

Securing your AOL account*

Email is an integral tool used every day to communicate and interact online, and can be used as a user ID when signing into websites. Hackers can attempt to gain access to your accounts by attacking email providers or employing social engineering techniques and malware to target you. It is important to utilize your email provider's security features and to take the appropriate steps if you believe your account has been compromised.

Email security best practices

- Maintain separate accounts for business and personal use, and don't use them interchangeably
- Create passwords of at least 10 characters, using a mix of upper- and lower-case letters, numbers and special characters. Change your passwords three or four times a year
- Be alert to social engineering attempts – cyber criminals may use emails that contain links, malware or viruses to gain confidential information
- Safeguard your information – use an email encryption tool when transmitting sensitive information
- Create “disposable” email addresses for websites that require an email as a user ID
- When accessing email accounts, ensure software on devices are up-to-date and consider using a Virtual Private Network (VPN) when using public Wi-Fi

Account security features

Strengthen your password

A strong password is your front line of defense against unauthorized access to your accounts.

- Navigate to **My Account** > Answer your **Account Security Question** > **Change Your Password** > [Enter your current password, then your new secure password and confirm] > **Save**

Enable 2-step verification

2-step verification is one of the strongest cyber-security measures available and adds an extra layer of protection from cyber criminals. After you've enabled 2-step verification, you will enter your password and an additional security code upon logging in.

- Navigate to **Account Security** > Click **Set up** next to 2-Step Verification > Follow activation steps > **Turn on**

If you access your AOL account using any non-AOL apps or other programs (e.g. Outlook, mobile Mail apps), create application specific passwords. If you have 2-step verification turned on and do not have application-specific passwords for your apps, you will receive an error that the apps cannot connect:

- After setting up 2-step verification, click **Get Application Passwords** > Choose an application from the drop-down menu > Enter device name > Open the app for which you created the password and enter the password into the “Password” field for this app

Note: Record your Disable code provided during set-up for future use in case you lose or cannot access your phone

Enable recovery contact information

In the event that you lose access to your email account, enabling recovery contact information can help expedite the account recovery process. To change the contact information already provided during account set-up:

- Navigate to **My Account** > Answer your **Account Security Question** > **Manage my account details** > **Update My Contact Information** > **Edit** > [Add alternate email address and mobile phone number] > **Save**

Filter suspicious emails

If you receive a suspicious or unwanted email, reporting it to AOL can help ensure you do not receive further suspicious emails to your inbox, and can help customize your account's spam filters.

- Click on the box to the left of the message > Click on **Spam** button in the toolbar above your emails
- Forward suspicious emails to **aol_phish@abuse.aol.com**

AOL gives the option to customize the default spam filters.

- Navigate to **Options** in the upper-right corner > **Mail Settings** > **Spam Settings** > Ensure the box next to **Enable Spam Filter** is checked > [Modify each setting to your level of risk comfort] > **Save**
 - **Content Filter:** choose to block messages containing pictures or specific words or phrases
 - **Blocked Mail:** choose to permanently delete or move blocked mail to the spam folder
Note: To block all incoming email messages, choose to automatically delete all emails
 - **Sender Filter:** block or allow emails from specific senders or domains

Premium security features

AOL provides premium security features through voluntary, subscription services. For additional information, consult the MyBenefits page:

- Navigate to **Help Main** > **MyBenefits** > **AOL Plans**

If you believe your account has been compromised, some best practices to mitigate the risk of future fraud occurring:

- Change your password on your various online accounts, using a different password for each account
- Enable two-factor authentication (two-step verification) wherever possible, including on your email, banking, e-commerce accounts
- Install anti-virus and anti-malware software, with auto-updates
- Ensure your operating system is up-to-date
- Contact your J.P. Morgan representative immediately

Tools to identify if your account has been compromised

Check email forwarding and filter settings

After compromising your account, hackers can modify email settings to forward, delete or even send emails on your behalf without your knowledge. Periodically check email forwarding and filter settings to verify that there have not been changes made to your account.

- Navigate to **Options** in the upper-right corner > **Mail Settings** > **Filters and Alerts** > [Ensure only filters you created are enabled]

Review recent activity

Regularly review recent activity, including recently connected devices and account changes for suspicious activity.

- Navigate to **Account Options** > **View My Account Activity** > Select a month from the drop-down menu > **Go**

Closing your account

In the event that you no longer are using an email account, it is important to properly close the account and delete its data so it cannot be accessed in the future. Your account will be permanently deleted and you will not be able to recover any data or settings.

Note: AOL automatically disables accounts that are inactive for 90 days.

- Navigate to **My Account** > Answer your **Account Security Question** > **Manage My Subscriptions** > **Cancel** > Select a reason for canceling your service > **Cancel AOL**