Find My Device.

[ ] Remove apps you do not use.
[ ] Protect your mobile carrier account with a strong password.
[ ] Add a carrier account PIN or port-out protection if available.
[ ] Be careful if your phone suddenly loses service.

Why this matters

If someone takes over your phone number, they may receive text-message codes meant for you.

That is one reason authenticator apps, passkeys, or security keys are often safer than text-message codes.

Step 10: Watch for Email Impersonation

If someone gets access to your email, they may send messages pretending to be you.

They may contact:

- Family
- Friends
- Clients
- Coworkers
- Banks
- Vendors
- Social media contacts

They may ask for money, gift cards, sensitive information, or urgent favors.

Warning signs your account may be misused

[ ] Friends say they received strange messages from you.
[ ] Sent messages appear that you did not send.
[ ] Replies appear to messages you do not remember sending.
[ ] Your contacts receive payment requests from you.
[ ] You see password reset emails you did not request.
[ ] You stop receiving expected emails.
[ ] Your inbox rules or forwarding settings changed.

If this happens, treat it seriously.

Provider-Specific Starting Points

Settings change over time, so use these as general directions.

If the exact menu looks different, search inside your account settings for words like:

- Security
- Privacy
- Sign-in
- Two-step verification
- Two-factor authentication
- Recovery
- Devices
- Recent activity
- Connected apps

Gmail / Google Account

Focus on:

[ ] Google Security Checkup.
[ ] 2-Step Verification.
[ ] Recovery phone.
[ ] Recovery email.
[ ] Recent security activity.
[ ] Your devices.
[ ] Third-party apps with account access.
[ ] Gmail forwarding settings.
[ ] Gmail filters.
[ ] App passwords, if used.
[ ] Google Advanced Protection, if you are at higher risk.

Good for:

- Gmail users
- Android users
- Google Drive users
- YouTube users
- Google Photos users
- People who use Google sign-in for other services

Outlook / Hotmail / Microsoft Account

Focus on:

[ ] Microsoft account security dashboard.
[ ] Two-step verification.
[ ] Security info.
[ ] Recent activity.
[ ] Sign-in methods.
[ ] Recovery email.
[ ] Recovery phone.
[ ] Devices.
[ ] App passwords, if used.
[ ] Outlook forwarding rules.
[ ] Inbox rules.
[ ] Connected apps and services.

Good for:

- Outlook users
- Hotmail users
- Windows users
- OneDrive users
- Xbox users
- Microsoft 365 users
- People who use Microsoft sign-in for other services

Apple / iCloud Email

Focus on:

[ ] Apple Account sign-in and security settings.
[ ] Two-factor authentication.
[ ] Trusted phone numbers.
[ ] Trusted devices.
[ ] Account recovery options.
[ ] Recovery key, if you choose to use one.
[ ] iCloud Mail settings.
[ ] Devices connected to your Apple Account.
[ ] Find My settings.
[ ] App-specific passwords, if used.

Good for:

- iPhone users
- iPad users
- Mac users
- iCloud Mail users
- Apple Photos users
- Apple Pay users
- People using Apple ID for purchases and subscriptions

Yahoo Mail

Focus on:

[ ] Account Security page.
[ ] Two-step verification.
[ ] Recovery phone.
[ ] Recovery email.
[ ] Recent activity.
[ ] App passwords, if used.
[ ] Mail forwarding.
[ ] Filters.
[ ] Connected apps.

Good for:

- Longtime Yahoo users
- People who still use Yahoo for password resets
- Older accounts connected to important services

Important:

Older email accounts are often forgotten but still connected to banks, shopping accounts, social media, or password resets. Do not ignore them.

Higher-Risk Users Should Add Stronger Protection

Some people should consider stronger email protection.

This may include:

- Public-facing professionals
- Journalists
- Activists
- Business owners
- Freelancers with client data
- People involved in legal disputes
- People who have already been targeted
- People helping older relatives with finances
- People with high-value financial accounts
- People with sensitive work or personal circumstances

Stronger options may include

[ ] Hardware security keys.
[ ] Passkeys.
[ ] Advanced account protection programs.
[ ] Separate recovery email used only for account recovery.
[ ] Stronger password manager setup.
[ ] Fewer connected apps.
[ ] More frequent review of account activity.
[ ] Separate email addresses for different purposes.

Do not add complexity unless you can manage it safely.

Simple protection used consistently is better than advanced protection you do not understand.

What Not to Do

Do not:

[ ] Reuse your email password.
[ ] Share your email password with anyone.
[ ] Share MFA codes.
[ ] Leave old recovery phone numbers on the account.
[ ] Keep unknown devices signed in.
[ ] Ignore strange forwarding rules.
[ ] Click email security links from suspicious messages.
[ ] Use public computers for important email unless necessary.
[ ] Stay signed in on shared devices.
[ ] Use weak security questions with answers found on social media.
[ ] Give remote access because of a pop-up or unexpected call.

If You Think Your Email Was Compromised

If you suspect someone accessed your email account, act quickly and calmly.

Immediate steps

[ ] Change the password from a trusted device.
[ ] Turn on MFA.
[ ] Sign out of other sessions.
[ ] Review recent activity.
[ ] Review recovery phone and email.
[ ] Remove unknown recovery options.
[ ] Check forwarding rules.
[ ] Check inbox filters.
[ ] Review connected apps.
[ ] Review sent messages.
[ ] Check trash, spam, archive, and hidden folders.
[ ] Warn important contacts if scam messages were sent from your account.
[ ] Check bank, payment, and shopping accounts for unusual activity.

If you cannot get back in

[ ] Use the official account recovery page for your email provider.
[ ] Do not pay random “account recovery” services.
[ ] Do not trust people who contact you claiming they can recover the account.
[ ] Contact the provider through official channels.
[ ] If financial accounts are affected, contact your bank immediately.

Email Security Review Schedule

Use this schedule to keep your account safer over time.

Once

[ ] Use a unique password.
[ ] Turn on MFA.
[ ] Update recovery options.
[ ] Save backup codes safely.
[ ] Review devices.
[ ] Review forwarding rules.
[ ] Review connected apps.

Monthly

[ ] Review recent security activity.
[ ] Check for unknown devices.
[ ] Check for suspicious emails or password reset notices.

Every 3–6 months

[ ] Review recovery phone and email.
[ ] Review connected apps.
[ ] Review forwarding and inbox rules.
[ ] Remove old devices.

After major life changes

Review your account after:

[ ] Changing phone numbers.
[ ] Losing a phone.
[ ] Replacing a computer.
[ ] Moving.
[ ] Divorce or separation.
[ ] Job change.
[ ] Death or illness in the family.
[ ] Suspicious messages or scam attempts.
[ ] Data breach notifications.

Family Email Safety Tips

If you help a parent, spouse, or older relative, begin with their main email account.

Help them review

[ ] Password uniqueness.
[ ] MFA status.
[ ] Recovery phone number.
[ ] Recovery email.
[ ] Devices signed in.
[ ] Suspicious forwarding rules.
[ ] Scam warning signs.
[ ] Who to call before clicking or sending money.

Important family rule

No one should share a verification code over the phone, by text, or by email.

Even with family, codes should be treated carefully.

Freelancer and Home-Office Email Tips

If you use email for freelance work, consulting, or home-office activity, your email may also protect client files, invoices, contracts, payment records, and business accounts.

Additional steps

[ ] Use a separate professional email if possible.
[ ] Turn on MFA.
[ ] Use a password manager.
[ ] Be careful with client attachments.
[ ] Verify payment-change requests.
[ ] Do not trust urgent bank-detail changes by email alone.
[ ] Back up important client records.
[ ] Keep personal and professional accounts separated where possible.

Payment-change warning

If a client, vendor, or colleague emails new payment instructions, verify through a known trusted channel before sending money.

Email accounts are often used for invoice and payment scams.

Personal Email Security Worksheet

My main email account

Email address: _____

Provider: _____

Security status

[ ] Unique password
[ ] MFA enabled
[ ] Recovery phone reviewed
[ ] Recovery email reviewed
[ ] Recent activity reviewed
[ ] Devices reviewed
[ ] Forwarding rules reviewed
[ ] Filters reviewed
[ ] Connected apps reviewed
[ ] Backup codes saved safely

My recovery email

Recovery email: _____

Is this account also protected with MFA?

[ ] Yes
[ ] No
[ ] Not sure

My recovery phone

Recovery phone: _____

Is my mobile carrier account protected with a PIN or extra security?

[ ] Yes
[ ] No
[ ] Not sure

Devices I recognize

Device 1: _____

Device 2: _____

Device 3: _____

Devices or activity I need to investigate

Final Email Safety Rules

Protect your email first.
Use a unique password.
Turn on MFA.
Keep recovery options current.
Do not share verification codes.
Review recent activity.
Remove old devices.
Check forwarding rules.
Watch for suspicious filters.
Protect your phone.
Do not click security links from suspicious messages.
Use official account settings instead.

Your email account is the front door to much of your digital life.

Protect it before something goes wrong.

Click Giraffe Reminder

Click Giraffe is a self-service digital safety membership.

It provides educational guides, checklists, tutorials, monthly scam alerts, and practical resources.

It does not provide live technical support, emergency support, remote access, account recovery, fraud recovery, legal advice, financial advice, medical advice, managed IT services, or guaranteed remediation.

If you are facing fraud, stolen money, identity theft, a compromised account, or an urgent incident, contact the relevant provider, financial institution, law enforcement agency, or qualified professional.