



Update from Rose.Net

Helpful information about

Spoof email Viruses Spam

Dear Rose.Net Users:

Over the last few weeks, we have seen a dramatic increase in spam and virus laden email being sent to our customers. As a part of our on-going customer service efforts, we would like to provide you with some information to help protect you and your computer from this annoying and crippling problem.

Rose.Net deploys virus software that screens email for viruses and catches

literally thousands of virus infected emails daily. When we detect a virus in an email, the email is deleted before it ever reaches your Inbox. While sometimes viruses are included in email attachments, other viruses are transmitted via a link contained in the email. If you click on the link in these types of emails, the virus will be downloaded to your computer. Many of our customers have reported receiving emails like this which appear to be from Rose.Net administrators advising the customers that their accounts are about to be disabled. The emails, which look legitimate, ask you to click on a link or enter personal account information to prevent this from occurring. These emails are NOT from Rose.Net but are hoax emails. Clicking on the link may launch a virus that will disable your computer.

We would like to assure you that Rose.Net will never ask for account passwords, personal account information, credit card information, or other sensitive data via an email. Please read the information below to learn more about spoof emails and how you can protect yourself from this growing problem.

Are you sick of receiving unwanted emails? Are you concerned about the types of email your children may receive? Spam or junk email is becoming an increasing problem for Internet users.

Spam a growing problem for Rose.Net users, so we are now offering a FREE email filtering service which allows you to screen your email before it ever hits your Inbox, helping you to limit the amount of spam you receive. The filtering service allows you, the user, to choose just how much or how little spam you receive by choosing the level of spam filtering you desire. You can also set up a "Whitelist" system so that you only receive email from the people you choose. While no filtering service can completely eliminate spam, Rose.Net's new spam filter will give you the tools you need to take control of your Inbox.

What is "spoof email?"

Spoof emails are hoax emails you receive that appear to be from Rose.Net, or some other well-known, legitimate company, asking you to reply with account information such as your password, or personal information, such as your credit card number, social security number, or bank account number.

The emails are known as "spoof emails" because they fake the appearance of a legitimate company in order to commit identity theft or infect your computer with a virus. Unfortunately, this practice is occurring more and more frequently. An example of a spoof or hoax email is shown below. Note the request to click on the link to prevent your account from being disabled. **NEVER respond to an email like this that appears as if it came from Rose.Net.** If it were ever necessary to disable your account because your computer had a virus, we would contact you by phone, not via email. We will never request your password in an email. This same principle applies not only to your Rose.Net email, but to all email you receive. We recommend that you NOT respond to email requests for any personal information and that you NOT open attachments or click on links unless you can verify the sender.



Example of 'spoof' email. Note that the body of the email is not personalized, and the link is displayed improperly. Clicking on this email will cause a virus to be installed on your computer.

Learn to identify the signs of a spoof email.

There are some warning signs to help you identify a spoof email. Look for the following:

1. **Account Status Threat:** Many spoof emails try to deceive you by threatening that your email will be disabled or your account will be closed unless you respond immediately to the email.
2. **Urgency:** Spoof emails often use urgency as a ploy, i.e., you must respond immediately to prevent your account from being shut down.
3. **Sender's Email Address:** Spoof emails use what appears to be a legitimate email address in the "From" field. Some may actually be real email addresses that have been forged.
4. **Email Greeting:** Most spoof emails have a general greeting such as Attention Rose.Net user.
5. **Requests Personal Information:** Requests for personal information such as Social Security number, User ID, account password, or bank account information are a clear indication that the email is a spoof. **AS NOTED, ROSE.NET WILL NEVER ASK FOR THIS TYPE OF INFORMATION IN AN EMAIL.**
6. **Links in the Email:** Spoof emails often contain links which appear to be legitimate. Remember that links can be forged.

Email Fact: The "From" field of an email can be altered. It may not have been sent by the name shown in the "From" field

What can I do to protect myself from spoof emails and viruses?

1. Your best defense is a good offense. Email viruses are proliferating throughout the Internet, and present a huge problem for both Rose.Net as your ISP and you as the user. As noted, we deploy virus protection software, but you should deploy virus detection software as well. Because so many new viruses are created and released, make sure your virus software is updated regularly. (Most virus software can be set to automatically update.)
2. Be cautious with emails that contain attachments or links. Do not open attachments or click on links unless you can validate the sender.
3. We recommend that you not respond to emails requesting personal or credit information. Unless encrypted, email is not secure, and you put yourself at risk by sending this type of information via email.
4. Know the signs of spoof email and screen your email carefully.
5. Disable the Message Preview Pane in Outlook and Outlook Express.

When in doubt, contact Rose.Net Technical Support at 229-227-7086 for assistance.