



Computers and stuff.

Sam Houliston.

Virus Warning.

Although a lot of virus warnings that get sent over the e-ether are hoaxes, this one is for real. If you see this message, which supposedly comes from “Microsoft Update Centre” - or anything like it - just hit the delete key.

It comes from “securityassurance@microsoft.com” and contains an attachment KB825559.exe which you should NOT open.


For obvious reasons, Microsoft never distributes updates via email. All updates are always sent via Windows/Microsoft Update or direct downloads from the Microsoft.com web site - any and all other 'updates' should be ignored.

Though most email programs (including Outlook 2003 and 2007) block .exe file attachments by default, for some reason this one gets through and it's surprising that the entire message doesn't end up in the Junk Email folder. Just the presence of a 'exe' attachment should be enough to put most emails into the suspicious category.

You can expect to see variations on this type of junk email in the weeks ahead - so don't just lookout for this particular email - watch for it to evolve into other forms.

XP Home Backup.

If you run Windows XP Home, you probably wonder why Mr Gates didn't include a 'Backup' facility with his program like he did with XP Professional. Well!!, funnily enough, he did, but he hid it, though no one can understand why. But, it's easy to find and this is how you do it.

1. Insert your Windows XP Home CD into the drive. If it doesn't start automatically, double-click the CD icon in My Computer.
2. On the Welcome to Microsoft Windows XP screen, click  **Perform Additional Tasks.**
3. Click **Browse this CD.**
4. Double-click the **ValueAdd** folder, then **Msft**, and then **Ntbackup.**
5. Double-click **Ntbackup.msi** to install the Backup utility.

And there you have it.

Easy Switching between Colour and Black and White printers.

With the cost of most printers falling over the years, it is now possible to buy a good printer that will print in both colour and black and white for not a lot of money. However, the cost of the printer might be low, but replacing the ink cartridges isn't so it's prudent to use the colour facility as seldom as possible and print in black and white as often as possible.



When you get the printer home, you will usually find it has been set up to print to the best quality (which means colour). That's because the printer makers want to show off their product and prevent returns to the store because the printer doesn't print as well as promised. Normally to change that high-quality setting you have to go to Printer Settings in the Print dialog.

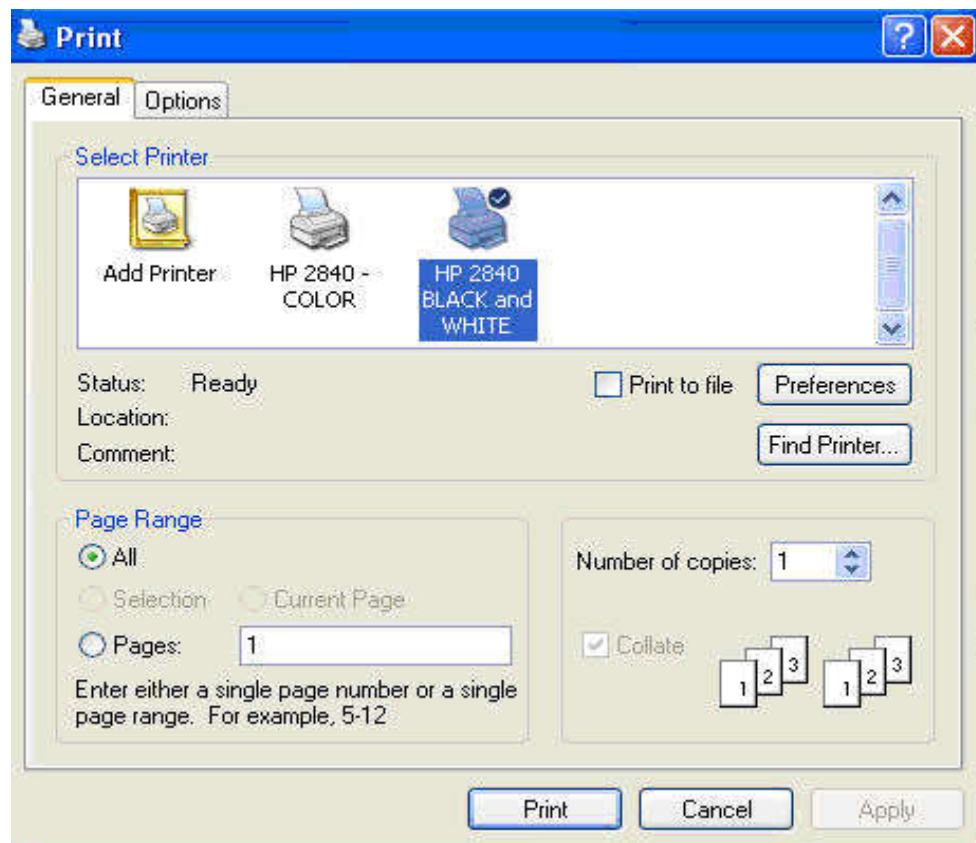
The problem is remembering to make the change to black and white printing (or back to colour). Most of us remember to do that only *after* the page is printed! What's needed is a way to quickly select between printer settings for the same printer. Here's

how!

It's quite easy to do and it's been possible for many years in Windows but it's not obvious. Once setup it works for any Windows program, not just Microsoft Office. In short, you create multiple 'printers' in Windows with different settings in each one, even though they all send output to the same physical printer. First thing to do is open the **Control Panel**, click **Printers and Faxes** and then right-click the printer that you have already installed and which you want to duplicate. Click **Rename** and rename the printer to **Colour**.

Now to make a 'new' printer. Click on **Add Printer**. You'll have to add the printer manually as the Wizard will not see any 'new' printers to add. This will require you to select the make and model of your printer from the list available, or use the set up CD that contains the driver that came with the printer. At one stage you'll be asked if you want to use the existing drivers - choose 'Keep existing driver'. You will get the chance to label the 'new' printer, call this one **Black and White**. Make this printer the default printer as it's the cheaper printing option. Now, right-click on the 'new' printer and choose 'Printing Preferences' to change the configuration - in this case from Colour to Black and White.

Now, when you want to print something, you'll get the window below, all you have to do is select colour or black and white, depending on your preference – and voila.



It's not hard to meet expenses... they're everywhere. Nana V.

Other printer settings

The same tip works for any printer settings you commonly use. For example you could make separate 'printers' in Windows for choices like:

- Duplex / Double-sided printing
- Two pages on a single sheet
- Paper sizes
- Paper type (plain paper, 'photo' paper etc)


This trick works in Windows XP and Windows Vista and most likely earlier versions of Windows as well.

Keyboard shortcut.

If you've got a bunch of programs open and running and you want to get back to your desktop momentarily, there a few ways to do it. The way most people do it is to minimise all open programs by clicking the (-) symbol up on the top right hand



corner of the screen until all open programs are dropped to the Task Bar, works, but it's a pain. However, there are two much better ways.

Pressing the Windows button on your keyboard (the one with the Windows logo on it) with (together) either the "M" key or the "D" key will do it for you instantly. Although the results look similar, they are slightly different. Windows M minimizes all windows that support the command, while Windows D actually raises the desktop to the top. When you're finished with the desktop, press Shift | Windows | M to bring up your minimized windows, or Windows | D to drop your desktop back down again. My pic – Windows D 

Another useful shortcut is Windows E which launches Windows Explorer, defaulting to My Computer. I find Windows Explorer the most useful program on my computer. There are heaps more, if you want to know more, see [HERE](#).

Routers, switches and hubs.

If you've got a couple of computers that are hooked together (networked) and connected to the internet, you will undoubtedly be using one or more of these – but what do they do, and what is the difference between them.

Well, networking can seem very confusing at first but once you get the facts straight, everything starts to make sense.

A computer that wants to connect to a network needs a network interface card (NIC). The network card is what converts the data into digital signals that travel across the network cables. Each network card has a certain numerical combination burned into it known as a MAC address. MAC stands for Media Access Control. This MAC address is the unique identifier of that card and in turn the computer that uses that card. Believe it or not, no two network cards in the world have the same MAC address (assuming the manufacturers follow regulations). So the MAC address gives the computer an identity on the network by virtue of the hardware (network card) installed.

Paddy was a hard working fisherman from Ireland who now lived in the little coastal village of Kettering in Tasmania. Daily he would row a heavy old punt out to Bruny Island then work a heavy iron grapple to bring up the sand oysters which he sold to the local fish shop. He was a man of regular habits and he always arrived home each day at a certain time. Sadly Paddy did not realise the heavy grappling was taking a toll on a faulty heart. One day he failed to come home, his wife contacted the Police to report him missing, they searched and found Paddy dead in the punt and beside him was a huge grapple full of oysters that he'd tried to hoist aboard.....

Headlines next day in the Mercury Newspaper.....*OYSTERS KILL PATRICK*

There is also another identifier for a computer in a network that is configured through the computer's software. That is the computer's IP address. IP stands for internet protocol. IP



addresses are of the form xxx.xxx.xxx.xxx. A computer on a network may have an IP address of 128.0.0.5. Other computers on the network would have a similar IP address like 128.0.0.4, 128.0.0.2, 128.0.0.3 and 128.0.0.6 and so on. The IP addresses of all the computers on a particular network are of the form 128.0.0.x where x is different for each computer. Someone else's network would have a totally different form of IP addresses such as 64.0.0.x or maybe 192.0.0.x. So basically the IP address does two things, it identifies a network as a

unique family and identifies each computer on that network.

When a computer wants to send data to another computer on a network, it doesn't just put data on the network, it sends it as a packet consisting of the data, as well as the address of the destination computer – the IP address, and the MAC address of the destination computer. So obviously the IP address and the MAC address are very important.

The difference between hubs, switches and routers, lies in how they interpret the address information in each data packet being sent over the network. Each of them helps the package along its way, by performing its own unique function. Here's what they do.

If we take Aust Post as an example, when you drop a letter into the letter box and it turns up at the mail sorting centre, they first look at the state you're sending it to. If it's going to a different state, they don't bother to read the city or street name and number. They simply send it off to the mail sorting centres in that destination state. The people there then look to see which city it's destined for. That's all they're interested in. They promptly send it off to that city and it becomes the problem of that city's mail sorting centre. This centre then reads the postcode and sends it to the local post office. And the local post office hands it to the postman, who reads the street name and number. So basically they all play their little role in making the letter reach its destination, but each performs a slightly different function.

Hubs, switches and routers are like these different processing centres. Each is only interested in what it needs to know to send the packet along on its way. Their combined contributions help a network run the way it does.

The Hub.

Hubs are devices with many ports (jacks into which network cables can plug in). Assume 4 computers are plugged into a hub – computer A, B, C and D. Lets imagine that computer A wants to send a message to computer C. Computer A's network card puts the data onto the network cable along with the IP and MAC address of the destination computer C. This data travels as electrical signals to the hub. Now the hub has to send the data to computer C. However hubs are not very intelligent devices. They don't understand IP addresses and MAC addresses. So the hub repeats the packet it received from computer A out through all its other ports hoping that one of the other computers plugged into it is the destination. That



way the same packet gets sent to computer B, computer C and computer D. Of course only computer C will accept the package because it has its address on it, while computer B and D simply discard it. As you see a hub is simply a multi-port repeater. It takes data signals in through one port, and repeats everything out through all the other ports, hoping that one of the computers plugged into it is the destination computer.

The disadvantage of this behaviour is that it causes unnecessary traffic. By sending out the same signal to every computer, it clogs up the lines keeping them busy and preventing other data from being sent over them.

The Switch

A switch is as a smart hub. It's a hub that understands MAC addresses (but not IP addresses). Let's look at the same situation – computer A, B, C and D, only this time they're plugged into a switch. Computer A decides to send a packet to computer C. The packet travels from computer A to the switch. Now this is where things work differently. A switch automatically learns the MAC addresses of all the computers plugged into it by communicating with them. It stores these in a little table. When it receives the packet from computer A, it reads the MAC address of the destination computer off the packet. It then looks up its table and says "Ah! I have a computer with this MAC address connected to one of my ports". And it proceeds to send that packet out through that port, and no other. So the packet goes only to computer C and not to computer B and D. This way the only cables being used are the ones that need to be, and the rest of the network is free to transfer other data.

The Router

The router, like the switch, is a smart hub. However, while the switch only concerns itself with MAC addresses, the router only concerns itself with IP addresses. And it doesn't concern itself with the individual IP address, but only the form of the IP address. Remember, not only are IP addresses unique to each computer on a network, the entire network takes on the same form of IP address. If you have two networks, one with computers that have IP addresses of the form 128.0.0.x, and the other with computers that have IP addresses of the form 64.0.0.x, you could plug a router in the centre between these two networks. If a computer within one network tried to communicate with another computer in its own network, the router would notice that the form of the destination IP address is the same as that of the network from which the message originated. Obviously the message was meant for a computer within this network itself. So the router would not allow this packet to pass through it – it would block it. It would make sure that information remained isolated within that network only but would not pass it onto any other computer in that network. But if a computer in one network wanted to communicate with a computer in the other network,



the router would allow the package to be sent into the other network. This way it allows two networks to communicate with each other, while at the same time limiting traffic to a bare minimum.

So, why not just replace switches with routers. That is possible in some situations, but not all. What if you had three computers with IP addresses 128.0.0.1, 128.0.0.2, and 128.0.0.3 connected to a router. All 3 IP addresses are of the form 128.0.0.x. If one computer tried to send a packet to the other, the router would think to itself “The IP address of the destination is of the same form as the IP address of the sender. The destination computer must obviously be on the same network. I should not allow this packet through me”. And so the packet would be blocked off and communication would be impossible.

It is possible to do away with hubs and just use switches in place of them, but switches are usually more expensive than hubs.

It's hard to make a comeback when you haven't been anywhere. Nana V.

SO!!! If you have two or more computers that you wish to connect to the internet, you will need 1 hub and 1 router. All computers will be connected to the hub and the hub will be connected to the router. The router will be connected directly to your internet service provider. Usually, these days, your ISP will provide you with a “black box” that contains both, you connect your computers to the “black box” via Ethernet cables and to the ISP via a phone line.

Firewalls

If you were to use your ISP's provided “Black Box” for a broadband connection, the main point of entry for anything from the internet would be through your router. All routers come with a basic firewall. If a hacker does break through that firewall, he won't be breaking into your computer, he will be breaking into the router. He's not going to find anything of value on your router. So routers are pretty safe however, you should reset the routers password for security, don't leave it as 1A2B3C4D5 as is the default for a lot of them

Regardless of what some people say, the Windows Firewall that comes with your operating system, when your computer is connected to the net via a router, is enough protection as far as I'm concerned.

Security

If you get a home wireless router, don't accept all the default values and end up with an SSID (Service Set Identifier) of Bigpond2649 or some other 'default' name. If you do the chances of having your bandwidth stolen are very high, unless you are on a remote cattle station or similar. A nearby neighbour could log on accidentally when the software on his/her machine tries to automatically just pick a connection that works. Or, someone could just park out in the street in

front of your house, with their laptop, and log onto your system. It's best to set up a form of encryption, choose a name other than the default name and for a little bit of extra security on the cheap, don't broadcast the SSID name. It might be easier to initially broadcast the SSID and once all of the devices have been set up, go back to the router setup and change it not to broadcast SSID.

It is easier to get older than it is to get wiser. Nana V.