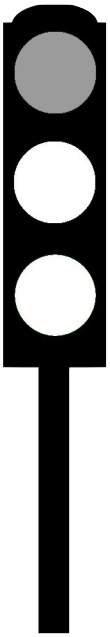
Red

FOR THE SERIOUSLY ACTIVE

Do everything in Green and Amber, then do these:



>Don't use Windows – use Linux

>Don’t use a smartphone at all

>Use Heavy Duty passwords

>Review your security regularly - watch out for new threats

>Encrypt your whole hard drive (should the data even be on the computer?)

>Clean out your emails regularly

>Avoid installing P2P programmes

>Avoid random disks / downloaded software. Only use your Linux distribution's own software repositories

>Don't store encryption keys on your computer – use removable disks and take them away

>Regularly check file/folder permissions and settings

>Don't let your computer run any services available to the internet – eg FTP, webserver. If you do run any services make sure your firewall is secure

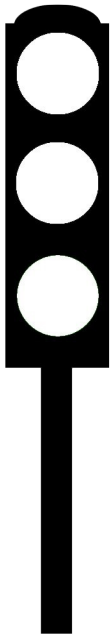
>Remove your hard drive and use Linux LiveCDs (with encrypted USB keys for the data)

>Use internet cafés randomly, use fake webmail accounts

COMPUTER SECURITY

Worried about viruses, Big Brother and computer security in general?

A simple practical guide to keep you and your computer safe



The Traffic Lights project is for people who want to know the basic steps to keep themselves safe when on the internet or just using computers.

Not everyone needs the same kind of security, so we have divided security measures into three levels – just choose the one that best fits your activities and needs:

Green is what everyone should be doing – no matter whether or not they are a campaigner.

Amber is an increased level of security for campaigners to aspire to.

Red is for those facing (or expecting) direct state or corporate interest.

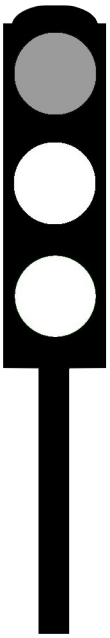
These are just outlines and suggestions for general use – at times you may want to use greater security. For details on any suggestions search the net.

This card has been designed for you to fold it up and stand it next to your computer as a quick guide and a regular reminder to take care out there...

Red

FOR THE SERIOUSLY ACTIVE

Do everything in Green and Amber, then do these:



>Don't use Windows – use Linux

>Don’t use a smartphone at all

>Use Heavy Duty passwords

>Review your security regularly - watch out for new threats

>Encrypt your whole hard drive (should the data even be on the computer?)

>Clean out your emails regularly

>Avoid installing P2P programmes

>Avoid random disks / downloaded software. Only use your Linux distribution's own software repositories

>Don't store encryption keys on your computer – use removable disks and take them away

>Regularly check file/folder permissions and other settings

>Don't let your computer run any services available to the internet – eg FTP, webserver. If you do run any services make sure your firewall is secure

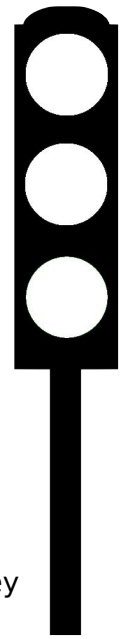
>Remove your hard drive and use Linux LiveCDs (with encrypted USB keys for the data)

>Use internet cafés randomly, use fake webmail accounts

COMPUTER SECURITY

Worried about viruses, Big Brother and computer security in general?

A simple practical guide to keep you and your computer safe



Download from: www.seedsforchange.org.uk/free/computersecuritypostcard.pdf v2.4 8/14

The Traffic Lights project is for people who want to know the basic steps to keep themselves safe when on the internet or just using computers.

Not everyone needs the same kind of security, so we have divided security measures into three levels – just choose the one that best fits your activities and needs:

Green is what everyone should be doing – no matter whether or not they are a campaigner.

Amber is an increased level of security for campaigners to aspire to.

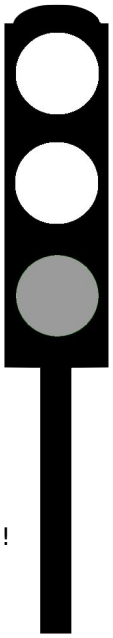
Red is for those facing (or expecting) direct state or corporate interest.

These are just outlines and suggestions for general use – at times you may want to use greater security. For details on any suggestions search the net.

This card has been designed for you to fold it up and stand it next to your computer as a quick guide and a regular reminder to take care out there...

Green

BASIC TIPS FOR EVERYONE



>*(Windows only)* Install anti-virus, firewall and spyware detection programmes. Make sure these are active and update regularly

>Don't open email attachments or download random software

>Don't put your regular email address anywhere on the web

>Delete spam, learn how to use spam filters

>Use decent passwords, don't post them on the side of your screen or under your keyboard!

>Don't allow others to use your email

>Don't use Chrome, Internet Explorer or Outlook – try Firefox (web browser) and Thunderbird (email) instead

>Don't use MS-Office – try Libreoffice.org instead

>Don't use social networking sites, ask friends not to post information (incl. photos) about you

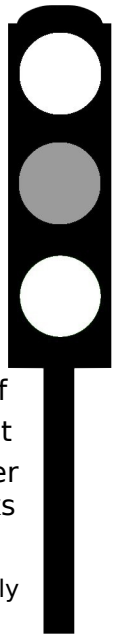
>Check your physical security – use chains to lock your computer down

>Maintain your computer and keep it tidy, especially your files and directories

>Change to Email providers using StartTLS, (eg aktivix.org, riseup.net). Consider using PGP or GPG

Amber

PROTECT PRIVACY AND DATA



Do everything in Green, then do these:

>Use strong passwords

>Regularly back up your files, and store them somewhere else

>Keep your software and OS up to date

>Turn off Java, Javascript and cookies on your web browser

>Don’t use a smartphone for activist stuff

>Use anonymisers (eg TOR) on the internet

>Use separate accounts on your computer and in email for different users and tasks

>Use PGP or GPG to encrypt your emails

>Check your files for metadata – particularly PDFs and MS-Office files

And, do these too:

>Regularly wipe data and free space

>Shred and/or burn printouts

>Regularly clear out tmp, cache and log folders

>Encrypt partitions/folders/files

>Switch to Linux

>Use fake details on internet accounts

>Avoid using wireless and infra-red equipment

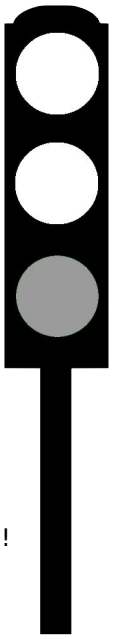
>Check that services, file sharing and file/folder permissions are set for security and privacy

>Password protect the BIOS

>Encrypt all your data

Green

BASIC TIPS FOR EVERYONE



>*(Windows only)* Install anti-virus, firewall and spyware detection programmes. Make sure these are active and update regularly

>Don't open email attachments or download random software

>Don't put your regular email address anywhere on the web

>Delete spam, learn how to use spam filters

>Use decent passwords, don't post them on the side of your screen or under your keyboard!

>Don't allow others to use your email

>Don't use Chrome, Internet Explorer or Outlook – try Firefox (web browser) and Thunderbird (email) instead

>Don't use MS-Office – try Libreoffice.org instead

>Don't use social networking sites, ask friends not to post information (incl. photos) about you

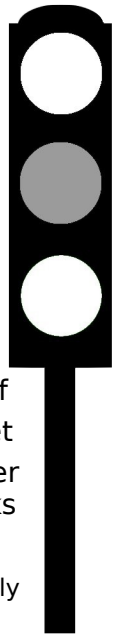
>Check your physical security – use chains to lock your computer down

>Maintain your computer and keep it tidy, especially your files and directories

>Change to an Email provider that uses StartTLS, (eg aktivix.org, riseup.net). Consider using PGP or GPG

Amber

PROTECT PRIVACY AND DATA



Do everything in Green, then do these:

>Use strong passwords

>Regularly back up your files, and store them somewhere else

>Keep your software and OS up to date

>Turn off Java, Javascript and cookies on your web browser

>Don’t use a smartphone for activist stuff

>Use anonymisers (eg TOR) on the internet

>Use separate accounts on your computer and in email for different users and tasks

>Use PGP or GPG to encrypt your emails

>Check your files for metadata – particularly PDFs and MS-Office files

And, do these too:

>Regularly wipe data and free space

>Shred and/or burn printouts

>Regularly clear out tmp, cache and log folders

>Encrypt partitions/folders/files

>Switch to Linux

>Use fake details on internet accounts

>Avoid using wireless and infra-red equipment

>Check that services, file sharing and file/folder permissions are set for security and privacy

>Password protect the BIOS

>Encrypt all your data