

NAPLES COMPUTERS HOW-TO • SECURITY & SAFETY

What to Do If Your Email Was Hacked

Friends getting strange emails from you? Password reset emails you didn't ask for? Your email account may have been hacked. This guide shows what to do: change your password from a clean device, turn on two-factor sign-in, remove forwarding and rules you didn't create in Outlook.com and Gmail, sign out devices you don't recognize, check your recovery info, scan your computer, and warn your contacts.

Signs your email **was** hacked

- ☐ Friends get spam or strange requests from you
- ☐ Sent messages you didn't write
Check your Sent and Deleted folders
- ☐ Password reset emails you didn't ask for
- ☐ Forwarding or rules you didn't set up
Your mail quietly goes somewhere else
- ☐ You can't sign in at all

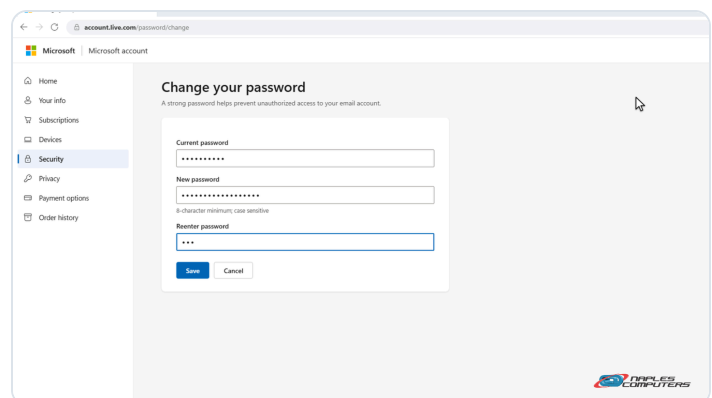
Step by step

1 Step 1: Change your password, from a clean device

Use a computer or phone you know is clean. In your Microsoft account, Security shows Recent activity: look for sign-ins you don't recognize.

WHAT TO DO

Click Change password, and choose a strong password you've never used anywhere else.



2 Turn on two-factor sign-in

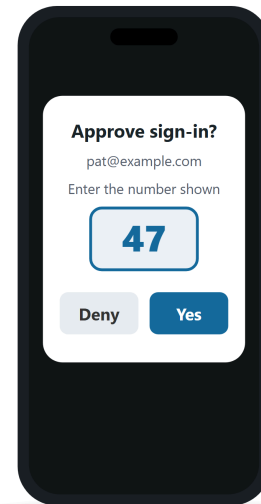
With two-factor sign-in, a stolen password isn't enough. You approve each new sign-in on your phone.

WHAT TO DO

Microsoft: Security → Manage how I sign in.

Google: Security & sign-in → 2-Step

Verification. See our two-factor video.



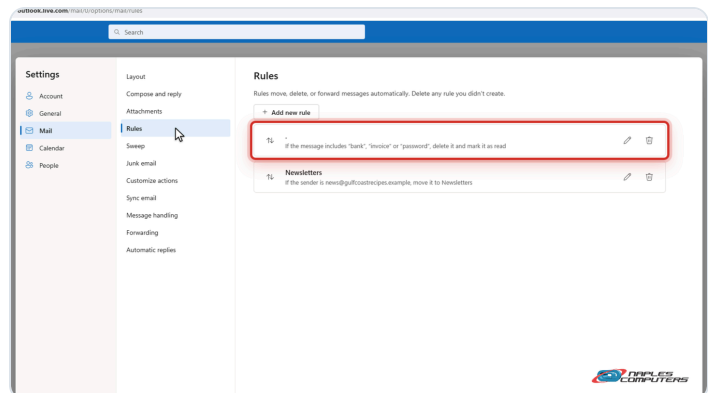
A stolen password isn't enough

3 Step 3: Outlook.com: turn off forwarding and delete rules you didn't create

Settings → Mail → Forwarding. If forwarding is on and you didn't set it up, uncheck Enable forwarding and click Save.

WHAT TO DO

Then Mail → Rules: delete any rule you didn't create, like one that deletes messages about your bank.

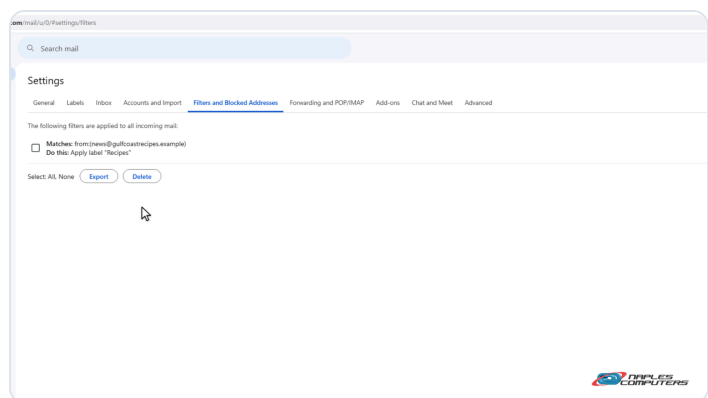


3 Step 3: Gmail: disable forwarding and delete filters you didn't create

Settings → See all settings → Forwarding and POP/IMAP. Choose Disable forwarding, then Save Changes.

WHAT TO DO

Then open Filters and Blocked Addresses, select any filter you didn't create, and click Delete.



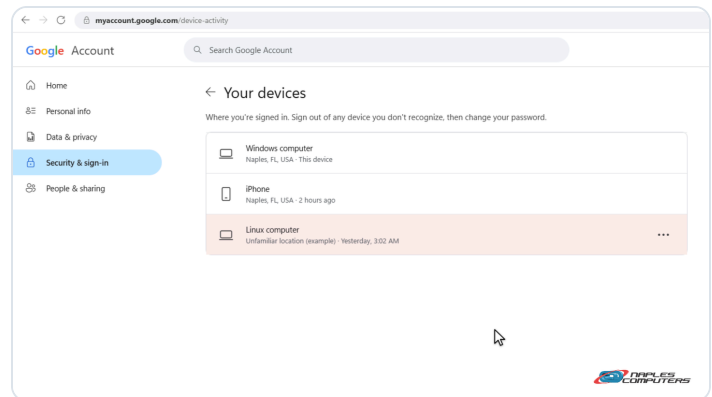
Step 4: Sign out devices you don't recognize, and check your recovery info

4 don't recognize, and check your recovery info

Google Account → Security & sign-in → Your devices. Next to a device you don't recognize, choose Sign out.

WHAT TO DO

Then make sure the recovery phone and recovery email are yours. Hackers change them to lock you out.



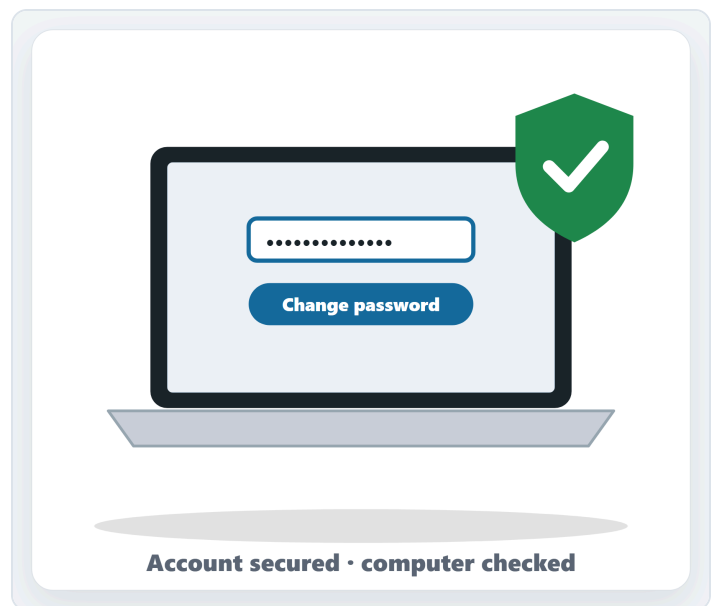
WE CAN HELP

+ Want us to check it for you?

We'll secure your email account, remove forwarding and rules, check your computer for malware, and set up two-factor sign-in.

WHAT TO DO

Call 239-513-1960 to schedule a remote session, then click Join Remote Session at naplescomputers.com.



Step 5: finish the cleanup

- ☐ Scan your computer
Run a full scan with your security software
- ☐ Warn your contacts
Ask them not to click links or send money "from you"
- ☐ Same password somewhere else?
Change it there too, starting with banking and shopping
- ☐ Watch for fake "helpers"
Naples Computers never cold-calls you to get on your computer

Recap: email hacked?

- | | |
|--|--|
| ☐ New password, from a clean device | ☐ Sign out other devices |
| ☐ Turn on two-factor sign-in | ☐ Check recovery phone & email |
| ☐ Remove forwarding & rules | ☐ Scan, warn contacts, fix reused passwords |

Naples Computers never cold-calls customers to get on your computer: our remote sessions are always scheduled, or started by you. Want help? Call 239-513-1960 to schedule, then click Join Remote Session at naplescomputers.com.



Email hacked? We can secure your account and check your computer.

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**