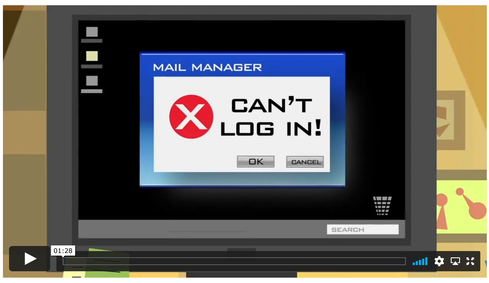
How To Recover Your Hacked Email or Social Media Account

There are lots of ways to protect your personal information and data from scammers. But what happens if your email or social media account gets hacked? Here are some quick steps to help you recover your email or social media account.



Signs That Your Email or Social Media Account Has Been Hacked

You might have been hacked if

- your social media account has posts you didn't make
- you can't log into your email or social media account
- your Sent folder has messages you didn't send, or has been emptied
- friends and family are getting emails or messages you didn't send, sometimes with random links or fake pleas for help or money

Steps To Get Back Into Your Account

1. Update your security software, run a scan, and delete any malware.

Start with this important step — especially if you're not sure how someone hacked into your account. Use either the security software that comes with your computer, phone, or tablet or download software from a reputable, well-known security company. Then, run it to scan your device for malware. If the scan identifies suspicious software, delete it, and restart your device.

2. Change your passwords.

If you're able to log into your email or social media account, change the password right away. If you use similar passwords for other accounts, change them, too. Make sure you create strong passwords that will be hard to guess.

If you can't log in to change your password, check the advice your email provider or social network has available. Several popular email service providers (like Gmail and Yahoo) and social media websites (like Facebook and Twitter) give advice on how to restore and protect your account. If someone took over your account, you might need to fill out forms to prove it's really you who's trying to get back into your account.

3. Set up multi-factor authentication.

While you're updating your password, check if your email or social media account lets you turn on multi-factor authentication. Multi-factor authentication requires a password plus something else — say, a code from an authenticator app — to prove it's really you.

What To Do Once You're Back in Your Account

1. Check your account settings.

After you log back in to your email account, check on a few things:

- Look at your signature block and make sure it doesn't have any unfamiliar links.
- Check your settings to see if there are "rules" set up to forward emails automatically. Delete any rules you didn't set up, so your messages aren't forwarded to someone else's address.
- On your social media account, look for changes since you last logged in — like any new "friends."

2. Take stock of what's in your inbox.

Consider what kind of information the hacker might have seen. Hackers look for information that can help them find usernames and passwords to important sites, like online banking or retirement accounts. Consider changing the usernames and passwords for accounts that may be at risk.

3. Look for tracks.

In your email account, review the Sent, Trash, or Deleted folders. You might be able to uncover clues about what the hacker did. Search for emails that the hacker sent from your account, or that the hacker may have viewed and then deleted.

In your social media account, check for messages that the hacker might have sent from your account.

This information will help you figure out what information was exposed. If it was, visit IdentityTheft.gov to find out what you should do next.

4. Report misused information at IdentityTheft.gov.

If you the hacker misused your sensitive information, like your Social Security number, to access or open new accounts, to apply for government benefits, to file federal taxes, or any other misuse, report it. At IdentityTheft.gov, you can create an individualized recovery plan to help you recover from identity theft.

5. Tell your friends.

Send your friends a quick email or text, or post something to let them know that you were hacked. Tell them not to click on links in emails from you or respond to a hacker's fake pleas for help or money. If you're emailing a bunch of people, put their email addresses in the Bcc line to keep them confidential. You could send them this article, too.

How To Protect Your Accounts From Getting Hacked

- **Use strong passwords.** That means at least 12 characters. Making a password longer is generally the easiest way to make it stronger. Consider using a passphrase of random words so that your password is more memorable, but avoid using common words or phrases. If the service you're using doesn't allow long passwords, you can make your password stronger by mixing uppercase and lowercase letters, numbers, and symbols. And don't reuse existing passwords from other accounts. If one of those accounts gets hacked, a hacker can try that same password to get into your email or social media account. For more tips, check out this Password Checklist.
- **Turn on multi-factor authentication.** Multi-factor authentication requires a password plus something else — say, a code from an authenticator app — to prove it's really you. This protects your account even if your password is stolen.
- **Protect your information.** Think twice when someone asks you to put in your username and password. Never give them out in response to an email. If the email or text seems to be from your bank, for example, visit the bank website directly. Don't click on any links or call any numbers in the message. Scammers impersonate well-known businesses to trick people into giving out personal information.
- **Install and update security software, and use a firewall.** Set your security software, internet browser, and operating system (like Windows or Mac OS X) to update automatically.
- **Get well-known software directly from the source.** Sites that offer lots of different browsers, PDF readers, and other popular software for free are more likely to include malware.
- **Don't treat public computers or a friend's phone like it's your own device.** If it's not ***your*** computer or phone, don't let a web browser remember your passwords. Avoid going to personal accounts — like bank accounts or email — from anywhere besides your own personal devices. And make sure to log out of any accounts when you're done. Limiting where you put your personal information reduces the chance that your information will get hacked. Also always avoid logging into your personal accounts when you're on public Wi-Fi because it's usually not secure.

Tagged with: computer security, email, hacker, password, social networking

May 2021