Troubleshooting Spam and Phishing Emails

All email, including internal email, is subject to spam filtering. However, this does not mean that spam and phishing emails never make it to your inbox. Inspect all emails carefully before opening them, and never click on links or attachments from unknown or suspicious senders. The information below describes what to do should you receive a spam or phishing email.

Related articles:

- Printing Troubleshooting
- Troubleshooting Mediasite
- Troubleshooting Respondus Exam Author
- How to Email Your Class for Faculty
- How to Forward an Email as an Attachment

Problem

I am receiving spam or phishing email.

Solution 1: Follow Best Practices

To lessen the amount of received spam mail, you should:

1. Be careful where you give out your email.
2. Do not open any links or attachments on spam emails.
3. Be careful when giving out your email for "Special Offers" and raffles. Email addresses given in this way are commonly compiled and sold to other vendors.
4. Select the spam email and have it directed to your Junk Mail folder.See this article from Microsoft on using the Junk Email filter in Outlook.

To safeguard your information, you should:

1. Learn to recognize what phishing email and links look like. See this article from Microsoft for an example of a phishing scam in an email message.
2. If you see a link in a suspicious email message, don't click on it.
3. Learn to recognize and report email scams. See this blog post from Information Security on how to protect yourself from phishing email scams.

Solution 2: Report Spam

Spam is any kind of email that you don't want and that you didn't sign up to receive. Spam is annoying but most is harmless,

1. Forward the spam email as an attachment to junk@office365.microsoft.com and InformationSecurity@missouristate.edu.
   See How to Forward an Email as an Attachment.

Solution 3: Report Phishing

Phishing email messages are designed to steal money or for gaining access to personal information such as banking and accounts and passwords. Cybercriminals do this by installing malicious software on your computer to steal personal information, or tricking you to give this information to them by posing as a legitimate company.

1. Forward the phishing email as an attachment to phish@office365.microsoft.com and InformationSecurity@missouristate.edu..
   See How to Forward an Email as an Attachment.

Solution 4: Report a Spam or Junk Email as False Positive

If a legitimate message ends up in your Junk Email folder, you may wish to report this as a false positive.

1. Forward the mail as an attachment to not_junk@office365.microsoft.com.
   See How to Forward an Email as an Attachment.