# Six steps to security

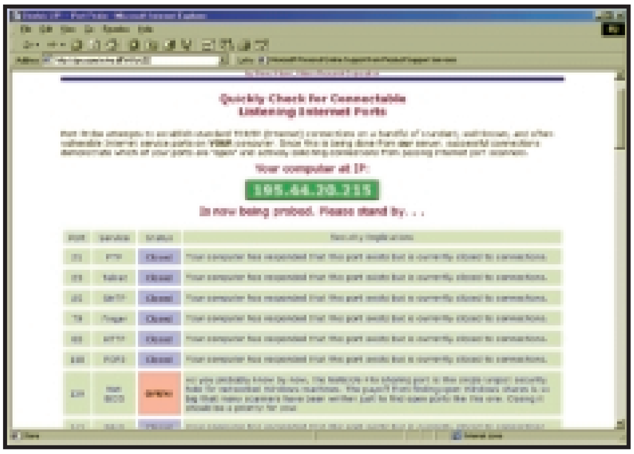
**Roger Gann takes those first, all-important steps in Internet safety – ignore them at your peril.**

At the moment, for the vast majority of casual Internet users, security isn't a significant problem. This is because most of us use dial-up to access our ISP via modems – we connect, do our Internet business, and then disconnect. We connect at random intervals, for random periods, which makes life pretty awkward for any wannabe hackers. And, just to make their life even more difficult, every time we connect, most of us are given a dynamic IP address, that is, we get a different IP address every single time we connect. So, even if a hacker did cotton on to your IP address and gain access to your PC, they could only do their dastardly deeds during that particular session, 'cos the next time you logged on, you'd be allocated a completely different IP address and they'd have a devil of a job trying to track you down again.

So far so good. But later on this year, the Internet security situation will change for the worse as more and more of us are blessed with Internet nirvana – continuous connections in the shape of ADSL and cable-modem fixed links. This will undoubtedly mean the blessed ones will stay hooked up to the Internet for much longer periods than before and expose themselves to greater security risks, simply because hackers will have more 'working' time to devote to their black arts.

Some users will no doubt leave their PCs on around the clock, listening to web broadcasts or enjoying other bandwidth-hungry tasks that were beyond economic feasibility under the old dial-up regime. These users may not know it, but they'll be running extraordinary security risks. Believe it or not, hacking is actually facilitated by these new technologies.

For example, while DSL networks are switched and users do not share transport media, cable modem networks are essentially LANs: cable users can share a common segment and thus may not only see other users' resource broadcasts but the actual data streams as well. US reports of users being able to browse their neighbours' hard disks have been common.



Quickly Check for Connectable Listening Internet Ports

Your computer at IP:

195.44.20.215

Is now being probed. Please stand by . . .

*Check out Steve Gibson's website and probe your ports*

Now, while it's true to say that in the UK ADSL and cable modem users will also be allocated dynamic IP addresses, which does reduce the exposure to risk somewhat, it's also likely that the 'leases' on these dynamic IP addresses will be relatively lengthy, perhaps as long as 24 hours, which is long enough for a teenager with too much spare time to have a real good rummage about on your hard disk before they lose the connection.

If you think I'm scare mongering, you could do a lot worse than to pay a visit to Steve Gibson's excellent website at http://grc.com. Steve wrote the excellent SpinRite hard disk repair utility; he also blew the lid off the Iomega Zip Click of Death problem with his clever Trouble in Paradise diagnostic program. Check out his Shields Up Page and get it to probe your ports – my guess is that you'll be very surprised at what it'll reveal.

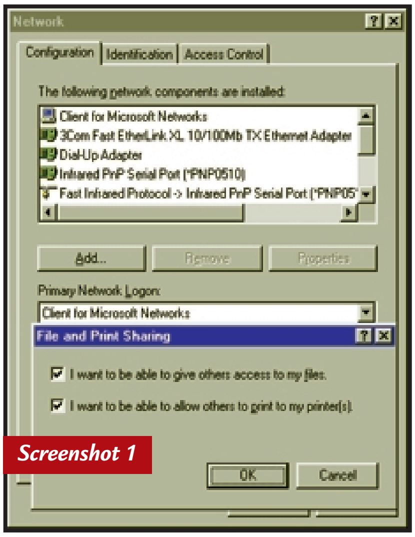
OK, that's enough bad news for now. The good news is that you can significantly tighten up your Internet security very easily and at no cost – all you have to do is tweak your network settings. Just run through the following checklist and you'll tighten your Internet security no end. Note that these tips are aimed largely at Windows 9x, which is particularly feeble when it comes to security; Windows NT has a far superior (although not perfect) security model. It also applies to standalone PCs as well as those forming part of a LAN.

## Security checklist

### 1 Turn off file and printer sharing

This is the very first thing you should do. When the Microsoft networking client is installed, TCP/IP File and Printer Sharing is turned on by default, binding the NetBIOS protocol to the TCP/IP protocol. This default setting generously extends your computer's file sharing services out across the entire Internet, something you're probably not aware of and you'd rather wasn't happening.

This amounts to a major breach in security and yet Microsoft has only lately seen the light: recent versions of Windows now display a warning message about this when you install TCP/IP. To turn it off, bring up the Properties for Networking, click the File and Print Sharing button and uncheck the two tick boxes (see screenshot 1). This kills *all* file and Printer Sharing. However, if your PC is on a network, just turn off File and



Network

The following network components are installed:

- Client for Microsoft Networks
- 3Com Fast EtherLink XL 10/100Mb TX Ethernet Adapter
- Dial-Up Adapter
- Infrared PnP Serial Port (*PNP0510)
- Fast Infrared Protocol -> Infrared PnP Serial Port (*PNP05

Primary Network Logon:

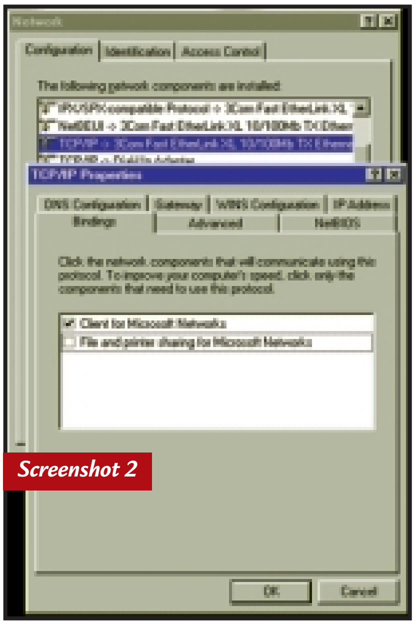
Client for Microsoft Networks

File and Print Sharing

☑ I want to be able to give others access to my files.

☑ I want to be able to allow others to print to my printer(s).

Screenshot 1



Network
Configuration | Identification | Access Control
The following network components are installed:
IPX/SPX-compatible Protocol -> 3Com Fast EtherLink XL
NetBEUI -> 3Com Fast EtherLink XL 10/100Mb TX Ethern
TCP/IP -> 3Com Fast EtherLink XL 10/100Mb TX Ethern
TCP/IP -> Dial-Up Adapter

TCP/IP Properties
DNS Configuration | Gateway | WINS Configuration | IP Address
Bindings | Advanced | NetBIOS
Click the network components that will communicate using this protocol. To improve your computer's speed, click only the components that need to use this protocol.
☑ Client for Microsoft Networks
□ File and printer sharing for Microsoft Networks

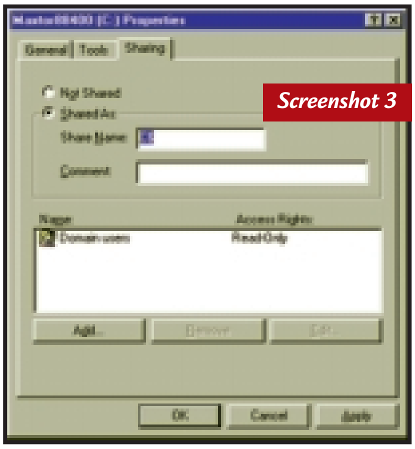
*Screenshot 2*

Printer Sharing for TCP/IP – select TCP/IP and click Properties, then uncheck the File and Printer Sharing tick box (see screenshot 2).

**2 Remove the Client for Microsoft Networks** If your PC is not connected to a LAN you don't need this client to achieve an Internet connection; it's only required when connecting your Microsoft operating system to other Microsoft OSs. You're strongly advised to remove it: when installed, the NetBIOS file-sharing ports 137-139 are opened and if the Networking Client is bound to the TCP/IP transport (as it is by default), Windows will be broadcasting your user, computer and workgroup names out over the Internet. Useful to hackers but very unhealthy for you.

**3 Passwords** If you're running a network and must have File and Printer sharing switched on, make sure your network shares are properly password protected. This is particularly important, given that Windows 9x doesn't offer any protection against password crackers or software that bombards your login prompts with a hail of passwords until it finds the right one. They work by using dictionaries (more correctly, lexicons) and run through every word in the list until they hit on the password you're using. By contrast, secure systems, such as NT4, will notify users of failed attempts or completely lock out remote access after a number of password failures. The solution is simple: don't use real words or proper names but use long strings of mixed alphanumeric characters. I know it's a pain, but if a password is guessable what's the point in having one?

**4 Hidden shares** If your PC is on a network that has Internet access then you can greatly improve security by hiding your shared network resources using the simple trick of adding a $ to its share name. This prevents that share from appearing in browse lists – so if you share your Drive C as 'C' it'll be visible, but it'll be invisible if shared as C$ (see screenshot 3). OK, this makes browsing impossible for all users, but security never makes life easier. One other thing, please don't use obvious share names either. Simply sharing Drive C as 'C$' wouldn't stop many hackers for too long. Better still, share individual folders or files rather than complete drives.



Maxtor88400 (C:) Properties
General | Tools | Sharing
○ Not Shared
● Shared As:
Share Name: C$
Comment:

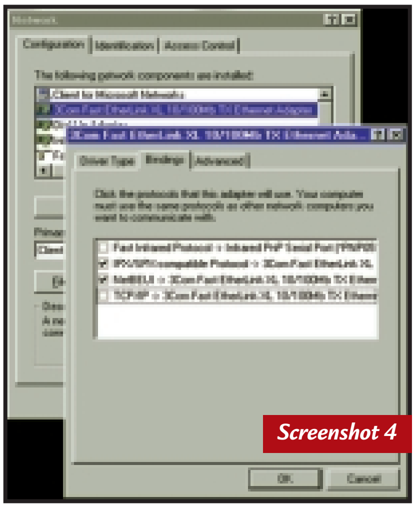
| Name | Access Rights |
|---|---|
| Domain users | Read Only |

*Screenshot 3*

**5 Bind TCP/IP only as necessary** By default, Windows 9x helpfully binds an installed network protocol to every network device. This does help guarantee that a network will work from the start but from a security point of view, it's decidedly dodgy.

Take a networked PC with dial-up Internet access – it'll have a network interface card (NIC) and a Dial-Up Adaptor installed as network devices. Windows 9x will have bound TCP/IP to both of these devices, when strictly speaking it's only the dial-up networking adaptor that requires access to the TCP/IP protocol. By leaving TCP/IP bound to the NIC, it exposes your network to attack from hackers, but by unbinding TCP/IP from the NIC, you limit external intrusion to just that PC.

To do this right-click the Network Neighborhood icon, select Properties and click on the network adaptor then click the Properties button. Finally, select the Bindings tab and uncheck the TCP/IP box (see screenshot 4). If you do have cable or ADSL Internet access, you'll have a second NIC installed to connect to that hardware. If you unbind TCP/IP from the NIC, make sure it's the right one!



Network
Configuration | Identification | Access Control
The following network components are installed:
Client for Microsoft Networks
3Com Fast EtherLink XL 10/100Mb TX Ethernet Adapter
Dial-Up Adapter

3Com Fast EtherLink XL 10/100Mb TX Ethernet Ada...
Driver Type | Bindings | Advanced
Click the protocols that this adapter will use. Your computer must use the same protocols as other network computers you want to communicate with.
□ Fast Infrared Protocol -> Infrared PnP Serial Port (*PNP0510)
☑ IPX/SPX-compatible Protocol -> 3Com Fast EtherLink XL
☑ NetBEUI -> 3Com Fast EtherLink XL 10/100Mb TX Ethern
□ TCP/IP -> 3Com Fast EtherLink XL 10/100Mb TX Ethern

*Screenshot 4*

**6 Remove TCP/IP from workstations that don't need it** If you're running a LAN and some workstations don't have or need Internet access then they don't need the TCP/IP protocol installed. Put another way, only those workstations that access the Internet need TCP/IP. For simple peer-to-peer connectivity good old unrouteable NetBEUI is perfect from a security point of view. If you're running client/server, then resort to IPX/SPX instead.

## Last words

These suggestions are just a starting point and other weaknesses in your system security will remain – just about any sort of Internet access is beset with security issues. Loopholes have been found in Microsoft's Personal Web Server, IRC, ICQ, TelNet, web browsers, email readers – the list is endless. You should keep your Windows 9x system as up-to-date as possible by running Windows Update regularly. Next month I'll be keeping the Internet-security fires stoked with a look at personal firewall software.

## CONTACTS

Roger Gann can be contacted at the usual *PCW* address or by emailing:
**networks@pcw.co.uk**