

Spring 2009 newsletter

1. **Service developments**
2. **Current promotions**
3. **Regulatory developments**
4. **Security developments**
5. **Tip-of-the-newsletter**
6. **Contacting us**

Service developments

Welcome to the Spring '09 edition of our newsletter. We've been fabulously busy for a long time, so much so that we skipped several issues of our newsletter, sorry about that! We hope this issue will make up for it.

- ◆ Did you know that every hosting account we sell comes with **OS Commerce**? This software can be used to create a **fully-fledged online shop**, complete with a catalogue, sample images, and credit-card processing. Several of our customers are using OS Commerce to trade online. We also have the skills inhouse to build and manage sites based on OS Commerce. This means you can start building your store, and call us in if you need to. The best part is that OS Commerce is open-source software, this means that you can **completely customise** your store, far beyond the comprehensive customisation abilities built into the control panel, limited only by your knowledge of PHP, and/or the skill of your developers.

If you're interested in online trading, we recommend you start by looking at this software. If you're a hosting customer, it's available to install from the "Web Tools" section of your hosting control panel. If you don't host with us, you can still use OS Commerce – you'll need to install it manually, however. For more information: <http://www.oscommerce.com/>

- ◆ Are you looking for a method to quickly notify your customers – or yourself – when specific events occur? We can now **integrate SMS (text messaging)** with your computer systems, such that a text message can be sent when almost any event occurs. For example, if a customer has ordered a product for delivery, you can text them when the product has been shipped. Or if a customer has a direct debit set up, you can text them a reminder a few days beforehand. Or, for example, if you would like to be notified whenever a customer places an order, or when a payment is made, that would also be possible.
- ◆ A hot-button topic right now is **website optimisation** (some might call it search engine optimisation or SEO but this is an overly narrow focus, in our opinion). And we can indeed optimise your site. What does it mean? A quality website optimisation project will do the following, amongst others:
 - improve user-friendliness/ease-of-use
 - improve search engine ranking
 - increase and conserve site traffic
 - integrate accessibility guidelines
 - integrate overlooked technology tweaks
 - ensure cross-browser compatibility
 - instigate performance monitoring

We have a **49-point checklist** which we use to do the work. We'll send you a copy of it before the work commences, so you can see the things that need to be fixed. We'll even analyse your site for free! Please see this page for more information:

http://www.blazingfibre.net/prodserv/website_optimisation.htm

- ◆ If you're looking for a quick way to check the availability of domainnames, look no further than our new **Domainname Availability Checker**. Just enter the domainname to query, and you'll see the availability for the .com, .net, .org, .biz, .info and .co.uk variations of the name! It's here: <http://www.blazingfibre.net/checker.php>
- ◆ We have two new treats in our support area, in addition to the substantial quantity of documents we've added and improved. The first is our **network status page**, which you can use to get quick overview of the status of our systems. It's found here: <http://www.blazingfibre.net/status.htm>

The other new item which we're also quite pleased with is our **searchbox**, which lets you quickly search every one of our support and product literature pages, with a single query. We liked it so much we embedded it into our homepage, and also our support page – however it can also be found here: <http://www.blazingfibre.net/search.php>

We know, it's not as sexy as Google, but it's early days for that particular component, and improvement is scheduled. If you are interested in a similar, possibly better-looking function on your own site, that would be possible.

- ◆ Did you know you can use SSL to **protect your FTP sessions**? All you need is an FTP client that supports FTPS. More details here: <http://www.blazingfibre.net/tech/ftps.htm>
- ◆ This issue, we have a special insert from our Finance Department, who do not usually grace these pages but have found the need on this occasion to issue the following statement:

Recent dislocation in financial markets has prompted the failure of a number of large companies, this failure usually being due to excessive debt. We'd just like to note that the financial position of Blazingfibre Limited is particularly solid, as the company has, from its inception, been run without debt of any kind. We have never had, do not have, and hopefully will never have, a loan from a bank, or anyone else. We also don't have a credit card, nor do we have an overdraft - we have no debt at all. Blazingfibre is 100% customer-financed - we don't need debt to survive, and our income covers our expenses, which are extremely low. Additionally, demand for our core services remains strong, as businesses need their computers to work, their data processed and their websites online, even during the bad times - perhaps moreso. Please be assured that Blazingfibre is very well-placed to ride out the recession. We are in fact hoping to emerge on the other side stronger and more capable than ever. The continuing development of our service offerings (visible in the first section of this and all our other newsletters) is helping us work toward this goal.

We'll close here, with a quote from Stephen King, managing director of economics at HSBC:

"Wealth ultimately comes from productivity gains. Those gains, in turn, hinge on advances in technology ..."

<http://www.independent.co.uk/news/business/comment/stephen-king/stephen-king-first-the-chinese-accumulated-dollars-now-everyone-is-joining-the-stampede-1067216.html>

Current promotions

The latest devastating deals.

- ◆ **Free hosting:** If you buy a website from us, we will throw in hosting **for 1 year, free** of charge! This is a nice way to get online, while keeping your costs low. Conditions do apply, for more information: <http://www.blazingfibre.net/prodserv/webdev.htm>
- ◆ **Training courses:** Boost your productivity and beat the credit crunch, with some new skills. We can teach you about Windows, your computer, the internet, networking, security, website development, and more. Each course is delivered as 4x1-hour one-on-one training sessions, at your premises, after-hours if required. You can even pick'n'mix your sessions, if you like! We're currently offering **16.6% off**, if you buy 3 or more courses. For more information: <http://www.blazingfibre.net/prodserv/training.htm>
- ◆ **Service contracts:** We've added **free remote monitoring** to our service contracts. This service enables us to monitor your systems for faults, automatically, every day. It can be purchased separately, however we're now offering free of charge to contract-based customers. For more information: <http://www.blazingfibre.net/prodserv/ssc.htm>
- ◆ **Website optimisation:** Are you unsure whether your website needs optimising? We're offering a **free site analysis**, so that you can find out, without risk or obligation to you. This service is sold for hundreds of pounds by our competition. We'll do it for free, because we're confident that once you've seen our report, you'll want us to do the work! Please see the first section for more details, or indeed, visit the relevant webpage here: http://www.blazingfibre.net/prodserv/website_optimisation.htm

Regulatory developments

(Please note: We are not a law firm, this is not legal advice, and if you have any doubts concerning your position, you should contact a solicitor.)

- ◆ We'd like to draw your attention to the UK's Distance Selling Regulations. If you're selling to consumers "at a distance" then you must comply with these regulations. The phrase "at a distance" **does include** e-commerce transactions. Therefore, if your website sells products to consumers, these regulations apply to you. Note that the regulations **do not** cover business-to-business transactions, they cover sales to consumers – "consumer" is defined by the Office of Fair Trading as "*any person who [...] is acting for purposes that are outside their business*". For more information, please see the writeup by Pinsent Masons at: <http://www.out-law.com/page-430>

The OFT also has a guide to the subject, which can be found at:
http://www.of.gov.uk/shared_of/business_leaflets/general/oft698.pdf

Security developments

This section in a single word: **PATCH**.

- ◆ Ransomware, scareware - self-replicating, self-updating, cryptographically-armoured, peer-to-peer botnets – it's a wild world out there right now, and the best remedy is to stay up-to-date with patches and signature updates. Most of these threats are avoidable if your system is up-to-date. Don't forget this also includes the software you use – old versions of Acrobat Reader are, for example, vulnerable to a simple "drive-by-download" attack, in which a malicious PDF is embedded in a webpage – you don't even need to click a link to a PDF, all you need to do is visit the page in your web browser, and you're cracked! Ensure you keep all the applications you use up-to-date, including your web browsers, media players, document viewers, and office software, in addition to anti-virus, anti-spyware and firewall software.

Note that it is important that you do this, not just for your own benefit, but for the protection of others. When a worm attacks your system, it is because someone else has failed to patch theirs. *Don't be that someone else*. If enough people patched, there would be an insufficient number of "propagation points" for malicious software to pose a threat. Unpatched machines are dangerous, and it is irresponsible to operate one.

Don't forget, alternatives to Windows do exist, such as the Ubuntu Linux-based desktop, or PC-BSD. It's no small project to migrate to unix (or even to a Mac), especially if you have legacy applications – but staying on top of security updates for Windows is no small project either. For more info:

<http://www.ubuntu.com/products/WhatIsUbuntu/desktopedition>

<http://www.pcbbsd.org/>

- ◆ A quick note concerning domainname renewals. This is not a new trick, however it's still happening – certain companies out there will send you an unsolicited invoice to renew your domainname. They can get your domainname, postal address and expiry information from your domainname record (which is visible to all internet users), and use that information to bill you. They send you an invoice, even though you are not their customer. And here's the catch – if you look on the back of that invoice, you'll see a **whole page** of fine print (we're not making this up) – and that fine print includes authorisation to transfer your domainname to them. *If you pay the invoice, your domainname will be transferred away from your existing registrar, and you will find it very difficult to get it back*. Again, we are not making this up, we have seen it first-hand.

If you receive an unexpected invoice like this, simply bin it (we recommend destroying it, in case it somehow resurfaces later). You **are not** obligated to pay. Note that you should, of course, renew your domainname in the usual way with your regular provider. However, your regular provider will invoice you directly for this. Do not pay an invoice relating to domainname renewal from someone other than your regular provider.

We actually warned about this in our Autumn 2004 newsletter, and while we haven't see any invoices recently from "Domain Registry Of America" or "Domain Registry Services", we do have an invoice right next to us from a company called "Domain Renewal Group" and it is very similar in style to those from the "Domain Registry Of America". Read more here: <http://www.blazingfibre.net/mkt/autumn04.pdf>

Tip-of-the-newsletter

by Dr C. P. Yu

If you have a query you'd like to see as tip-of-the-newsletter, send it in! Contact details are at the end.

Tip #5: blocking phish

You may have noticed email from various banks in your inbox, claiming that your account details need updating, or some such similar wheeze, despite the fact that you are not a customer of those banks.

These mails don't pose much of a security risk since you know you're not their customer, and thus you can spot them easily and simply delete them. However if you're unlucky, you may have a quantity of these "phishing" emails arrive each day. If this happens, it can get annoying, simply deleting them.

If you'd like to block these phish entirely, so that they are either deleted or removed from your inbox automatically, there is a simple and effective method to do so. All you need is a mail program such as Outlook Express, which is capable of filtering incoming mail based on rules.

In the example below, we're just going to block one bank, however the process can be repeated any number of times – whenever you receive a phish, simply add a new rule to handle it. You can either wait until you get a phish from a particular company, and create new rules as you need them, or you can just use the list I provide (see next page). If you do use my list, don't forget to remove your own bank from it, if it's listed – but only if they send you email.

Example: blocking email from Bad Banking Corp with Outlook Express

In this example, we assume that Bad Banking Corp (a hypothetical bank) uses the domain name **badbankingcorp.com**

1. Open Outlook Express
2. Create a new folder called "phish". You only need to do this once, not every time you make a rule. The folder can be called whatever you like, we use "phish" as an example. To create a new folder, in the left pane, right-click "Local Folders" and select New Folder, then enter the name of the new folder, and click OK
3. In the menu at the top, click Tools.. Message Rules.. and select Mail...
4. click the New button
5. in the 'Conditions for your rule' box, tick the box 'Where the from line contains people'
6. in the 'Actions for your rule' box, tick the box 'Move it to the specified folder'
7. in the 'Rule description' box, click 'contains people'
8. enter **badbankingcorp.com** into the box, click the Add button, then click OK
9. in the 'Rule description' box, click 'specified'
10. select your phish folder (created in step 2), then click OK, OK again to save the rule, and OK again to close the rule editor

All mail from anyone @badbankingcorp.com will now be automatically moved to your "phish" folder.

Why is this so simple, when blocking spam is so difficult? It's because unlike spam, phish are trying to fool you into thinking they are legitimate mails. For this reason, the name of the company they are trying to impersonate is almost always listed in the sender's email address ("from line"). That means that we can identify and remove them, simply by searching for the company names they are impersonating, in the sender's email address. And that is exactly what we do with the above rule.

Note: while this method currently works well, there may come a time when the "phishermen" get wise to it, and start "obfuscating" their "from line" (in order to defeat the filters above). If this happens, we'll post again on the subject, in this column.

Our list of search strings is below. Note that some strings aren't domainnames, while others are partial domainnames. This is intentional. You can use some, all, or none of the list, as you choose. You can also add your own, if you need to.

Royal Bank of Scotland
bankofscotland.co.uk
HSBC
NatWest
lloydstsb.co.uk
lloydstsb.com
lloyds.co.uk
halifax.co.uk
abbeynational.co.uk
@abbey.co.uk
@abbey.com
barclays.co.uk
barclays.com
cahoot.com
CitiBusiness
@citi.com
citibank.com
equifax.com
commercebank.com
bankofamerica
wachovia.com
capitalone.com
@nationalcity.com
tdbanknorth.com
.chase.com
@chase.com
americanexpress.com

Contacting us

We'd love to hear your suggestions and comments. Our contact details are as follows. And yes, **we do** pick up the phone on weekends!

- web: <http://www.blazingfibre.net/>
- email: support@blazingfibre.net
- telephone: +44-794-473-1092
- snailmail: blazingfibre.net / PO Box 2855 / London W1A 6LW
- feedback form: <http://www.blazingfibre.net/feedback.htm>
- GPG key: <http://www.blazingfibre.net/fibre.key>

Blazingfibre Limited is registered in England and Wales, company # 5178087; registered office: 64 Paul St, London UK EC2A 4TT