

## Contents

<b>Spam</b> .....	2
What is Spam?.....	2
Why Spam is Bad.....	2
Reduce Spam .....	2
Volcano Webmail Spam Filter.....	4
Dangers of Spam .....	9

## Spam

### What is Spam?

So exactly what is spam? A basic definition of spam is unsolicited bulk email, meaning emails sent without permission, addressed to many email accounts, sometimes in the millions. Although, if you have ever used email before, you know spam when you see it and don't need a techy sounding definition. To most people, any email trying to sell you products you don't want from people you don't know, or anything that you did not request receiving, is spam.

### Why Spam is Bad

Spam is no longer just an online nuisance. Today, instead of just being annoying emails trying to sell dubious products, spam has become an engine for criminality. Today's spam can trick you into going to a web site that pretends to be your bank, which could lead to your bank account being hacked, or identity theft. Spam can trick you into installing malicious software that can log what you enter in your keyboard, or even worse give someone complete access to your computer and all it contains. As a further insult spam can lead to your computer becoming a spam sending zombie, sending thousands of junk emails from your computer.

Malicious software or 'malware' is a category of programs that have some sort of malicious intent. Viruses, Trojans, worms, spyware, adware, and bots are all types of malware, and can be contained in spam emails.

We'll give you tips on how to reduce the amount of spam that you receive, and on how to recognize and avoid the dangers of spam.

### Reduce Spam

Even if the spam you receive does not contain malware and is just plain old spam, you still don't want it in your Inbox. Here are some steps you can take to reduce the amount of spam.

#### Keep your Volcano.net email address private

Give out your Volcano.net email address (or any address where you want to avoid spam) only to those you know and trust. Websites and services may require an email address to use whatever service is being provided. Avoid giving your address to register at websites unless you are confident they your address will be kept private.

Often websites that collect email addresses sell them off and then the addresses can get into the hands of spammers. Either only give your address to websites that state your email address will be kept private, or use a

#### Spam Tips

- Keep your Volcano.net email address private
- Choose a unique address
- Turn off Preview Pane or disable image viewing
- Don't open unexpected attachments
- Do not click on links in unsolicited emails
- Never respond to spam
- Don't click the Unsubscribe link in spam
- Never buy products advertised in spam
- Adjust anti-spam settings in client or webmail
- Use spam filter program

secondary email account. There are free email services from Yahoo, Hotmail, and Google to name a few where you can get a secondary email account. Use this address to register at websites you are unsure about.

## **Choose a unique email address**

Spammers use automated programs that generate email addresses with common names. If you use your first name or a common last name as your email address, you may get spam right off the bat. Although some people have found that they do not receive that much spam to their address which has a common name, using a unique address should help stop spam being sent to your account.

## **Never respond to spam or click the "Unsubscribe or Remove Me" link**

While it might seem tempting, clicking anything in a spam email is not a good idea. Clicking the unsubscribe link will only confirm to the spammer that a real person is at the end of your email address. Your address then becomes valuable to them and other spammers and you will get more spam.

## **Turn off the Preview Pane and disable viewing of images**

Most modern email clients will automatically disable images from email that may be dangerous and while useful, this is not foolproof. Turning off the "Preview Pane" will stop the content of emails from being displayed automatically, and possibly prevents the downloading of malicious code.

Disabling image viewing prevents a connection made from your computer to a server where that image is stored. When such an image is downloaded, the spammer then knows a person is viewing their spam.

## **Do not buy products advertised in spam**

Somebody is doing it...don't let it be you. Much of today's spam isn't so much a direct attempt to sell something, but instead a vehicle to invade. Even still, don't ever buy anything from anything that looks like spam.

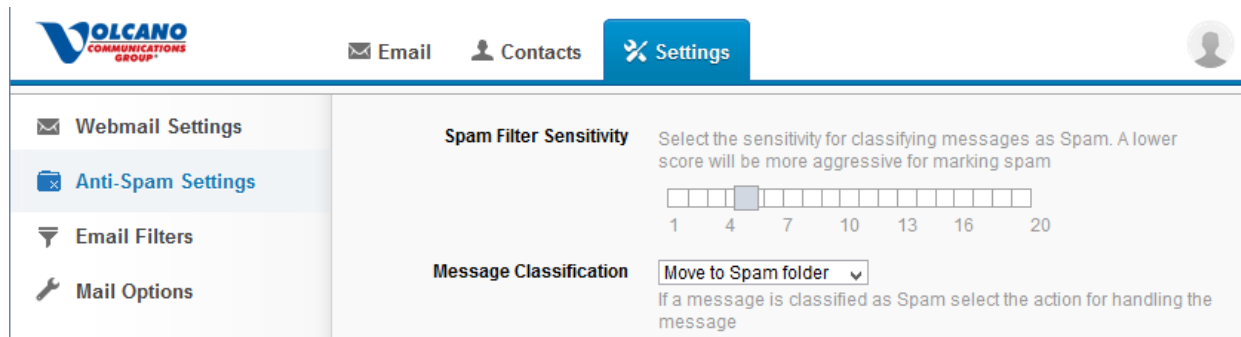
## **Spam Filter Settings**

You can adjust the spam or junk email filter in your email client and on Volcano Webmail to reduce the amount of spam getting to your inbox. Your email client may have junk email filters and controls that you can change to stop more spam. Check your email program to see what is available.

Security programs like firewall or anti-virus software sometimes have spam filters as well and there are many stand alone spam filter programs available for free or for purchase.

## Volcano Webmail Spam Filter

By logging into Volcano Webmail you have access to adjust the anti-spam controls for your account on the email server. By adjusting the sensitivity of the spam filter, you can stop spam before it gets to your computer.



### Spam Filter Sensitivity

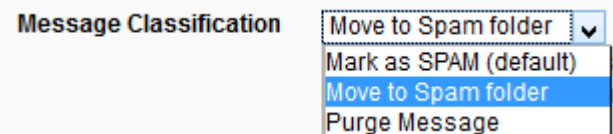
The Spam Filter Sensitivity is controlled with a slider bar that is numbered from 1 to 20. Simply, here's how it works. Lowering the value by moving the slider to the left, will block more emails. Raising the value by moving the slider to the right will allow more email to reach your inbox. This may seem backwards, so let's take a look how the setting works.

As email is scanned by the server spam engine, it is given points for having characteristics of spam, with more points being given for more obvious signs of spam. When the email is to be sent to your account, the total amount of points are compared against the number set on the Spam Filter Sensitivity bar. If the email has less points than the Spam Filter Sensitivity setting, the email is sent to your inbox. If the message has more points than the value set, it is sent to your Spam Folder.

If you find too many legitimate emails are being sent to the Spam folder, try raising the Spam Filter Sensitivity higher. False positives, in this case good emails being labeled as spam, can be just as frustrating as dealing with spam itself.

### Message Classification

This setting controls what happens to an email that is determined to be spam. The email can be Marked as Spam with a label in the Subject and sent to your inbox. Or it can be sent directly to the Spam folder by selecting Move to Spam folder. The Purge Message setting will automatically delete spam, but this may also lead to a legitimate email being deleted. Use this setting with caution.



### Spam Filter Sensitivity

- Lower value will block more email from reaching your inbox. Normal email may be tagged as spam.
- Higher value will allow more email to your inbox. Spam may be sent to your inbox.

## Spam Tag

Email determined to be spam will have the text in the Spam Tag box will appear in the message subject. This will help you easily identify spam, and you can change the text to whatever you would like.

Spam Tag

{SPAM}

If a message is marked as Spam rewrite the header to include the following text.

## Whitelist/Blacklist Senders

To always allow email from specific senders to be delivered to your inbox, enter that email address in the Whitelist sender box. To allow all email from a specific domain, like gmail.com or yahoo.com, enter the domain in the Whitelist senders. To always block email for a specific sender or domain, enter that address or domain in the Blacklist sender list.

Here some examples of whitelisted and blacklisted email addresses and domains. When entering a domain, just type the domain name, without the @ symbol.

Whitelist senders

someone@abc.com  
gmail.com  
yahoo.com

Specify a list of email addresses and domains to whitelist. Each entry must be on its own line. Any email or domain that matches will automatically be flagged as trusted without being classified as Spam.

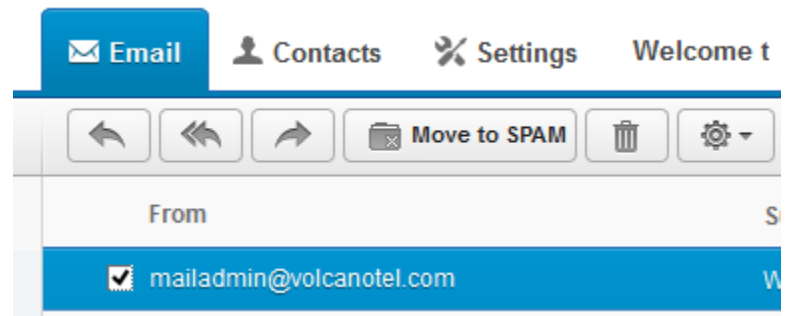
Blacklist senders

badguy@spamsender.com  
spamsender.com

Specify a list of email addresses and domains to blacklist. Each entry must be on its own line. Any email or domain that matches will automatically be classified as Spam.

## Move to SPAM

You can easily move messages that make it to your inbox to the Spam folder a few different ways. While in the Inbox, select the message by checking the box to the left of the message, then the Move to SPAM button becomes active. Then just click that button to move that email to the Spam folder. You can also

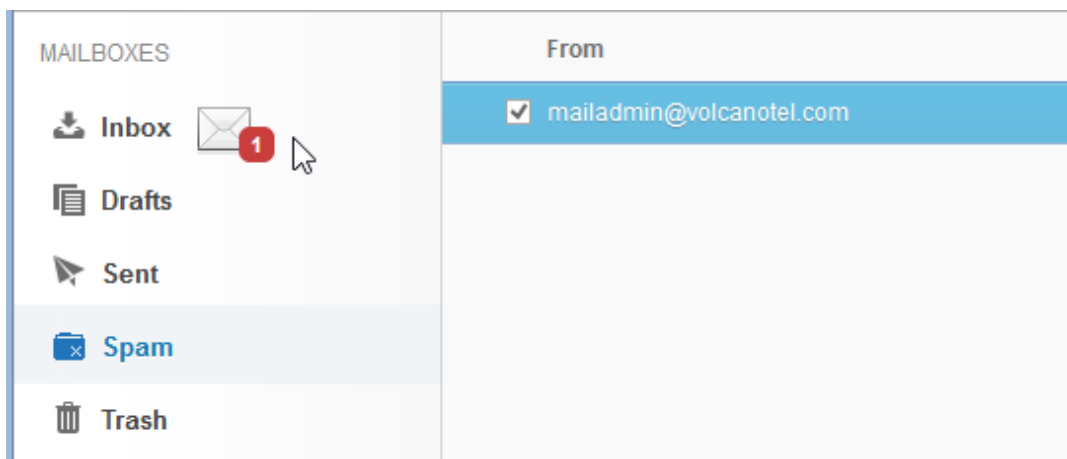


open the message and click the Move to SPAM button, or just click and drag the message to the Spam folder.

Not only will this move the email to the Spam folder, an entry in your blacklist will be created so that this sender's email will always go to the Spam folder. We'll have more on this Autopopulate Blacklist/Whitelist feature a little later.

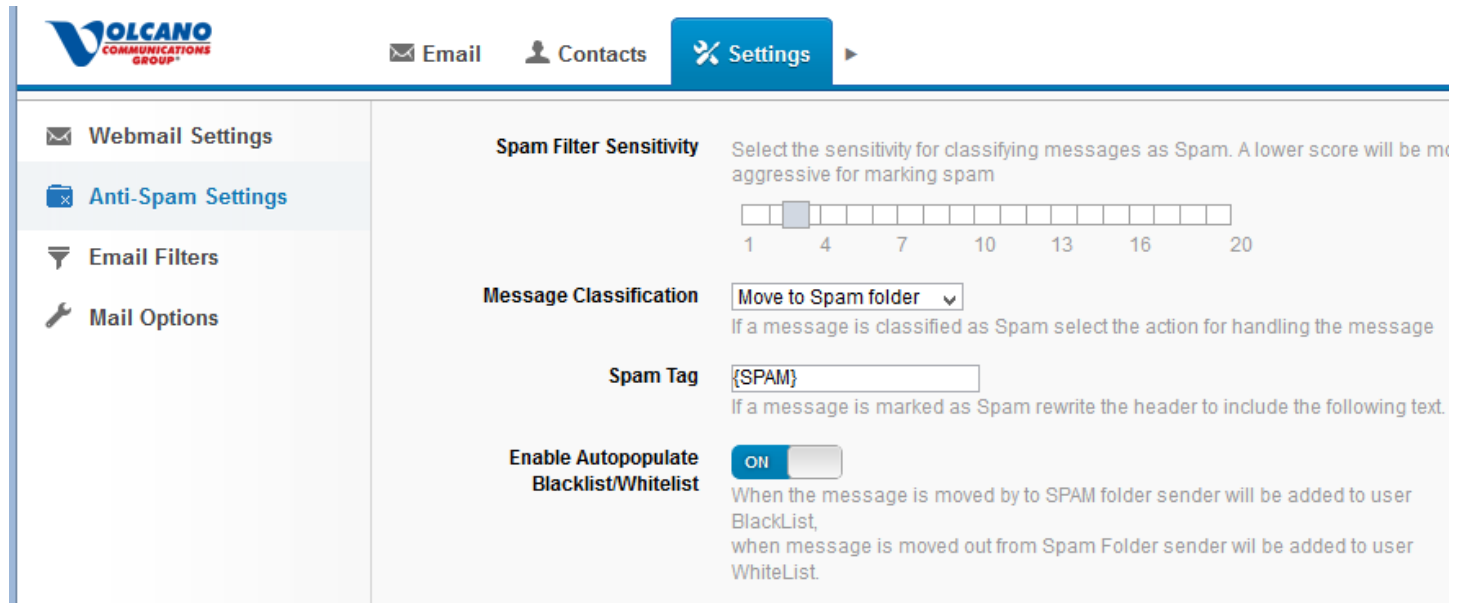
## But it's Not Spam

If a normal legitimate email has made it to the Spam folder, you can simply drag that message from the Spam folder to the Inbox. This will create an entry in the whitelist so that email from this sender will always go to your Inbox. This is also a function of the Autopopulate Blacklist/Whitelist feature.



## Enable Autopopulate Blacklist/Whitelist

With the Enable Autopopulate Blacklist/Whitelist turned on, senders of email that has been moved to the Spam folder will be automatically added to the blacklist. Senders of email that is moved from the Spam folder to the Inbox will be added to your whitelist. This setting is enabled by default and you get to this setting by clicking the Settings tab, then Anti-Spam Settings.



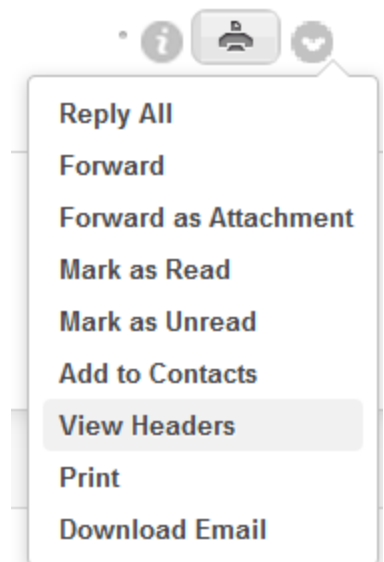
The screenshot shows the webmail interface with the 'Settings' tab selected. The left sidebar contains 'Webmail Settings', 'Anti-Spam Settings' (highlighted), 'Email Filters', and 'Mail Options'. The main content area shows the following settings:

- Spam Filter Sensitivity:** A slider set to 4. Description: "Select the sensitivity for classifying messages as Spam. A lower score will be more aggressive for marking spam." Scale: 1, 4, 7, 10, 13, 16, 20.
- Message Classification:** A dropdown menu set to "Move to Spam folder". Description: "If a message is classified as Spam select the action for handling the message."
- Spam Tag:** A text input field containing "{SPAM}". Description: "If a message is marked as Spam rewrite the header to include the following text."
- Enable Autopopulate Blacklist/Whitelist:** A toggle switch set to "ON". Description: "When the message is moved by to SPAM folder sender will be added to user BlackList, when message is moved out from Spam Folder sender will be added to user WhiteList."

## Sender Check – Email Header

If you are not sure if an email was sent from where it claims, you can quickly check the "header" and see what the original destination was.

While in the Inbox with a message selected, click the down arrow icon and select "View Headers"



The screenshot shows a context menu for an email with the following options:

- Reply All
- Forward
- Forward as Attachment
- Mark as Read
- Mark as Unread
- Add to Contacts
- View Headers** (highlighted)
- Print
- Download Email

This will expand the top section of the email to show some technical details. Without the header information this email would show that the sender in the From line is American Airlines. However, by looking at the Return-path, the Received, and From lines in the header you can see where the email really was sent from. This will help you figure out if an email is really spam.

```
Return-path <custsupport@millerplumbingheatingandair.com>
Envelope-to [redacted]@volcano.net
Received from [12.7.106.115] (helo=millerplumbingheatingandair.com) by vipmail.volcano.net with sm
Message-id <002b01cfdde59a57ddcc9101a8c0@SAMTERM>
From "American Airlines" <custsupport@millerplumbingheatingandair.com>
To [redacted]@volcano.net
Subject Please download your ticket #NR00731728
Date Wed, 01 Oct 2014 21:07:22 -0500
Mime-version 1.0
Content-type multipart/mixed; boundary="-----_NextPart_000_0026_01CFDDBB.B1810800"
X-priority 3
X-msmail-
priority Normal
X-mailer XimianEvolution1.4.6
X-mimeole Produced By XimianEvolution1.4.6
```

## Newsletters

If you have subscribed to a legitimate newsletter with your volcano.net email address, but no longer wish to receive those emails, go ahead and unsubscribe to the list. Then you would not need to add that address to the blacklist. Be careful to make sure that the newsletter is legitimate and will honor your unsubscribe request.



## Dangers of Spam

Spam can look like it is from a friend, with an attachment about something interesting. Curiosity may get the best of you and once that attachment is open, you now have a virus that encrypts your files and demands payment to unencrypt the files. Now you have two bad choices...pay the ransom (but really don't ever do this), or lose your files. This is just one possible scenario of many equally bad scenarios. It really does happen.

These types of attacks are normally accomplished by what is called social engineering, tricking people by claiming to be a known contact, or a familiar or otherwise legitimate organization or company, thereby gaining an amount of initial trust and then using that trust to infiltrate a computer system. A social engineering technique called phishing is used by spammers to get users to either download malware or to visit a compromised website. Phishing is something that you should be on alert for when dealing with spam or email in general.

## Don't Get Phished

Your judgment and action are the best ways to protect yourself from the effects of spam. While spam can be filtered at the server and at your computer, spammers are continually adjusting their methods to get around filters. Unfortunately some spam will get to your inbox and this is where you will have to be on the lookout for phishing attempts. Here are some things to keep in mind to avoid becoming a phishing victim.

## Never open an attachment that you are not expecting

Even if it's from Mom. If the sender is someone you do know, get a hold of them and ask if they meant to send the attachment. Email with a From address of someone you know could still be spam and contain a virus or other type of malicious software.

Some other spam may look like it's coming from legitimate places like Visa or maybe your bank, alerting you that your account information must be updated by completing the attached form. Attachments are often sent with emails to entice a user to install a malicious software. This is one of the more common ways computers are infected with malware. You can see why phishing was chosen as the name of this technique.

### Dangers of Spam

- Viruses, worms, bots
- Loss of privacy
- Loss of data
- Computer becoming a spam sending zombie
- Files held by ransom
- Stolen passwords leading to hacked accounts

### Email Safety Tips

- Never open an attachment that you are not expecting
- Never click on a link in an email you are not expecting

## Never click on a link in an email you are not expecting

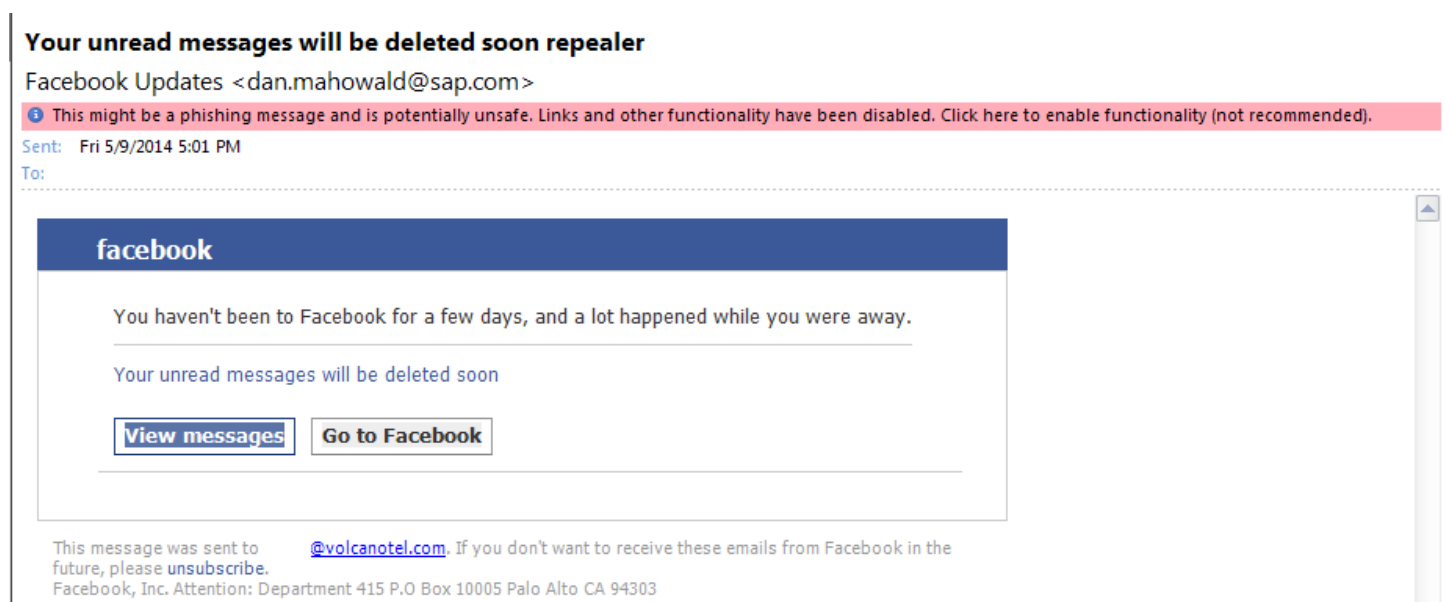
This rule is a little harder to follow because some types of spam look very real. Spam pretending to be from your bank, Facebook, or other web sites that may actually use, can lure you with a delivery notification, friend request or other type of normal interaction. The email will have official logos and look just fine, but when you click on link you are taken not to the real site, but to a web site that can steal your personal information. Take a look at some examples.

## What Phishing Looks Like

Here's an email that looks to be from Facebook, but taking a closer look will reveal this to be fake.

Some email programs have built-in phishing detection. Here Microsoft Outlook has determined this email to be a phishing attempt and is alerting with a red highlighted message. Some email programs may not have messages like this, or sometimes we don't really head alerts, so let's look at something else about the email.

## Message detected as a phishing attempt by email program



**Your unread messages will be deleted soon repealer**  
Facebook Updates <dan.mahowald@sap.com>

**This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).**

Sent: Fri 5/9/2014 5:01 PM  
To:

**facebook**

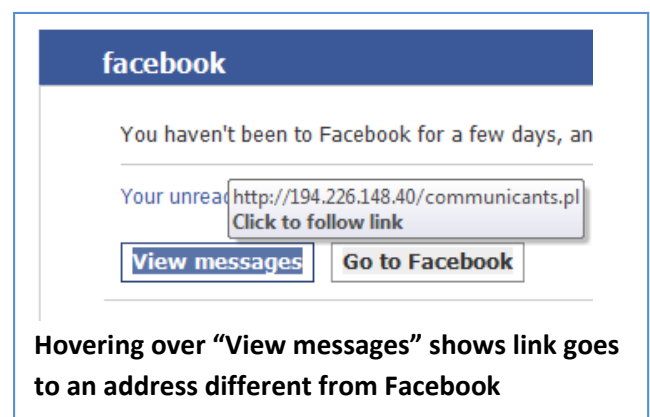
You haven't been to Facebook for a few days, and a lot happened while you were away.

Your unread messages will be deleted soon

[View messages](#) [Go to Facebook](#)

This message was sent to [@volcanotel.com](mailto:dan.mahowald@sap.com). If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).  
Facebook, Inc. Attention: Department 415 P.O. Box 10005 Palo Alto CA 94303

When placing the cursor on a hyperlink (either text or an image), most email programs will display the actual URL that you be directed to if you click the link. On this email the "View messages" link shows a URL that is something different from what is expected. Here the URL is <http://194.226.148.40/communicants.pl>, an address that does not at all look like Facebook. Clicking on the link will take you to this address where your computer may be infected with malware.



**facebook**

You haven't been to Facebook for a few days, an

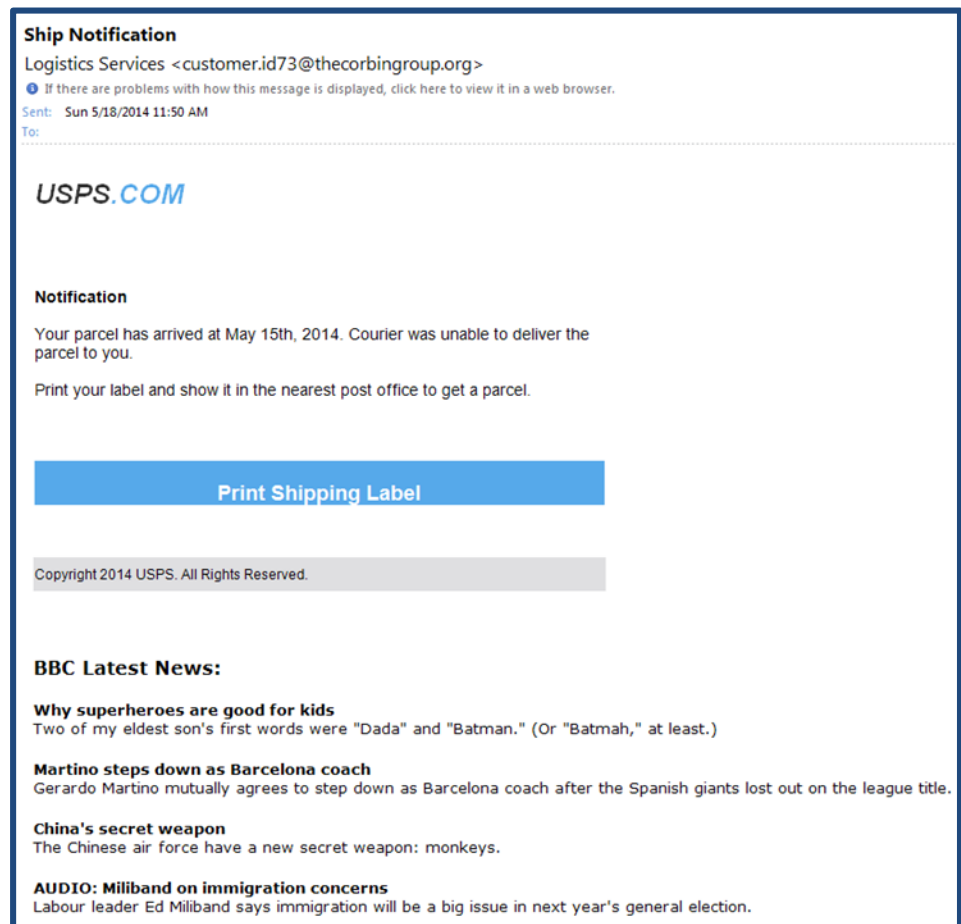
Your unread messages will be deleted soon

[View messages](#) [Go to Facebook](#)

Hovering over "View messages" shows link goes to an address different from Facebook

This email claiming to be from the USPS was not detected by Outlook as a phishing attempt, but that is indeed what this is. The spammer behind this one included some news headlines to try to legitimize the email, but this should be red flag also. Why are BBC news headlines in an email from the USPS?

**Phishing attempt – notice the BBC headlines and the senders address are not related to printing a USPS shipping label**



Placing the cursor over the "Print Shipping Label" section shows the URL to be a Russian domain (.ru), which obviously does not have anything to do with the United States Postal Service, and exposes this email as illegitimate.

These types of emails are very common, but by taking a few seconds to notice some details you can avoid opening files or clicking links that may cause problems on your computer and compromise your privacy.

