

# Granite Broadband Newsletter

Oct 2010  
Issue 3

## Protecting Yourself Against Internet Crime on Social Network Sites



### ABOUT THIS ISSUE

Protect Yourself Against Internet Crime

Securing your Wireless Router

Featured Website of the Month

Granite Broadband's NEW Spam & Virus Filter

Beware of Phishing Emails & Scams

*We would Love to hear your comments and suggestions about our newsletter.*

*Please email [Felecia@gbandinc.com](mailto:Felecia@gbandinc.com)*

Follow Us On:



## Is Your Internet Connection and Wireless Router Secure?

For many people, the answer is no. The majority of wireless routers are just plugged in and left with default settings when hooked up to the user's Internet connection. This is a big problem as it can allow anyone with a mobile device to steal your connection and can cause you all sorts of issues, including downloading illegal materials, stealing your personal information, and other unwanted activities.

Here are some things you can do in your router configuration

It is very important to make sure your personal information is protected when it comes to the Internet. So much so we have dedicated this issue to reminding our customers of the dangers the Internet and email can pose. This Newsletter includes many helpful tips to make sure you are technologically secure and begins with some important information you should know when using Social Network sites.

### Social Networking

Social networking has changed the way we socialize and it is here to stay. Millions of people use social network sites to connect with friends and family near and far. Many

social network sites are free to use, convenient, and fun, but using these sites can threaten your personal information and put you in danger of identify theft. Here are some tips to remember when using social network sites:

- 1.) Rule number one, NEVER give away your personal information. This includes such things as your address, phone, and social security number.
- 2.) On Facebook, we recommend setting your account to allow only friends to see it. This can be done by clicking on the "account" link and then going to "privacy settings." This will ensure the



only people viewing your profile are your friends, the people you give permission to view your information. Also, we recommend checking your privacy settings every now and then just to make sure nothing has been changed.

- 3.) Lastly, Read the social network sites privacy policy. It is important to understand what risks are involved and whether or not your information is sold for marketing purposes.

to curtail these problems:

- 1.) Enable WPA (or WPA2) encryption for your wireless connections. You do not want to use WEP encryption as it is weak and outdated.
- 2.) Disable broadcasting your SSID and change the SSID. The SSID is the name of your network that appears as available when devices are searching for connections. If you disable the broadcasting it will make your network essentially invisible to people looking for free connections.

- 3.) If your router has Remote Administration capabilities, disable it. If for any reason someone needs to get access, you can turn it back on. This is something you do not want running unsupervised 24/7.

- 4.) If your router has firewall capabilities, use it. A firewall running between your internet provider and your wireless network is an excellent measure to enhance security.

If you implement these actions, you will be ahead of the game in protecting yourself in the wild west frontier of wireless.



## We have a NEW Spam & Virus Email Filter!



### FEATURED WEBSITE OF THE MONTH:

[Newseum](http://www.newseum.org/todaysfrontpages/default.asp)

<http://www.newseum.org/todaysfrontpages/default.asp>

Front pages of Newspapers from around the world, including several from WI.

Granite Broadband has chosen to switch our email filtering services from Postini to GFiMax Mail Protection from GFI Software. The new filtering system has received great reviews and comments from our customers so far. The purpose of email filters

are to protect your Dotnet or Granite Broadband email account from potentially harmful virus emails and scams. Many users do not even know that these filters are put in place, but without them email accounts could get hundreds and even

thousands of junk emails each day. You can find more information about GFiMax Mail Protection by going to our website [www.gbandinc.com](http://www.gbandinc.com) and clicking on the “news and updates” link on the upper left corner of the homepage, or [click here](#).

## Beware of Phishing Emails!

Phishing is the illegal process of acquiring personal information, such as passwords and bank account information, most commonly through emails or instant messaging. Phishing emails are cleverly disguised to trick you into responding with your personal information.

Recently a phishing email was released to many of our Dotnet & Granite Broadband email users disguised as being from our Company. It is very important for us to notify our customers of the dangers of phishing & scam emails. Millions of email users are tricked by phishing emails every year. The following are a few helpful tips we have compiled to help you avoid getting hooked on a phishing trap.

1.) Do not respond to any email that is requesting personal information from you. Even if you “think” you know who it is from. Phishing emails are designed to trick you, so they may not be from who they say they are from.

2.) Phishing emails most commonly request the following information from you: Email account, passwords, bank account information, and credit card information. So, if someone is requesting this information from you, there is a good chance it is a phishing scam.

3.) Beware of website forgery, a common phishing tactic. Website forgery is when you are routed to a website that looks as if it is a secure site, such as a bank website, but it really is a scam trying to get you to enter your personal information.

4.) Do not be manipulated by the “From” address. You can actually put any email address in the “From” field. Here are some examples of “From” addresses we have seen in phishing emails:  
From: [webmaster@dotnet.com](mailto:webmaster@dotnet.com)  
From: [support@usbank.com](mailto:support@usbank.com)  
From: [account@paypal.com](mailto:account@paypal.com)



### How Do Phishing Emails Get Through Email Filters?

Phishing emails are designed to trick email filters. The purpose of phishing emails are to trick you so Phishers will do everything they can to get their emails to you.

One common technique Phishers use is turning emails into images rather than texted. Filters are designed to pick up on text commonly used in phishing and spam emails, but they are unable to pick up on texted inside of an image.