WHAT TO DO IF YOU GET HACKED

LISTED ARE SOME STEPS ONE CAN TAKE AFTER GETTING HACKED.

Step #1: CHANGE YOUR PASSWORD

The very first thing you should do is keep the hacker from getting back into your email account. Change your password to a strong password that is not related to your prior password; if your last password was billyjoe1, don’t pick billyjoe2—and if your name is actually BillyJoe, you shouldn’t have been using your name as your password in the first place.

Try using a meaningful sentence as the basis of your new password. For example, “I go to the gym in the morning” turns into “Ig2tGYMItm” using the first letter of each word in the sentence, mixing uppercase and lowercase letters and replacing the word “to” with “2.”

Step #2: RECLAIM YOUR ACCOUNT

If you’re lucky, the hacker only logged into your account to send a mass email to all of your contacts. If you’re not so lucky, the hacker changed your password too, locking you out of your account. If that’s the case, you’ll need to reclaim your account, usually a matter of using the “forgot your password” link and answering your security questions or using your backup email address. Check out the specific recommendations for reclaiming possession of your account for Gmail, Outlook.com and Hotmail, Yahoo! and AOL.
STEP #3: ENABLE TWO-FACTOR AUTHENTICATION

Set your email account to require a second form of authentication in addition to your password whenever you log into your email account from a new device. When you log in, you’ll also need to enter a special one-time use code the site will text to your phone or generated via an app. Check out two-step authentication setup instructions here [https://twofactorauth.org/#email](https://twofactorauth.org/#email)

STEP #4: CHECK YOUR EMAIL SETTINGS

Sometimes hackers might change your settings to forward a copy of every email you receive to themselves, so they can watch for any emails containing login information for other sites.

Check your mail forwarding settings to ensure no unexpected email addresses have been added. Next, check your email signature to see if the hacker added a spammy signature that will continue to peddle their dubious wares even after they've been locked out. Last, check to make sure the hackers haven’t turned on an auto-responder, turning your out-of-office notification into a spam machine.

STEP #5: SCAN YOUR COMPUTER FOR MALWARE

Run a full scan with your anti-malware program. You do have an anti-malware program on your computer, right? If not, download the free version of Malwarebytes and run a full scan with it.

I recommend running Malwarebytes even if you already have another anti-malware program; if the problem is malware, your original program obviously didn’t stop it, and Malwarebytes has resolved problems for me that even Symantec’s Norton Internet Security wasn’t able to resolve.

Scan other computers you log in from, such as your work computer, as well. If any of your scans detect malware, fix it and then go back and change your email password again (because when you changed it in Step #1, the malware was still on your computer)