An adult's guide to keeping yourself safe online

Sometimes as adults we can be guilty of giving children lots of advice as to how to keep themselves safe when they are online but not always follow the same advice ourselves. Below are a few tips to ensure that you are as safe online as your children should be.

Social Networks

Lots of children and adults enjoy using a variety of social networks to keep in touch with their friends and family, including those who have moved elsewhere on the planet.

Social networks can be absolutely fantastic for keeping in touch with people you don't get to see very often but are you making sure that you are leaving a positive digital footprint when you use them?

Privacy settings

Lots of adults use social networks but many of them do not always use the privacy settings that they offer people for protection. On most social networks, the default setting is such that anyone who uses the same social network (or sometimes even those who do not) can see everything that you put online.

This includes the pictures that you post, the comments that you write and the way you respond to other people's comments. Most of the times this might be fine. However, if you are tagged in something that you would rather not be tagged in or if you post something you later regret posting, then everyone is able to see this and comment on it.

In extreme cases, this could affect future career prospects. Make sure you investigate how to ensure that your settings are private and that only your friends can see the things that you post. Every social network's settings are slightly different so have a look on their help pages if you are struggling to find what you need to.

Keeping personal information private

A lot of this can be managed by ensuring that your privacy settings are set to only show information to friends. However, think about what you share with people online and how much of this you need to share. Is it necessary to share your phone number, date of birth or email address on your profile? Wouldn't your close friends already have these things?

By posting this information online and allowing other people to see them, you run the risk that someone could use some of this information for the purposes of obtaining credit in your name.

Although this may seem extreme, every piece of information such as this can be gathered by unscrupulous individuals who wish to make some 'easy money' and leave you to foot the bill.

A Digital Footprint that you leave behind should be a positive one

If the term 'Digital Footprint' is not one you have heard before, it simply means the information you leave behind on the Internet. This might mean the pictures that you post online, the comments that you make on other people's pictures or blogs or simply be your own business' website.

Most of the time, if you have set your privacy setting correctly, this should not affect you. However, if this is not the case, anything that you put online is then out of your control.

For example, if in the heat of the moment you make a comment on somebody's profile that you later regret, you can remove the comment and feel that this is the end of the issue. However, if someone decided to screen shot that comment or copy and paste it, then the comment has not truly been deleted.

The rule of thumb that we guide by is that when you post something online, think "would my parents, or grandparents, be happy if they knew I was posting this?"

If as adults we apply the same rule, we can generally make sure that our Digital Footprint is a positive one.

Google your own name with some key words

If you are unsure what your Digital Footprint is like, it can be a good idea to Google your own name with a few other key words, such as the town that you live in and see what comes up.

Sometimes you might find an old profile from a social network you had forgotten you were even a member of. If it a website that you no longer use, is it worth keeping your information on it?

Go back to that social network and see how you can close your account and reduce your Digital Footprint.

Passwords

Passwords are perhaps the most important way that we protect our identity and private information online but how safe do you make them?

Passwords should be like your toothbrush; you never share them with anyone else and change them regularly

Everyone has had the situation where they have forgotten the password that they use to access a website at some point. The danger is that we rectify this by using the same password for every different website that we use or make them easy to remember.

The first question you should ask is do you want your password to your favourite social network site to be the same as your online banking password? What if someone knows your social network password or manages to hack your account? They could now also have your online banking password and be one step closer to accessing your financial details.

It is important, therefore, to make sure you use different passwords for your online banking, email, and other sites that you access online. Also, as the news frequently reminds us, banks and other websites are frequently the victims of online hacking scandals and, therefore, it is equally important to change your password frequently to guard against this your details been accessed by these people.

Make your passwords difficult to guess

Parents can be particularly guilty of making their passwords surprisingly easy to guess. What can seem secure to them (their child's name, abbreviation of their children's initials or dates of birth) is routine fodder for an experienced hacker. They can gather most of the information they need from social network sites (if your settings are not private) and use this to create common combinations of passwords.

A good tip for making your passwords more secure is to use something you are interested in but abbreviate this heavily and mix it up with capital and lowercase letters and unrelated numbers. For example, Betty99 can be quite easy for a hacker to guess but fTbA33 (an abbreviation of football and the number 33) is much more challenging to guess.

If you use filtering software to protect your children from online content, make sure you use a completely different password to secure this to any other one that you use and your children might have access to

Children often know a few of their parents' passwords, as they may use them to access their parents' phones or to unlock the computer at home. If you use a similar password for your filtering software, you may leave the software useless as your children may be able to guess the password to by-pass it.

Cookies and Tracking Data

Have you ever wondered why you get adverts on your social networking site or another website for products that you have just viewed online? Have you always put this down to a strange coincidence? Unfortunately, this just is not true. When you visit a website, your computer or device will usually download a small file called a cookie.

This file enables you to load the website more quickly the next time you visit it or allow other websites to see where you have visited previously. Most website have a 'view how this website uses cookies' agreement when you first visit them. Some websites will close automatically if you fail to agree to their use of cookies. This means it has become rather difficult to avoid these little files on your computer and, in some cases, you may not wish to avoid them anyway.

However, it is a really good idea to frequently delete your browsing history and clear the cookies on your computer. Not only will it marginally increase the space on your computer's memory, but it will also stop website being able to bombard you with adverts for products you have recently viewed.

Pop-ups and Junk Mail

Most people who have used the Internet for a long time will be all too familiar with web page that suddenly pop-up out of nowhere. They will also probably have received a multitude of junk mail in their inbox. Below are some simple tips to consider when you have issues like these.

Pop-ups

These tend to not be regarded as such as issue as they were in the past as many web-browsers now have the capacity to block them without you even knowing that they have protected you from them. However, a few can still get through and clicking on them can be something that you will live to regret.

Many of these pop-ups contain pictures and images that are designed to entice you to click on them. For example, they may tell you that you have won a prize. However, when you click on them, they might redirect you to a site you did not want to visit or may even download a virus to your system.

The rule of thumb we guide by is "if you didn't enter a competition, how can you have won a prize?"

Equally, if the link looks too good to be true, it probably is. Always navigate to website you want to visit directly, do not follow the pop-ups.

Junk mail

Anyone who has had an email account will have encountered junk mail in some form or another.

It might simply be an advert that you did not want, or, in many cases, it might be something more sinister. Sometimes the email can even appear to be from a friend or company, but they have used an unusual title line or a generic one that could apply to anyone.

This type of junk mail is usually sent to do only one thing – steal as much information from your computer as possible. They may contain a link to another website or have a document attached to them (they may even be what appears to be a relatively harmless Word Document). However, embedded into the macros on the document or via the link can be a harmful virus that is put there with the express purpose of stealing as much of your information as possible.

This information can then be used to access your bank accounts or set up credit in your name. The junk mail is always made to seem inviting.

One of the latest scams is to send you an email from a registered company – an address that they have hacked – and send you a 'receipt' for a transaction you supposedly made in the form of a Word document. When you open the document and allow the macros to run, you then allow a virus to enter your computer. Always make sure that you only open attachments from someone you know or from companies that were supposed to be sending you documents online.

If you are unsure about whether an email is genuine or not, search the title of the email online. Often this will quickly show you if there is a scam going on related to the name of this email. Also, always view attachments in your email's 'view online' option first (if they have one). This way, you can view the content of the document before choosing whether it is appropriate to download to your device.

Anti-Virus and Security Software

If you look on online forums, Anti-Virus and Security Software can often be a hotly debated topic. Some people argue that they are too intrusive and slow their computers down too much, other people argue that they are an essential.

Some people argue that Apple Mac computers do not need the same level of security as PCs, due to the fact that they function in a different way to PCs and, currently, have fewer viruses designed to target them.

Undertaking your own research into Anti-Virus and Security Software is something everybody should do before deciding to install it or not. However, do bear in mind that many online banks insist on you using some form of it in their terms and conditions if you use their online facilities.

Online Banking and Scams

In today's busy modern world, online banking can save a huge amount of time and effort and make transactions much easier to keep a close eye on. However, it is important to guard your online banking details against attacks.

Never give out your bank details to anyone online or over the phone unless you are buying something from a trusted business

A common scam is for someone claiming to be from your bank or building society to email you or ring you and request your banking details to sort out some kind of error on your account.

Most banks will tell you that they never do this and that this is most likely to be someone trying to steal your bank account details so they can steal your money.

Before paying for anything online, always check a website's reputation with a simple online search

Some websites can be very cleverly designed to look like websites of genuine products that you can buy in the shops but, in fact, offer sub-standard copies of the same product or, even worse, don't provide you with the product at all.

Before shopping anywhere new online, it is always a good idea to check out reviews of a website before you purchase from it to see how highly other people rated the product or service that they received from them.

Disposing of Old Computing Technology

When upgrading to a new phone or computer it can be so exciting that we forget about the product we have just decided to dispose of. This can be a dangerous mistake.

The product that you are getting rid of you may have used to look at online banking details or may contain files that are private to you.

Before disposing of any technology, always ensure that you complete a factory reset and ensure you dispose of it with a company that has a reputable standard for disposing of these kinds of products.

E-safety and the Coronavirus Pandemic

The coronavirus has been classified as a global emergency by the World Health Organisation (WHO). Unfortunately, criminals are now preying on people's fear by launching various fraud and phishing campaigns.

Since lockdown began, a total of £11,316,266 has been reported lost by 2,866 victims of coronavirus-related scams.

Over £16 million has been lost to online shopping fraud, with people aged 18-26 most at risk.

As of 15 May, the UK's cybercrime agency had uncovered 7,796 phishing emails linked to COVID-19.

Many reports are related to online shopping scams where people have ordered protective face masks, hand sanitiser and other products which have never arrived.

One victim reported losing over £15K when they purchased face masks that were never delivered. Reporting numbers are expected to rise as the virus continues to spread across the world.

They have also received over 200 reports of coronavirus themed phishing emails attempting to trick people into opening malicious attachments or revealing sensitive personal and financial information.

Some of the tactics being used in phishing emails include:

- Fraudsters purporting to be from a research group that mimic the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO). They claim to provide the victim with a list of active infections in their area but to access this information the victim needs to either: click on a link which redirects them to a credential stealing page; or make a donation of support in the form of a payment into a Bitcoin account.

- Fraudsters providing articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates.

- Fraudsters sending investment scheme and trading advice encouraging people to take advantage of the coronavirus downturn.

- Fraudsters purporting to be from HMRC offering a tax refund and directing victim to a fake website to harvest their personal and financial details. The emails often display the HMRC logo making it look reasonably genuine and convincing.

Protect yourself

Watch out for scam messages

Do not click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details.

Protect your devices from the latest threats

Always install the latest software and app updates to protect your devices from the latest threats.

Shopping online

If you are making a purchase from a company or person you do not know or trust, carry out some research first and ask a friend or family member for advice before completing the purchase. Where possible, use a credit card to make the payment as most major credit card providers insure online purchases.

For more information on how to shop safely, please visit the Action Fraud website.

https://www.actionfraud.police.uk/shoponlinesafely