

Hacked email account? Here's what to do next.



HOW AND WHY DO HACKERS GAIN ACCESS TO EMAIL ACCOUNTS?

How? By convincing you to open attachments or links that contain malware (a code or a file that is designed to steal data and cause damage to computers and networks). This is a very good reason not to open attachments that you aren't expecting.

Why? Email addresses are a gold mine of information. You have an address book full of names that hackers can send emails to and infect even more computers. You may have emails from your bank, medical provider, business contacts, and online retailers to name a few.

SIGNS THAT YOUR EMAIL HAS BEEN HACKED

You can't log in to your email account

You try to log in to your email account multiple times but each time the log in fails. There's a good chance that a hacker has access to your password. The hacker logged in and then changed your password so they can control your account.

One of your contacts asks, "Did you send me this email?"

Someone you know receives an email sent from your email address, but it doesn't "sound" like you. The hacker may include attachments or links that are infected with malware. Your contact opens the link or attachments and now their computer has been hacked, too.

REGAIN CONTROL OF YOUR EMAIL AND DISCOURAGE HACKERS

Reach out to your contacts

Let your contacts know that your email account has been hacked and to not open emails from you that contain attachments or links until you are able to secure your account.

Change your password, if you can

Create a strong, long, unique password. Most browsers and operating systems (e.g. Google, Safari) have password managers that will create and save strong passwords for you. For more information, see [Password Dos and Don'ts](#).

If you can't change your password...

Most email providers have dedicated pages to help you if you have lost your password or had your password stolen. For example, [Gmail account help can be found here](#).

Use two-factor authentication

Two-factor authentication is an added layer of security. When logging in to your account a PIN is sent to your cellphone to ensure that you are who you say you are. If accounts offer two-factor authentication, use it. Yes, it is an extra step, but it is one of the strongest layers of security for all of your accounts.