# Securing your Yahoo 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 contact 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 **Settings** ⚙ > **Account Info** > **Account security** > **Change Password** > Enter and confirm your new password > **Continue** (a confirmation appears) > **Continue** to finish

### Two-step verification

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

- Navigate to **Settings** ⚙ > **Account Info** > **Account security** > Switch ON: **Two-step Verification** > Enter your mobile number > **Send SMS** to verify your mobile number via text message > Enter the verification code > **Verify**

### 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.

- Navigate to **Settings** ⚙ > **Account Info** > **Account security** > **Email addresses** > **Add recovery email address** > **Send verification email** > [click the verification link in the email sent to your recovery email address] > **Verify**

## Filter suspicious emails

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

Mark an email as spam:

- Select the checkbox next to the email(s) you're reporting > **Spam** > Your selected email(s) will be sent to your Spam folder

Yahoo also has the ability to report an email sent from a hacked account, a phishing email or emails that were intended for someone else.

Report email sent from a hacked account:

- Select the email you're reporting > Click the down arrow next to **Spam** > **Report a Hacked Account**

Report phishing scams:

- Select the email you're reporting > Click the down arrow next to **Spam** > **Report a Phishing Scam**

Report emails intended for someone else:

- Select the email you're reporting > Click the down arrow next to **Spam** > **Not My Mail**

## Disposable addresses

If you don't want to reveal your "real" email address, you can create disposable addresses. Each disposable address consists of a base name (common to all you create) and a keyword (up to 500). You can use disposable addresses for spam control, privacy, organization, or anonymity.

Create a base name:

- Navigate to **Settings** ⚙ > **Security** > **Create base name** (if you have already created a base name, click **Add** to create additional keywords) > **Enter a base name in the pop-up window** (ensure you're happy with your base name before you create it. You only get one per account and it is not possible to delete a base name once you've created it.) > **Create** > You will return to the Security Setting page and your base name will appear to the right of "Disposable Addresses"

Create a keyword:

- Navigate to **Settings** ⚙ > **Security** > **Add** > Enter the keyword in the field next to your base name > Select the folder where emails addresses to your disposable address will be delivered to > Make changes any changes to your Sending Name needed > **Save**

Send and receive with your disposable address:

- Create a new email > Click the drop-down menu beside From > Select the disposable address from the list, then compose and send the message.

**Note:** Messages sent to your disposable addresses will be delivered right to your Inbox or the folder you selected when you created the address

## 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 **Settings** ⚙ > **Accounts** > Select the appropriate email account > Ensure all email addresses listed belong to you > **Save**

### Review recent activity

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

- Navigate to **Settings** ⚙ > **Account Info** > **Recent Activity** > Review location and device info for any suspicious activity

## 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.

- Navigate to **Terminating your Yahoo account** > Read the information under “Before continuing, please consider the following information” > Confirm your password > **Terminate this Account**