Class 5 – Parent Information Presentation on Internet Safety

Slide 1

Welcome to Class 5's Parent Information session all about Internet Safety.

Today we will tell you about the ways you can keep your family safe online.

Although technology and the Internet are so valuable to us, it is vital that we know how to keep safe when online.

Let's watch a video to find out more!

Slide 2

[https://www.youtube.com/watch?v=2IcpwISszbQ]

I can't believe that more people own a mobile device, such as phone or tablet, than a toothbrush! Yuck!

Slide 3

Did you know that if Facebook was a country it would **have** the largest population in the world?

Did you know that it is believed that 93% of our buying and purchasing decisions are influenced by social media?

Did you know that excessive use of social media and the Internet is resulting in both adults and children now having **shorter** attention spans.

2 out of every 3 people get their news from the Internet but how can you tell what is real and what is fake news?

If you are not sure of something, such as a question on your homework, or the opening times of a shop, it is so easy to search on the Internet, so why would you look anywhere else?

Nowadays, there is also an app for almost anything you can think of!

Slide 4

Perhaps you were able to recognise some of the apps in the quiz earlier.

In the meantime, please raise your hand if you would like to guess, on average, how many apps are released each day … we'll take three guesses!

The answer is 6,100 new apps each day!

This is very worrying, because apps are being released **too** quickly for the police and other safeguarding agencies to check they are safe for us to use.

It is especially worrying to think that vulnerable people, such as those with learning difficulties or disabilities, might be able to access harmful material.

However, it is not just vulnerable people who can face difficulties on the Internet.

Slide 5

Did you know that it is possible for cyber attackers to steal your **private** information when you are using **public** Wi-Fi, such as at a café, pub or restaurant?

As data is being sent from your device such as phone or tablet, to the website you are hoping to use, Internet hackers can **intercept** the transmissions and read what you are writing.

The best way to know your information is safe while using public Wi-Fi is to use a virtual private network (VPN), like Norton Wi-Fi Privacy. Just type VPN into Google to find out how!

So what are the 'Do's and Don'ts' of using public Wi-Fi …?

Do disable file sharing – if you are sharing a file over public Wi-Fi, it could be accessed by strangers.

Only visit sites using HTTPS and remember to log out of accounts when finished.

Don't allow your Wi-Fi to auto-connect to networks.

Don't log into any account via an app if it contains sensitive information, such as online banking. Go to the website instead and verify it uses HTTPS before logging in.

Slide 6

Most of us couldn't live without the Internet, but why?

Well, many people use it to find things out. Using the Internet to do a simple search, such as looking on Google, accounts for 4% of the Internet's usage.

We call this the **surface** web.

Only 4% though? How else do we use it?

Well 90% of Internet usage is on the **deep** web. The deep web includes use of secure websites and online activities such as Internet banking and online shopping.

To access the **deep** web you usually need to use passwords.

Slide 7

You might be surprised to learn that 6% of Internet usage is on the **dark** web.

The dark web is the part of the Internet that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

There are many legitimate reasons to use the dark web, such as security for the military and specialist services.

However, it is on the dark web that illegal activity can take place, for example terrorism, searches for inappropriate pictures and documents, as well as purchasing illegal items, such as weapons.

So not everyone who uses the Internet can be trusted.

Another thing to be aware of is the use of webcams.

Slide 8

Nowadays, most computers and tablets have camera and video software installed. Did you know that it is now possible for hackers to remotely access your webcam?

Someone might be recording you without your knowledge.

What can we do to stop that happening?

You can cover your webcam with a sticker to stop hackers.

Why would someone access your webcam? What's the point?

If a hacker was able to record you doing something embarrassing or illegal, they could blackmail you.

For example, if you were playing with your phone while sat on the toilet, a hacker could record this and threaten to publish the embarrassing video of you using the loo on the Internet, unless you paid them not to.

Or perhaps you have left your laptop open on your desk and you are getting changed for school or work, somebody could video that and distribute it over the Internet.

Your computer doesn't have to be switched on for a hacker to record you, it is now possible for hackers to turn on your computers remotely.

It doesn't take long to cover your webcams. So please don't forget!

Some people are not very careful with what they post on the Internet. If you post too much information about yourselves, it is possible for criminals to find out all about you and your family.

Slide 9

If you post a picture of your child on their first day of school you could be accidentally giving away your personal information to criminals.

Just by looking at one picture, a criminal could find out your address or what school your child goes to.

For example, just by looking at the colour of the school uniform and the logo, a criminal could easily find out where children attend school.

In this picture, we can tell that these children live at number 34 and have a plum-coloured front door.

It won't take a criminal long to find the street the children live on, if they get in their car and drive along some of the streets near to the school these children attend.

If a criminal has found out where you live and later on, you post a comment on Facebook about how excited you are to be going on your holidays, you are also advertising when your house will be empty which leaves you at risk of being burgled.

If your settings are not private on Facebook, it would be easy for a criminal to look at all your posts and learn all about you.

Slide 10

Children should remember to keep their personal information private and report anything that makes them feel nervous or uncomfortable.

Slide 11

Did you know you have to be at least 13 years old to use Facebook?

It is vital that parents monitor what their children go on. A lot of the time children are accessing inappropriate content, such as video games rated 15 or 18.

Video games are given a rating for a reason – to make sure they are appropriate.

Some websites require you to use passwords, so surely these are safe to use?

Slide 12

But how safe are our passwords? These are the most common passwords currently in use.

Think of one of your online passwords …

Do you use the same password for everything?

Have you written your passwords down?

What would happen if someone accessed your password because it is easy to guess or has been written down somewhere that is easy to access? Perhaps you've jotted it down on paper and then you've been burgled? Could a criminal now have access to your Internet banking?

Is your password strong?

Does it contain numbers, letters and symbols?

Slide 13

Let's find out more!

[https://www.youtube.com/watch?v=opRMrEfAIiI] **–18 secs – 2mins 30**

If your password is easy to guess, please change it this evening!

Slide 14

Thank you for listening today.

We hope you found the information useful and that we have given you lots to think about.

For further information, you can visit any of these websites.