

E-mail Account and Password Safety

Each Road Runner subscriber has five e-mail addresses available to them. This includes the primary e-mail address provided upon installation of your services. It is important to keep passwords associated with your e-mail addresses private. If someone were to obtain your primary e-mail address and password, they could potentially create an e-mail subaccount, or secondary account, and use it to send out large volumes of unsolicited e-mail (spam) and/or other inappropriate messages via the Road Runner Web mail program. Such e-mail would appear to come from an address associated with your Road Runner account even if you did not send them.

All Web mail accounts, not just Road Runner accounts, are subject to this type of compromise. We believe it is important to inform you about such risks and provide you with guidance on what to look for and how to react should suspicious activity occur with your Road Runner e-mail account.

Simple steps you should take include:

- Visit <http://help.rr.com/>
- Click the “Account Management” button on the left side under “Help & Member Services.”
- Select your division, if prompted, and then log in as directed.
- Click the “User Management” button at the top.

If you see e-mail accounts listed that are not familiar to you or your family members, it may mean your primary e-mail address and/or subaccount password(s) may have been compromised. The best thing to do, at that point, would be to delete the suspect e-mail accounts using the “Delete User” option and then change your all passwords for each user name. We recommend you create a strong and safe password using a combination of eight or more letters, upper case and lower case, and numbers. We suggest that you adopt the practice of changing your passwords every 30 to 90 days. Microsoft offers a free password checker to help you determine how strong your password is; just visit <http://www.microsoft.com/protect/yourself/password/checker.mspx>. Microsoft has additional information in regards to creating strong passwords at <http://www.microsoft.com/protect/yourself/password/create.mspx>. Also note that there are plenty of free password generators available on the Internet.

If after removing a suspicious account it should re-appear at a later date, or a different one has been added without your knowledge, we recommend you contact the BHN security department via e-mail at abusedesk@tampabay.rr.com for assistance.