Thanks for choosing LookNet as your hosting service!

If you experience problems or have questions, contact <support@look.net> or call 1-888-566-5638.

About your folder

Practically everything about your account is held in a single directory. Your directory is laid out like so:

~/	anything on this level is NOT web accessible.
~/cgi-bin/	your script-aliased directory
~/homes/	if you set up users, their files go in here
~/logs/	the log files for your site
~/mail/	your mail folder
~/website/	this is the root of your website

The website folder contains your entire website. In other words, everything inside the website folder is exposed to the web; anything outside of it is not.

The various dot files (.procmailrc, .spamassassin, etc) are configuration files for their respective services.

The control panels

There are two separate control panels. The Webmin control panel is for configuring various parts of your service. The Usermin control panel is for user-type activities (reading email, uploading files, etc). See the Quick Reference for access details.

You can do the following under the Webmin control panel:

- Set up email accounts
- Set up email forwarding
- View web log statistics
- Create/Edit MySQL tables (if enabled)
- Edit apache options for your site
- Create .htpasswd and .htaccess files
- Upload/Download files
- Use a graphic File Manager with editing functions
- Schedule timed jobs
- Change passwords for yourself and your users
- Edit the DNS data (be very careful here)

You (and your users) can do the following under the Usermin control panel:

- Read email
- Create/Edit various mail filters
- Mail forwarding
- Edit some apache options
- File Manager access

Check through both control panels to familiarize yourself with them.

Setting up your email

There is already one email account set up for you. See the Quick Reference for access details.

If you are using IMAP to check your email you may need to add a *prefix* in your mail programs settings. The prefix would typically by **~/mail**. Keep in mind that any email you keep stored on the server takes away from your storage space on the server.

If you are using this mail server to *send* email you'll need to set your mail program up for SMTP AUTH. There is typically an area to specify this at the area

where you enter the name of the SMTP server. Set these values to your email login and password.

Anti-Virus filtering and SpamAssassin scoring are set on by default. Neither is set to delete email. Instead, each adds special headers to the email:

X-Virus-Status: Yes, No or Fail (if fail, the message wasn't scanned)
X-Virus-Report: List of any viruses found
X-Spam-Status: SpamAssassin status header
X-Spam-Level: SpamAssassin reporting level header

If a email containing a detected virus/worm/trojan is received for you it is added to your **IN.infected** mailbox. If a email that scores as spam to the default SpamAssassin installation is detected it is sent into your **Spam** mailbox. You can control your SpamAssassin parameters through the SpamAssassin module in the Usermin control panel. You can control all your mail filtering through the Procmail module.

Note: Do not set up rules or filters to bounce viruses or warning messages back to the sender. Nearly all modern viruses use forged mail headers, meaning the sender noted on the message has nothing to do with it. Sending a warning to them does nothing but annoy an innocent party.

Aliases (mail forwarding) set up through the Virtual Email control panel do not go through the virus checking or SpamAssassin. You can use Procmail filters to set up forwarding that goes through the checks. You will see two program filter rules (one for ClamAssassin, one for SpamAssassin) and two mailbox filter rules (one sending spam to Spam and one sending infected email to IN.infected).

Website specifics

The default pages should be named, in order of preference: index, default or home using .html, .htm, .shtml or .php as the extension.

You can use a .htaccess file to control directory-specific options such as password protecting a directory. You can set up and control .htaccess files

through the control panel. See the Apache documentation for details about .htaccess files and other Apache options. We'll walk you through creating one password-protected directory in the next section.

Website Statistics

Webalizer is already installed and setup to generate statistics for your site. It is recommended that you set up protection for this directory to keep others from viewing your statistics. Let's walk you through how to do that right now:

1. Open your Webmin control panel in your web browser
2. Go to **Others**
3. Go to **Protected Web Directories**
4. Click **Add protection for a new directory**
5. At the **Directory path** field, click the button at the end
6. In the pop-up, double-click **website** and then double-click **stats**, then the **OK** button
7. Leave **File containing users** on automatic, leave encryption on **Unix crypt**
8. Set the **Authentication realm** to something like **stats**
9. Click **Create**

You'll now see an entry for what you just added. Notice in the second column that no users have been defined.

10. Click the **Add new user...** link

11. Enter a username (its probably easiest to use the same username you logged in with)
12. Leave **Enabled** switched on
13. Change **Password** to **Set to** and enter a password, hit the **Save** button

When you return to the main screen you'll see the user you just set up inhabiting the second column. When you add more users to the file they'll be there as well. Click on a user to change that users password, delete the user or disable the user.

Passwords

We've designed this system to be very picky about passwords for your protection. Minimum of 6 characters. You cant have your username in the password, nor can the password be a simple dictionary word. Keep these facts in mind when creating new users or changing your own password. Its a good idea to change your password every so often. When you change it via the Change Password module it will change globally across the server, including your MySQL password (if enabled).

If you make a certain number of failed login attempts, regardless of the *type* of login, you will find yourself locked out for a period of time. This is to protect you against brute force attacks when someone throws thousands of passwords at your account in an attempt to gain access.

Access

Your account is accessible through the following protocols:

ftp
ssh/scp
WebDAV

Within the Virtual Mail control panel you have the choice of allowing both mail and ftp access to any of your users.

CGI & scripting

Your cgi-bin is script aliased, so no specific extension is needed to run programs from it. Your apache installation has SuExec running, so all scripts are executed as your username. Perl, Ruby, Python, C, C++, Obj-C, tcl and shell scripting are available.

As far as php, both open_base_dir and SafeMode are in effect. Open_base_dir is set to your home directory. Use .php or .php4 for your php files.

SSI, or server-side includes, are functioning with the exception of *exec*. Any server-parsed files need to end with .shtml to be processed by the SSI module.

Most of the typical modules for each scripting environment are installed. If there is a module you need to have installed please let us know via <support@look.net>.

Software used

Here's a listing of some of the software involved, for your reference:

Apache <http://www.apache.org>
PHP <http://www.php.net>
Procmail <http://www.procmail.org>
Spamassassin <http://www.spamassassin.org>
ClamAV <http://www.clamav.net>
Perl <http://www.cpan.org>
Python <http://www.python.org>
MySQL <http://www.mysql.org>
Webalizer <http://www.webalizer.net>