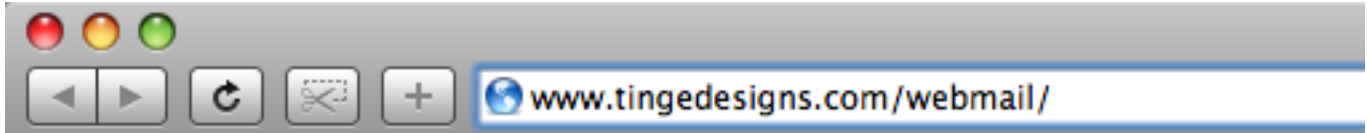


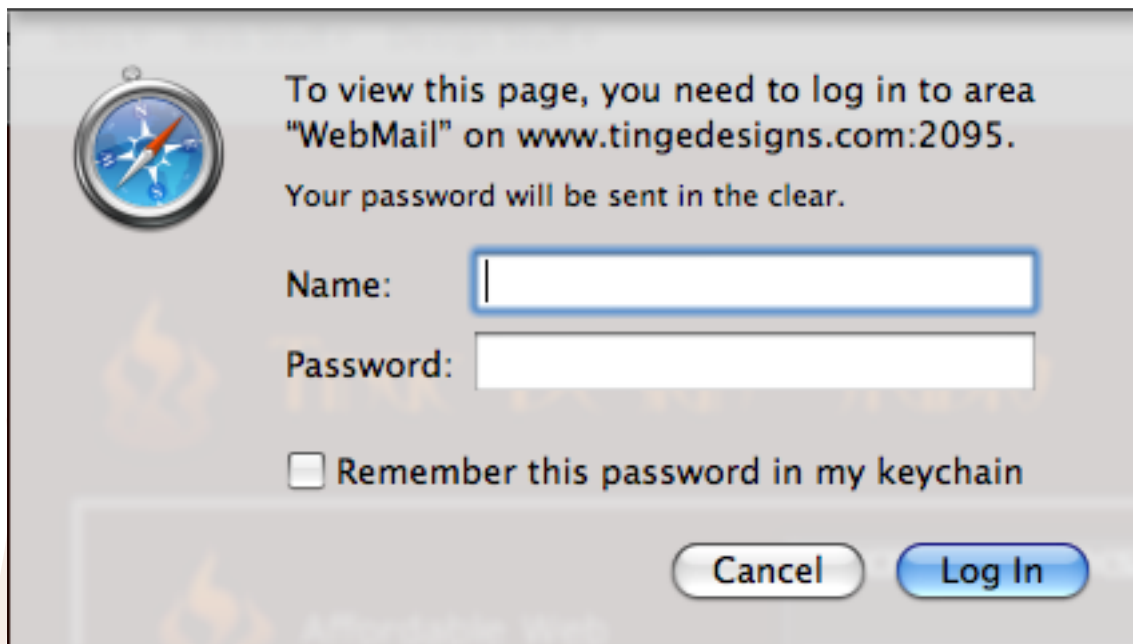
Accessing Your Email

If Tinge Design Studio is hosting your site, you have received at least one free email. This document will show you how to access this email through your web browser. You can also set up your email to be routed to your gmail accounts or viewed through outlook or windows mail.

1. Open your browser and navigate to your domain name.
2. Once at your site's index page, add "webmail/" (i.e. www.yoursite.com/webmail/).



3. You will be prompted for the username and password you have been provided.



4. This next screen gives you a number of useful options (see screenshot):

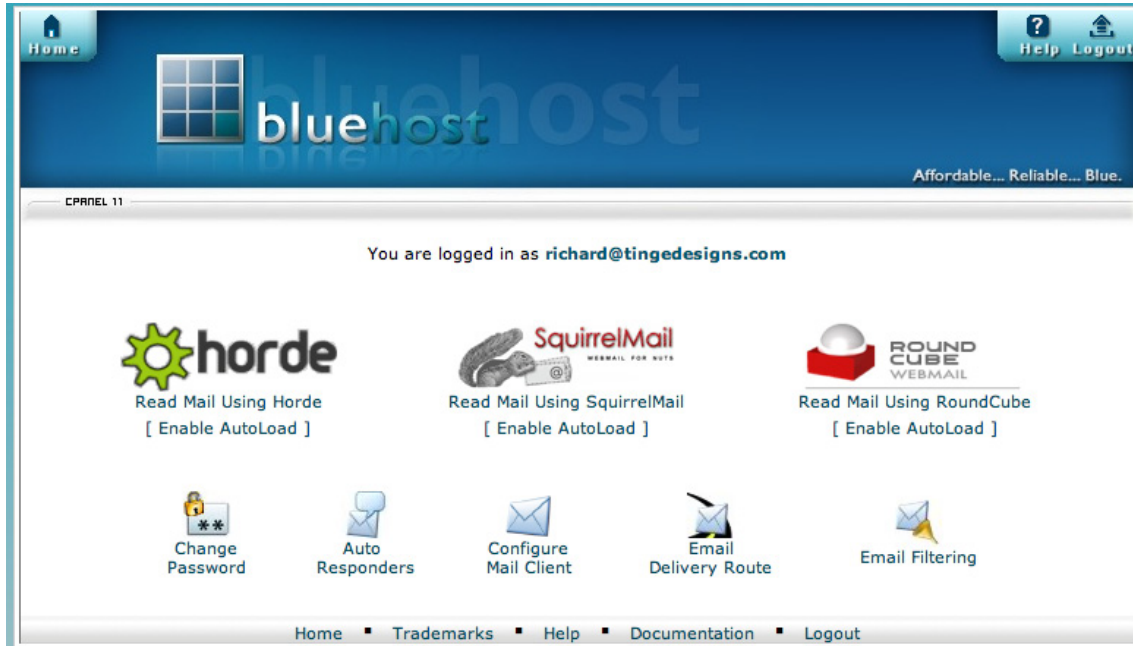
View Email - You have 3 choices for webmail software to use. I personally use RoundCube when accessing my email through the web. Click on the image of the software you want to use. If you want one of the options to automatically load each time you visit, click the "Enable Autoload"

Change Password - changes your password. If you forget the new password you use, you will have to contact me to change it again.

Auto Responders - You can use autoresponders to send a message back automatically to anyone who sends an email to a certain account. This can be useful for times when you are on vacation or unavailable, or if you have a generic message that you wish to send for a support email address.

Configure Mail Client - Setup your email to work with Gmail, Outlook or any other pop3 mail client. Detailed instructions for gmail pop settings can be found here:

<http://mail.google.com/support/bin/answer.py?hl=en&answer=13273>



5. You now have access to your email. See the next page for tips on how to avoid email spam.

Tips to Avoid Spam

1. Do not post your e-mail address in an unobfuscated form on the Internet. If you need to post your e-mail address, obfuscate it so it cannot be easily harvested such as "name -at- hotmail - dot- com," Or if you need to include your e-mail address in your signature, include a small graphic image containing your e-mail address.
2. When filling in Web forms, check the site's privacy policy to ensure it will not be sold or passed on to other companies. There may be a checkbox to opt out of third party mailings. Consider opting out to receive less opt-in e-mail.
3. Never respond to spam. If you reply, even to request removing your e-mail address from the mailing list, you are confirming that your e-mail address is valid and the spam has been successfully delivered to your inbox, not filtered by a spam filter, that you opened the message, read the contents, and responded to the spammer. Lists of confirmed e-mail addresses are more valuable to spammers than unconfirmed lists, and they are frequently bought and sold by spammers.
4. Do not open spam messages wherever possible. Frequently spam messages include "Web beacons" enabling the spammer to determine how many, or which e-mail addresses have received and opened the message. Or use an e-mail client that does not automatically load remote graphic images, such as the most recent versions of Microsoft® Outlook® and Mozilla Thunderbird.
5. Do not click on the links in spam messages, including unsubscribe links. These frequently contain a code that identifies the e-mail address of the recipient, and can confirm the spam has been delivered and that you responded.
6. Never buy any goods from spammers. The spammers rely on very small percentages of people responding to spam and buying goods. If spamming becomes unprofitable and takes lots of effort for little return, spammers have less incentive to continue spamming.
7. If you have an e-mail address that receives a very large amount of spam, consider replacing it with a new address and informing your contacts of the new address. Once you are on lots of spammers' mailing lists, it is likely that the address will receive more and more spam.
8. Make sure that your anti-virus software is up to date. Many viruses and Trojans scan the hard disk for e-mail addresses to send spam and viruses. Avoid spamming your colleagues by keeping your anti-virus software up to date.
9. Use the firewall included with your operating system, or use a firewall from a reputable company, to avoid your computer being hacked or infected with a worm and used as a spam-sending zombie.
10. Do not respond to e-mail requests to validate or confirm any of your account details. Your bank, credit card company, eBay, Paypal, etc., already have your account details, so would not need you to validate them. If you are unsure if a request for personal information from a company is legitimate, contact the company directly or type the Web site URL directly into your browser. Do not click on the links in the e-mail, as they may be fake links to phishing Web sites.
11. Do not click on unusual links. Confirm the sender did send the e-mail if it looks suspicious.
12. Never give out your login details to anyone.