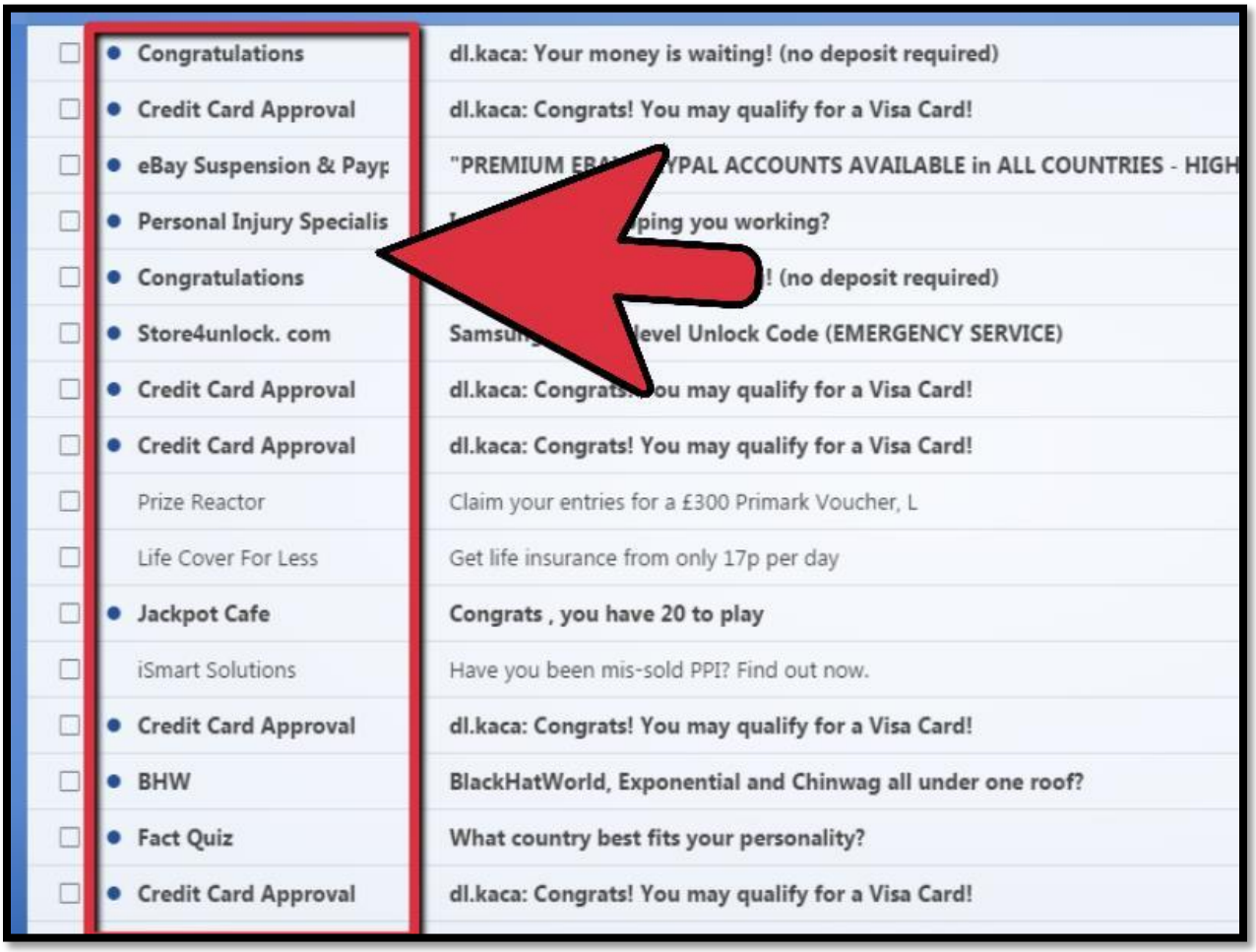
How to avoid email SPAM

Introduction

Many people unknowingly open themselves up to receiving unsolicited junk emails by their own actions. Helpful information from Canada's Anti-Spam Legislation: http://fightspam.gc.ca

The guide below will provide some tips on how to avoid spam.

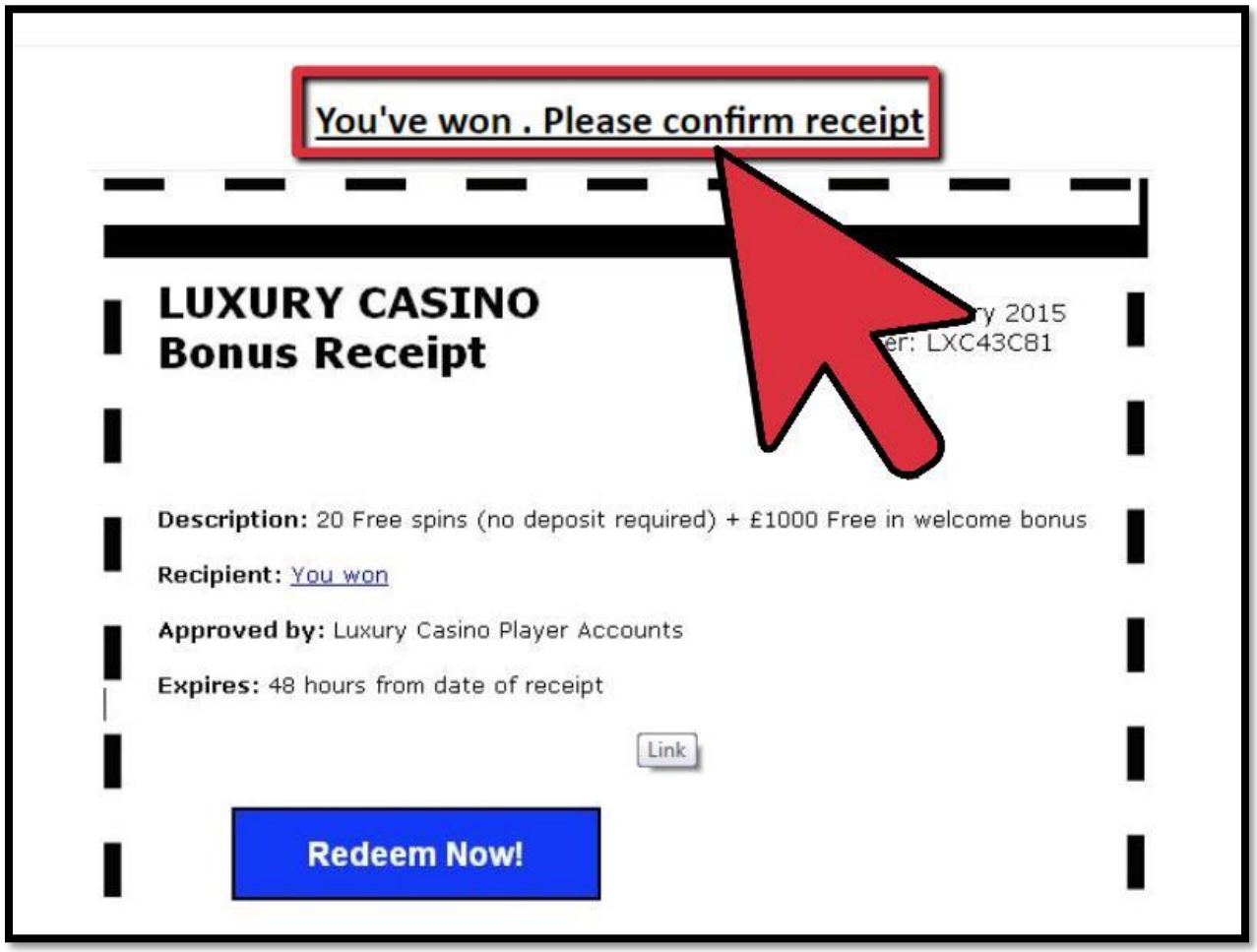
1 - **Check who it's from.** Spam will almost always come from an unrecognized sender, often with odd email addresses. That doesn't mean that all unrecognized email is spam. Legitimate newsletters, website administration emails (password resets, authentication requests, etc.), and more may come from addresses you don't recognize.



2 - **Be careful who you give your email to**. Many websites will ask you for your email address to sign up. Before freely providing this information you should locate and review the sites privacy policy. If they don't explicitly state that your personal information will not be shared, you should avoid giving your address. Most reputable sites don't share your email address and personal information.

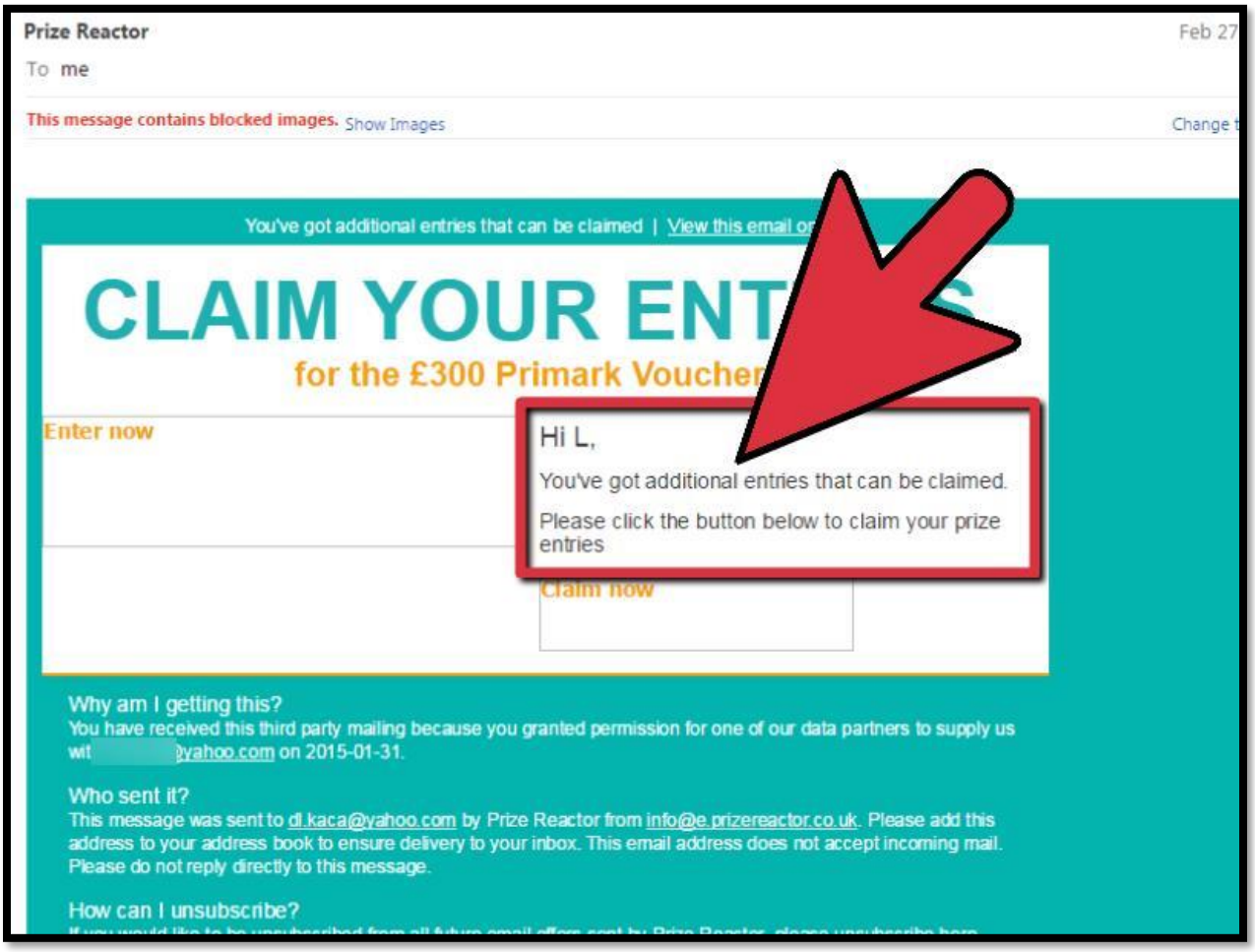
3 - Personal Websites. If you have a personal website, do not publish your work or personal email on it. Spammers use scanners that harvest such emails as well. Use free email services for this purpose.

4 - Look for links. Only click links from trusted senders. The entire purpose of spam is to get you to click a link. If an email contains a link and you don't recognize the sender, chances are it is spam. Hover your mouse over any link to see the destination in your browser or email client's status bar.

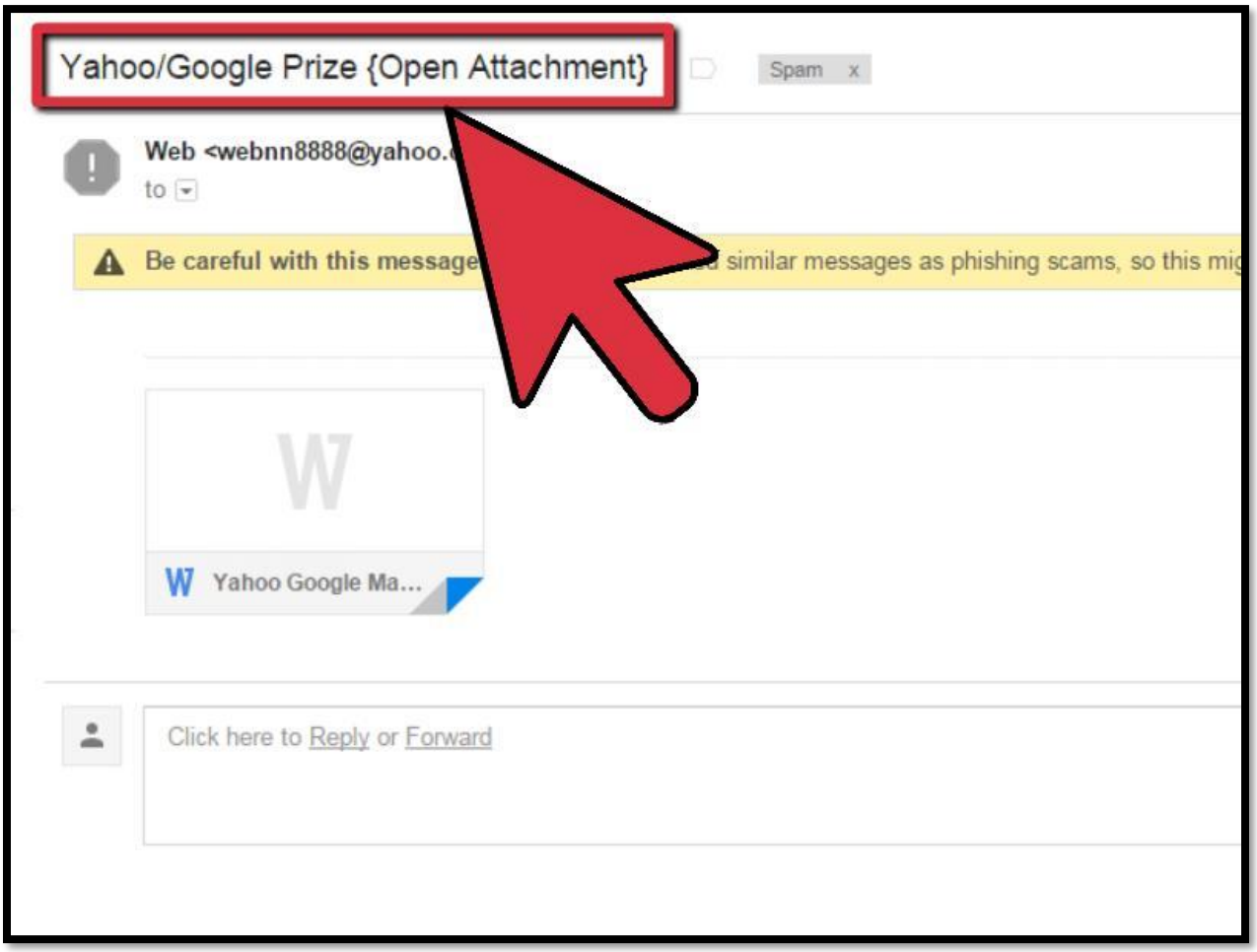


5 - **Don't use out of office replies to external messages**. If possible do not send out of office replies outside of your company, any spam you receive will get a reply letting them know that there is a valid email address on their list, *yours*. They will sell it. If you must allow external out of office messages, don't give information such as cell phone numbers or other people's email addresses as spammers will record this information. You are better off giving your company's main number and having your receptionist route calls while you are out.

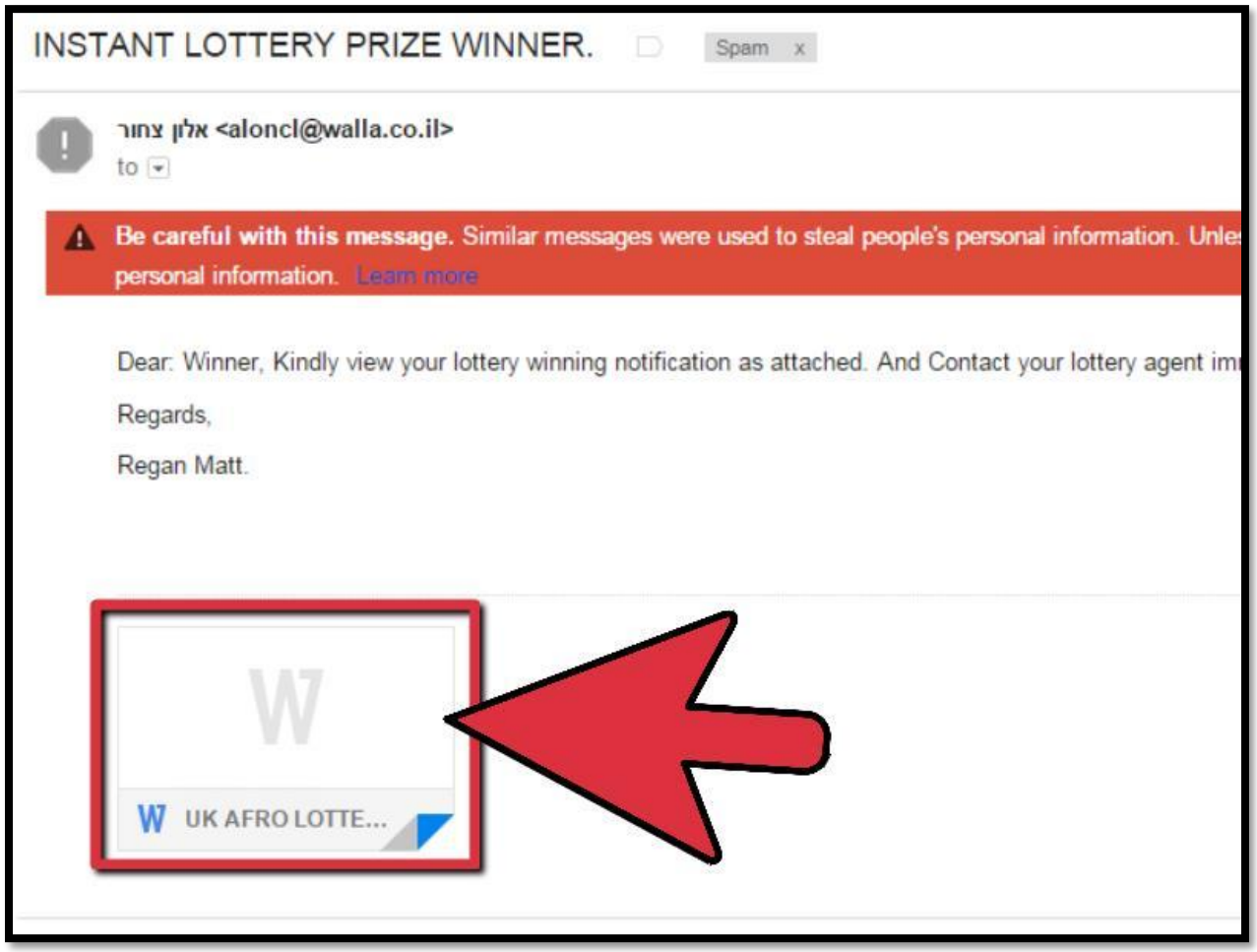
6 - **Check the spelling**. Spam often contains misspellings and oddly-worded sentences. This can include bizarre capitalization and weird punctuation. Many have gibberish at the end of the message.



7 - **Read the message.** Anything that claims you are a winner for a contest you never entered, offers you access to unclaimed money, or promises free electronics or pills is never legitimate. Any message that asks for your password is never real (all legitimate websites have automated password reset programs). Requests from strangers should always be ignored. Many email services have a preview window, which will allow you to read an email message without opening it.

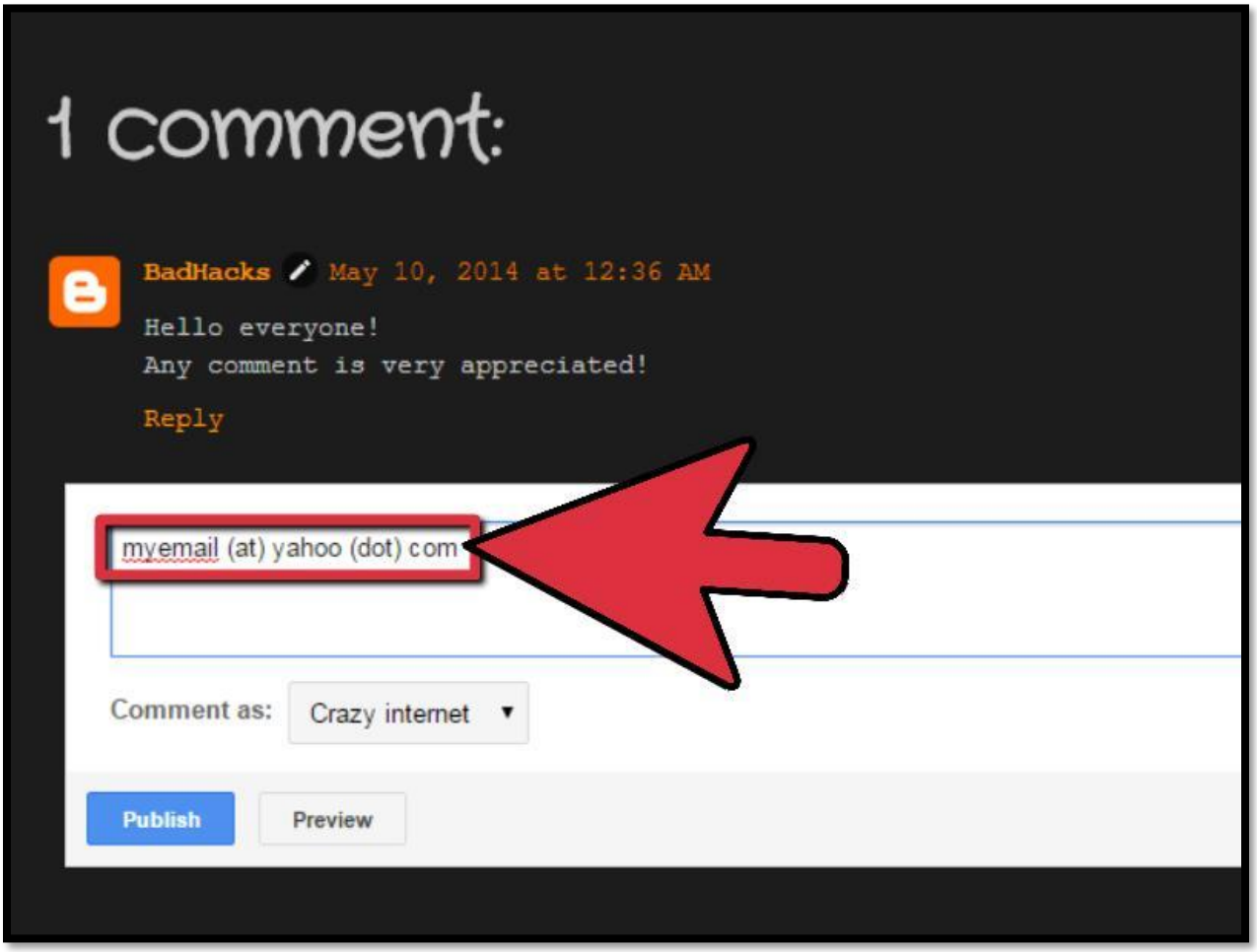


8 - **Look for attachments.** Malware and viruses are often disguised as email attachments. Never download an attachment from a sender that you do not trust or were not expecting.

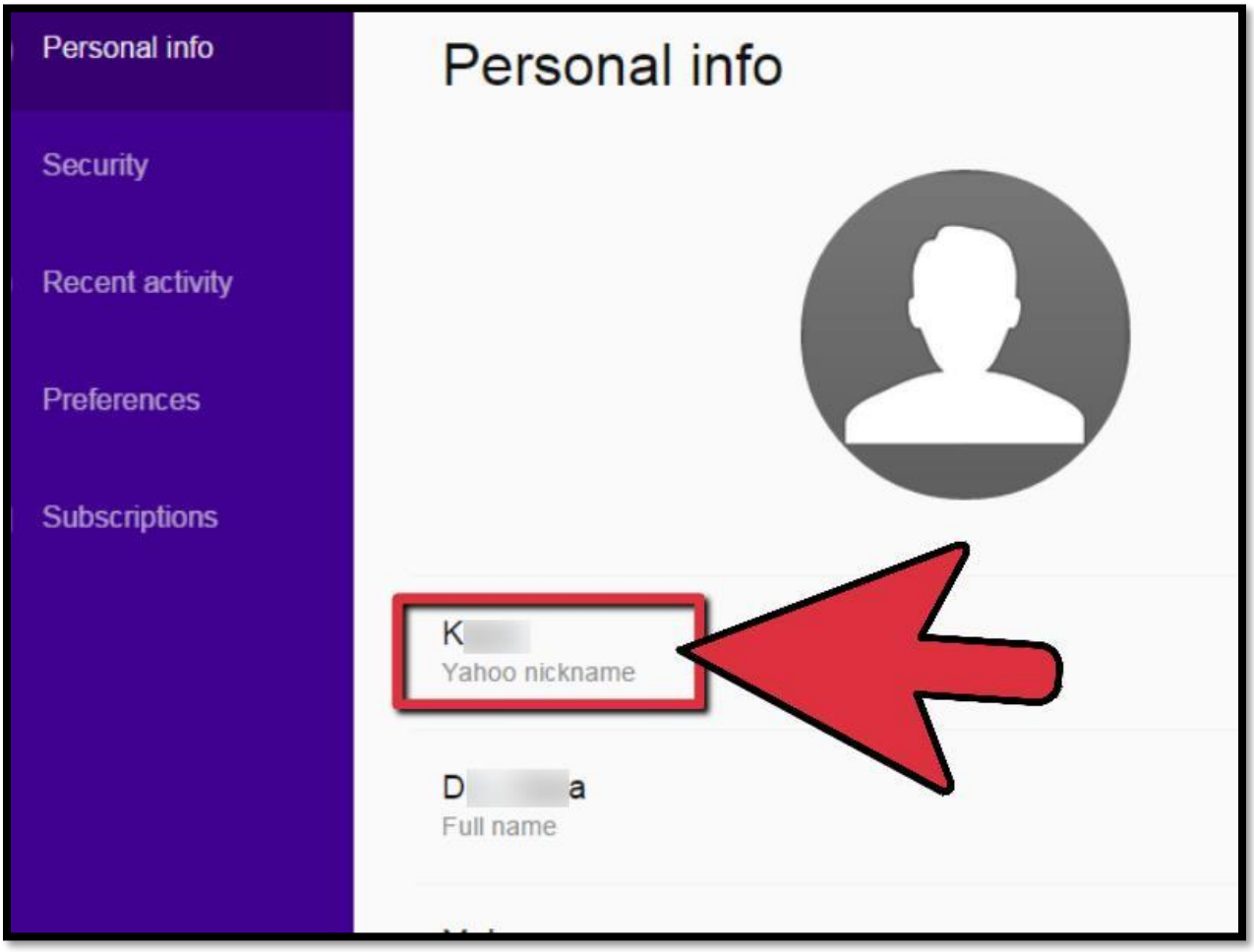


9 - **Don't give out your email address online.** "Robots" (scripts created to scrape websites for addresses) can quickly gather thousands of emails at a time from websites where the email addresses are made public. Also, sometimes humans actually grab e-mails off websites to use them for sign-up offers in order to get free stuff (iPods, Ringtones, Televisions, etc.).

10 - **Make your email address unscannable.** If you must provide contact information, try writing it out in creative ways (me [at] yahoo [dot] com). There are alternative ways of displaying your e-mail address while making it hard for spambots to harvest it. Such methods include using image picture of your e-mail address or using JavaScript to dynamically construct the display of your email.



11 - **Don't make your username the same as your email address.** Usernames are almost always public, and it's simply a matter of figuring out the correct service to add at the end. Services such as Yahoo! Chat make this even easier, since chances are everyone using it has a @yahoo.com email address. Avoid using a chatroom that is tied to your email address.

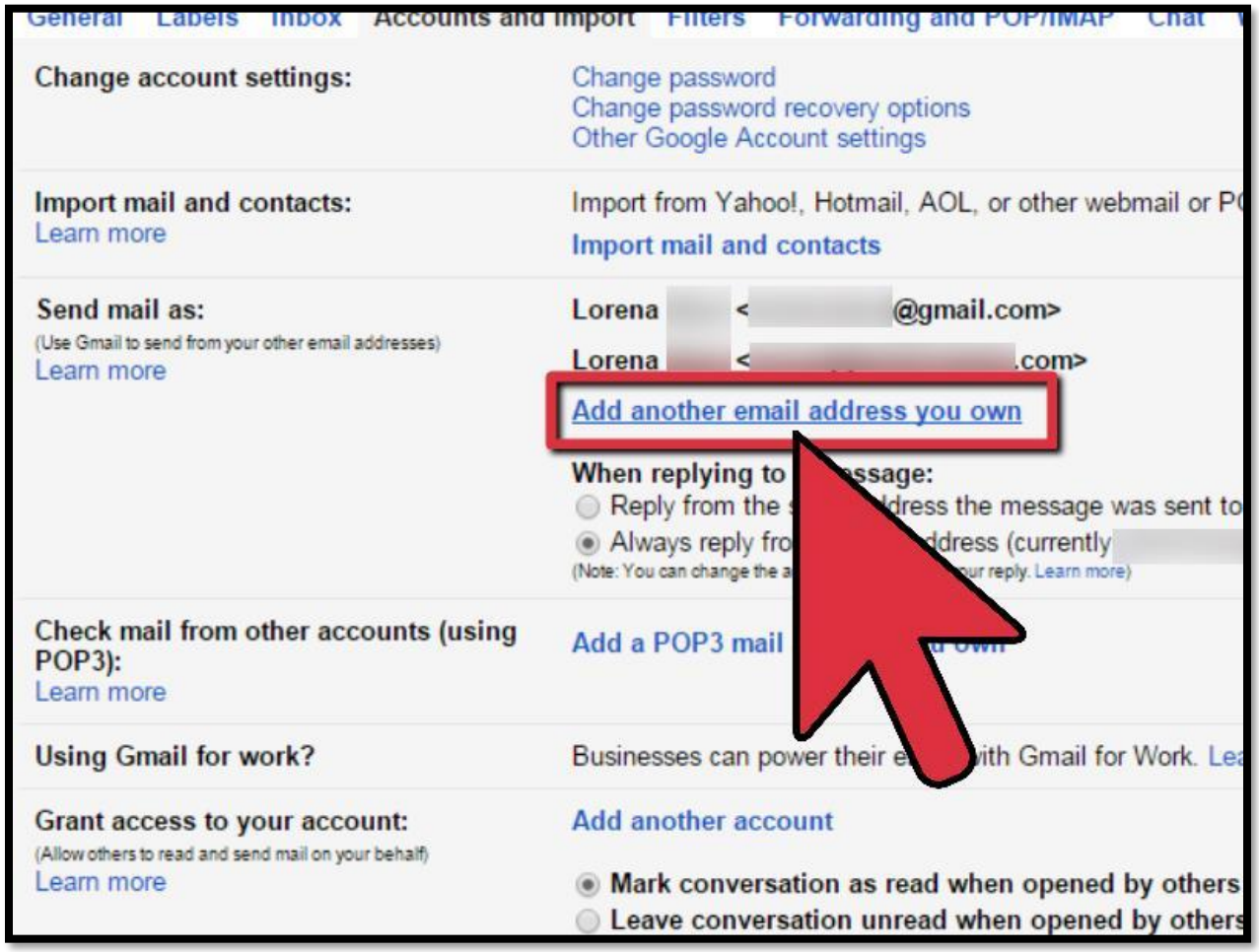


12 - **Use disposable email addresses to identify and shake off sources of spam.** Have one main account, and then make a separate account for different purposes (one for friends, one for entertainment sites, one for your financial websites, etc.).

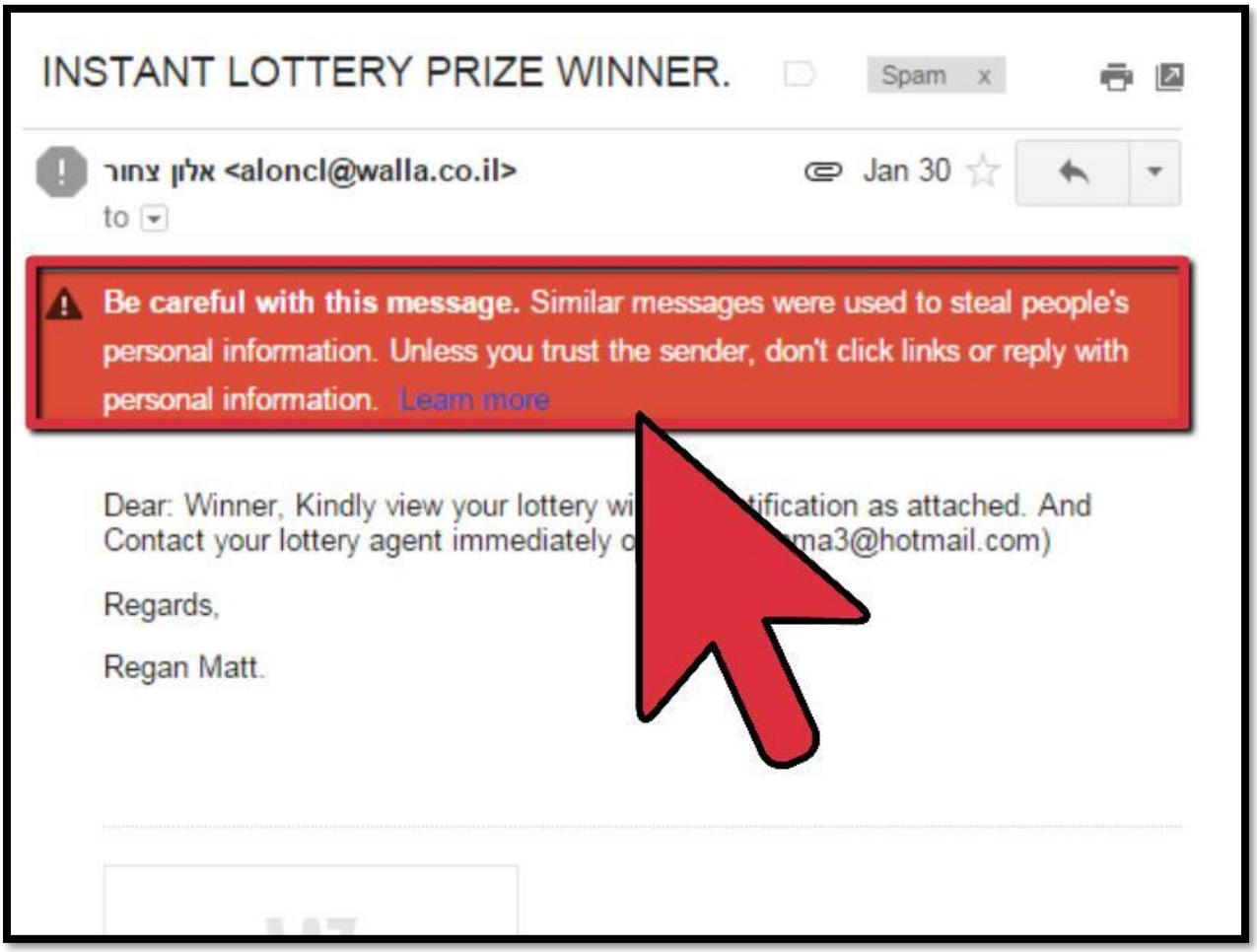
In Gmail, you can add a "+" button to your email address. For example, you can sign up for newsletters with JohnDoe+Newsletters@gmail.com if your email address is JohnDoe@gmail.com

Set all those addresses to <u>forward the mail to your main account</u> so that you do not have to check multiple accounts.

If you start receiving spam through one of your alternates, you can trace it to one of your disposable addresses and simply delete that account.



13 - **Never respond to spam.** Replying or clicking the “Unsubscribe” link will only generate more spam, because they now know that the email address is valid. It is best to report and delete the spam using the steps in the section below.

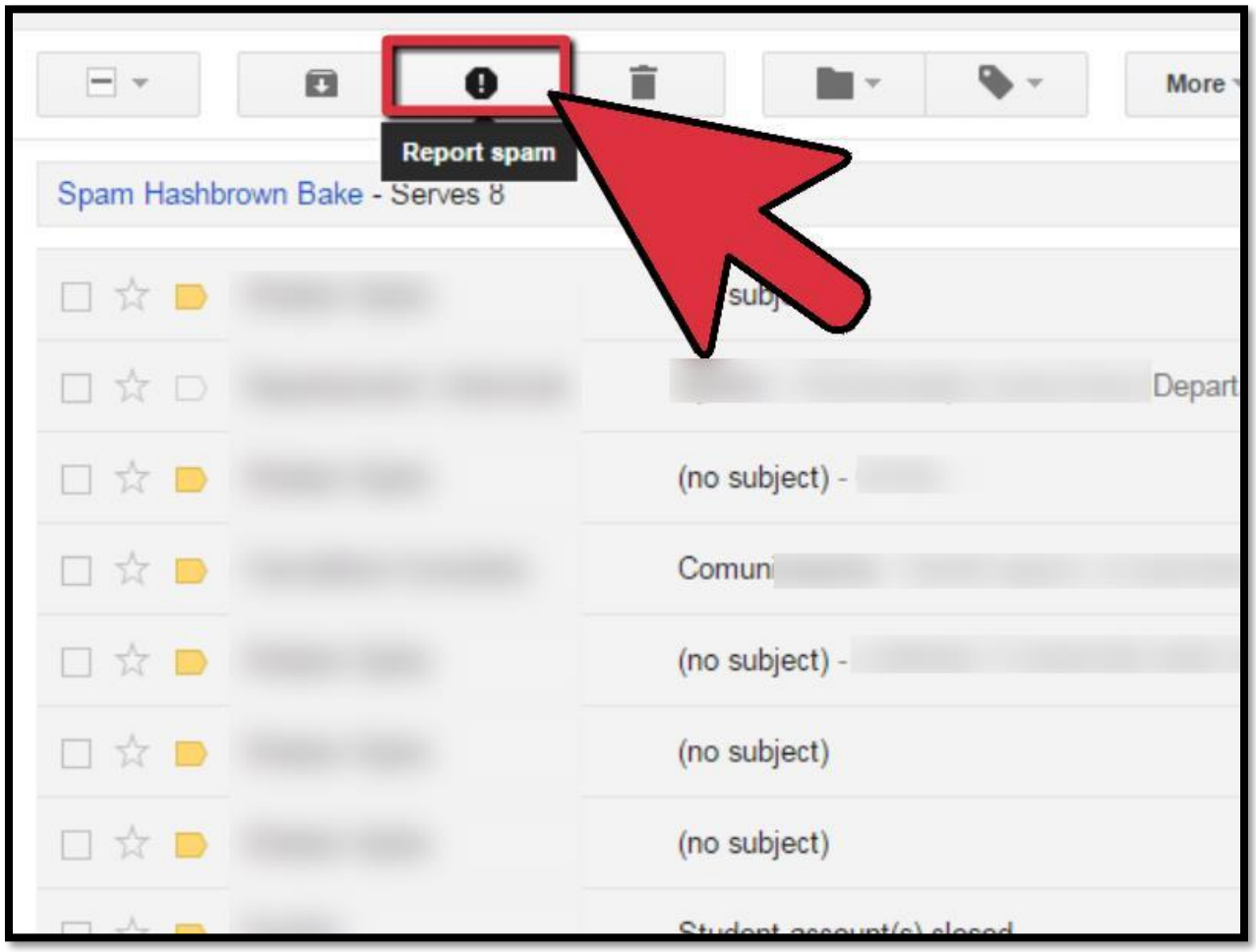


14 - **Block and report spam in Gmail.** Most spam is automatically detected and placed in your Spam folder, where it will be deleted after 30 days. If you receive a message in your inbox that you believe is spam, check the box next to it and click the "Report Spam" button in the top toolbar.

If you do this accidentally, you can click the Undo link at the top of the page to recover it.

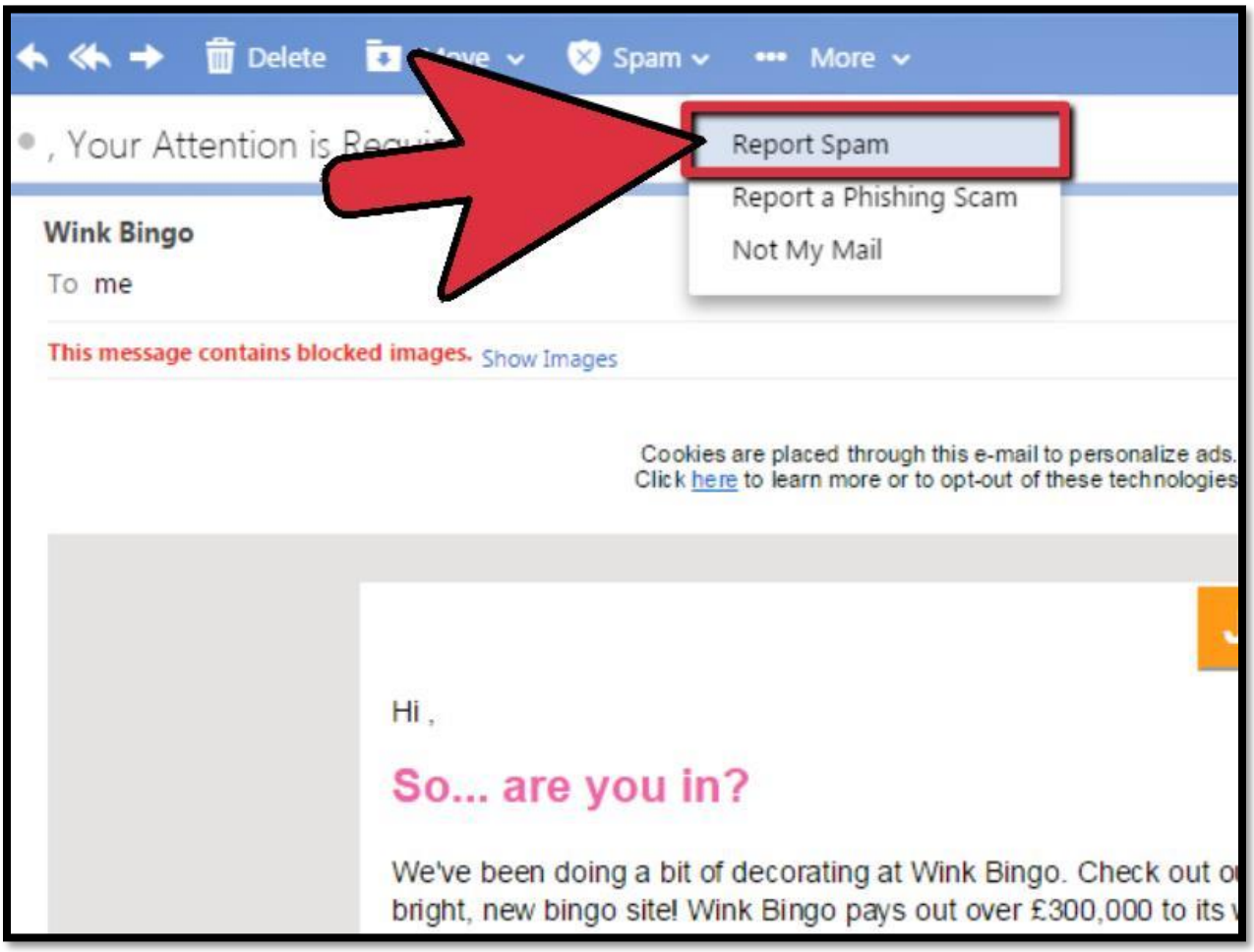
As you report messages as spam, Gmail will improve its automatic filtering.

If there is a message in your Spam folder that is a legitimate email, check it and click the "Not spam" button. Ensure that it is truly a legitimate email before doing this.



15 - **Block and report spam in Yahoo! Mail**. Yahoo! has a strong spam filter and most spam messages will automatically be sent to the Spam folder. If you find a message in your inbox that you believe is spam, check the box next to it and click the "Spam" button in the upper toolbar.

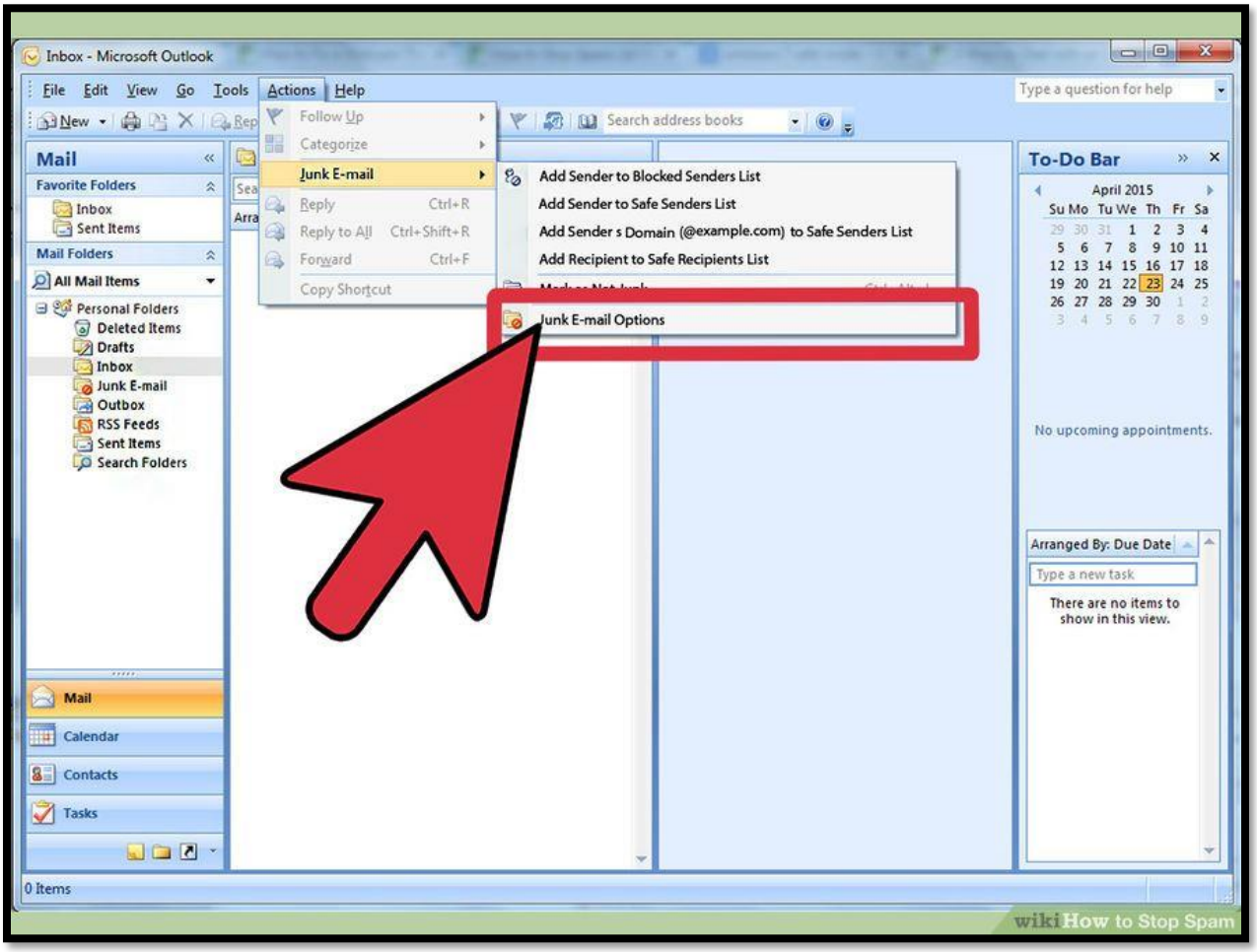
You can add senders and domains to your Blocked list, but this may only be a minor help, as spam senders often change addresses or use temporary domains.



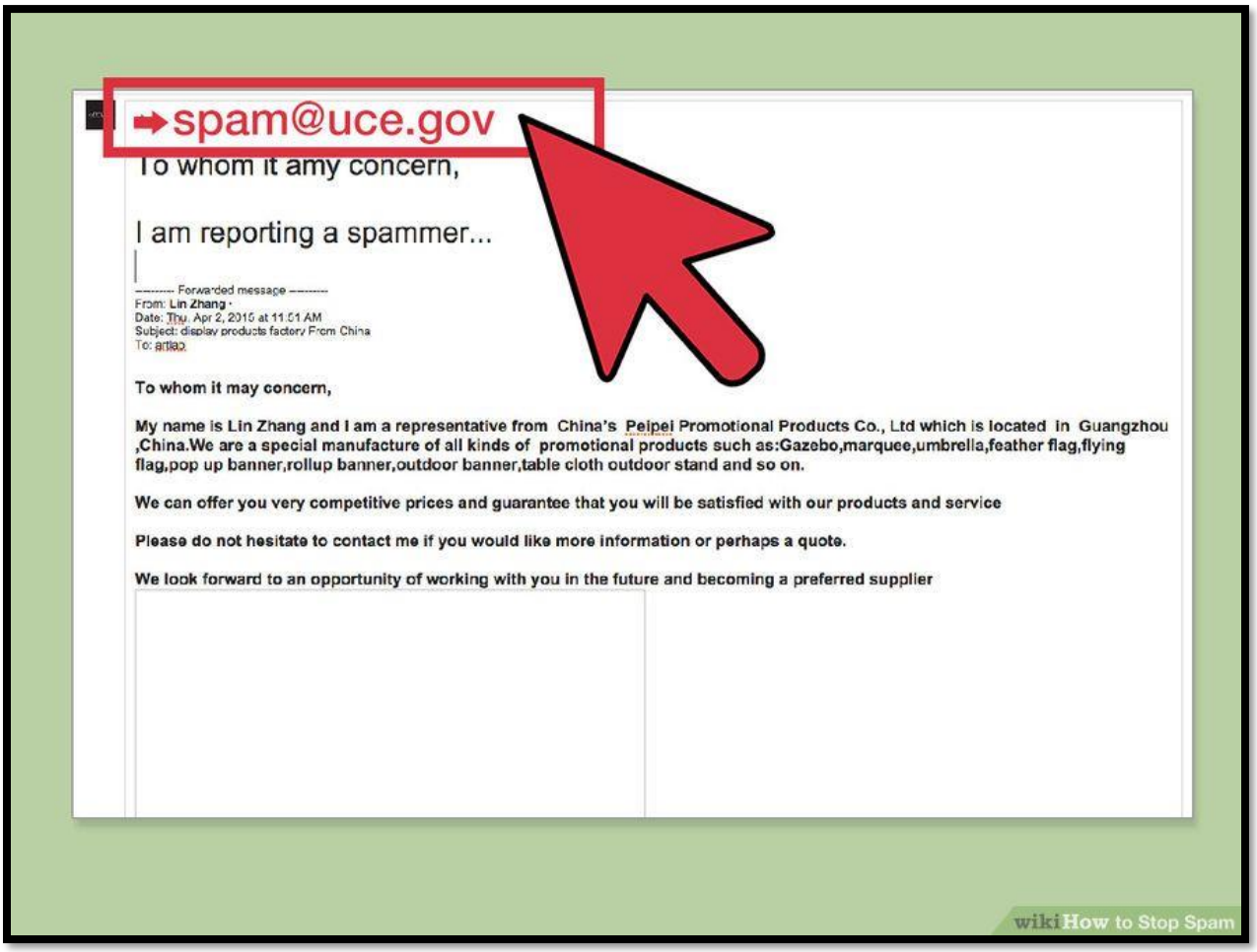
16 - **Block spam in Outlook.** Outlook comes installed with a Junk Filter which is set to Low protection. This will catch most obvious spam and direct it to the Junk folder. You can increase the strength of the filter by clicking the Home tab and then clicking Junk. Select “Junk E-mail Options”. Click the Options tab and set the filter to the strength you want.[4]

Each level of filter strength is explained. Setting it to High may move legitimate emails to your Junk folder, so be sure to check it periodically.

Install a third-party spam blocker. There are a variety of third-party spam filters that can be installed into Outlook. These will provide extra filtering and updated anti-spam information. Popular add-ons include DesktopOne, SpamAid, and Spam Reader



17 - **Report spam**. Before you delete your spam, forward your spam to: spam@uce.gov. This is the Spam box for FTC (Federal Trade Commission). Mail sent to this box is investigated. If it is indeed spam, the original sender can be charged $500 per email. The more mail they get from different users but same spammer, the more it's likely to be investigated. You can report spam to anti-spam organizations such as SpamCop and KnujOn, who will report spammers to ISPs and government agencies.



Conclusion

These tips are mostly common sense, but many people don't think about them. Spam has become a constant fixture in our online lives. While it's easy to gloss over spam in your inbox, accidentally clicking a spam link can lead to virus infection and identity theft. Take the fight to the spammers by actively blocking the spam that you receive, as well as preventing future spam. Your inbox will thank you.