Dacorum U3A

Computer Support Group

29th March 2019

Agenda

- Open forum
- Identify subjects for breakout groups and later meetings
- Cyber Security presentation
- Tea and Coffee break (about 3.00 pm?)
- Continue Presentation
- Breakout groups looking at individual problems

Cyber Security

This presentation will look at various aspects of ensuring that you remain secure when using the World Wide Web

- Your connection to the Web
- Email connection
- Web pages
- The Dark Web

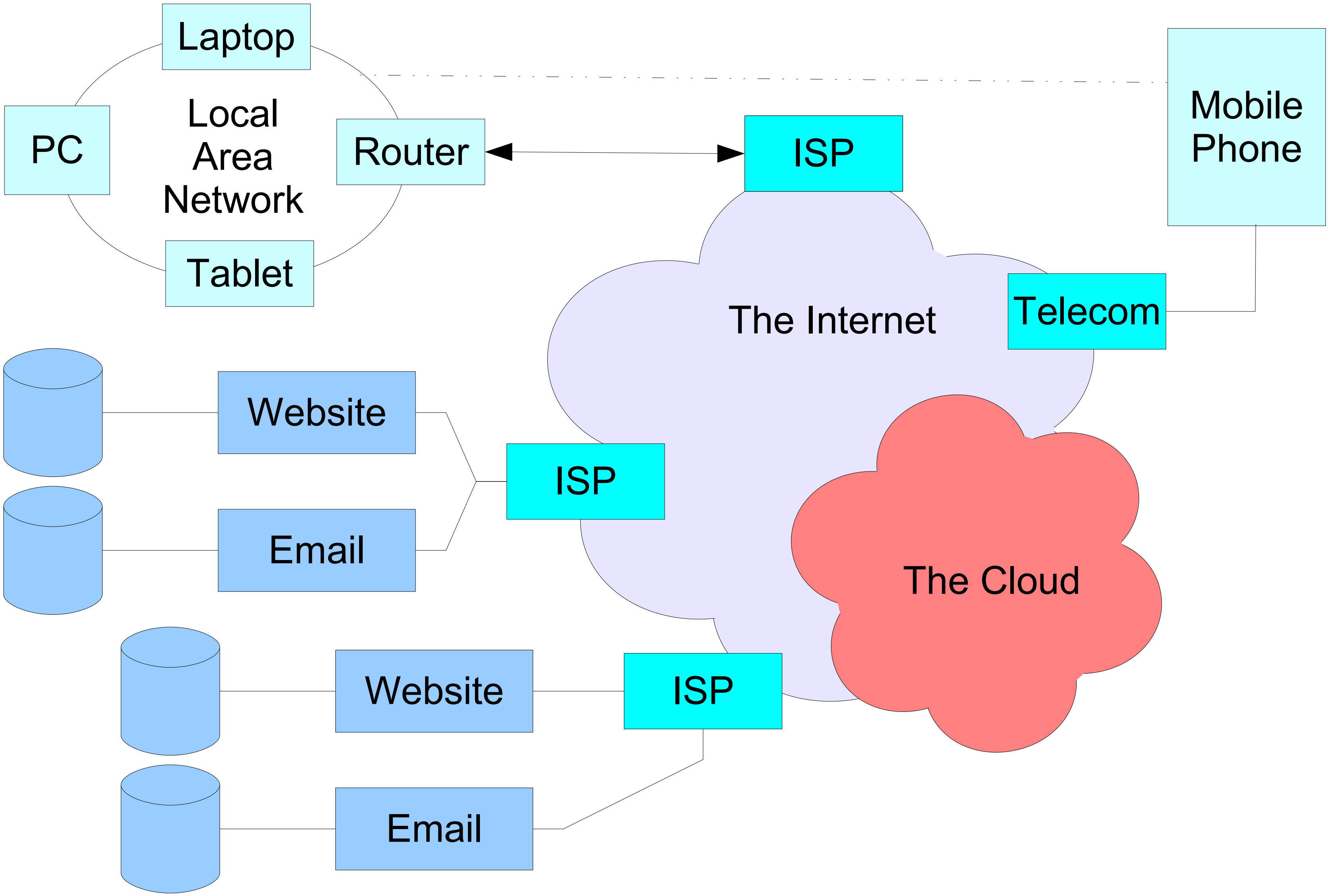
The Internet

The Internet consists of 3 parts:

- Local Area Networks (LAN)
  - If you have a router, you have a LAN
- Global inter-connections (closely related to the Cloud)
- Servers
- A computer on a LAN can be a server, e.g. a printer is, in many ways, a server.

The following diagram is a simplified view

Network View



Connection of a Mobile

If a mobile phone or tablet that is connected directly to mobile provider for Internet or Email purposes, there will be not be a Local area Network (LAN) involved.

In this case, the connection is encrypted using information in the Sim card.

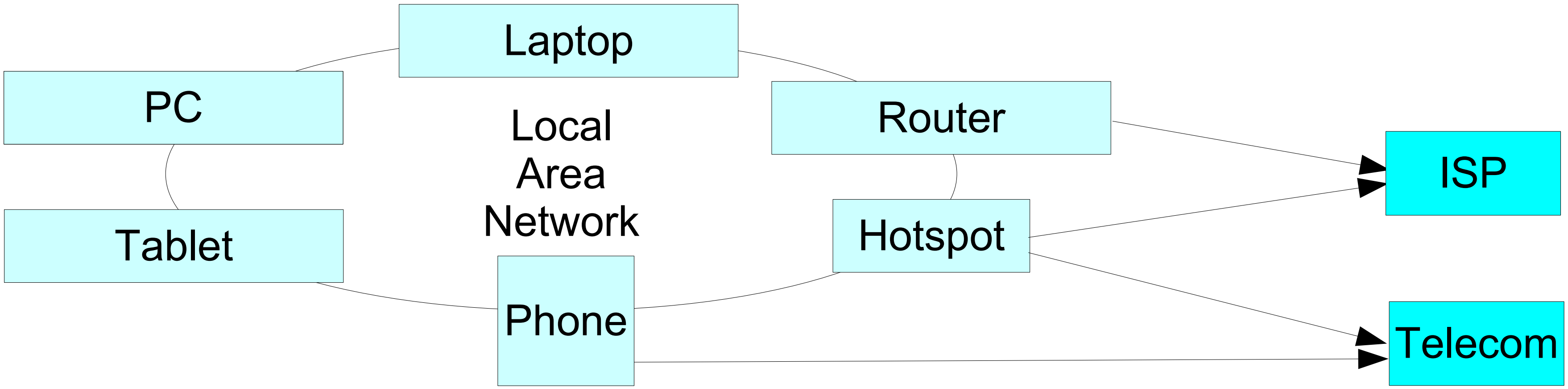
If the connection is not connected in this way then there will be a LAN and the provisions below will come into play.

Local Area Network

With exception of a mobile (see above), there will be is a LAN even if only there is only one device is involved.

The Network will consist of at least an Internet interface device (Router) and one or more device(s) whether PC, Laptop, Tablet or Mobile Phone. The Router can be connected to the Internet through a telephone line/optical fibre. Alternatively it can be a mobile ‘phone’ connected through the mobile network.

Your local network

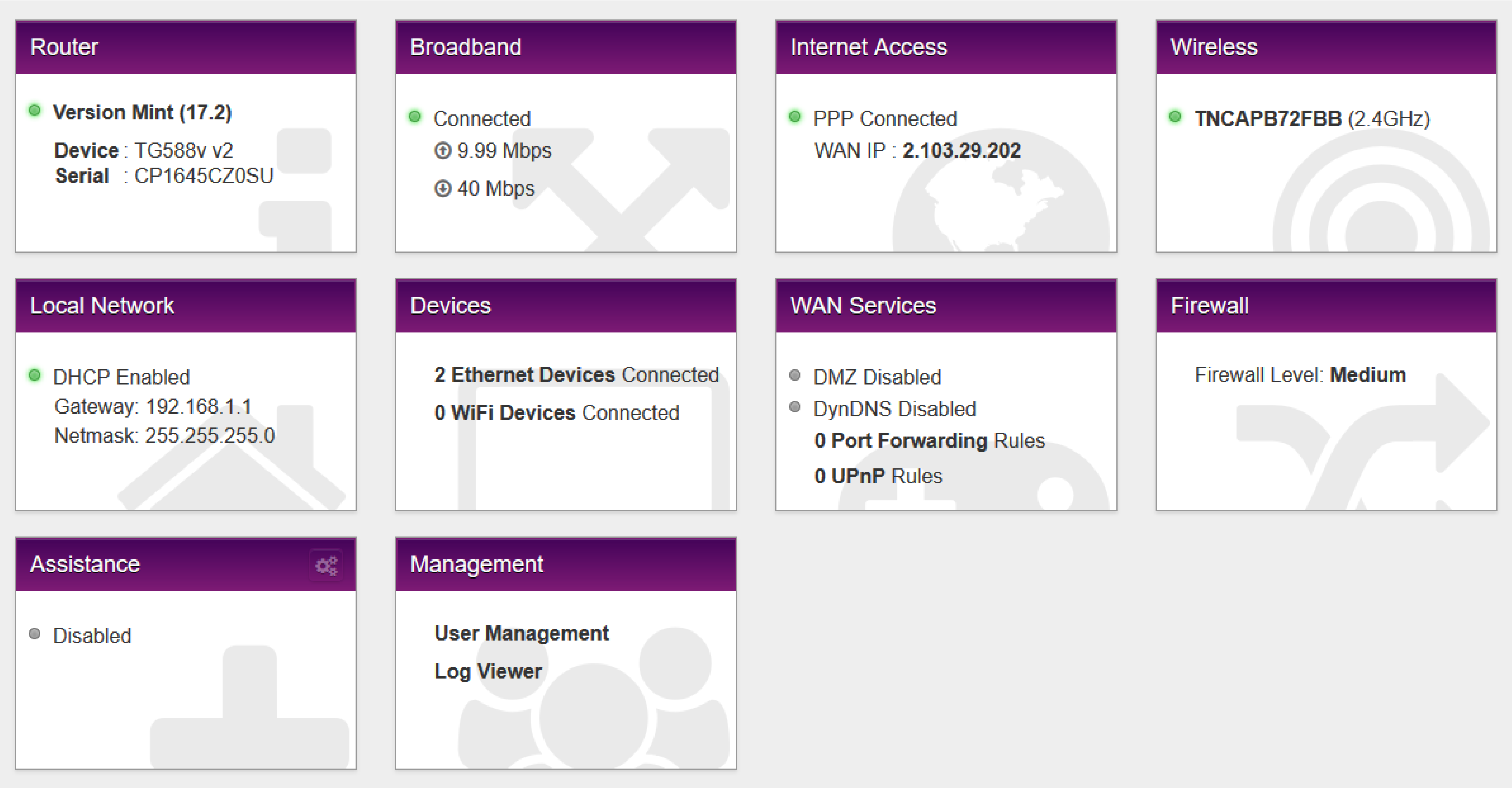


Physical connection can be:

- – Physical Cable
- – Home Plug
- – WiFi direct or via a ‘hotspot’
- – Mobile Phone direct or as a ‘hopspot’

Router

The router will probably be configurable it will probaly be addressable as 192.168.1.1. Eg:



Router

- ● **Version Mint (17.2)**

  Device : TG588v v2
  Serial : CP1645CZ0SU

Broadband

- ● Connected

  ⇧ 9.99 Mbps

  ⇩ 40 Mbps

Internet Access

- ● PPP Connected

  WAN IP : **2.103.29.202**

Wireless

- ● **TNCAPB72FBB** (2.4GHz)

Local Network

- ● DHCP Enabled

  Gateway: 192.168.1.1
  Netmask: 255.255.255.0

Devices

2 Ethernet Devices Connected

0 WiFi Devices Connected

WAN Services

- ● DMZ Disabled
- ● DynDNS Disabled

  0 Port Forwarding Rules

  0 UPnP Rules

Firewall

Firewall Level: **Medium**

Assistance

- ● Disabled

Management

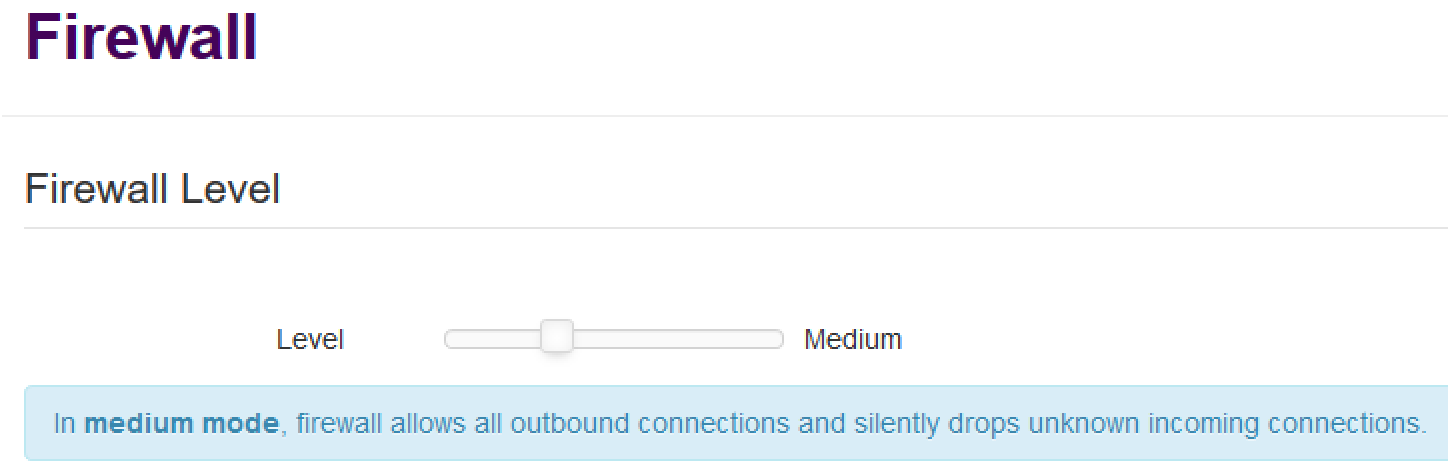
User Management

Log Viewer

Router 2

Each make of router will have a different display format and control possibilities. All will have a password. Many have a known default, if so, always change it.

Probably has a firewall which applies to all devices in the LAN. Eg:



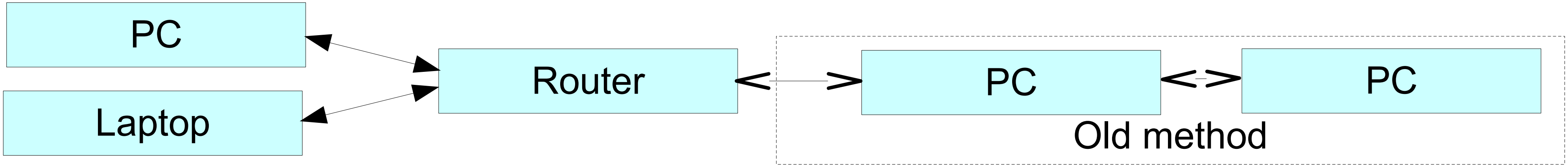
Firewall

Firewall Level

Level Medium

In **medium mode**, firewall allows all outbound connections and silently drops unknown incoming connections.

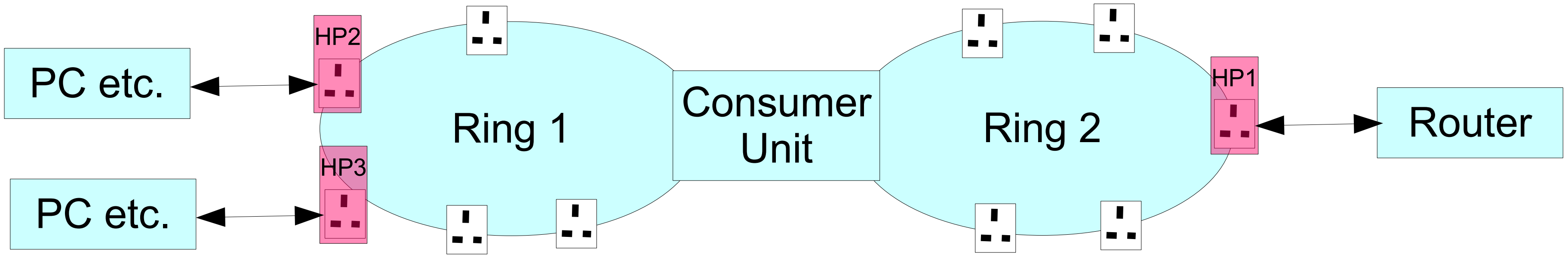
Physical Cable



Separate cable from router to each device (old 'daisy chain' connection not used now)

- Very secure as you have full control to the cables
- Many devices (phones, tablets etc.) have no port to connect cable to
- Limited number of 'ports' on the router separate splitter would be required

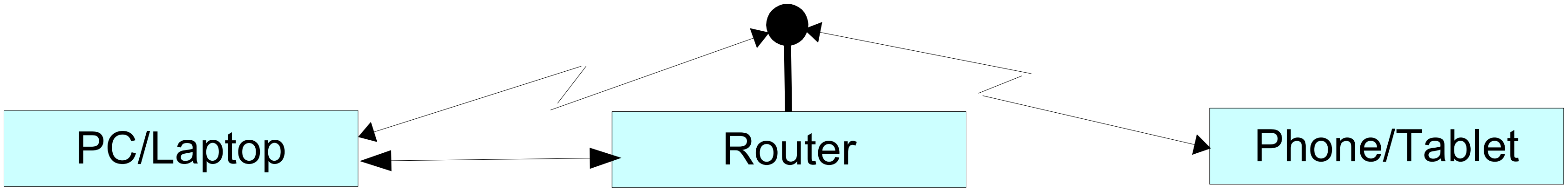
Home Phone



Uses the House wiring to provide the LAN connections. Any home plug can be plugged into any mains socket.

- Effectively no limit on the number of connections (only 1 connection used by the router).
- Each home plug must be ‘added’ before it can connect. User has complete control over the plugs.
- Security is very high as the signal should not be able able to pass through the electricity meter.
- Network can extend as far as the mains goes.

Wifi through router



The router can send/receive a wifi signal to any devices within range. The wifi can be public (have no password) or private (with a password).

If it is public, there is NO security. Any device within range can receive and potentially record all messages through the router.

Wifi through router 2

If it is private then all messages are encrypted so are secure. Note however that many routers have a default, well known password so security depends on whether the default has been changed.

– The security depends on the router password. Communication between the router and the devices are encrypted.

– The password controls whether an individual device can connect to the LAN

– If it is not connected then the encryption key will not be set

Other ‘networks’

A Wifi device can connect to any router within range. That is it can connect to a neighbour’s network (probably requires the password!)

In addition, many places provide Wifi access either to the internet or to local services. Eg trains, buses, shopping centres, libraries, hotels, B&B etc.

Many of these are public (no security), some require a login but may still be insecure (remember that all devices on a network can will be able to receive all wifi messages.

Mobile Phone

A mobile phone can connected directly to the mobile telephone network or to a LAN (through wifi). In the latter case, it will not be included in the phone’s data allowance but will be included in the LAN’s data allowance.

A mobile phone can also be used as a ‘hotspot’. In effect this is a router with only wifi communications.

Virtual Private Network (VPN)

VPNs provide a ‘secure’ way to connect to another point on the network. They were originally intended to allow a company to set up a server for its staff to use with secure access.

They can be used by anybody but there are question marks on both their security and usefulness:

- The connection is to a single point. Onward connection is through the ‘normal’ internet
- The single point could be hacked, giving access to anything entered.
- Some email servers ‘blacklist’ email origins. With a VPN, the origin will not be your ISP.

VPN 2

Another system, related to a VPN is ‘Rapport’. This provides extra protection, not to a single endpoint but rather to communications to individual websites.

This applies to many Bank systems so is probably a useful facility. Many Banks provide the system for free.

The Dark Web

Another system similar to VPN is what is known as the Dark Web. This is a set of Web sites where access is invisible to the authorities.

It uses the normal web but uses special browsers which provide specialised connection to special websites (rather like a VPN). That website initiates a connection to another similar site and so end. After many of these connections, the endpoint is effectively obscured.

Although this is all within the standard web, most of the elements are slightly different.

Website access

Probably the most likely way in which viruses can enter a system is through a Website.

In may cases, it is impossible for a user to know whether a site is safe or not. This reflects that fact that **any** website could become infected through hacking.

There are many vulnerabilities to website use:

- Installing software
- Installing an Add-on
- Websites which use a piece of hacked code

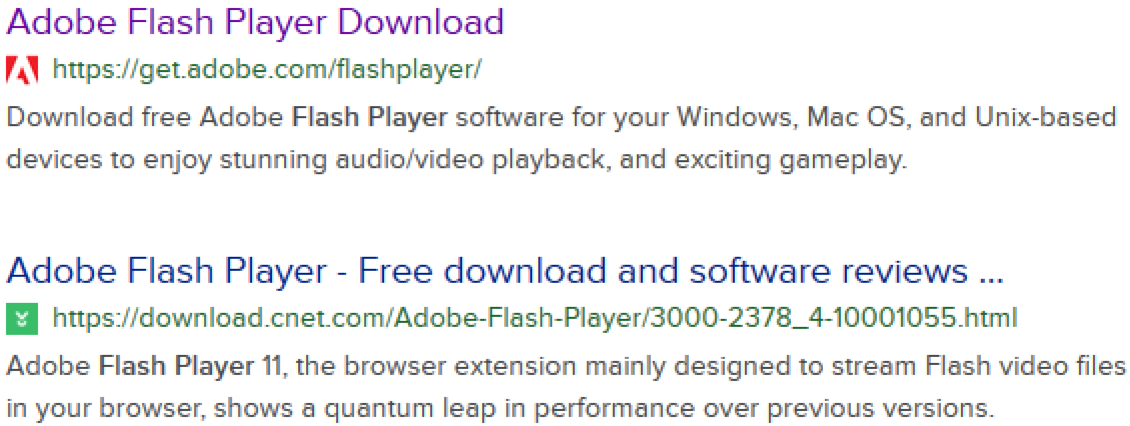
Installing Software

Ensure that the site **is** the owner of the software.

- Remember that the URL is decoded from the right. So barclays.bank.co.uk is not necessarily barclays but barclays.co.uk probably is
- The company name might be different from the software name e.g. CCleaner comes from Piriform.
- Software is commonly installed in two or more stages (the first stage downloads the next) so that running the downloaded file through a virus checked doesn’t mean much

Installing Software 2

- Download only from the company site



Adobe Flash Player Download

https://get.adobe.com/flashplayer/

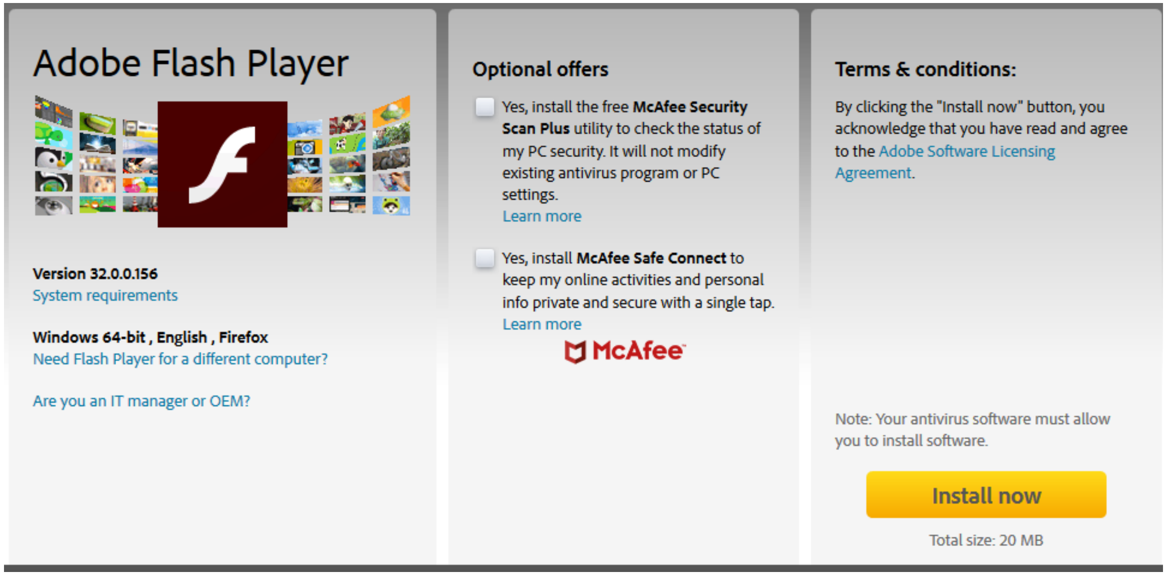
Download free Adobe **Flash Player** software for your Windows, Mac OS, and Unix-based devices to enjoy stunning audio/video playback, and exciting gameplay.

Adobe Flash Player - Free download and software reviews ...

https://download.cnet.com/Adobe-Flash-Player/3000-2378_4-10001055.html

Adobe **Flash Player** 11, the browser extension mainly designed to stream Flash video files in your browser, shows a quantum leap in performance over previous versions.

- Beware of optional software, only install it if you want it



Adobe Flash Player

Version 32.0.0.156

System requirements

Windows 64-bit , English , Firefox

Need Flash Player for a different computer?

Are you an IT manager or OEM?

Optional offers

☐ Yes, install the free **McAfee Security Scan Plus** utility to check the status of my PC security. It will not modify existing antivirus program or PC settings.
Learn more

☐ Yes, install **McAfee Safe Connect** to keep my online activities and personal info private and secure with a single tap.
Learn more

Terms & conditions:

By clicking the "Install now" button, you acknowledge that you have read and agree to the Adobe Software Licensing Agreement.

Note: Your antivirus software must allow you to install software.

Total size: 20 MB

Add ons

Although these should be OK, there is no guarantee

Any program that is installed effectively bypasses many of the safeguards so be sceptical!

Passwords

Ensure that you use a different password for each site.

Use a password vault if you have problems with this.

Personally I record information that modifies something that only I know the answer to (and can remember!)

Include numeric and non alpha characters such as :, ; # etc (different sites have different rules)

Online Banking

Probably the safest is an electronic device provided by the bank that you insert a smart card, enter the PIN and then enter the resulting value into the website in lieu of a password.

The next safest is a device that you enter the PIN but which doesn’t require the smart card.

Always ensure that your virus software includes a key logger.

Email

Generally reading emails does not pose any risk.

However there are some situation where care is required:

- Following (clicking on) a link of any sort
- Replying to an unexpected email or from an unknown source
- Where the email does not appear to come from where it purports to
- Pleas for money from relatives/acquaintances
- Threats

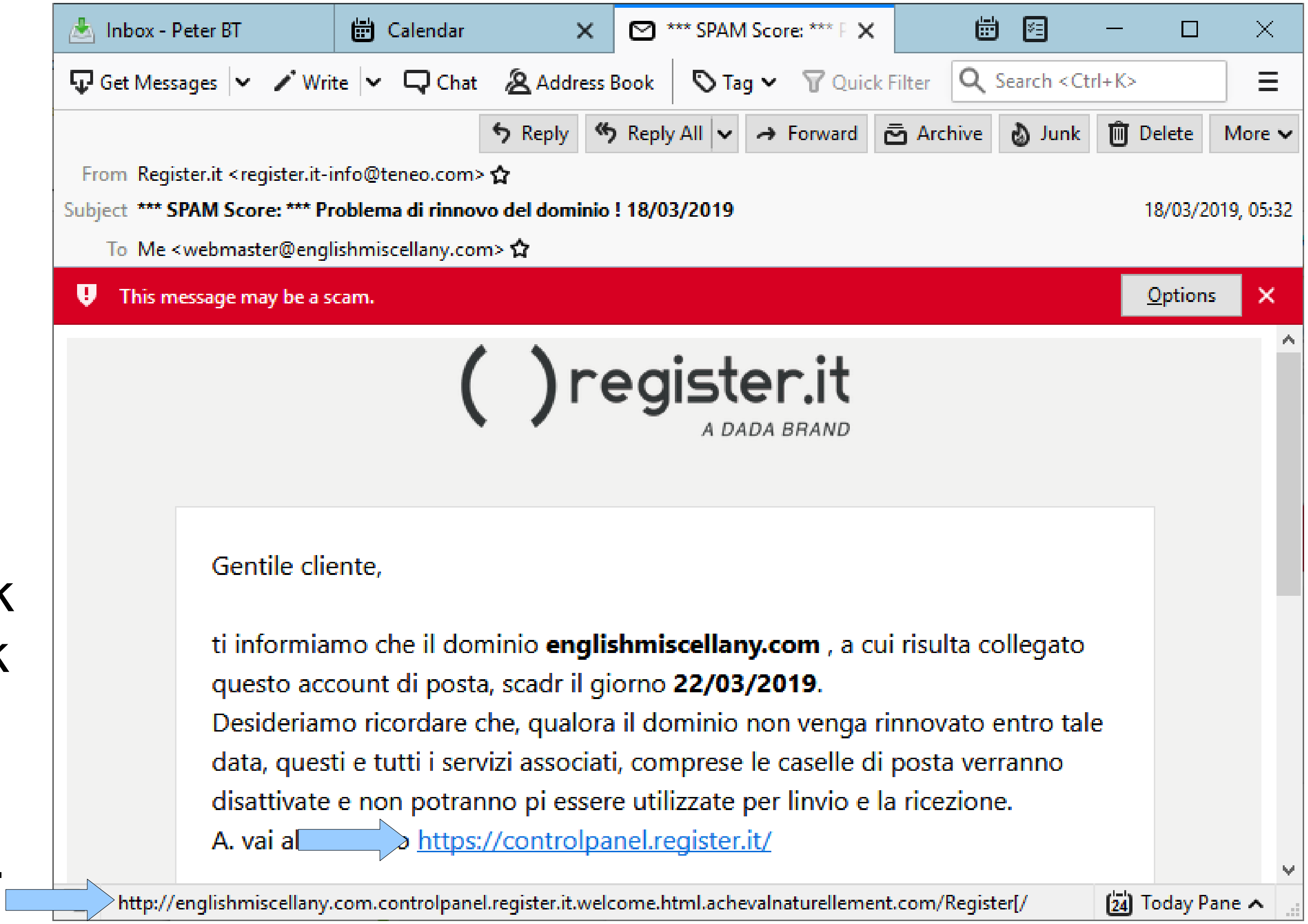
Clicking on an email link

It is always good to check that the link is what it appears to be. The text on the link does not have to agree with where the link points.

Not only is this email in Italian for english miscellany but the link doesn't even vaguely reference 'register.it'.

To see where it points hover over it (Thunderbird). Other email systems will have other methods of viewing the link source (probably right click on the link).

Clicking on it may also tell them that you have read it.



From Register.it <register.it-info@teneo.com>

Subject *** SPAM Score: *** Problema di rinnovo del dominio ! 18/03/2019 18/03/2019, 05:32

To Me <webmaster@englishmiscellany.com>

This message may be a scam.

( )register.it
A DADA BRAND

Gentile cliente,

ti informiamo che il dominio **englishmiscellany.com** , a cui risulta collegato questo account di posta, scadr il giorno **22/03/2019**.
Desideriamo ricordare che, qualora il dominio non venga rinnovato entro tale data, questi e tutti i servizi associati, comprese le caselle di posta verranno disattivate e non potranno pi essere utilizzate per linvio e la ricezione.
A. vai al o https://controlpanel.register.it/

http://englishmiscellany.com.controlpanel.register.it.welcome.html.achevalnaturellement.com/Register[/

Clicking on an email link 2

Note that it is not safe to click on a document link as they can contain macros which can contain viruses. If you really want to see the contents then **save** the file and open it with the ‘no macro’ open set.

Saving a file shold not be dangerous. However, if you save it then run it through your anti virus program before opening it.

Email not what they purport

Emails purporting to come from a Bank or the tax office are relatively common. If the email is just to inform you of a secure communication then this is probably OK.

If you were to look at the link, it would probably look just like the bank’s login page; this is because it is! The large amount of html (webpage code) will have been minutely changed to send the login request not to the bank’s system.

Unexpected emails

An unexpected email may just be an attempt to see if the email address is (still) valid. If no reply is heard, the original sender doesn’t know if it is working or not.

Also, if the (apparent sender) is known, it may be that their address book has been hacked (not that uncommon). It is very easy to forge the sending address.

I have seen many such emails with a link to goo.gle/…..

Pleas for money

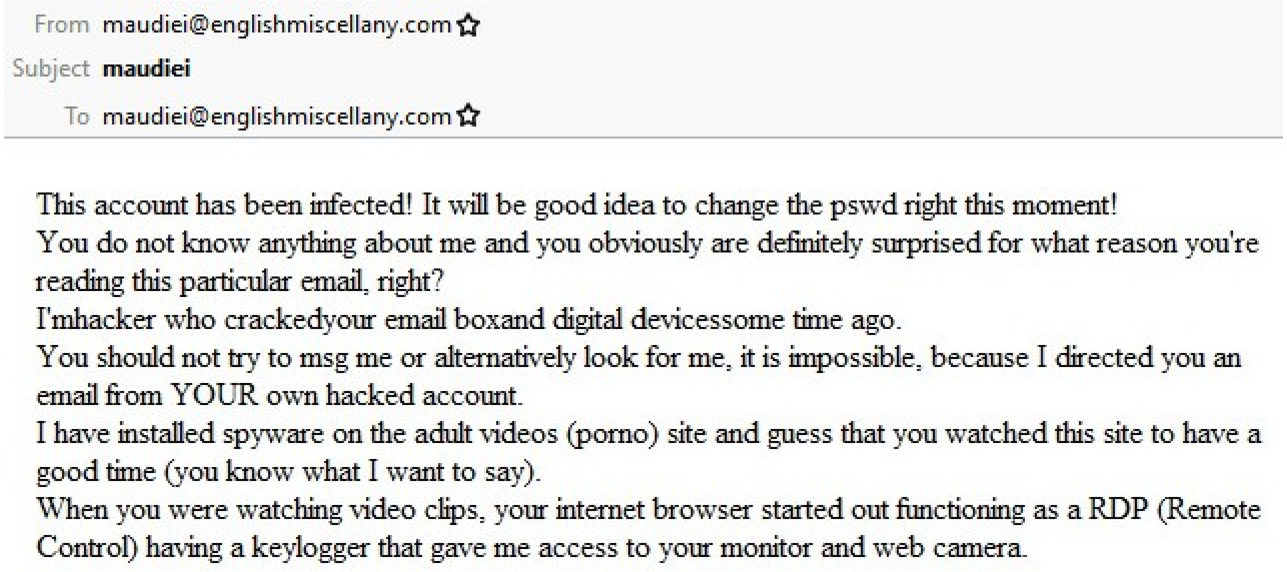
A favourite ploy by fraudsters is to get a user’s address book (by hacking).

Then emails are sent to people who are obviously relations claiming that he hacked person is stranded abroad without funds and asking for funds to be sent to an account.

These are almost always fictitious. Always check by talking to the person (they would normally be able to make a reverse charge call from wherever they are.)

Email Threats

Here is an email I received. The email address is invalid so I got it as postmaster for the domain.



From maudiei@englishmiscellany.com ☆
Subject **maudiei**
To maudiei@englishmiscellany.com ☆

This account has been infected! It will be good idea to change the pswd right this moment!
You do not know anything about me and you obviously are definitely surprised for what reason you're reading this particular email, right?
I'mhacker who crackedyour email boxand digital devicessome time ago.
You should not try to msg me or alternatively look for me, it is impossible, because I directed you an email from YOUR own hacked account.
I have installed spyware on the adult videos (porno) site and guess that you watched this site to have a good time (you know what I want to say).
When you were watching video clips, your internet browser started out functioning as a RDP (Remote Control) having a keylogger that gave me access to your monitor and web camera.

Note that it appears to have come from the same invalid email address as it was sent to (typical of people who want to hide their identity. Further down it also claims to have inserted a pixel to know whether the receiver has read it; this isn’t true, it is just a jpeg.

Don’t believe what this type of thing says!

Sending sensitive info

Remember, email contents are inherently unsafe. Many email systems do not even allow encryption.

If it is necessary to communicate account info, passwords, etc. Do so in parts using different methods.

This could be part by email and part by text or telephone. It is very unlikely that anyone could intercept both parts.

To make it even more secure do so on different days.

Sandbox

A sandbox is a software system that allows a program to run in an environment which is separate from the rest of the system. This allows a program which may adversely affect the system.

This is not a panacea for testing programs, especially new ones. A virus program will probably not immediately show itself when running it in a sandbox.

However, it is a safe way to follow links from emails.

Anti Virus

Anti virus systems are not 100% effective vigilance is still required (even if for no other reason, it takes time for detection of a new virus to be added).

Apparently, malware on a USB stick may not be detected early.

Which seems to suggest that AVG Free is amongst the best.

Firewall

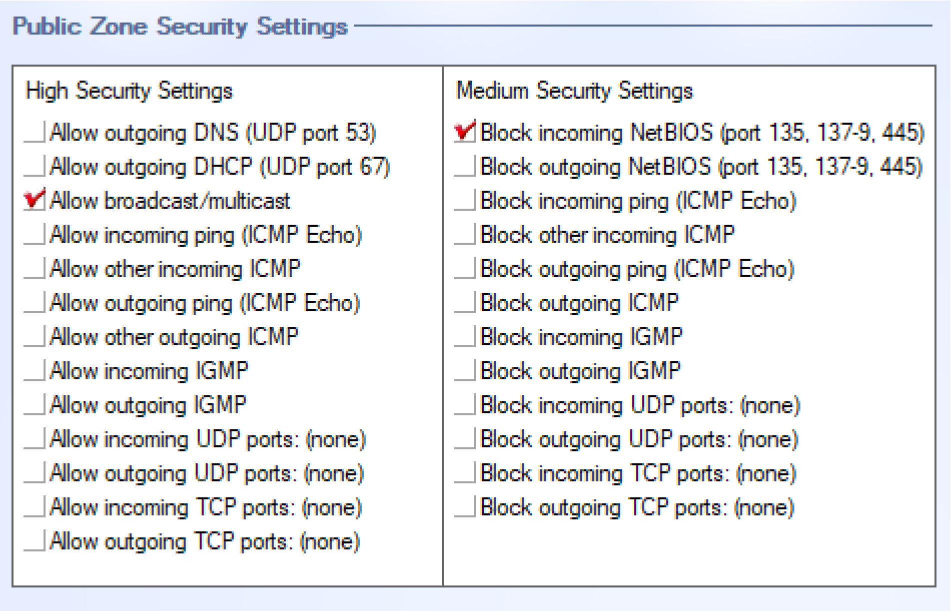
A firewall is designed to protect a computer from external attacks. It does this by recognising ‘unusual’ messages being sent/received from the network.

The router will probably have a simple firewall.

Windows (not XP) has Windows Defender

Firewall 2

Some firewalls are configurable and allow control over individual network messages and restrict access across the LAN.



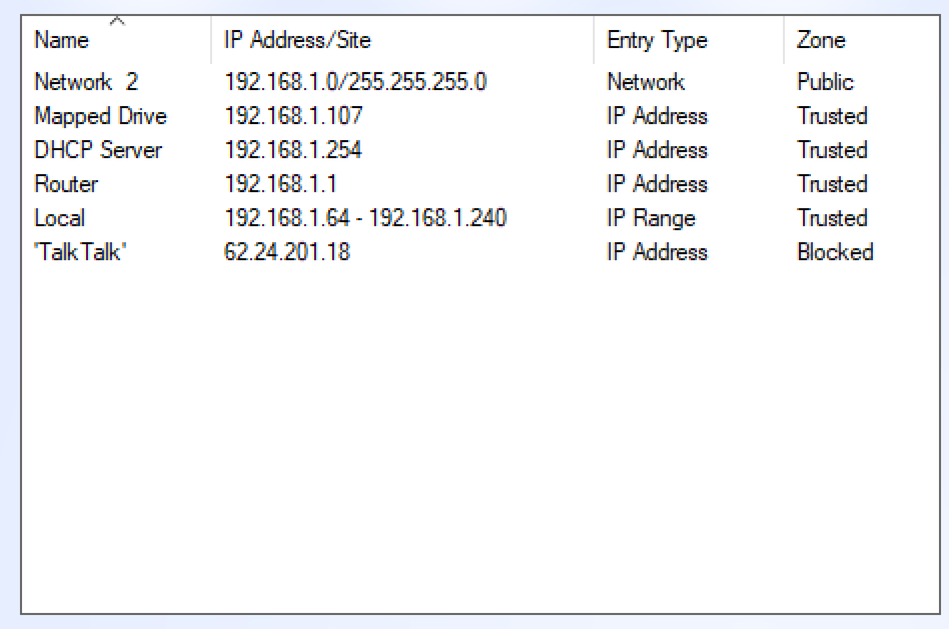
Public Zone Security Settings

High Security Settings

- ☐ Allow outgoing DNS (UDP port 53)
- ☐ Allow outgoing DHCP (UDP port 67)
- ☑ Allow broadcast/multicast
- ☐ Allow incoming ping (ICMP Echo)
- ☐ Allow other incoming ICMP
- ☐ Allow outgoing ping (ICMP Echo)
- ☐ Allow other outgoing ICMP
- ☐ Allow incoming IGMP
- ☐ Allow outgoing IGMP
- ☐ Allow incoming UDP ports: (none)
- ☐ Allow outgoing UDP ports: (none)
- ☐ Allow incoming TCP ports: (none)
- ☐ Allow outgoing TCP ports: (none)

Medium Security Settings

- ☑ Block incoming NetBIOS (port 135, 137-9, 445)
- ☐ Block outgoing NetBIOS (port 135, 137-9, 445)
- ☐ Block incoming ping (ICMP Echo)
- ☐ Block other incoming ICMP
- ☐ Block outgoing ping (ICMP Echo)
- ☐ Block outgoing ICMP
- ☐ Block incoming IGMP
- ☐ Block outgoing IGMP
- ☐ Block incoming UDP ports: (none)
- ☐ Block outgoing UDP ports: (none)
- ☐ Block incoming TCP ports: (none)
- ☐ Block outgoing TCP ports: (none)



Name	IP Address/Site	Entry Type	Zone
Network 2	192.168.1.0/255.255.255.0	Network	Public
Mapped Drive	192.168.1.107	IP Address	Trusted
DHCP Server	192.168.1.254	IP Address	Trusted
Router	192.168.1.1	IP Address	Trusted
Local	192.168.1.64 - 192.168.1.240	IP Range	Trusted
'TalkTalk'	62.24.201.18	IP Address	Blocked

Summary

Don’t Panic!

Be Careful