



August 2008

Web page for Cobourg Internet Customers only

To see all previous newsletters plus articles referenced, go to this page.

www.cobourginternet.com/webnewsletters.htm. Bookmark it so you can come back at other times. Recently added: How to set up email accounts on Outlook and Outlook Express (now separated from C-Panel setup document) and short version of how to access web-mail.

Spam, Viruses and Phishing

We all have email and we all get unwanted email - if it's unwanted, it's spam. But the reasons for "not wanting" vary. If it's an ad for something you don't want - viagra or worse, cheap medications, etc - it can be spotted and deleted, hopefully before it even gets to you. If it includes a virus, then your anti-virus will most likely catch it. If it's phishing it may be harder. Phishing is when someone pretends to be a bank or similar and asks for personal information to be "confirmed" to re-establish an account or similar. Protection against phishing relies on you to spot them. If you remember that no banks ever send emails asking for confirmation then you'll know not to click any links in such emails. If in doubt, phone the bank and ask about it.

So what does Cobourg Internet do about all this?

For Phishing, you need to be careful - there is little else that can be done. But it does require you to enter personal info and if you never do that in response to an email, you are safe.

Email that goes through your web site (e.g. yourname@yourdomain.ca) can have spam trappers added that reduce or eliminate spam. First, spam mail can be identified using **Spam Assassin**. When this program gives an email a really bad rating (10 out of 10), it gets deleted. The rest gets "Spam" put in the subject line. Second, you can have **Box Trapper** activated. It will ask senders to confirm that they are not a computer by asking them to reply to an automated email. If they pass that test, all future emails are passed with no further confirmations required. You can look in the box-trapper queue via CPanel access to see if anyone got trapped that you do in fact want (e.g. a newsletter). You don't have to delete anything since they are only held for 15 days. These programs are not automatically set-up. But if you are getting too much spam, let me know and it can be setup.

Note that ISPs like Sympatico and Cogeco do similar things - if they did not, the average person would get about 80% spam.

Viruses

These days, most viruses do not arrive via email - they come via a corrupted internet site. So if you only surf to known or major sites you should be OK. Sites like Cobourg Internet use security measures to protect against being corrupted - e.g. regular automatic updates, banning of people doing (possibly) malicious things and more - so that a virus on your site is unlikely.

On your own computer, you need a good Anti-Virus program that is updated daily. I currently recommend NOD32 as the best Anti-virus program - it works fast, is non-intrusive and is effective even on very new viruses. It catches spyware as well as viruses - price is \$40US at their web site: www.eset.com The catch? Not quite as easy to set up as Norton. But I've not met one techie who likes Norton - McAfee is worse. Free versions Avast, AVG and Avira all work better than these two - download from [C-Net](http://www.c-net.com). Note that Norton is very effective, it just bogs down your computer somethin' awful. (That's geek talk for "slows it down a lot"). Note that if you change to a different

AV program, be sure to fully uninstall your current one - call me if you need help with this.

What else is being done?

In addition to the above, the Internet community actively fights spam by blacklisting servers (hosts) that are known to generate spam. This is not based on the "from address" which can be faked, but on the IP address which cannot. Apart from rejecting email from known spammers, it also means that no-one wants to host spammers - hopefully that slows them down!!

Backups

You probably assumed I did this anyway but I thought you'd like to know for sure: I have five backups of each site's files. One on the same computer done from time to time, another on a separate networked computer that backs everything up every night, then daily, weekly and monthly backups are made and kept at the remote host location (this is an upgrade from previously). So even if a hacker does make it through all the shields, we can always return to a clean version no more than a day old - for the whole site or just individual files.

I trust everyone is managing to have a good summer - catching some sun between the storms. I have a short trip to Kingston and Ottawa coming up but I'll have my laptop so I'll stay on top of any changes.

John Draper

--

To unsubscribe from this list visit [this link](#)

To update your preferences such as format and particular newsletters you want, visit [this link](#)