So your email has been hacked? Here are some steps you can take to resolve the problem and protect yourself from future attacks..

Step 1: get into your email account

The first step is to assess the damage. Go to the website of your email provider, and log into your email account.

If the password has been changed, then try the password reset mechanism by clicking on the link marked “Forgotten your password?” or similar.

Once you’re into your email account, the very first thing you should do is change your password. Change it to something long and strong, using multiple cases, numbers and special characters. Avoid using real words. We'll deal with password security later, but for now, change it so the hacker can't get back into your email account.

Step 2: check your other accounts

Once you’ve changed the password for your email account it is important to change the password of any other accounts with other services such as Facebook, Twitter, Amazon or your internet banking that may have had the same password.

It is especially important if you use your email address as the username for those accounts, as the hackers now have both your username and password for those services.

Check both your inbox and trash for any password reset emails from other services or accounts linked to your email address *not* instigated by you. The hacker could have attempted to change your password on other sites, using access to your email to perform password resets.

Step 3: check for spam

Some hackers compromise email accounts in order to attack your friends or contacts. They use your email address to send spam or phishing emails attempting to trick them into thinking you need help, buy something or into giving up personal information.

While it can be difficult to tell if your email account was abused in this way, a quick check of your sent email or your inbox for dodgy replies will help identify anyone who was targeted from your contacts list.

If you do find someone contacted by the hacker, let them know that you didn't send the email to them via another communication method if you can, or by email if that's your only contact with them.

Step 4: sort out your apps

Once you've secured your email account, and dealt with any potential fallout from the violation, you need to make sure you can access your email address in all your usual places.

If you use an email program, something like Outlook, Windows Mail, Mac Mail or you get your email on a phone or tablet computer, you will have to swap the compromised password on each device for your newly created secure password.

Each program will be different, but as a general rule of thumb you have to go into the settings menu for your email account in the program and modify the account details to enter the new password.

Instructions for how to do that are listed on the help websites for Outlook, Windows Mail, and Apple's support forum for Apple Mail. On Android smartphones and tablets your password can be changed in the accounts section of the settings app. For the iPhone and iPad, your password can be changed under the mail, contacts and calendar section of the settings app.

Step 5: protect yourself for the future

The risk of having your email account or other services hacked is increasing, but there are some things you can do to prevent it.

The humble password is not as secure as it used to be, but choosing a strong password can help.

• The longer the password the better. The more characters there are in your password the longer it will take for a hacker to break it, making it less likely they will continue trying.

• Use a mixture of numbers, lowercase and uppercase letters and special characters (punctuation) as it increases the complexity of your password and increases its strength.

• Do not use real words in your passwords. The majority of hacking attacks cycle through dictionary words, which means if you use a real word in your password it is more likely to be broken.

• The best passwords are a randomly generated strings of characters numbering 16 or more. Of course, that makes them very difficult to remember.

• Never use a password twice.

To solve the issue of trying to remember long complex passwords, password managers like LastPass or 1Password can help, storing all your passwords in a secure place, ready to fill in any login you need right in your browser.

By using a password manager you are only as secure as the password to your password manager. Remembering one really complex and long password is a lot easier than remember 10 or 20 of them, however.

Another layer of security

In addition to passwords, a different type of security mechanism called two-factor authentication is becoming increasingly available.

In principle it is very simple. In addition to your username and password you have another form of identification, normally consisting of a code generated by a key fob or a smartphone app, that has to be put in at the time of login and changes every minute or so.

It means you keep something the hacker cannot get to, securing your account with another layer of security.

Banks have been using them for a while, some giving out card readers that force you to enter your Pin to generate a code to input into your internet banking. Now most email providers and a variety of other online services

offer two-factor or two-step authentication for free, so it is worth activating on your accounts if it is available.