



Hintlink Technology



Web site Owners Guide (including domains, web pages and email)

Introduction

Web sites and e-mail for different hosted domains at Hintlink Technology fall under the following categories:

- (i) Fully managed – Hintlink Technology makes all changes to e-mail and web page(s)
- (ii) Partly managed – Hintlink Technology does the majority, some content edited by user
- (iii) Not managed – Hintlink Technology does only e-mail account set-up

This document explains the features and extent to which site management rests with Hintlink Technology or the site owner.

For the technical

The server can run most Open Source web applications and already runs the following:

Operating System	FreeBSD UNIX
Web server	Apache
E-mail receipt	POP3. Use pop.yourdomain.org (or com)
E-mail sending	SMTP (procmail). Use smtp.yourdomain.org (or com)
E-mail reminders	Cron
E-mail groups	/etc/aliases
FTP server	FTPPro. g4bki.iserver.net
Audio server	wav, mp3
CSS server	Cascading Style Sheets enabled
CGI	CGI scripts
mySQL server	Database server
Perl	Perl server
phpMyAdmin	Database Admin suite
PHP server	PHP3/PHP4/PHP5
Python server	Python based programs
Twig server	Browser based e-mail, etc.
SpamAssassin	Bayesian filter Spam blocker
Spam-bot blocking	System added to stop harvesting of e-mail addresses
Wordpress	Blogging system
Mailman	Mail list system
RSS	RSS newsfeeds are added simply
Java/JavaScript	Java applications
Browser based FTP	For use in remote locations

Other applications may be installed. These may be commercial packages, in which case the license & installation will be charged by Hintlink Technology to the customer. Other Open Source applications can be installed but installation, data conversion and testing will be charged by Hintlink Technology to the customer.

Specific Management Tasks (automated) performed by the server

At the time of first set-up of your account the following functions were/are installed:

- A billing reminder on the first day of the month (or in some cases, the first day of the quarter). These are sent a few minutes after 00:00UTC. Your reminder is sent to the person who is responsible for billing (and *maybe* copies to others). It contains important information – the amount – the Hosting Agreement and when your domain will next expire.
- A log file of all accesses to your domain. Executed a few minutes after 01:00UTC each day. A few files generated by this will appear each day in your area, such as log.htm and a number of .png files used in the report. **PLEASE do not use other page “counters”**. Why? The built-in log provides much more detail than external sites AND it reduces the traffic that is taken from deep within your web pages and then handed off to a “trusted” service. Your log file analysis may be found always at: <http://mydomain.com/log.htm>.
- A sitemap file is generated and sent to Google search. Executed a few minutes before 01:00UTC each day. This makes sure that changes in your web page are continuously updated at Google. On large sites this may be executed more frequently. **For verification reasons a zero sized file called GOOGLE21ae7740639fd55d.html (or similar) is located in the root area of your web space. Do not remove this file.**

Other Free Tasks performed at set-up

favicon. A small icon picture which will show in the address bar, tab bar and favourites/bookmarks of browsers which visit your page.

FTP account. An FTP account is opened so that web content can be uploaded by the domain holder. The login and password may or may not be the same as your e-mail account. **DO NOT** give this information to anybody who may destroy your web site.

A folder called /analog *may* be installed in your area. This contains image data for the log function. **DO NOT REMOVE or alter.**

A folder called /admin is installed in your area. This contains the settings for the sitemap sent to Google search each day. It generates a file called sitemap.xml in your area. **DO NOT REMOVE or alter this area or that file.**

A folder called /email-lists is *often* installed in your area. This provides a means to add and subtract a list of e-mail addresses to be used with e-mail announcements to a wide group of people.

A folder called /nobot is *often* installed in your area. This is a PHP script which secures your e-mail addresses on your website from robots. **DO NOT REMOVE or alter.**

A file called `.htaccess` is installed in your area. This adds a number of features available to your website (such as Server-Side Includes). It also blocks a large number of robots from harvesting e-mail addresses and links from your site. **DO NOT REMOVE or alter in any way**. Don't confuse this with other `.htaccess` files which may be used for security in lower levels of your area.

A folder called `iCal` *may* be installed in your area. This is used if you have an on-line calendar for your clients. `phpCalendar` doesn't make your calendar, you can do that using `iCal` on the Mac or Mozilla Sunbird.

A folder called `.spamassassin` *may* be installed in your area. This appears only if the username for your e-mail and FTP are the same. If not, your personal Spamassassin details are contained in another hidden folder a long way up the server file system. It's operation is automatic, but if removed would cascade you with spam.

e-mail

Most accounts are set up for you by Hintlink Technology.

Important notes:

You should have the following settings in your e-mail client (Thunderbird, Mozilla, Eudora, OE6 or Outlook)

Username: frfred	The actual e-mail account on the server for you only.
Password: <anything>	Must be set by Hintlink Technology, but cannot be recalled.
e-mail address:	fatherfred@somechurch.org
return e-mail address:	fatherfred@somechurch.org
POP3 (incoming):	pop.hintlink.com
SMTP (outgoing):	smtp.hintlink.com
Authenticate before sending must be set to ON.	

NOTE! Your e-mail address and your username are NOT the same. If you put your e-mail address in the POP3 server field you will never log in (because that is not an allowed username).

Preventing e-mail harvesting from your web site:

Despite the inclusion of a `.htaccess` robot blocker file, more can be done. The **nobot**TM feature allows you to remove any "mailto:" tags in your web page and replace them with a hyperlink, as follows:

Conventional (dangerous) way: [e-mail link]

e.g. `mailto:frfred@somechurch.org` easily picked up by a bot.

(Much) Better way: [hyperlink through a PHP program]

e.g. `http://somechurch.org/nobot/?u=frfred&d=somechurch.org&s=hello world`

not picked out by a bot and leaves it in a dead end, so it *crashes*.

NOTE: ALL Hintlink Technology authored domains have this structure. Those that webmaster their own pages should request the installation of the **robot**TM script and replace all of their mailto: tags with hyperlinks **AS SOON AS POSSIBLE**.

How e-mail works on the Apache Server:

- It's checked that it's come to the right place(!).
- The sender (or their entire domain) is checked against a list of known bad addresses. If it matches, the message is immediately destroyed. No ifs or buts [part of Apache].
- The sender (or their entire domain) is checked against a White List. If it matches, it is let through as a trusted source with no further screening [part of Spamassassin].
- The *entire* message is checked by the Bayesian adaptive system of spam detection. Spam and Ham are sampled randomly and used to further refine the spam search.

The destination for the e-mail is then determined by a virtmaps file:

father@somechurch.org	ffred
fatherfred@somechurch.org	ffred
father.fred@somechurch.org	ffred
office@somechurch.org	scadmin
finance@somechurch.org	scmoney
youth@somechurch.org	daisy
music@somechurch.org	organslayer@hotmail.com
congregation@somechurch.org	scfolks
somechurch.org	kill

Notice how multiple e-mail addresses can be collected by one user.

Notice that the e-mail goes to a given username.

Notice that the last line is a "catch all". Any address that doesn't match will go there. In this case it goes to a special account which just dumps any bad e-mail. So, e-mail for abc@somechurch.org will get dumped. This doesn't have to be kill, it could be, for example, be office@somechurch.org, just as long as they are prepared to receive a lot of spam.

Notice that if the music person doesn't have a computer at work, e-mail is just redirected to their other e-mail account (organslayer@hotmail.com).

Let's say that youth@somechurch.org needs to duplicate their e-mail to home, well there's a way to do that by using an alias:

```
daisy: daisy, somename@someisp.com
```

This sends all e-mail for youth@somechurch.org to daisy and to e.g. fredblogs@tampabay.rr.com.

Finally, a special list can be made:

```
scfolks: ~/usr/local/home/httpd/htdocs/somechurch/email-lists/congregation.txt
```

When an e-mail is sent to congregation@somechurch.org, it goes to everybody listed in congregation.txt, which is in your own web space and can therefore be updated by you, without any help.

HOWEVER, ONE major warning:

Always have only one person control such a list

Always have that one person send messages out as BCC (blind carbon copy)

DON'T EVER have anybody put that address in an e-mail address book.

OTHERWISE, one person on the list can get a virus or spam and pass it to everybody without even knowing it.

For a better system, request the use of Mailman from Hintlink Technology to be installed for your group.

Preferred Programs:

FTP client for uploading and downloading web page content (in order):

FileZilla (free)

CuteFTP

WS_FTP

SmartFTP

Browser (in order):

Mozilla FireFox (free)

Opera

Safari (Mac OS-X)

Internet Explorer (free)

e-mail client (in order):

Mozilla Thunderbird (free)

Eudora

Outlook Express 6 (free)

Outlook (MS Office bundle)

RSS Readers (in order):

Abilon

FeedReader

RSS Authoring Tools (in order):

ListGarden (free)

RSSBuilder (free)

Web page Authoring Tools (in order):

Nvu (free)

Mozilla Composer (free)

Many others: Word, HotMetalPro, DreamWeaver, OpenOffice, etc.

Note: not all web authoring tools structure files in the same way. It can be disastrous to load an Nvu file, for example, into Word just *once*.

USER RESPONSIBILITIES

The days of the ISP being able to look after you completely have gone. Automated one hour server lookups of Spam & Virus databases (which our server does) cannot catch everything before it can get to users.

Therefore, for the sake of your computers, network and server(s) you must have the following on each PC attached (doesn't include Apple or *NIX boxes):

A hardware firewall – if you have a router (Linksys, Hawking, D-Link) this is there.

A software firewall – the best is ZoneAlarm (free)

An anti-virus program – the best is AVG (free)

A bot detector and killer – the best is Spybot S&D (free)

An Adware detector and killer – the best is Ad-Aware SE (free)

Install an RSS feed reader. This is the way forward for reducing spam and other issues.

In future MOST Hintlink Technology announcements, billing reminders, etc. will be sent by this method.

Other Notes:

The stcgrenada.com (March 2006), dunedinsystems.com (August 2006) and sciencetechnologyconsultants.com (May 2008) will be phased out. POP3 and SMTP settings using these should be changed before then, preferable ASAP.

Most D-Link routers are unreliable and crash. Some can be retrofitted with “hacked” software by Open Source developers on the web, which make them stable and add new features!

Linksys/Cisco routers are extremely reliable.

Applications based on Microsoft .NET and ActiveX are not to be trusted.

In some pages you may see the HintLink™ button. This is online help for users.

