A Guide to Fighting and Identifying Spam

This guide will provide you with the means to improve the spam filter by giving you options for reporting spam. This guide will also arm you with some tips you can use to identify spam in your inbox.

Reporting Spam

If you get spam or other suspicious emails in your inbox, there are two actions you can take.

- **Forward the email** – You can forward your spam email message by right-clicking on the email, choosing Forward and then sending it to our spam account for analysis. The email address to send to is spambox@roselleschools.org
- **Mark as Spam** – You can also mark the email as spam. This will help our spam filter to learn what items should be sent to junk mail. To do this, right-click on the email and choose Actions -> Mark -> Spam. This will flag the message as spam.

Following these options will help us to ensure that spam does not reach your inbox.

Reporting False Positives

One of the biggest challenges when dealing with spam is minimizing false positives. There are lots of hallmarks that can help you to identify spam but often a legitimate email will possess many of those same hallmarks. As such, we are constantly working to ensure our spam settings block as much spam as possible while also not flagging legitimate email as spam.

If you run into any email in your junk mail folder that should not be there, you can also mark it as not spam. This helps the spam filter to identify legitimate emails that could otherwise be treated as spam. To do this, right-click on the email and choose Actions -> Mark -> Not Spam.

Tips for Identifying Spam

This section is intended to give you some ideas of things to watch out for when you are looking at emails in your inbox. While these tips will certainly help you to identify spam, the important thing is to remember to always be cautious when dealing with email, particularly when you receive anything unexpected.

- **Be wary of unsolicited emails from companies** – A lot of spam will claim to be coming from a major company such as a bank, telephone company, internet retailer or big box store. These sorts of companies will generally not email you unless you have asked them to do so (by signing up for a newsletter, placing a password reset request, etc)
- **Be wary of unsolicited emails from individuals you don't know** – Generally random strangers will not send you real emails. Be especially wary if they claim to have some amazing money making opportunity or to have always been secretly interested in you or anything along those lines.

- **Watch out for emails that are selling a product** – Unless you have signed up to be notified when a store is having a sale, you usually will not be emailed opportunities to purchase products from legitimate business. These emails that claim to offer a top-brand product (whether purporting to be from a major company or not) are almost always spam
- **Real businesses will never ask for account information via email** – Your bank will never email you to tell you that you need to log in to your account to reset your password or that your account is locked. The same is true for E-Bay, Amazon, Facebook and most other companies.
- **Never give out personal information in response to an unsolicited email** – You should never enter your social insurance number, credit number or other personal details in response to an unsolicited email.
- **Check the URL** – If you do see an email that you think might actually be from your bank or another institution you trust, hover your mouse over the hyperlink, this will bring up the actual URL at the bottom of the page. Make sure that the URL is pointing to the exact site you expect. Not an IP address (like 123.123.123.123), not realcompanyname.somerandomsite.com, not realcompanyname.unexpecteddomain (like amazon.in or something like that). If the URL does not appear when you hover over the message then the user has probably taken steps to hide the URL. A legitimate business is very unlikely to do that.
- **You will never win a prize via email** – Unless you have entered in to some local raffle or amateur contest, you will never win a prize where you are notified via email. This is especially true for big lotto winnings and contests you didn't even know you had entered.
- **Watch out for unexpected attachments** – If you get an email that you weren't expecting that contains an attachment, be very suspicious. Often spam emails will purport to contain a PDF or a JPG that they want you to open, but if you don't trust the source you should never do this. Even if you do trust the source, if you weren't expecting this email, be wary and make sure the attachment is what it says it is. A spam message could claim to be from someone you know when it's actually from a spammer**.** If they send you a JPG file, be sure it's actually a JPG before you open it and not file.jpg.exe or something like that.
- **Be skeptical** – Whenever you are dealing with email, there is the possibility of a spam message. So you should always be skeptical of anything being sent to you via email particularly if it urges you to take some action that requires opening an attachment or going to a specific website.