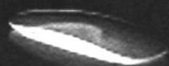
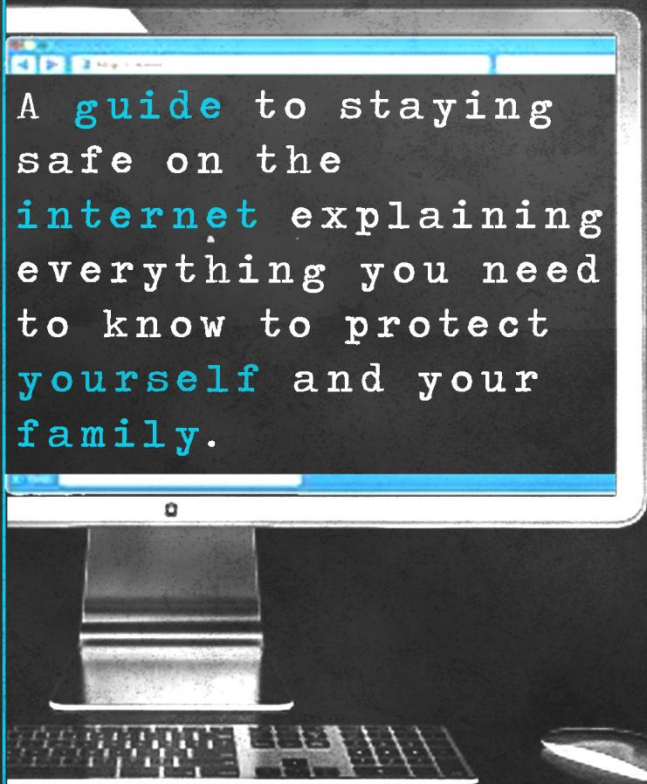


STAY SAFE USING THE INTERNET.

A
Complete
Guide!

A **guide** to staying
safe on the
internet explaining
everything you need
to know to protect
yourself and your
family.



Contents Page

Introduction	3
Internet Connection.....	3
Wi-Fi	3
Wired.....	5
LAN (Local Area Network)	6
WAN (Wide Area Network).....	8
Email Safety.....	9
Security	9
Viruses.....	11
Social Networking Safety	13
Privacy	14
Parental Guidance.....	15
Cyber Bullying	16
HTTPS	18
Disadvantages of Online shopping.....	21
Fraud and security liabilities	21
Stay safe using the internet Quiz	22
Quiz answers	27

Introduction

There are many different kind people who use the internet, some understanding the risks and some not. The internet can be a dangerous place, even though it is very helpful no matter what you ask of it. With this booklet we will help you to understand some of the benefits and risks of general factors of the internet. We will be discussing a general internet connect, Email safety, online shopping safety and social networking - safety. With this you will be able to understand the basics of all these factors which will help you to be more confident when using the internet.

Internet Connection

There are many different types of internet connections, which are used by different kinds of people, whether they are expert at computing or intermediate. The two main types of internet connection which is used are wired and wireless connection also known as WI-FI.

Wi-Fi

Wi-Fi is usually the connection that is used nowadays. It allows you to have a connection without having the



need of any wires, it is done wirelessly using the computers wireless feature which connects directly to the internet hub. There are also many advantages and disadvantages to using Wi-Fi.

Advantages of Wi-Fi

- It gives you the freedom of moving around your home or business; however you see fit and still have an internet connection.
- There will be no clutter of wires all over the place.
- No wires need to be bought for other computers, as wireless eliminates the use of wires when connecting to the internet.
- You can connect any devices you wish to the internet, whether it be mobile phones, tablets, laptops or computers using wireless connection.

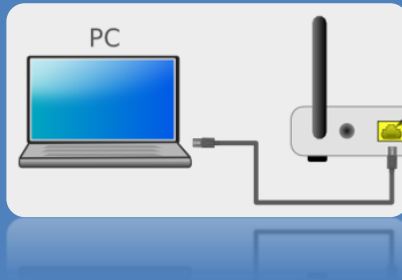
Disadvantages of Wi-Fi

- It's more difficult to setup than wired as a wireless hub is needed, and a passcode is used to connect.
- The connection can easily be lost, which means that you could easily lose connection when connecting wirelessly.

- It is more exposed to being hacked when using a wireless connection, as hackers could intercept the connection.

Wired

A wired connection is when you are connected to the internet using a wire. The wire that is used is an Ethernet cable, which can be supplied by your internet provider or purchased from many different shops. Having a wired connection has its advantage and disadvantages.



Advantages of Wired connection

- It is cheap to setup, and does not require any skill, as all that needs to be done is plug the cable into the computer or laptop which then connects to the internet provider box found in your house.
- It is a lot safer than using wireless, as less people can intercept the signal and hack into the connection. Having a wired connection

eliminates the possibility of someone being able to hack into the connection.

- It provides a stronger signal than wireless, which could possibly be the reason why you can have faster internet when using wired, which is why it is preferred to some users who tend to game using an internet connection.

Disadvantages of wired connection

- It can be difficult to setup a wired connection if the Ethernet cable is not long enough to reach the computer,
- It does not allow you to be mobile when using your laptop or device, as you always have to worry if the cable will reach where you want to go.
- If you want to use more than one computer with wired connection it could be difficult as it will make your home messy due to the clutter of all the wires.

LAN (Local Area Network)

LAN is short for Local Area Network. A local area network is used in a lot of small business, schools, or homes. A LAN is usually used to help the organisation to share information, data or software. They are expensive

to setup however is more convenient than a WAN as WAN is mainly used for much larger organisations.

Advantages of LAN

- Devices such as printers can all be shared among the computers within this LAN as well as WAN, which eliminates buying devices in excess.
- The network file server can be used for employees to save or upload work to, and will be able to be accessed at any other computer within the LAN.
- There is easy communication in LAN, which makes it easy to send information or data whenever is needed.

Disadvantages of LAN

- If problems arise the whole server could be affected, which will cost more to fix and also could be a cause of loss of important data.
- LAN needs constant maintenance, so technicians may need to be hired.



- Viruses can easily be spread if a virus was to breach the LAN.

WAN (Wide Area Network)

WAN is short for wide area network. A wide area network is mainly known to be for a larger area than a local. The network is connected over a geographic area. Many companies, governments and businesses tend to use WAN, as they want to have all employees/workers in the same network.

Advantages of WAN

- Information can be passed around a larger area and also faster than any other network.
- Devices such as printers can all be shared among the computers within this WAN, which eliminates buying devices in excess.
- Data can be updated more frequently, which means all employers will have an updated version of the data, which causes less confusion.

Disadvantages of WAN

- WAN can be very expensive and complicated to setup.

- All data can be accessed from any computer which is connected to the WAN, so this could be more affected by a security breach.

Email Safety

Email is short for electronic mail. It is widely used by everyone in the world to send and receive information to friends, family, businesses and others easily and efficiently, for absolutely free over a network. However it is important to learn how to protect yourself and your personal information from viruses and hackers so that your information will stay secure and safe.



Security

Choosing Your Password

One of the most important aspects of keeping your email account safe and secure is firstly choosing a **secure password**. Your password should be hard to guess and not something predictable. The password

should be at least 8 characters long and have a combination of upper case and lower case letters along with at least one number. Having a mix of characters like this will make it harder to guess by hackers.

An example of a good secure password would be *"AssetT689."*

Keeping Password Private

You should never disclose your password to anyone or write it down anywhere as there is more risk your account will be hacked. It is always best to not having the same password for all your accounts such as email or online banking.



Do not ever save your password if you are on a **public computer** or sharing a computer with someone else since this will keep your password in the browser making is very easy for anyone to access your account.

If you get these prompts you should always click No and after your session you should always clear the history and password history just to make sure.

Changing Your Password Every Month

To help keep your account safe more efficiently you should change your password regularly every month. This is extremely important if you use public computers on a regular basis to access your account since there is always a chance that your account may be hacked easier for public systems.

Viruses

Keep your anti-virus software up to date

Viruses can easily be transferred to your computer by emails. One of the first steps you should take to prevent this from happening is making sure you have anti-virus on your computer and updating it on a regular basis. The anti-virus will help detect any viruses and protect you from the viruses.

Always Have the Computer's Firewall On

Firewall software should always be on, doing this will help prevent people or malware from gaining access to your computer through the Internet via your emails.

Always scan your emails and attachments

Before you open any type of email it is best to always scan the email to check if there are any viruses, this is extremely important when opening emails with attachments inside since once opened it will start affecting your system straight away. If you receive an email from an unknown sender with an attachment you should never open it since it is most likely a virus.

Spam and Phishing

Spam emails are emails that are unwanted and are junk emails, which are filtered into your junk inbox. You should never open spam emails as most of them contain viruses and malware.

Even if you wish to open to unsubscribe from the email you still should not open it as opening the message will indicate to your email account that this email is wanted. So it is best just to delete these.



Social Networking Safety

Social networking is websites that allows commination between users who join that networking site. The users will have many contacts that can be like a small community of people to discuss or show point of interest on daily activities to one another. A user is able to find other users with 'Email Address' or 'Similar Interests'.

Examples of social networking sites

- Facebook
- Instagram
- Twitter
- YouTube
- My Space
- Etc.



Social networking is very large, most compared to the world we live in. Social networking can be both positive and negatives in many ways if you the user don't approach it safely.

Privacy

Social networking has issues with 'Privacy' that leads to many debates on how users information should be kept or protected. Users which want to interact with others with social networking will need to keep in mind that personal information can be accessed and personal images or videos which are uploaded by the user can be seen.

Each social networking sites as steps in place, which gives help to users to protect their information's and privacy.

Example of privacy protection for users is shown by 'Facebook' above; the user has an option to allow a set of people to see the users profile. This can be from 'Private', 'Friends' or 'Public'.

- Private – This gives you the option for the user to see their own profile and information and gives the user full protection whether if their profile can be viewed.
- Moderate (Friends) – This gives the user accepted contacts to see the users profile and access personal information.

- Public – This gives the user no protection and is then the most dangerous way of showing of the users profile. As it is public the users information can be accessed by anyone around the world.

Parental Guidance

Parents or Guardians will need to monitor the users under the age of 18. The parent is the responsible carer who is active for the sole user to oversee their communication to friends and others. The parents has an options for them to access their child under 18s information with ease to see what their child are safe online.

Parents can set passwords on what the child can view on social networking sites.

When in comes to guidance the parents can only explain how far and what the child should and shouldn't do, example to this is –

- Don't share your own password
- Don't accept no one you know
- Don't give out personal address or date of births
- Don't share mobile numbers
- Don't upload images or videos that you will regret as they will stay online forever and can be spread around really fast.

Cyber Bullying

When social networking becomes a fun environment to communicate on there often are those who would bully one user and then target them with their friends. This is a very common thing, which occurs on social networking sites. A user will be bullying a users to a point law enforcement will be involved to resolve the matter.



Cyber bullying is very dangerous as it happens 24 hours in a day, 7 days in a week. A user can be targeted on their sexual orientation or the way they look. When it comes to cyber bullying it is based on segregation or not liking a certain user.

The types of Cyber bullying that can come to affect are -

- Exploitation of messages and images of a user and can be uploaded anonymously and spread out very quickly to get the user very paranoid. As social networking is online every one will be able to have access to this.

- Fake Accounts can be created to target a user to befriend then attack when asked to meet up.

When a user feels targeted online, if they are aged 18 and younger should tell their parents or guardian who could look at the matter. An adult has more power over a minor so can be the one to go to. If bullying goes to more extreme levels then users will need to report it to the social networking site and report it to law enforcements, which will look at what has been done to the user.

The law enforcement would be able to find the user who is bullying another user and from there the matter of bullying level the user can be given an arrest for questioning and so on.

Cyber bullying is closer than you would think. As mobile phones and personal computers are in our pockets users can over see their social networking profile and be targeted by their own mobile.

Online shopping Safety

Is a form electronic commerce which lets a customer purchase a product directly over the internet using a web browser. Today many types of services and products are available online for example online goods such as electronic books streaming media and software. Retail services such as banking and food ordering can also be done in just a click of a button. An example of some of today's biggest the biggest online retailers are eBay, Amazon, and Alibaba. Online stores now play a pivotal role in the success of companies today.



HTTPS

Hypertext Transfer Protocol Secure is a type of communication protocol to ensure security over a computer network. It is used by web servers to enable them to display content safely.

HTTPS is used by most websites which collect sensitive customer data usually on e-commerce websites. There are two ways to know a website is using HTTPS. The first way is to see if there is a lock icon in the browser window pane, the second way is to look at the URL and it should start off with https://, you should always be aware that the hypertext is present to ensure security when browsing or doing online shopping.



Security questions

A security question is used as an extra security measure for authentication; this procedure is usually carried out by banks, cable companies, and wireless providers. Security questions came into wide spread use from the year 2000, it was mainly used as a safety precaution as a self-service system when resetting a password.

It is essential that this type of procedure is carried out in all online shopping websites as users may tend to forget their password for their accounts which may hold sensitive information.

This procedure reduces the risk for users not only for online shopping but for emails and other online accounts.

Advantages of Online Shopping

Practicality

Online stores are usually available 24 hours a day. Most customers have internet connection from either their home or workplace, they could also shop online on the go on their mobile phone or tablet, and because of the internet's efficiency you would be able to shop on the go, e.g. on a bus journey. Most online stores also have fair return policies to give customers assurance.

Reviews and feedback

Most online stores describe products with text or images and multimedia files to give a description. Some online stores also provide additional product information such as instructions, demonstrations, manufacturing terms and safety precautions which should be carried out.

Price and options

One main advantage online shopping provides is the ability to compare prices and show all competitors

available. This tool allows customers to choose the best product for them and which option that is most practical e.g. shipping and the cost of each item for example offers may vary between two sellers on a website such as eBay based on their policy.

Disadvantages of online shopping

Fraud and security liabilities

Although there are many security measurements taken for online shopping there are still a few risk factors which customers should look out for. For example when purchasing products from a website such as eBay some customers are misled with false information or a picture of the product may not be what you expect as a customer as you cannot physically inspect the product.

Unclear cost disclosure

Cost disclosure which is not clear may cause issues for some customers, although it is easy to do prices comparisons with competing shops it may not be straight forward to get the final price of an item upfront, additional fees such as tax, vat and shipping may not be clearly stated, in some cases customers purchasing products from international seas end up paying VAT separately.

Stay safe using the internet Quiz

This is the quiz section of the booklet if you are viewing this on **PDF** all you have to do is press the answer you think is correct and you will find out if your answer is correct or wrong.

If you are reading the **book version** then simply circle your answers and find out the answers on [page 27](#) where the correct answers will be highlighted green.

1. Which type of internet connection gives a stronger signal?

a) Wired

b) Wireless

2. Which type of internet connection is safer from hackers?

a) Wired

b) Wireless

3. Who should you share your passwords with?

a) Family

b) Friends

c) No one

4. What to do if you receive a suspicious email?

a) Open it

b) Delete it

c) Reply

d) Download
Attachment

5. Best privacy option for social networking sites to keep personal information safe?

a) Private

b) Moderate

c) Public

6. What to do if someone adds you who you don't know?

a) Block and Decline Invitation

b) Accept

c) Meet them

7. What to ensure when shopping online?

a) Website Looks Nice

b) HTTPS

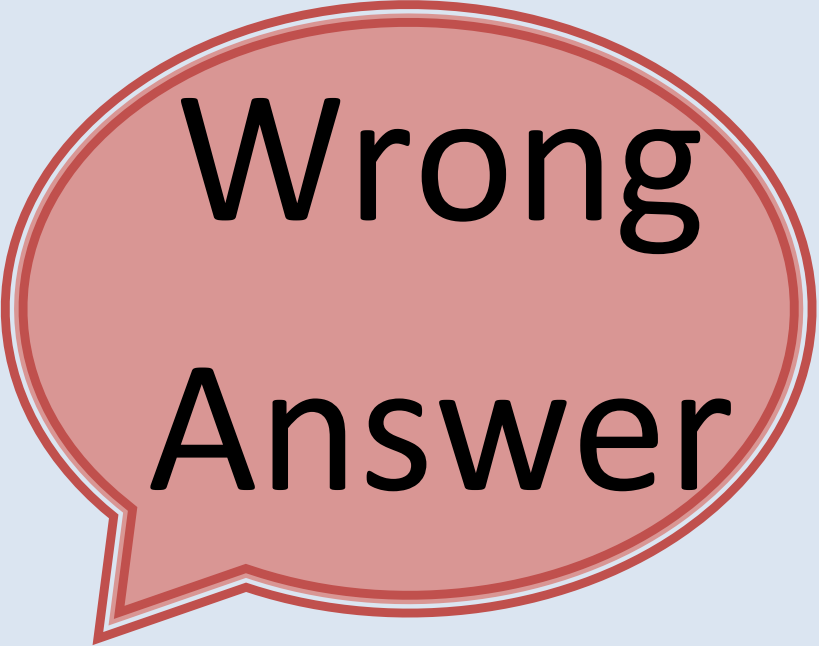
c) Has Nice Images

8. Best thing to do before making a purchase?

a) Ask a Friend

b) Read user Reviews

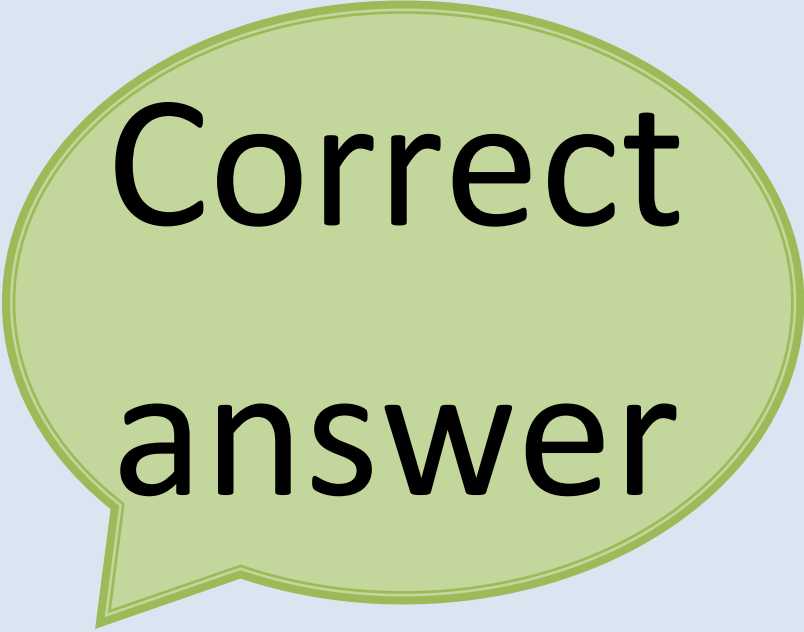
c) Nothing



Wrong Answer

Sorry this is the wrong answer, you may need to go back and read the guide again or try again by clicking the button below.

[Back to quiz Questions](#)



Correct answer

Well done that is the correct answer!

To go back to the quiz questions click the button below

[Back to quiz Questions](#)

Quiz answers

1. Which type of internet connection gives a stronger signal?

- a) **Wired** b) **Wireless**

2. Which type of internet connection is safer from hackers?

- a) **Wired** b) **Wireless**

3. Who should you share your passwords with?

- a) **Family** b) **Friends** c) **No one**

4. What to do if you receive a suspicious email?

- a) **Open it** b) **Delete it** c) **Reply** d) **Download attachment**

5. Best privacy option for social networking sites to keep personal information safe?

- a) **Private** b) **Moderate** c) **Public**

6. What to do if someone adds you who you don't know?

- a) **Block and decline invitation** b) **Accept** c) **Meet them**

7. What to ensure when shopping online?

- a) **Website looks nice** b) **HTTPS** c) **Has nice images**

8. Best thing to do before making a purchase?

- a) **Ask a friend** b) **Read user reviews** c) **Nothing**

STAY SAFE USING THE INTERNET

This booklet contains all the information you need to know about the internet and how to remain safe and secure when you and your family are using it.

The areas this booklet cover are :

- ▶ Emails
- ▶ Social Networking
- ▶ Online Shopping
- ▶ Internet Connection

This is perfect for parents who are new to the world of the internet and want to make the most out of using it while still remaining safe.

This booklet is available as a print booklet and also a PDF booklet online!

