



Royal Caribbean Group

# Scam Awareness Handbook

A guide to identifying and avoiding scams, and what to do if you've been victimized.



## A. DEFINITION — What is a scam?

A scam is a fraudulent scheme generally involving money and some sort of business transaction, especially for making a quick profit.

Scams are meant to look like the real thing and catch you off guard when you least expect it.

Scammers are getting smarter and taking advantage of new technology, new products or services, and major events to create believable stories that will convince you to give them your money or personal details.

## B. IDENTIFYING SCAMS

If it is too good to be true, then it probably is.

### Example of scams

Jobs and employment

- Recruiters charge fees even when none are required
- Recruiters charge for non-existent jobs

### Internet fraud

- Phishing
- Vishing (voice phishing)

### “This is my new number”

You receive a text message from an unknown number, claiming to be a relative, and they will ask for money or load credits.

### Unexpected winnings

These scams try to trick you into giving money or your personal information to receive a prize from a lottery or competition that you did not enter.

# SALARY @ SEA SCAM WARNING: DO NOT CLICK ON ANY SUSPICIOUS LINK OR SHARE YOUR S@S INFORMATION!

## ACTUAL EMAIL SCAM SENT TO CREW MEMBERS



ROYAL CARIBBEAN CRUISES LTD.



Dear Valued Crew Member –

The ROYAL CARIBBEAN INTERNATIONAL ship company mourns the corona virus outbreak (covid19).

In this case each crew member will be given an additional salary bonus. Please confirm your salary payment bonus on the web:

<https://salaryrcicrew.cruises/>

<https://salaryrcicrew.cruises/>



Thank you for being such a special part of Royal Caribbean. I speak for the entire executive team when

I say we appreciate you and we look forward to seeing you at sea again. We are a family, and we will get through this together, no matter where we may be around the world.

Sincerely,



Michael Bayley





## ACTUAL FACEBOOK SCAM SENT TO CREW MEMBERS

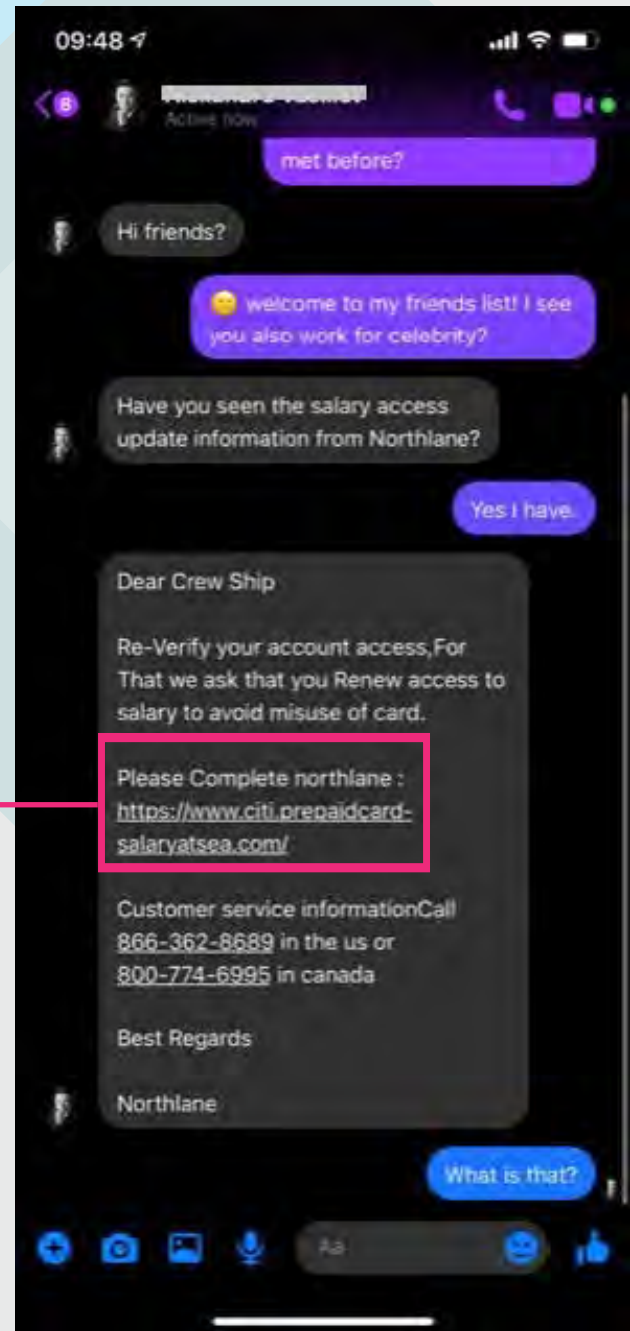
hey check Bonus ..  
you already check the bonus of \$  
100 in account citiprepaid, \$ 100  
bonus that comes from sea @  
salary .. try you check click and  
check the bonus \$ 100 in account  
citiprepaid

<http://card-citiprepaid.com/>



**NEVER** click on links like this:  
<http://card-citiprepaid.com>

## ACTUAL FACEBOOK SCAM SENT TO CREW MEMBERS



**NEVER** click on links like this:

<https://www.citi.prepaidcard-salaryatsea.com>

**Be careful** when accepting friend requests or responding to messages from strangers/non-contacts.

## ACTUAL EMAIL PHISHING SCAM SENT TO CREW MEMBERS

On Friday, 22 June 2018, 1:53:30 AM GMT-4, [REDACTED] wrote:

Hello Dear Crew Member

Find additional data on salary and bonuses while on board  
click the link: <https://access-na-citipreaid-wirecard.com>

For all crew members to confirm that our data can make it easier for you to earn a salary

Thanks for the cooperation.

Click - <https://access-na-citipreaid-wirecard.com>

@2018Wirecard Citiprepaid



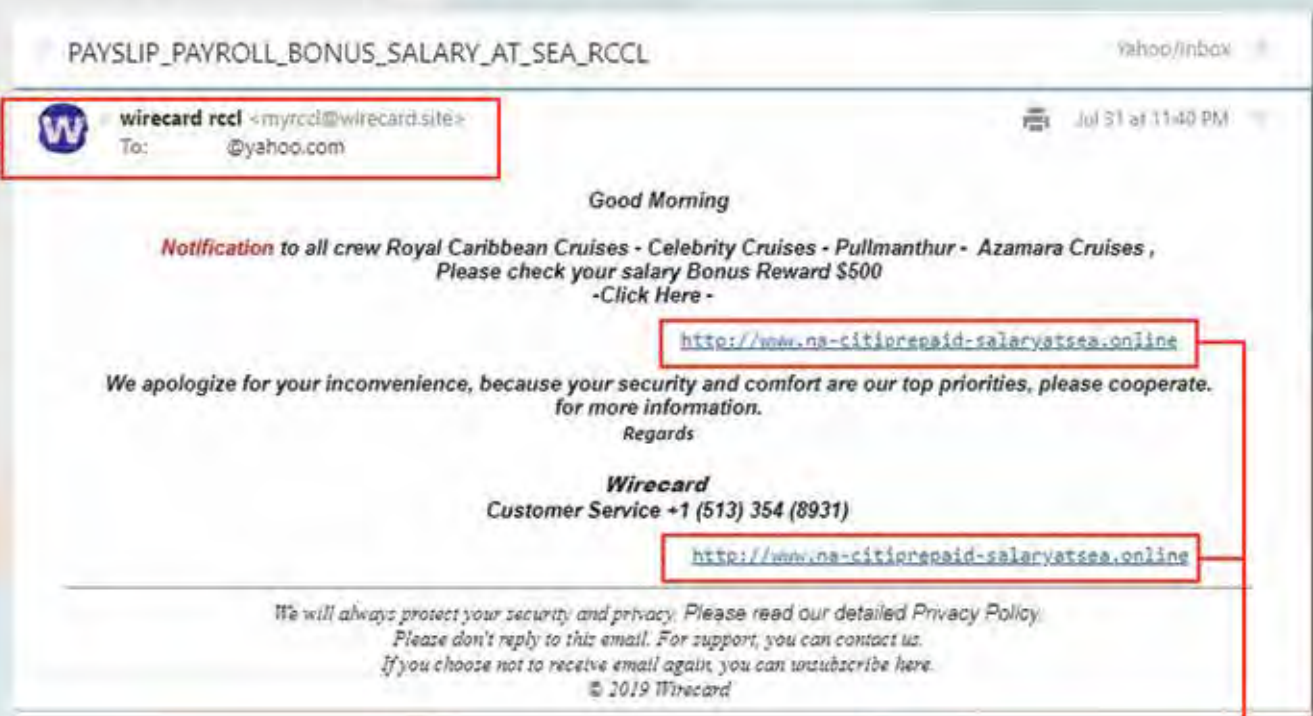
**NEVER** click on links like these:

<http://access-na-citipreaid-wirecard.com>

<http://na-citiprepaid-salaryatsea.online>



## ACTUAL EMAIL PHISHING SCAM SENT TO CREW MEMBERS

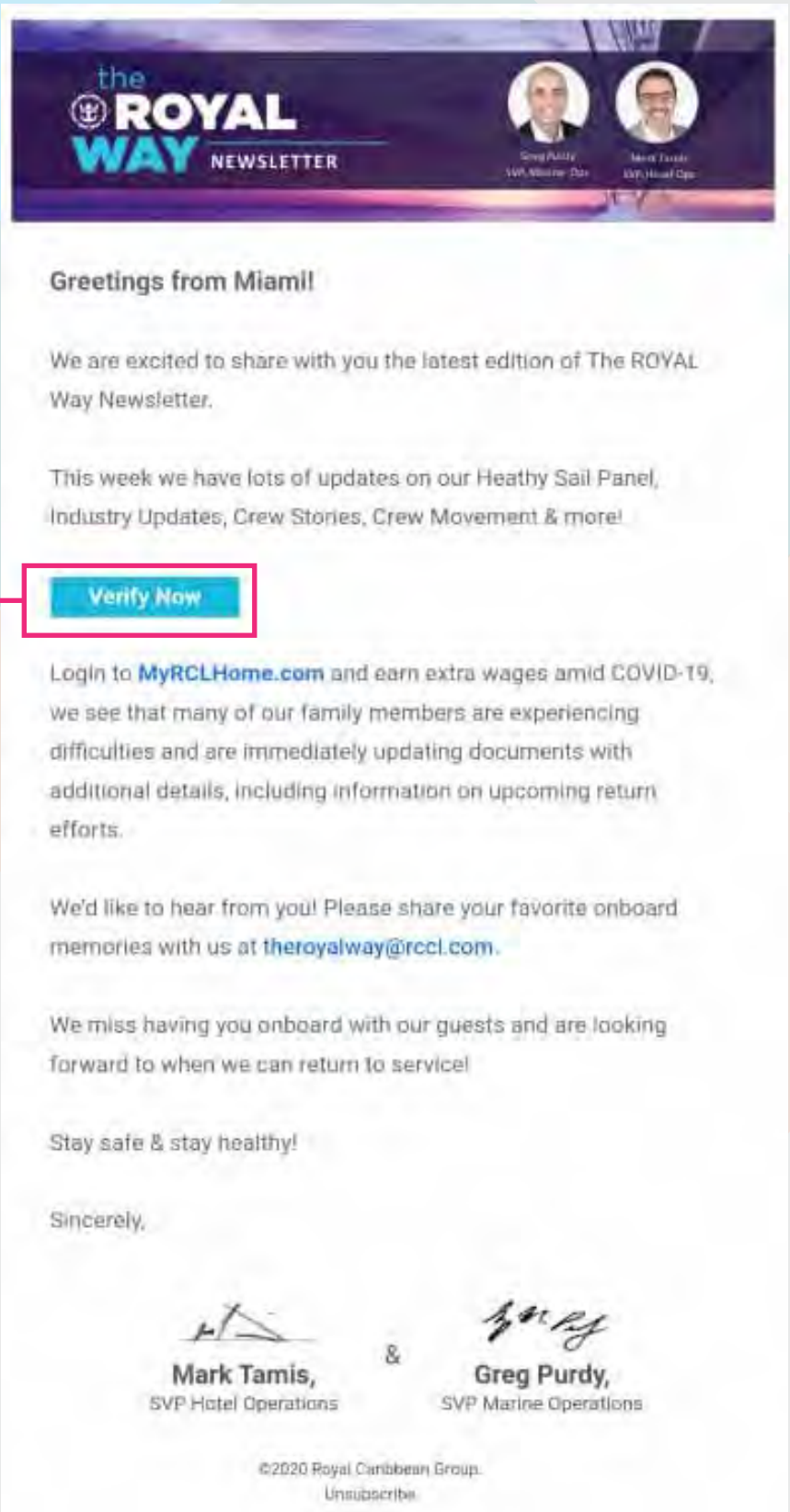


(Fake email address)



**NEVER** click on links like this:  
<http://na-citiprepaid-salaryatsea.online.com>

# ACTUAL PHISHING SCAM SENT TO CREW MEMBERS



**the ROYAL WAY NEWSLETTER**

Greg Purdy  
SVP Marine Ops

Mark Tamis  
SVP Hotel Ops

**Greetings from Miami!**

We are excited to share with you the latest edition of The ROYAL Way Newsletter.

This week we have lots of updates on our Heathy Sail Panel, Industry Updates, Crew Stories, Crew Movement & more!

**Verify Now**


Login to [MyRCLHome.com](https://MyRCLHome.com) and earn extra wages amid COVID-19. We see that many of our family members are experiencing difficulties and are immediately updating documents with additional details, including information on upcoming return efforts.

We'd like to hear from you! Please share your favorite onboard memories with us at [theroyalway@rccl.com](mailto:theroyalway@rccl.com).

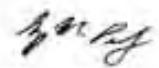
We miss having you onboard with our guests and are looking forward to when we can return to service!

Stay safe & stay healthy!

Sincerely,

  
**Mark Tamis,**  
SVP Hotel Operations

&

  
**Greg Purdy,**  
SVP Marine Operations

©2020 Royal Caribbean Group.  
[Unsubscribe](#)



**NEVER** click on links  
from sender of fake  
Company newsletters!



## ACTUAL PHISHING SCAM SENT TO CREW MEMBERS

**From:** [information@helpnorthlane.agency](mailto:information@helpnorthlane.agency)

**Date:** January 8, 2021 at 14:36:45 GMT-5

**To:** [hotmail.com](mailto:hotmail.com)

**Subject:** PAYROLL INFORMATION



**Greetings from Miami!**

We saw some activity trying to get into your account. we therefore freeze all your account activity. and we'll deactivate the card and make sure it's temporarily secure.

Until you contact us again to reactivate it, on the official Wirecard-Northlane website.

Enter here to confirm your account.

[Confirm account](#)

Is there something wrong with the link I attached?  
please reply if you can't access it.

We want to hear from you please reply to this email  
Stay safe & stay healthy!



- NEVER click on links that ask you to enter your account information!
- Beware of fake email North Lane addresses like:

**[information@helpnorthlane.agency](mailto:information@helpnorthlane.agency)**

## ACTUAL PHISHING SCAM SENT TO CREW MEMBERS

Αρχή προωθημένου μηνύματος:

Από: [servicesmember@northlane.help](mailto:servicesmember@northlane.help)

Ημερομηνία: 13 Ιανουαρίου 2021, 2:00:10 πμ EET

Προς: [servicesmember@hotmail.com](mailto:servicesmember@hotmail.com)

Θέμα: Security Notification



Your account has just logged in on a suspicious new [device](#). You're getting this email to make sure it's really you. immediately confirm if this is not you.

[Check activity](#)

**CONFIDENTIALITY NOTE:** *This message may contain confidential or legally privileged information. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or taking any action in reliance on these contents is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this e-mail and then delete it from your system.*

Mark Tamis,  
SVP, Hotel  
Operations

&

Greg Purdy,  
SVP, Marine  
Operations

©2020 Royal Caribbean International.  
Unsubscribe.



- Never click on suspicious links like these!
- Beware of fake North Lane email addresses like: [servicesmember@northlane.help](mailto:servicesmember@northlane.help)

## ACTUAL PHISHING SCAM SENT TO CREW MEMBERS

**From:** [cs\\_crewadministrator@salarysearchcl.com](mailto:cs_crewadministrator@salarysearchcl.com)  
**Date:** January 13, 2021 at 12:51:37 GMT-5  
**To:** [psid@northlane.com](mailto:psid@northlane.com), [spass@northlane.com](mailto:spass@northlane.com)  
**Subject:** This notification is to confirm our system in your account!

Good day, |

This notification is for confirm your latest account registration or changing your online account settings, the system or device that you are using will be automatically stored in our system. Please note you cannot log in if you have not changed your account settings.

Immediately confirm your account here [www.login.northlane.com](http://www.login.northlane.com)

Salary at sea card has now been blocked.

Please advised further procedures / action in retrieving my balance and activation of my salary at sea card.

Sincerely,  
North Lane

[login.northlane.com](http://login.northlane.com)



- NEVER click on fake North Lane links!
- Beware of fake shipboard email addresses like:  
**[cs\\_administrator@salarysearchcl.com](mailto:cs_administrator@salarysearchcl.com)**

# ACTUAL SCAM WIRECARD WEBSITE



**wirecard**

ACCESS AND MANAGE YOUR ACCOUNT

Username  Forgot Username  
Password  Forgot Password

Enter the card below

**Log In**

**Register Your Card**  
Register Your Card for online access

**In a hurry?**  
Click here to view your balance and transactions.

**Have a Payment Code?**  
Click here to activate your payment

ACCESS ANOTHER CARD

**NOTICE:** Citigroup Inc. has sold its prepaid card business to Wirecard AG. The trademarks "Citi", "Citibank", "Citigroup", the Blue Wave, and the Arc design and all similar trademarks and derivations thereof or other trademarks owned or used by Citigroup are used temporarily under license by Wirecard AG from Citigroup Inc. and related group entities.

**IMPORTANT:** Our Card Services Team will NEVER contact you by phone, email or text message for your card information, like your card number or PIN (if you have one) unless you contact us first. To protect yourself please do NOT provide your card information to anyone.

**Password Update Notice**  
Wirecard recommends resetting your password periodically to ensure an optimal level of security and decrease the opportunity for identity theft.

Please note that when you access your account online you may be required to provide additional verification as a secondary proof of your identity. This requirement protects your personal information from unauthorized access.



- **NEVER** click on suspicious links like these!
- **BEWARE** of fake email addresses like:  
[wirecardrccl<myrccl@wirecard.site.com](mailto:wirecardrccl<myrccl@wirecard.site.com)
- **BEWARE** of fake websites like:  
<http://www.a-citipaid-salaryatsea.online.site.com>



## C. HOW TO PROTECT YOURSELF

### Beware of phishing

- Don't open files, click on links, or enter credentials in suspicious emails.
- Opening suspicious files or clicking links could expose your system to a virus or spyware designed to steal your information or passwords.
- Forward suspicious emails to **abuse@rccl.com**.

### Always be alert

Never share personal information (usernames, passwords, security questions and answers) or financial information with anyone, including other crew members.

Scammers also create email accounts that are similar to those used by shipboard finance teams (Finance Controller, Payroll Purser, Crew Payroll Manager) to trick crew into thinking that a finance team member has emailed them.

Remember: Legitimate shipboard email addresses have the following domains:

- **@rccl.com**
- **@celebrity.com**
- **@azamara.com**

### Secure your devices/information

Keep your information secure/locked away where others (including cabin mates) cannot access it.

### Keep software current

- Use firewalls, anti-virus software, and anti-spyware software for your devices.
- Apply updates for operating systems and applications to ensure the latest security features.

### Practice password security

- Use strong passwords or passphrases and keep them private.
- Protect your accounts by using a combination of letters, numbers, and special characters for your passwords. More secure strategies encourage the use of passphrases or password vaults.
- Never share your passwords with anyone.
- Change your passwords regularly and don't use the same passwords for every account.
- Use multi-factor authentication for bank and email accounts.



### Stay safe on social media

Phishing is now occurring on social media sites like Facebook via friend requests. Be careful of the friend request you accept and never share personal or financial information via messages

Don't overshare on social media. Sharing personal information on Facebook, TikTok, etc. can give scammers information about you and your loved ones.

### Erase information on old gadgets

- When selling or giving away your old computer, laptop, or mobile device, make sure to factory-reset, delete, or destroy all personal information.
- This includes login names and passwords, bank-account details, passport and other ID details, etc.

### Protect your bank account.

- Go directly (don't click on links in emails) to your account to check if your balance is correct.
- Review all recent activity for unfamiliar or suspicious transactions or transfers.
- Check personal or contact information that has been

changed without your knowledge (i.e. email, username, bank info).

- Set up multi-factor authentication and monitor your account frequently to ensure that the activity is expected.

### Keep your Salary@Sea account safe

- NEVER click on any website links in emails that have been sent to you.
- NEVER use an internet search to locate the North Lane URL login address.
- ALWAYS use the North Lane web access (<https://login.Northlane.com/rccl>) or the North Lane app to access your account.
- AVOID public computers for logging into your account. NEVER click on "Save Password" if you are using a public computer, always remember to logout.
- NEVER share your password or PIN number with anyone.
- ALWAYS change your password regularly and immediately if you think your account might have been compromised.
- NEVER respond to a North Lane email unless you

requested specific information from the North Lane help email account. Go directly to your account if there is an issue.

Use the **North Lane app** to access your account; it is more secure than using the website. The app is available from the Google Play Store and Apple App Store.

(If you have the *Wirecard* app already installed, it will automatically update to the North Lane app).

Remember, if you receive a suspicious email and aren't sure if it's legitimate send it to **abuse@rccl.com**.

NEVER forward suspicious emails to anyone else in the company, only to ABUSE.

**For your reference, here are our LEGITIMATE NORTH LANE EMAIL ADDRESSES:**



- **Help@Northlane.com**
- **PremiumFX.Support@northlane.com**
- **Client.Services@northlane.com**
- **Fraud.Forms@northlane.com**

Any other addresses are scams and are not safe.

## **LEGITIMATE NORTH LANE WEBSITE:**

**<https://login.Northlane.com/rccl>**

Any other website address is a scam and is not safe.

While off the ship, any Salary@Sea related e-mails must be sent to **SalaryatSea@rccl.com**.

## **D. FILING A CLAIM**

Immediately notify customer service if you see unauthorized activity on your card or account or if you find anything suspicious.

We can block your card and a fraud claim can be submitted. Any delay in notifying us might cause you to lose money or become financially liable for some of all the transactions you claim.

1. Submit a fraud claim by contacting customer service via email or telephone: **Help@Northlane.com** or **1-866-326-8689**

You may also contact North Lane Technologies, Inc. directly at:

**1-866-326-8689** or  
**1-610-941-4607**

Send an email to  
**Help@Northlane.com**

Visit the website:  
**<https://login.Northlane.com>** or  
**<https://login.Northlane.com/rccl>**  
(from the ship)

**IMPORTANT:** Remember, delays in identifying unauthorized transactions in your account and filing your claim could result in financial liabilities. If this happens, you will be responsible for those charges, and a portion or all your claim will not be paid to you.

2. An investigator may contact you with additional questions regarding your case. Please provide complete details in your answers within the timeframe given so that your case remains open. Without the required information, we may not have enough to proceed with your claim and your case could be closed.

3. Most fraud investigations are completed within 45 days from receipt; however, it may take up to 90 days to finalize depending on the nature of the disputed charges. If a claim takes longer than 10 business days to reach a decision, a provisional credit will be issued to the account. Once concluded, cardholders will be notified via email about the decision on their claim.

In cases of denial, cardholders can request their claim be reopened via Customer Service by providing additional details that may change the decision. Please note that while all requests are reviewed, clean reopening is not guaranteed and may be denied.





## E. Block scam-related email addresses.

### In Gmail:

1. Log into your Gmail account.
2. Open the message from the sender you want to block.
3. On the right side, look for and select the **three dots** next to the reply icon.
4. Select **Block "senders name"**.
5. In the **Block this email address** window that comes up, you will be asked if you want to mark all future message from the sender to be marked as Spam. Click **Block** to confirm.

### In Hotmail or Outlook:

1. Log into your Hotmail or Outlook.com account.
2. Open the message from the sender you want to block.
3. Go to the Outlook Mail toolbar, click the **Sweep** button.
4. In the **Move To** box, select **Deleted Items**.
5. Select **OK**.

Outlook will remove all messages from that sender that are in the current folder.

**NOTE:** Emails in other folders, like Archive, won't be deleted.

Moving forward, emails from anyone on your blocked senders list will be sent to the Deleted Items folder.

### In Yahoo Mail:

1. Log into your Yahoo Mail account.
2. Copy the email address you want to block and paste it somewhere temporary – a sticky note or an unsaved document.
3. Go back to your email window. In the upper-right corner, select the **gear icon** to access Settings.
4. At the bottom part of the Settings pane, select **More Settings**.
5. On the left side, select the **Security and Privacy** category.
6. Next to where it says **Blocked Addresses**, select **Add**.
7. In the **Add an Email Address to Block** section, go to the **Address** text box.
8. Copy and paste the email address you want to block in the text box.
9. Select **Save**.

**Any email addresses you block will appear in the Blocked Addresses section.**