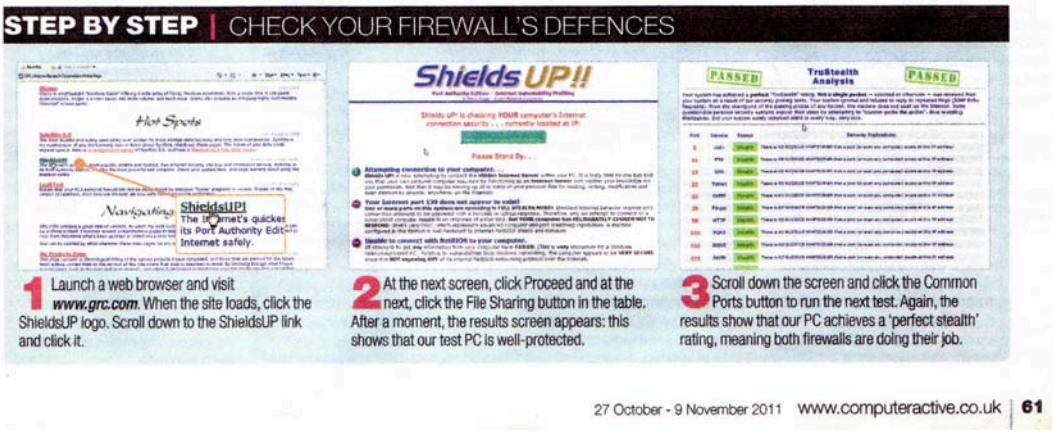
SUSSEX NHW FEDERATION

CYBER CRIME - PREVENTION MEASURE

Ever wished that you were better informed? The bad guys are getting better so how can you re-assure yourself?

The Sussex NHW Federation is not endorsing this, but provides it on an 'information sharing' basis. Comparisons *(in italics)* are however made to NHW crime prevention advice and guidance to aid understanding.

This advice was sourced from the fortnightly magazine Computer Active dated 27 October to 9 November 2011. **www.computeractive.co.uk**


STEP BY STEP | CHECK YOUR FIREWALL'S DEFENCES

Shields UP!!

PASSED TruStealth Analysis PASSED

1 Launch a web browser and visit www.grc.com. When the site loads, click the ShieldsUP logo. Scroll down to the ShieldsUP link and click it.

2 At the next screen, click Proceed and at the next, click the File Sharing button in the table. After a moment, the results screen appears: this shows that our test PC is well-protected.

3 Scroll down the screen and click the Common Ports button to run the next test. Again, the results show that our PC achieves a 'perfect stealth' rating, meaning both firewalls are doing their job.

27 October - 9 November 2011 www.computeractive.co.uk | 61

It is a test that you can do at home of the 'firewall' defences within your Windows based home computer and any additional firewall within your modem / (cabled / wireless) router box. The additional firewall is important as the modem / router box is where your local house network (wired / cabled / wireless) is connected.

A firewall is a barrier between the internet / world-wide-web and your own computer or network.

Think of it as a highly dedicated security guard who stops anyone coming into your computer if they're not on the guest list, and anyone leaving if they don't have permission.	*NHW*

However, a firewall provides limited or no protection against the following:

- If it is switched off, disabled or contains many exceptions or **open ports**.
- If you or a virus has created a **back door** through the firewall.

Think 'open ports' = windows left open or ajar. *Think 'back doors' = back doors open whilst you answer the front door.*	*NHW*

Also if you have large hard disc drive storage (giving remote access away from home) this may also be connected directly (cabled) to the router box.

The test program has been devised by a 'White Knight' (good guys) as opposed to the 'Black Knights' (hackers) and to undertake it you will have to trust / authorise the test to be undertaken. You choose to use this free test facility.

The 'White Knight' is **Steven Gibson**, an American software engineer, security researcher, and IT security proponent. In the early 1980s, Gibson was best known for his work on light pen technology for use with Apple and Atari systems. He now runs a company called Gibson Research Corporation (GRC).

His 'White Knight' research probe tests covered **81,000,000 routers** around the world over 5.5 months (June – December 2012) which comprised of 1,500 different router types and comprising 6,900 models. Out of the 81 million routers 0 (zero) should be exposed. He found **23,000,000** were exposed to a 'remote code execution' (i.e. not hacker proof). That is 22% failed!! All the modem manufacturers / distributers were very interested in his results but not all may have issued or offered you up-dated software.
{see 'You Tube' video under References below}

This test program called 'Shields Up' has now been used on over **96,714,104** computers world-wide. ShieldsUP! has arguably taken the lead to become the Net's most authoritative and reliable Internet port vulnerability scanning facility.

For your home computer this is a 'Stealth Test' to see if:- • *Your computer 'Talks to Strangers' and gives away family secrets;* • *How promiscuous it is on the internet;* • *How invisible your computer is on the internet.*	*NHW*

1.	Launch an internet Web Browser (Internet Explorer / Moxilla Firefox / Google Chrome)	
2.	Type in and visit web site www.grc.com	
3.	When the site loads, scroll down the page and click on the **ShieldsUP link**.	
4.	At the next screen, click **Proceed**	
5.	At the next screen, click **File Sharing** button in the table.	
6.	After a moment the results screen appears in a text box. This should show and report that your Personal Computer is well protected.	
7.	*I leave my filing cabinet un-locked – please help yourself.*	*NHW*
8.	Scroll down the screen and click **Common Ports** button to run the next test.	

	Wait about 5 seconds.	
9.	Again the results should show 'Passed' banners that your Personal Computer achieves a perfect 'Stealth Rating'. (i.e. meaning <u>both</u> Firewalls are doing their job) {Firewall in your computer + firewall in your router/modem}	
10.	*Are all my downstairs doors and windows shut and locked?*	*NHW*
11.	Click on **All ServicePorts** button to run the next assurance test. Wait one minute for a complete scan.	
12.	Results should be displayed in a text box and show 'Passed' icons and 1,056 ports should all be green or maybe some blue. If any are red you have a problem.	
13.	*Are all my doors and windows shut and locked?*	*NHW*
14.	Click on **Messenger Spam Test** button to run the next test. (optional) 'Spam me with this note'.	
15.	The note in the box should NOT appear as 'Messenger Service' pop-up box somewhere on your screen.	
16.	*No junk mail / scam mail here please.*	*NHW*
17.	Click on **Modem / Router Test** icon to run the next test. This a UPnP Internet Exposure Test (Plug and Play). Wait five seconds.	
18.	Results should be displayed in text box and hopefully be green. Also might say 'Did not respond to probe' or 'Rejected probe'. 22% of the world's routers fail this test!!	
19.	*My main front door key should be in the lock inside my house, not I leave my key in the lock outside my main front door so that others may pop in at anytime.*	*NHW*
20.	If there is a Gaming / X box / Skype facility in your household try to get UPnP configured as **OFF**. This stops exposure to the world wide web / public internet.	
21.	*This is equivalent to creating a 'No Cold Calling Zone' at your front door.*	*NHW*
22.	After satisfactory test results you may leave or find and delete the following test files if you wish:- • Shoot the messenger[1].exe • Securable[1].exe • Mousetrap[1].exe	

References

1. Computer Active magazine Active Page 61 dated 27 October to 9 November 2011. **www.computeractive.co.uk**
2. You Tube video. **https//www.youtube.com/watch?v=WEa43qM4jQ#t=09m44s**
3. Titled 'Security Now' – Steve Gibson. Watch from 9 mins 44 secs onwards by dragging slider along

FIREWALLS

Because the internet is a public network, any connected computer can find and connect to any other connected computer. A firewall is a barrier between the internet and your own computer or network. Think of it as a highly dedicated security guard who stops anyone coming into your computer if they're not on the guest list, and anyone leaving if they don't have permission.

Get started...

- *Ensure your firewall is switched on at all times.*

A firewall protects you against:

- Hackers breaking into your computer.
- Worms – types of viruses that spread from computer to computer over the internet.
- Some outgoing traffic originating from a virus infection.

What a firewall does NOT do:

A firewall isn't sufficient on its own to guarantee security, but it is the first line of defence. You also need to take the other protective steps outlined on this website. However, a firewall provides limited or no protection against the following:

- If you give permission for other computers to connect to yours.
- If it is switched off, disabled or contains many exceptions or open ports.
- Most viruses.
- Spam.
- Spyware installations.
- Any kind of fraud or criminal activity online.
- If you or a virus has created a back door through the firewall.
- People with physical access to your computer or network.
- Data introduced to the computer other than online, eg via USB connected devices, CD/DVD etc.
- Attacks after a network has been compromised.
- Traffic that appears to be legitimate.

However, none of these things give a reason NOT to install a firewall, as this alone is not enough for complete security.
It is safest to assume that your internet service provider does NOT provide any kind of firewall, so make sure you have the right software to protect yourself.

Types of firewalls

Personal firewalls

Personal firewalls should be installed on each computer that is connected to the internet and monitors (and blocks, where necessary) internet traffic. They are also sometimes known as 'software firewalls' or 'desktop firewalls'.
Windows Firewall is a basic personal firewall. It is free, included with Windows operating systems. In Windows 8, Windows 7 and Vista, the Firewall defaults to active, so you do not need to worry about configuring it yourself.

If you wish, you could replace Windows Firewall with another personal firewall of your choice, including the type incorporated in some internet security packages, or standalone firewall software which can be downloaded from the internet, some of which is free of charge.

Hardware firewalls
Medium-sized and large businesses may need a hardware firewall – in addition to personal firewalls – depending on the configuration of their IT infrastructure. Your internal or external IT support resource will be able to recommend, source, install and configure the most suitable one for your business needs.

Check if your Windows Firewall is switched on:

In Windows 8 and Windows 7, go to **Control Panel**, select **System and Security**, then select Windows Firewall. The Windows Firewall state is indicated under Home or work (private) networks.

In Windows Vista, go to Control Panel, select Security, then select Windows Firewall. The Windows Firewall state is indicated.
In Windows XP, go to Control Panel, select Security Center. The Windows Firewall state is indicated.

Source: www.getsafeonline.org.uk