10 scam tricks via email

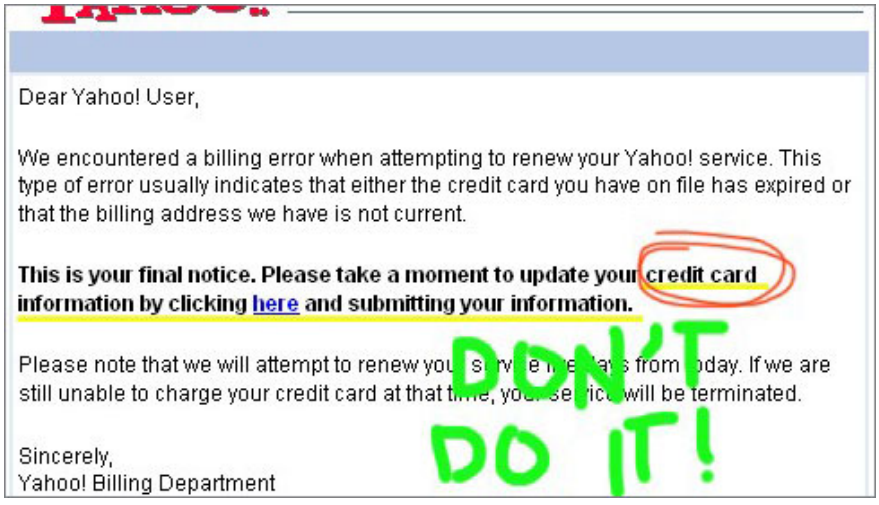
Too many emails sent daily can make even the most cautious people reduce the level of potential 'risk' in emails.

Too many emails sent daily can make even the most cautious people reduce the level of potential 'risk' in emails.

In a hurry to keep up with the progress of your work, it is easy to get into the trap of email scammers. Here are 10 of the most common signs in email scams.

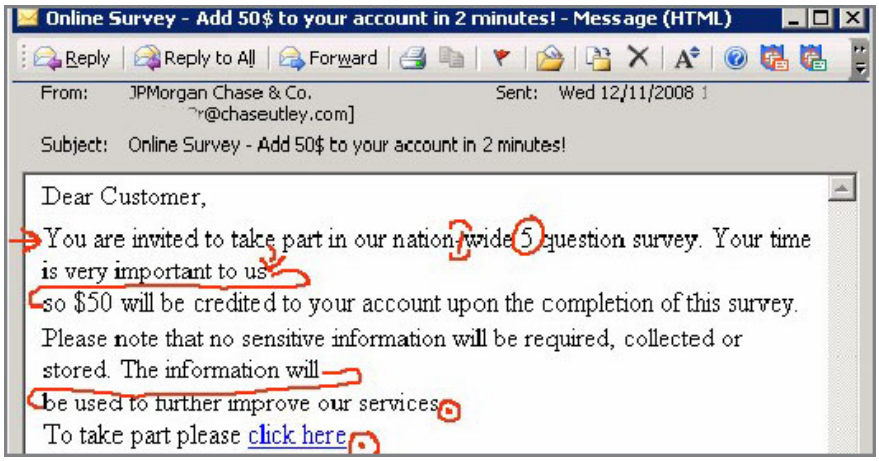
1. Request to provide personal information

No organization requires you to provide a bank account or PIN via email, they also do not include a link or a form form that requires you to enter data into it. Regardless of how formal the email looks, ignore them.



2. Look at grammatical or spelling errors

Phishing experts are clever people, but many people don't have basic grammar knowledge, especially emails sent from non-English speaking countries. Look at errors such as an inappropriate hyphen or confusion between ' *your* ' and ' *you're* '. If the email has many misspellings, the probability that the message is not that of mainstream organizations is very high.

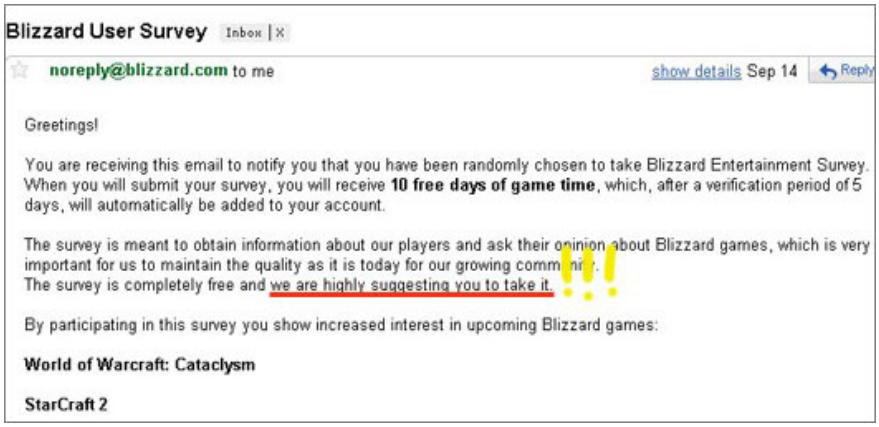


3. Attach the link in the email

Don't trust the links in emails, even though it may look like a trusted web address. These links often connect to the third site, which may look very orthodox but actually managed by scammers.

4. Research or survey requires personal information

Sending fake email marketing letters is a classic scam. You will be invited to participate in the survey or contest, and be asked to enter personal information. Once you do that, scammers can use that information for bad purposes.



5. Tips for " *hot* " stocks

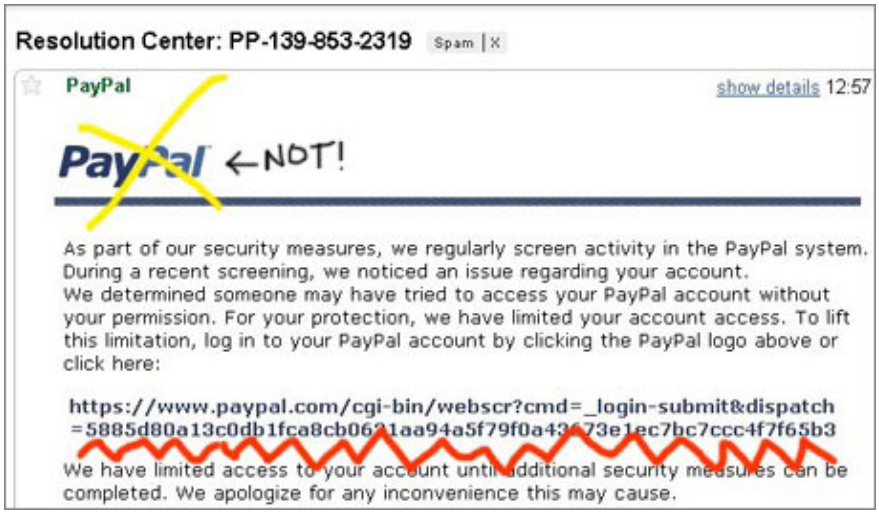
You get information about ' *hot* ' stocks, will the price increase even increase 2-3 times in a short time? It was a rumor to inflate stock prices. The person who sent the information owned the stock of some company. He spread rumors about that stock to increase stock prices to make a profit.

6. Email attachments from people you don't know

This is a common advice you may have heard thousands of times: Don't open email attachments from people you don't know, whether it's from your credit card or your bank. Because of the risk of infection with viruses and software stealing information from spyware when opening these files is very high.

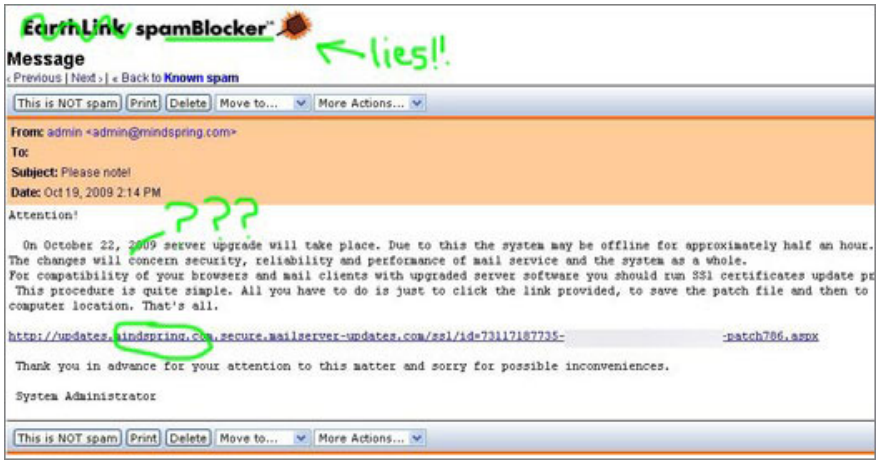
7. Unsigned emails

Some e-mails do not have words, only images are very dangerous. Clicking on any area in that email can lead to a website to lure you to log in personal information or become infected with spyware.



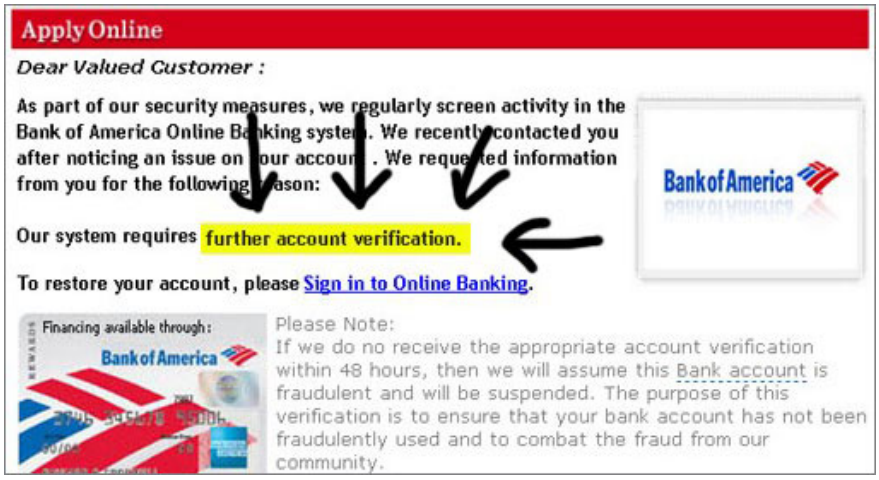
8. Information missing updates

Some scammers like to act as customer or technical support from a company you know but don't update new information. For example (as in the picture), the sender forgot that Earthlink (Internet service provider) bought Mindspring in 2000.



9. Information section highlighted

If you receive an email with bold text asking you to ' *confirm your account information* ', ' *you have won the lottery* ', or ' *if you do not respond in xx now, your account will be closed* '. Those emails are deceptive. Please click the delete button first without reviewing again.



10. General greetings

The emails starting with " *Dear member* " or " *Hello friend* " can be ignored. Because if the bank or credit card company sends, they will know who you are. Email to friends, too.