Training module 8

Staying safe online

In this module you will:

- Find out how to protect your privacy online
- Consider the risks of using social media and how to stay safe
- Discover how to identify scam emails
- Find out how to stay safe when shopping and banking online
- Find out about computer viruses and how to avoid them.

Registered office: Bradmere House, Brook Way, Leatherhead, Surrey KT22 7NA
www.transformhousing.org.uk ■ info@transformhousing.org.uk

Registered charity: 264133 ■ **Company limited by guarantee registered in England:** 01057984
Registered provider of social housing: H2452

Training module 8: Staying safe online

April 2018

Module contents

Introduction: Description of module

How can this module help me?

This module is aimed at anybody who uses the internet and who wants some general advice and guidance on how to stay safe. It is not overly technical and no attempt has been made to provide actual instructions on **how** to use the internet – this would require a very long module indeed! Instead it considers some of the main ways in which the internet is used and suggests techniques for staying safe.

Because this module is focussed on staying safe, there is a strong emphasis on the risks of using the internet. This might make the module sound quite negative or critical of the internet on occasion. This is not our intention. The internet offers countless benefits and resources which are increasingly important in today's world. When this module talks about risk it is not with a view to putting you off using the internet, but rather to help you identify ways in which you can reduce these risks so you can enjoy using the internet and all it offers safely.

How does this module work?

This module is made up of 11 sections, each one dealing with an aspect of internet use – a list of these sections is provided in the contents page at the front of this module. Each section can be divided roughly into three parts:

- Explanation of the topic being considered
- Examination of the risks involved
- Examples of ways to tackle these risks and stay safe

Throughout the module you will find various coloured boxes as detailed below:

Exercise

The green boxes contain checklists for you to complete.

Remember

The blue boxes give you important information to help you stay safe online

Did you know?

The purple 'Did you know?' boxes give information that you will (hopefully!) find interesting

Part 1: Searching the internet safely

To search the internet you need to use two tools; a web browser and a search engine. It doesn't matter if you are using a smartphone, tablet, PC or laptop – web browsers and search engines are vital.

Web browsers are apps (short for applications) or programs that allow you to access and view information on the internet.

Search engines are websites that help you find the information you want by using keywords that you enter into the engine.

One way of thinking about it is to compare using the internet with driving a car; the web browser is the windscreen through which you view the internet. The search engine is the steering wheel that helps you to navigate the internet. In this section of the module we will look at how to use web browsers and search engines safely.

Choosing and customising a web browser

A good browser will protect you from viruses and phishing attacks by identifying dangerous sites and blocking them (please see part 7 of this module for more details about viruses). For this reason, it is best to use the most secure internet browser you can. Some of the most commonly used internet browsers are:

- Microsoft Internet Explorer
- Microsoft Edge (Windows 10 only)
- Google Chrome
- Mozilla FireFox
- Apple Safari

Browser updates are released regularly to keep you safe from the latest viruses, so make sure you download the latest update for your browser.

Choosing which browser is right for you is very much a matter of personal taste, but it is important to consider security when making your decision. For a review of the security of each of the main web browsers, please follow this link**:**
https://www.makeuseof.com/tag/most-secure-mainstream-browser/

Did you know?

The five browsers mentioned above are generally used on PC's and laptops. For mobile devices, the two most commonly used web browsers are Google Chrome (which is the most popular) and Apple Safari (because of the high prevalence of iPhones).

Chrome has a 60% market share and is generally regarded as having solid security. Chrome automatically defaults to the most secure settings whilst still providing a good user experience and so you don't generally need to customise anything to make sure your internet use is secure. The downside is that Google collects huge amounts of data when you use its products and then uses this to create personalised adverts. In short, with Chrome, security is good but privacy is not so good.

It is possible to customise settings on your browser to make them more secure. There are often options to choose the level of security to ensure safer searching and to block those sites which are in any way suspicious. If you would like to know more about customising security settings for the most commonly used browsers, please follow this link: **https://imss.caltech.edu/node/243**

Using search engines

As mentioned, search engines enable you to find specific web sites by entering key words. The top three most commonly used search engines are:

- Google
- Microsoft Bing
- Yahoo! Search

To help you use your chosen search engine safely, you might want to consider some of the following suggestions:

- Search engines often have the option to turn on 'Safe search'. This will block violent and adult content. Just go to the settings menu to activate this.
- To avoid unwanted search results, choose your search terms carefully.
- If you come across content during a search that you consider to be illegal such as child abuse images, you should report this to the Internet Watch Foundation: **https://www.iwf.org.uk/**
- If you come across content that you consider illegal such as racist or terrorist content, you should report this to the police.
- Some sites are more likely to contain viruses than others. In particular, sites which contain pornography, file sharing sites, gambling sites and sites selling new psychoactive substances (previously known as legal highs) all tend to be very high risk and are best avoided.

Privacy

Browser history:

When you use the internet your browser keeps a record of which sites you have visited in its 'history'. In addition, websites you visit are visible to both your Internet Service Provider (this is the company that provides you with internet access such as BT, Sky and Virgin) and also your browser provider. You can delete your browsing history and turn on private browser settings to increase your privacy, but this will only prevent other people who are using your computer or mobile device from seeing which sites you have visited. Your Internet Service Provider will still be able to see which sites you have visited or keywords you have searched for. Should a crime be committed, the police will also be able to retrieve this information.

Cookies:

You may well have heard of cookies before, but might be a little unclear on what, exactly, they are. Cookies are small files of data that store information about your browsing habits. When you visit a site for the first time, a cookie is downloaded onto your PC or mobile device. The next time you visit that site, your device checks to see if it has a cookie that is relevant. If it finds one, it sends the information contained in that cookie back to the site. The site then knows that you have visited before and might tailor the site to suit you. This can provide a smoother, more pleasing experience.

The downside is that cookies provide organisations with information about you. This information can then be used to develop marketing lists and to target advertising and some people might not like the idea of this. Generally, however, cookies are not something to be scared of; they are just a part of the workings of the internet.

When you use a site for the first time it will tell you if it stores cookies. If it does, it will ask for your permission to store and retrieve information about your browsing habits. Sometimes you will need to actively give permission, whilst other times permission will be assumed if you continue to use the site. You can choose whether to give permission or not, but it is worth noting that there are many sites that you will not be able to access unless you give permission for cookies.

It is possible to delete cookies by choosing the appropriate option within your browser settings. This will delete the information that organisations have about your browsing habits on your computer.

Remember

Before you enter private information on a website you should check to make sure it is secure. There are two ways to do this:

- There should be a padlock symbol in the browser window. You can click on this padlock to find out security information about the site, including the dates of any security certificates issued and the name of the organisation that authorised the certification (for example VeriSign).
- The web address should begin with ‘https://’ where the ‘s’ stands for ‘secure’.

The padlock and ‘s’ indicate that the information transmitted from that website has been encrypted and protected from being intercepted or stolen by third parties. This, of course, is vital if you are entering personal information such as account details into the website.

Part 2: Social media

What is social media?

When you hear the term ‘social media’ you might immediately think of Facebook, being the biggest social networking site at the moment. Social media, however, has a very broad definition and has many different forms.

In this section of the module we are going to look at the different types of social media that currently exist and the risks which they pose. To start us off, let’s look at some of the different types of social media:

Social networking sites:
These are perhaps the most well-known of all social media. They are online platforms that allow you to create a public profile and interact with other users on the site. The sites work by asking you to create a profile which often includes a photo and some biographical information. You will receive suggestions of other site users who you have a connection with (often the site will get these suggestions from your email or phone address book). You can then invite other site users to connect with you. If they agree, then they will be able to view your profile and you will be able to view theirs. You can then post information to your site which can be viewed by any of the people you have a connection with. Some examples of social networking sites are Facebook and Friends Reunited.

Blogging sites:
The word ‘blog’ is derived from the term ‘web log’ and is a frequently updated online personal diary. It will often have a particular focus, such as a food blog or a blog about being a mother. There are also micro-blogs which are blogs where the entries are very short. Examples of popular blogging platforms are Twitter and Tumblr.

Photo sharing sites:
These are sites with a particular focus on sharing your photos with others. Popular platforms include Flickr, Instagram and Pinterest

Video sharing sites:
These are much like photo sharing sites, but with the focus on video. Such sites often allow users to comment on the videos that have been posted and rate them. The most popular video sharing sites are YouTube, Vimeo and Viddler.

Messenger apps:
Messenger apps work much like text messaging in that they enable you to send messages direct to your contacts. Unlike text messaging, however, messenger apps use the internet to send the message and so bypass costs associated with sending text messages. In particular, apps such as WhatsApp allow you to send photos, audio and video at no extra cost. They also allow for group conversations.

These distinctions between various types of social media can be useful in understanding the differences that exist between platforms. Increasingly, however, platforms provide a number of different functions in one place. Indeed, Facebook has its own messenger app (creatively named Facebook Messenger) and also owns WhatsApp. Meanwhile, Google owns YouTube whilst also running Google Plus. For the purposes of this module, understanding the differences between the various kinds of social media is less important that understanding the risks which they might pose, and it is to this that we will now turn.

The risks of social media

Nobody would deny the usefulness of social media in today's world. Used appropriately it is a genuine force for good which can bring people together and empower them. The key words here, however, are 'used appropriately'. With something as powerful as social media, which can spread a thought across the world in a matter of minutes, if it is used without care and consideration it can be the cause of great harm. If you use social media, it is crucial that you are aware of the risks so you can make sure you avoid them. The aim here is not to put you off using social media; it is to make you aware of the various risks so you can use social media safely and responsibly.

On the next few pages are some of the main risk areas which you might encounter when using social media. For each area:

- You are asked the question 'Is this a risk area for you?' Please tick the box 'Yes' or 'No' to indicate if this is a risk area.
- If it is a risk area for you, there are some suggested action points to help you reduce the risk. Tick the box to the left of the action point if it is relevant to you.
- If there are any action points not listed that you would like to include, just write these in the box labelled 'other'.
- Once you have considered all risk areas mentioned, you should have an action plan to help you stay safe when using social media.

1. The risk: Private information becoming public

Probably the number one risk of using social media is giving away too much information about yourself. Revealing information such as your home address, details of your family or where you work all compromise your privacy. At its worst, a cyber-criminal might pick through your postings and find out enough information to impersonate you and commit fraud.

Is this a risk for you? **Yes** ☐ **No** ☐

If 'Yes' tick below to indicate which actions you will take to reduce the risk

- Read the site's privacy policy and use privacy and security settings to control who can see your personal information. ☐
- Make absolutely sure your profile is not open to the public; only friends and family should be able to see your pages ☐
- Do not post any personal information online such as your address, email, mobile number or date of birth ☐
- Do not pick a username which reveals any information about you (**sarahjane_guildford** is not a good choice as it reveals both a full name and a geographic location) ☐
- Other (please state below): ☐

2. The risk: Photos that reveal more information than you intended

The pictures you post online may say more than you want them to. If a picture is of you standing by your home, then you may inadvertently be revealing your home address to the world at large.

Is this a risk for you? **Yes** ☐ **No** ☐

If 'Yes' tick below to indicate which actions you will take to reduce the risk

- Avoid posting photos of your home, work or any places you are strongly associated with. ☐
- Look at a photo carefully before you post it – does it inadvertently contain something you wouldn't want to reveal (for example, a phone number)? ☐
- Think very carefully before posting any revealing photos of yourself ☐
- Other (please state below): ☐

3. The risk: Impact on mental health

Excessive use of social media can affect sleep. Equally, using social media to compare your lifestyle with others can reduce self-esteem and lead to isolation and anxiety. If your use of social media is having a negative impact on your mental health then you may want to consider making some changes.

Is this a risk for you? **Yes** ☐ **No** ☐

If 'Yes' tick below to indicate which actions you will take to reduce the risk

- Limit how much you use social media each day ☐
- Don't use mobile devices in bed. The blue light they emit makes it harder to sleep ☐
- Social networking can be positive, but make sure it doesn't replace meeting people face-to-face and socialising. ☐
- If you think your use of social media is having a negative impact on your metal health speak to your keyworker or a trusted friend or family member. ☐
- Remember that it isn't a popularity contest – try and avoid comparing yourself with others. ☐
- Other (please state below): ☐

4. The risk: Old posts that come back to haunt you

Many employers check the online profile of an applicant before offering an interview. If you have posted anything which presents you in a less than flattering light, you may find it hard to get a job interview. Assume everything you post online, including all photos and videos, will be available online permanently. Although it is possible to delete an account, it is better to avoid posting things you might later need to delete in the first place.

Is this a risk for you? **Yes** ☐ **No** ☐

If 'Yes' tick below to indicate which actions you will take to reduce the risk

- Avoid posting anything which you might later regret or which will present you in a negative light. If such posts exist, delete them or restrict access to them. ☐
- Consider googling yourself to see what information comes back (it's a good way to see yourself as others may see you online). If the results you get concern you for any reason, you might want to discuss this with Transform staff. ☐
- Before you post anything online imagine someone in authority, someone you respect, viewing it. Would they approve? If not, don't post it. ☐
- Avoid posting anything when you are drunk or have been using drugs. You may well later regret it. ☐
- Other (please state below): ☐

5. The risk: Being burgled

If you give details of a holiday you are going on, or post-holiday photos whilst you are away, you are effectively informing people that your home will be unoccupied. Criminals scour social networks to find empty properties to burgle.

Is this a risk for you? **Yes** ☐ **No** ☐

If 'Yes' tick below to indicate which actions you will take to reduce the risk

- Don't post information that lets people know when you are away from home (if you do and you are burgled, your insurance company may refuse to pay out). ☐
- Be aware that some messaging apps (including Snapchat) can disclose your location. If you do not want others to know your whereabouts, make sure you disable this. ☐
- Other (please state below): ☐

6. The risk: Breaking the law

Posting comments which are threatening, discriminatory or abusive may be illegal and leave you open to prosecution. Even if you are saying something 'as a joke' it is easy for such things to be misinterpreted online.

Is this a risk for you? **Yes** ☐ **No** ☐

If 'Yes' tick below to indicate which actions you will take to reduce the risk

- If you wouldn't say it or do it in public, then don't post it online. ☐
- If you are angry and need to vent, don't use social media as a forum to do this. Instead call a friend and keep your venting private. ☐
- Be very careful what you post as a joke online. What seems funny to you may offend others. ☐
- Other (please state below): ☐

7. The risk: Following/friending a stranger

Criminals can create fake online accounts in order to befriend others. Once you connect with them, they can then harvest your personal information.

Is this a risk for you? **Yes** ☐ **No** ☐

If 'Yes' tick below to indicate which actions you will take to reduce the risk

- Don't accept every friend or follower request you get. It is best to only connect with those you know in real life. ☐
- Some social media sites provide a system to check that an account is officially verified – often this is in the form of a white tick in a blue circle next to their name. Check to see if this is available on the social media sites you use. ☐
- Remember – people you meet online might not be who they pretend to be. ☐
- Other (please state below): ☐

8. The risk: Hacking and identity theft

Hackers can target social media accounts and hack them. They can then use the hacked accounts to send posts which contain viruses or phishing scams. Because the posts appear to come from a trusted source, the receiver is more likely to click on a file or link. In addition, social media sites are used by cyber criminals to launch viral attacks and to defraud users by stealing their identity. Viruses or spyware contained within message attachments or photographs are common techniques for this

Is this a risk for you? **Yes** ☐ **No** ☐

If 'Yes' tick below to indicate which actions you will take to reduce the risk

- Use strong passwords (containing upper and lower-case letters, numbers and symbols) when setting up your account ☐
- Avoid logging in from public hotspots unless they are secure – only login from trusted wireless networks ☐
- Don't click on a link or file if you are unsure about the source – it may contain a virus or lead to a fraudulent site ☐
- Keep your anti-virus software up to date (please see part 8 of this module) ☐
- Be aware of the risk of phishing scams (please see part 3 of this module) ☐
- Other (please state below): ☐

Did you know?

Facebook is certainly not the only social media site available, but it is, for the time being at least, the biggest. Just to give you a sense of how big it is, here are a few facts about Facebook:

- Facebook has over two billion monthly active users.
- 100 million hours of video are watched on Facebook each day
- More than 250 billion photos have been uploaded to Facebook
- Facebook stores approximately 300 petabytes of user data on its servers. There are 1 million gigabytes in a petabyte. To put this into perspective, the entire written works of humankind in every known language from the dawn of recorded history would occupy approximately 50 petabytes.

Part 3: Email: spam, scams and phishing

What is spam email?

Email is a very effective and useful communication tool used throughout the world. Unfortunately, there is a downside to email, spam. Spam email is digital junk email, which is to say email that you didn't want or ask to receive, and it has become so prolific that it represents the vast majority of all emails sent in any given day. The most common forms of spam are adverts for online pharmacies, pornography, weight loss and dating sites. Most spam emails tend to be detected by email providers and automatically moved into a 'junk' folder within your email account, however some spam emails get through this system and arrive in your email inbox.

Did you know?

You may wonder how the spam sender knows your email address in the first place. There are a whole range of techniques for finding out your email address; sometimes the sender just uses automated software to guess email addresses until they hit upon the right one, sometimes you will have given your email address to a company who then sells it on to others, and sometimes your email address may have been obtained either by hacking or because you have been tricked into entering your details into a fraudulent website.

Some spam emails are just irritating, inconvenient and clog up your inbox. More serious, however, are those emails which can be genuinely harmful and the most common of these are 'scam' and 'phishing' emails.

What are scam emails?

Scam emails are designed to trick you into giving information that will be used to steal your identity and commit fraud. Essentially, scam emails tend to either appeal to our desire for financial, physical or emotional gain or they play on our fear or curiosity. Below are two examples of scam emails:

The mystery shopper scam:
Here you are told of a wonderful opportunity to work from home and earn a generous salary. All you have to do is go around shops acting as a 'mystery shopper'. You will usually be asked to send money up front to pay for training materials. If you do send the money, the materials will never arrive.

The Nigerian cheque scam:
You receive an email from someone who sounds important (perhaps with a title) asking for your help to recover a large sum of money from a foreign bank. In exchange, you will be given a proportion of the sum to be recovered. The bank is often said to be in Nigeria, hence the name of the scam (in actuality, however, the scam can come from anywhere in the world). If you do respond to this email, you will be asked for your bank details to pay the money in to. You will also be asked to pay the bank transfer fees. If you pay, there will inevitably be some kind of issue requiring you to pay more. This will continue until you realise you are being scammed.

What is ‘phishing’

‘Phishing’ is where an email is sent out to thousands of people in the hope that a few will take the bait and ‘bite’ by clicking on the link contained within the email. Most phishing scams pretend to come from banks, shops, credit card companies or similar that are well known and well trusted organisations. The email will often try and scare you into clicking on a link. They may, for example, tell you that your password has been hacked and you need to change it. They will then provide a link for you to click on within the email. The link says it will take you to the authentic website of the company concerned (for example PayPal) but it actually takes you to a fraudulent website that looks exactly like the real thing. You will be asked to enter your log in details and password at which point you will actually be giving your PayPal or bank log in details to someone who can then steal your identity and commit fraud.

Phishing scams can be remarkably convincing and will often play on our anxieties or fear. Some examples of phishing scams are:

- You receive an email from a delivery company (usually around Christmas) telling you that they failed to make a delivery and asking you to log on to rearrange
- You receive an email saying you have been caught speeding and will receive a fine
- An email comes from a hospital telling you that they have important test results for you.

These emails will be sent out to many thousands of people. For many recipients, it will be evident that the email is a scam because (for example) they aren’t waiting on a delivery, they do not drive or they have not recently had any medical tests. There will be enough people, however, for whom the email will seem entirely relevant and this will automatically create a sense of authenticity. This, combined with natural anxiety, will make you much more inclined to click on the link. In some instances, the link will take you to a fraudulent website which asks for your personal details. In other instances, the link will lead to a site which downloads a virus to your computer.

How to spot scams

Hopefully it is clear that email scams and phishing are a genuine and serious problem and can be very difficult to spot. There are, however, some tell-tale signs that an email is fraudulent. On the next page is a list of spam and scam warning signs. Give this a quick read and then, on page 14, are some examples of scam emails. See which of the warning signs you can spot in the examples.

Remember

Although we are focussing here on spam and scam emails, much of the information is equally relevant to text messages. It is important to be just as careful about the texts you receive and what you respond to as you are with your emails. If you receive a spam text, do not reply, but delete it.

You can report spam texts to your mobile phone provider by forwarding the message to **7726** (the numbers spell out ‘spam’ on a phone keypad).

Top 10 spam and scam warning signs

! **1. The email contains misspellings**	If the email contains misspelt words such as “p0rn” instead or “porn” then it is spam trying to bypass your email filter.
! **2. The sender’s email address is suspicious**	If the email claims to be from a company but the sender is an individual, then you can be pretty sure it isn’t genuine.
! **3. They don’t know who you are**	If you do business with a company, then they know who you are. They will not write to ‘Dear valued customer’ but will write to you by name. Equally, if your name does not appear in the ‘To’ field then it is a good sign that it is a scam.
! **4. They ask you to give personal details**	Reputable companies will not email you directly and ask you to disclose personal details or passwords. If they do, it is probably a scam.
! **5. The offer seems too good to be true**	It’s a cliché, but if an offer seems too good to be true, then it probably is. This includes remarkable deals on the latest Apple device or jobs that pay you excellently for doing very little.
! **6. The link URL is not legitimate**	If you hover the mouse over the ‘click here’ part of the email it will display where the link will take you. If it takes you to somewhere strange (and not where it says it will) then this is a scam.
! **7. The email contains a threat or is urgent**	If the email carries an implicit threat, such as ‘your account will be blocked unless you click on this link straight away’ then be very careful. They are trying to pressure you into acting rashly.
! **8. You have won money or a prize**	Any email promising money or a prize is almost always a scam.
! **9. The email contains a virus warning**	If an email warns that you have been the subject of a virus attack, then assume it is a scam. If you click on the link, then it will probably result in you accidentally downloading the very virus it was pretending to warn you about.
! **10. The email contains .exe, .zip or .txt files**	.exe, .zip and .txt files are the files most at risk of containing a virus. If the email contains an attachment which ends with .exe, .zip or .txt then don’t click on it unless you know it’s safe.

Examples of scam emails:

Below are two examples of scam emails. What would make you suspicious of them?

PayPal

Dear Customer,

Your account has been suspended, as we have reasons to believe that it has been hacked.

To continue to use PayPal you must urgently update your password – if you do not act soon your account will be permanently closed. Please click on the link below to update.

Update your information

Signs that this is a scam are that the email was not addressed to you personally. It has some spelling errors and is putting you under pressure to act urgently. In addition, the email is asking for sensitive data including your password, which is highly suspicious. If you were to hover over the link, it would show where it actually takes you – if this is not PayPal itself, then this would show that this is definitely a scam.

amazon

Refund Notification

Due to a system error you were double charged for your last order, A refund process has initiated but is incomplete due to errors in your billing information.

Error reference code: 1256AVE

To claim your refund, please click on the link below and provide your address and billing information.

Click here to update your account details

After your information has been validated you should get your refund within three business days.

We hope to see you again soon.
Amazon.co.uk

This is a classic example of a scam email which is luring you in by suggesting that you will lose money if you don't respond. Signs that this is a scam are that it is an unsolicited email which is asking for you to provide sensistive data – this is not something that a company such as Amazon would do. You should therefore be immediately suspicious. Hover over the link to see where it would actually take you, but do not click on it. Rather than click on the link, you could email Amazon directly to see if there has been an overpayment.

How can I stay safe?

By following some simple common-sense rules, you can keep yourself safe from email scams. Read the steps below and then fill in the action points to say how you will keep yourself safe from scam emails.

✓	If an email meets any of the criteria mentioned on page 16 then assume it is a scam.
✓	If you are not sure if an email is genuine then contact the person or organisation concerned directly to find out. Do not use the contact details provided in the email but use another source.
✓	Do not open attachments or click on links from unknown sources
✓	Be careful with every email you receive – read the email twice before responding. Be particularly careful with any emails where you do not know the sender.
✓	Do not respond to emails from unknown sources or reply to unwanted emails. The email that was sent to you may well have been randomly generated – by responding you are confirming that yours is a genuine email address.
✓	Make sure you have switched on your spam filtering. You might want to check your spam folder every now and again as sometimes genuine emails can be sent there by mistake.
✓	If you do disclose confidential data, such as your username and password, only to find that the site was fraudulent, then go to the real site and change your details immediately.

To help protect me from email scams I will…	
Action 1	
Action 2	
Action 3	

Part 4: Shopping online

Not only is shopping online extremely convenient, but it can often save you money. By searching around the web, you can often find the best deal on an item in a fraction of the time it would take you to find something on the high street. These are the advantages of online shopping. As with everything we look at in this module, however, there is a darker side to online shopping, and it is this which we will now be considering.

What are the risks of online shopping?

There are three main areas of risk around online shopping:

Risk 1 – Fraud

The risk here is having your payment details stolen when you shop online. The main ways in which this might happen are:

- Making payments over unsecured webpages
- Making payments over unsecured Wi-Fi

Risk 2 – The item never arrives

The risk here is that you never receive the item you have purchased online, most often because the website you purchased the item from was bogus.

Risk 3 – The item is not as described

This is where the item you receive is not what you were expecting. It may be a fake, or just an inferior item, but in some way the item is disappointing.

How to stay safe when shopping online

- Use online retailers that are familiar to you. If you do find yourself needing to use an online retailer that you have never used before then it is best to do some research beforehand and read reviews to make sure they are authentic and reliable. You might also want to check that they have a valid physical address (including postcode) and a telephone contact number.
- Before you enter payment details into a website, make sure it is secure. You can tell if a site is secure because the address will begin ‘https’ (with the ‘s’ meaning secure) and there will be a padlock symbol in your browser window. If, when you are purchasing an item, you are forwarded to a third-party payment service, make sure this website is also secure.
- Before you finalise a purchase, double check the details so that you are not surprised or disappointed when the item arrives. Where appropriate, make sure the item is described as ‘new’ and that you have chosen the relevant size and colour where such options exist.
- Consider how best to make payment so that you have some redress if things go wrong. For information on safe payment options, please refer to the section ‘Safe ways to make payment’ on the next page.
- Once you have finished making a purchase, make sure you fully log out of the site – just closing the browser is not enough to ensure privacy.
- Check your bank statements regularly to make sure you were charged the correct amount for the item purchased.
- Once received, check the item thoroughly to make sure it is what you wanted.

Remember

Know your rights! The **Consumer Contracts Regulations** gives you rights when shopping online or by phone. The Consumer Contracts Regulations came into force in June 2014 and replaces the Distance Selling Regulations. The new regulations describe what information you should be given when buying something online as well as your right to return the item up to 14 days following receipt. For more details on your rights, follow the link below:

https://www.which.co.uk/consumer-rights/regulation/consumer-contracts-regulations

Safe ways to make payment

When making online payments, there are a number of ways you can protect yourself. If you have a credit card and the item being purchased costs between £100 and £30,000 then you will automatically be protected by the Consumer Credit Act, which means that the credit card company will be liable for any defects. This, however, only applies to UK websites, so it is best to avoid making purchases from websites outside the UK. Just because a website has an address which ends **.co.uk** does not necessarily mean they are located in the UK; it is best to check the postal address to be sure.

If you use a debit card to make a purchase online you may be protected by the Chargeback scheme. This is a scheme which, although not enshrined in law, is one which many banks sign up to. Where you have paid for goods which did not arrive or which are damaged, you can use the Chargeback scheme to reclaim your money. For more details on this scheme and how to submit an application, please follow the link below:

https://www.which.co.uk/consumer-rights/advice/how-do-i-use-chargeback

In addition to the protection provided by credit and debit cards, you might also choose to make payments using PayPal. This is a payment option owned by eBay that uses encryption to keep your payment safe. PayPal has a buyer protection feature where you can claim for goods up to the value of £250 at no additional cost on the condition that you make your complaint within 30 days of payment.

Price comparison websites

Price comparison websites can help save you money by providing a comparison of prices for things like insurance, gas and electric, phone contracts and, increasingly, any item you might be shopping for. If used appropriately, they can help you identify the best deal and save you money. When using price comparison websites, remember:

- Only use reputable price comparison websites – ideally ones which have been recommended to you by someone you trust.
- Don't rely on just one price comparison site – search several of them and compare the results to get the best deal.
- It isn't all down to cost – think of quality as well. For example, cheap insurance might have a hefty excess that you have to cover should you make a claim.

- Some boxes can come pre-ticked and some add-ons can be automatically added. Check all of these and make changes to suit your needs.
- Price comparison websites do not show every provider on the market, for example Direct Line and Aviva aren't included on insurance comparison sites. For these companies, you will need to check out their prices directly.
- For more information and suggestions on price comparison websites you may find helpful, follow the link below:

  https://www.moneyadviceservice.org.uk/en/articles/price-comparison-sites-guide

Auction sites

Auction sites such as eBay are increasingly popular as a way of buying and selling both new and used goods. They most commonly work by putting an item up for auction for which you can then submit a bid. The person who puts in the highest bid by the close of the auction is the successful bidder, and they will be expected to pay the sum they bid for the item concerned. As such, auction sites carry all the risks associated with online shopping, but there are a few other additional risks which are unique to them. When using auction sites:

- Only bid the amount you are willing to pay – do not overbid as you will be expected to honour your bid if you are successful.
- Look at the item carefully to make sure it is what you want. In particular, be wary of fake items
- Make sure you are familiar with the rules of the auction site when buying and selling items. In particular, find out what redress you would have if something went wrong
- If you are selling an item, make sure you only post it once you have received payment.
- Read the reviews for buyers and sellers to make sure they have a good rating and are reliable. You might also want to check if they are based in the UK as, if they are not, they may be harder to chase.
- Be clear about shipping and delivery cost. Sometimes the item can be priced cheaply, but the delivery costs are very high.
- When communicating with other sellers or buyers only provide the minimum necessary personal information.

Did you know?

As well as being convenient, it is possible to save money shopping online. Below are a couple of links to sites that provide some tips to help save money when shopping online:

https://www.moneyadviceservice.org.uk/en/articles/smarter-shopping---tips-and-tricks-to-save-money-when-shopping

https://www.moneysavingexpert.com/shopping/cheap-online-shopping-shopbots

Part 5: Banking online

Banking online is very convenient and secure and offers you choice, flexibility and control. You do need to take certain steps, however, to keep yourself safe. In this part of the module we will look at banking online as well as mobile banking. We will consider the key risks and how you can help stay safe.

What are the risks?

In a word, the risks associated with online banking relate to fraud. Essentially, you need to be wary of people trying to gain access to your bank account. This is usually achieved by trying to trick you into handing over security information such as your username, passwords or memorable information. There are two main techniques which might be used to try and get hold of this information:

- You could be tricked by phishing emails (that is, emails which pretend to come from banks but are actually fraudulent) into disclosing your password or other confidential details
- Identity theft caused by viruses or spyware which give someone access to your bank account

Remember

The same scams you face online you may also face by telephone. The most common scam is something called 'vishing'. Vishing is short for 'voice phishing'. It is where you receive a phone call from someone pretending to be who they are not. With online banking, the risk is that you might receive a vishing call pretending to be from your bank and then asking for your bank account and password details. **Actual banks will never ask you to confirm password details over the phone**. Should you receive a call from someone saying they are from your bank, if you are in any doubt, call them back using a number which you have confirmed is a recognised number for your bank (most debit and credit cards have a bank contact number on the reverse).

How can you keep yourself safe?

- Never login to your bank website through a link in an email
  Even if the email appears to have come from your bank, always type the web address for the bank into your browser directly. This will prevent you from being redirected to a fraudulent website.
- When you log in to your bank website, make sure the site is secure.
  As we have seen previously in this module, you can tell if a site is secure because the address will begin 'https' (with the 's' meaning secure) and there will be a padlock symbol in your browser window.
- When creating your login password for your bank, make sure it is strong.
  Make sure you use numbers, capital and lower cases and characters such as $%&. Also ensure your bank password is different to the passwords you use for social media. For tips on creating strong passwords, please see part 9 of this module
- Do not click on any pop ups which might appear when you are banking online.
  Indeed, the appearance of pop ups might be an indicator that something is wrong.
- Never disclose your bank login details whether via email or phone.
  You should never be asked to do this by a genuine bank.
- Go through your bank statements regularly and check all transactions.
  If you spot any which you did not authorise, contact your bank straight away.

Did you know?

Two factor authentication (or 2FA for short) is a process often used by banks to improve security. It adds an extra check to ensure you are authorised to access your account. Many banks provide a small electronic device which produces a one-time passcode for you to use in conjunction with your normal password before you can carry out a transaction. Other forms of 2FA include fingerprint scans, facial and voice recognition.

What should you do if you are a victim of fraud?

If you are the victim of fraud or if you are concerned your bank login details may have been compromised you should contact your bank immediately. It is important to remember that you are protected by law. This means that you will not be liable for any losses unless you have acted fraudulently or without reasonable care.

Mobile banking

Mobile banking involves using apps or mobile websites on smartphones and tablets to access your bank account while out and about. This form of banking is becoming increasingly popular and below are some specific tips to help you stay safe when using mobile banking:

- Only download banking apps from official stores.
  Only use the official app provided by your bank – it is worth reading the app reviews to check it is the official version.
- Do not use unsecured Wi-Fi networks for banking.
  It is better to use your 3G or 4G connection as it is more secure. For more advice on using public networks safely, please see part 6 of this module.
- Your banking app may provide the option of you being sent a text message.
  Some apps have the option of automatically sending a text every time a transaction occurs. If it does, it is worth turning this on so you are notified if any unauthorised transaction occurs.
- Make sure your mobile device is password or PIN protected.
  Increasingly protection might include fingerprint scans or facial recognition.

Did you know?

Contactless payment is where you pay for items without needing to use a card and PIN. It works using something called Near Field Communication (or NFC). NFC works through a wireless chip embedded either in your mobile phone, smartwatch or in your payment card. The chip contains your payment details and enables you to make payments of up to £30 at certain stores simply by waving your mobile phone, smartwatch or payment card over an NFC reader. Because you do not need to enter a PIN, the process is fast and convenient. For the same reasons, however, it is a potential security risk. If you make use of contactless payment, make sure your mobile phone is password/PIN protected and check your bank statements regularly.

Part 6: Using public computers and public Wi-Fi

You may find yourself out and about with your mobile device and using a public Wi-Fi hotspot such as those often provided in coffee shops. Alternatively, you may use public computers such as those provided in libraries and internet cafes. Use of public computers and public Wi-Fi is very common but there are some real risks. To help keep you safe, try following the suggestions below.

Using public Wi-Fi hotspots

- Use a secured network:
  Not all Wi-Fi networks are secure. If you can, when using a public Wi-Fi network, make sure it is secured. When you want to pick a Wi-Fi hotspot to log into, try and find one that by default has locked you out (i.e. it has the padlock symbol next to it). This indicates that you will need a password or some login details to access the network. Unsecured networks will not have any kind of security such as passwords or login. If you use an unsecured network there is a real risk that someone could intercept what you are doing online, such as capturing your passwords.
- Be careful leaving Wi-Fi on all the time:
  Sometimes your device may automatically connect to a signal without your knowledge. Consider turning Wi-Fi off when you are not using it.
- Be careful what network you choose:
  Unscrupulous people can set up spoof Wi-Fi hotspots with very similar names to those you might be looking to use. Let's say you are at Café Nero and you want to use their Wi-Fi. You search for available networks and find one called 'Café Ner0'. This is very likely a fraudulent network set up to capture all that you do online. It is always best to choose a provider who gives you log in details, so you can be sure of which network you are using.
- Limit what you do on a public network:
  Try and avoid doing anything on a public network which requires using sensitive data. In particular avoid any financial transactions, including any online shopping.
- Use a well-known provider:
  Where you can, make sure the hot spot is provided by a well-known and reputable company such as BT OpenZone or T-Mobile.

Using public computers (for example, in libraries)

- Don't leave the computer unattended with sensitive information on the screen:
  If you do need to leave the computer for a time, make sure you log out of any programs and close any windows which might show sensitive information. Be careful who may be watching over your shoulder when you are entering sensitive information
- Don't save logon information:
  If a site asks if you would like it to remember your username and password, be sure to click 'No'. It is also important, once you have logged in to a site, that you log out when done. It is not enough to just close the window – you will still be logged in.
- Avoid financial transactions:
  Try and avoid using public computers for anything that requires you to enter really sensitive information such as your bank account details or credit card number.
- Delete your browsing history
  Once you have finished using a public computer, make sure to delete your browsing history

Part 7: Viruses

What are viruses?

Viruses are programs that can attack devices such as computers, laptops, tablets and smartphones. There are many different forms of virus and a few of the most common are listed below:

- **Spyware**
  This is a particular form of virus which is designed to steal information about your activity on a computer, particularly your personal details. Some versions of spyware can log the keys you type (called key logging) and from this can steal information such as passwords and bank login details. Other forms can take screen shots of sites you visit and some can even take control of the camera on your device.

- **Trojans**
  These are programs which appear harmless but which contain hidden, harmful functions. Just like the Trojan horse in Greek mythology, trojan viruses are often hidden within what appear to be otherwise legitimate software. These might be files from music sharing sites, but can take the form of any file download or even an attachment to an email. Once the file has been downloaded, the trojan then enters your system where it can create a backdoor to gain unauthorised access to your computer.

- **Worms**
  These exploit security vulnerabilities to spread automatically to other computers through networks. They literally 'worm' their way from one network to the next, infecting as they go. They are able to replicate and spread to other systems without any warning or activation and this makes them much harder to contain and hence one of the most dangerous forms of virus.

- **Ransomware**
  This is a form of virus that locks a computer and then displays a message stating that the computer will only be unlocked if a sum of money is paid. The most common version of ransomware at the moment is 'CryptoLocker', so named as it encrypts all your data and the only way to unlock the encryption and get your data back is to pay the ransom. In some instances, the message will try and make it difficult for you to seek help by alleging that you have been involved in illegal activity or by displaying an embarrassing pornographic image on the screen. Often the amount of the ransom is not very high, making it very tempting to pay so you can recover your encrypted files. Payment of the ransom, however, does not guarantee that you will get your data back and, even if you do, it might encourage criminals to target you again in future.

These are just a few of the most common forms of virus and, unfortunately, there will no doubt be many more forms created in the future. Some viruses can have a whole range of effects, for example a virus might enter your computer as a Trojan before spying on you and then worming its way into other systems. It is not necessary to know every different type of virus that exists – it is enough to know that they exist and that they can do harm.

How could my system become infected?

Below is a table which describes the most common ways in which a virus can enter your device:

! **Visiting corrupt websites**	Especially high risk are pornographic websites or sites selling so called 'legal highs'. This can be a common way in which a ransomware virus can be picked up.
! **Downloading from websites**	Peer-to-peer file sharing sites can be particularly hazardous. If you download material illegally, for example music from a file sharing site, then there is a significant risk that the download will contain a virus.
! **Opening infected email attachments**	Emails received from unknown sources or which are unexpected are a high risk, and email attachments which end in **.exe, .txt or .zip** especially so.
! **Through removable media**	Memory sticks, external hard drives, CDs and DVDs can all contain viruses. This is especially the case if the media is not from a known and reliable source.
! **Downloading free software or apps**	Free software can often contain viruses and spyware, particularly if it is from an unknown or unreliable source. This can even include apps from an official store.
! **Connecting to a computer**	If you connect your mobile device to another computer, for example to install updates or load music, then you may inadvertently transfer a virus over from the computer.

How can I stay safe?

The impact of viruses on a computer can vary from simply slowing your system down, to completely crashing your system. Combine this with the risks of having your personal details stolen or having all your data encrypted and it is clear that it is worth taking all reasonable steps to avoid getting a virus on your computer or mobile device. To keep the risk of a viral attack to a minimum there are two things you can do:

1. Avoid doing those things which increase the risk of a viral attack (as above)
2. Ensure you have good internet security software installed in your device.

We will look at internet security in the next part of this module, but first we will look at some simple steps you can take to reduce the risk of a viral attack. Look at the table on the next page which gives tips on how to avoid viruses and then fill in the boxes to state how you are going to help keep yourself safe in future.

Tips for avoiding viruses	
✔	Do not click on links contained in emails from companies or individuals you do not recognise. Instead either type the full address out in a separate browser or hover over the link to find out where it will actually take you.
✔	Do not open attachments within emails unless you are absolutely certain they are legitimate.
✔	Visit only websites you know to be reputable.
✔	Check that anything you install or download is from a known and trusted source. Only download music from paid sites such as iTunes or Napster.
✔	Do not connect any removable media (such as memory sticks) to your computer unless you know they are safe.
✔	Because of the very real risk of a ransomware attack, it is worth creating a regular back up of all your important data. If you are unlucky enough to be the victim of a ransomware attack then you can re-install your backed-up data. For instructions on how to create a backup of your data, please click on the link below: **https://www.wikihow.com/Back-Up-Data**
✔	Most viruses require you to click on something to activate them and can tempt you to click on a link by pretending to be something they are not. Never click on 'pop up' messages as these often hide viruses.

If in doubt, don't click on it!

To help protect me from viruses I will…	
Action 1	
Action 2	
Action 3	

Part 8: Internet security

Even if you are very careful and make sure you follow all the precautions outlined on the previous page, it is impossible to avoid all viruses. This is why you need to ensure you have good internet security in place. Internet security/antivirus software works by:

- Scanning incoming emails for attached viruses
- Monitoring files as they are opened to make sure they are not infected
- Regularly scanning files on your computer
- Some software also scans external media as it is connecting

Did you know?

Viruses do not just infect computers. They can infect mobile devices such as tablets and smartphones. Even devices which were previously thought to be safe, such as iPhones, can now be infected by viruses. Even so, the risk of a virus infecting a mobile device is relatively low – most viruses are directed toward computers operating Windows.

You may well already have antivirus software installed on your devices, but if you do not then below are some of the most well-known suppliers:

- Avast
- AVG
- Bitdefender
- Bullguard
- Kaspersky
- McAfee
- Norton
- Sophos

For advice and reviews on internet security software, the link below provides some independent advice. Most security software charges an annual fee; however, some is free of charge and one example is included in the link:

https://www.techadvisor.co.uk/test-centre/security/best-antivirus-2018-free-paid-antivirus-reviews-3651652/

Make sure you have antivirus software installed and that you keep the software up to date. When your software runs out of date, make sure it is either renewed or replaced with a different software package.

Remember

Beware of antivirus software scams. These generally take the form of pop-ups which inform you that you have a virus on your computer and ask you to click on the pop-up to run a scan. If you do click on the pop-up, then rather than run a scan you will unknowingly download a virus onto your computer which stops it from working properly. You will then be asked to make a payment to fix the infection. To avoid this, if you see a pop-up warning you of a virus, run a full scan of your computer using your normal anti-virus software – don't click on the pop-up itself.

Part 9: Identity theft

What is identity theft?

Identity theft involves unauthorised use of your name and personal details to either steal from you or commit a crime in your name. In the UK it is the fastest growing method used to carry out criminal activity. Crucial personal information includes:

- Your name
- Your address
- Your date of birth
- Your phone number
- Your National Insurance number
- Your credit card number and CVC code
- Your bank account number and sort code
- Your passwords and PINs

It is important to protect your personal information while you are using the internet. Below are some of the best ways to protect your identity when online.

Remember

This module is focussed on staying safe online. The risks of identity theft, however, are not just limited to use of the internet – there are very real risks of identity theft from printed documents as well. A lot of information about you can be gleaned from printed bank statements and utility bills. Make sure you file such documents away safely. If you no longer need them, try and ensure they are shredded before you bin them. Alternatively, arrange for paperless bills or statements so that you do not have any printed copies to worry about.

Creating safe passwords:

Probably the most important way to protect your identity is to make sure you use effective passwords. It is very tempting to choose passwords which we can easily remember. The problem is that passwords which are easy to remember tend to be equally easy to hack.

If you use passwords which can be predicted, for example words which appear in a dictionary, then your password could quite easily be hacked using what is known as a 'brute force attack'. A brute force attack is one where a computer will simply guess your password until it gets it right. Because computers can make hundreds of thousands of such guesses a second, they can work their way through every word in the dictionary pretty quickly. To protect yourself, follow the three guidelines below:

1. Use strong passwords which contain a combination of upper and lower-case letters, numbers and special characters such as !@*&:
    - Example of a poor password – **banklogin**
    - Example of a strong password – **B@nkL0g1n**
2. Make sure you change your passwords regularly
3. Do not use the same password for all your accounts. In particular, do not use the same password for financial services as you do for your social media accounts.

All of this might sound rather difficult and you might be anxious that, if you follow these rules, you will simply forget all your passwords. That is where a password manager can

come in useful. Password managers remember your credentials – username and password – for a website and fill them in when you land on its logon page. You can create unique and complex passwords for each account you have and all you need to remember is your master password to access your password manager. If you don't want to create your own passwords, then password managers can also automatically generate and remember them for you. Be aware, however, that some password managers may make a charge for using their service. Some common password managers are 1Password and LastPass. To find out more information about password managers, please follow the link below.

http://uk.pcmag.com/password-managers-products/4296/guide/the-best-password-managers-of-2018

If you don't like the idea of using a password manager, then instead you might want to use one of the tips below to help you create memorable and safe passwords.

Use a base password.

Have a standard password that you can then tweak according to the service. For example, start with your favourite colour, for example orange. You can then create your base password by making this strong – **Or@ng3**. You can then use this base password for all your accounts by adding a second part which is unique to the account. For example, your bank account password can be created by adding **M1B@nk-** to the beginning. This would give you the password **M1B@nk-Or@ng3**. Your Twitter account might be **Tw1tt3R-Or@ng3** and so on.

Create your own code

You can replace the same letters with the same numbers or special characters each time you create a password. As long as you apply your rules consistently, this should help you remember whilst also making your passwords stronger.

Choose a favourite book

Build a password based on (for example) the first paragraph of your favourite book. You can include the page number, the first and last word of the second, third, or fourth line etc.

Build a password from a favourite song

For example, the lyrics from "My Way" might give you the password – **@nd-5o-th3-End.** Remember to use special characters, numbers and upper and lower-case letters.

Did you know?

There are some passwords which are so commonly used that they are not really secure at all. The most commonly used passwords include:

- Any numerical sequence such as 123456 or 654321 (almost one in five people use this type of password)
- Any repeated number such as 111111
- The word 'password' or 'password1'
- The word 'qwerty'

In addition to these, it is best to avoid any password which is based on a pet's name or the name of your favourite sports team. Both of these are pieces of information which might well be obtained from your social media profile.

Don’t give your personal information unless you know it is safe:

Above we considered a list of crucial personal information. This is the information that you want to keep safe and secure. If someone wants to steal your identity, it is this sort of information that they will need. To keep this information safe, make sure you follow the steps below.

Secure websites:

When shopping online only use reputable sites which are known to you. Before entering payment information into any website, make sure the site address begins with ‘https’ – the ‘s’ at the end shows that this is a secure website. If the site just has ‘http’ don’t use it. Your browser should also display a padlock symbol if the site is safe to use – you can click on this symbol to find out more information regarding the security of the site.

Email phishing:

Never respond to any emails which ask you to provide personal details such as passwords or account information. In all likelihood, such emails will be phishing scams designed to steal your personal details and use them fraudulently.

Social media:

Avoid including personal information in your social media profiles. Details like your phone number and address are sensitive personal information and need to be protected. Also, check your social media privacy settings regularly to ensure they are strong. For example, you might want to change your Facebook settings to ‘Friends Only’ for all posts. Facebook often makes changes to these settings and, when it does, this can even reset your secure settings.

Computer viruses:

Viruses can use spyware to steal your personal data. To protect yourself from these viruses, when using a PC or laptop make sure you have effective and up-to-date antivirus software running.

Remember

Make sure your device is PIN or password protected (or fingerprint/facial recognition protected) so that, should you lose it, a stranger will not be able to access all your personal data.

Part 10: Online dating

Should you decide to use dating sites or dating apps there is plenty of advice online about how to stay safe. We have tried to pull together the most useful information in this section of the module. As always, the purpose is not to scare, but to warn in the hope that the information will help you to stay safe.

Broadly speaking, there are two main risk areas when it comes to online dating:

1. **The risks you face online**. These risks tend to be of a financial nature such as being defrauded of your money, identity theft, blackmail etc.
2. **The risks you face when meeting in person**. These risks might occur when you actually meet the person, if you reveal where you live, or if the person picks you up for a date. The risks are of sexual assault, harassment or stalking.

In this section of the module we will look at these two risk areas separately and provide some advice on how you can stay safe when using online dating apps.

The risks you face online

The key risk area here is that the person you meet online may not be who they say they are. Indeed, their motives may not be to try and find a partner at all. Instead, their motive may be to make money from you. There are some warning signs which you might want to look out for:

- Asking for money. This might take the form of hard luck stories where they suddenly need money such as helping a sick relative. Alternatively, it might be a wonderful business opportunity, if only they had the money.
- Asking that you get off the dating site and communicate using a different (often less well protected) system
- Early and vocal expressions of love. If someone expresses strong feelings after a relatively short period of online contact then something is probably wrong. Often they are trying to manipulate your emotions.
- Asking for any personal information – for example email address, mobile number or even your home address so they can send you flowers.

This all might sound rather cynical, but the reality is that if you experience any of the warning signs above then something is probably wrong. The warning lights should start flashing in your head and you should probably stop any contact with the person.

On the next two pages are some guidelines on how to behave when using online dating sites or apps. Consider the suggestions and then fill in the action plan to say how you will keep yourself safe.

Remember

If you are the victim of any act of violence or abuse, you should report this to the police straight away. You could also contact Victim Support on:

- Call 0808 168 9111
- Visit https://www.victimsupport.org.uk/more-us/contact-us

Tips for staying safe when using online dating sites	
✓	Do not give out your personal information, including your email address. If you do want to give out an email address, then create one specifically for this purpose, so you can stop using the account if you need to.
✓	Use a photo of yourself taken specifically for the purpose. Do not use the same photo as you have on your social media as a Google image search will lead to your account
✓	Make sure that you have set privacy settings on your social media so that people who you meet on a dating site cannot find out any details about you that you do not want them to know.
✓	Be careful what username you choose. Avoid a username which reveals personal information (for example avoid using your surname, your date of birth or your location in your username).
✓	Use only reputable and trusted dating sites. At the time of writing, there are approximately 11,000 dating sites worldwide and not all of them are to be trusted. Ideally the dating site will be a member of the Online Dating Association and will display their logo (as shown on the right). ODA MEMBER
✓	At the first sign of any suspicious behaviour from another person, delete them and report them to the dating site.
✓	Beware of links and attachments. Avoid clicking on any links or attachments you might be sent – they could contain a virus.
✓	Don't share pictures or information that may give someone any sort of hold over you (for example photos of a sexual nature). They may use this to try and blackmail you. If someone does start to menace money out of you, don't pay. They would just be back for more. Instead, report them to the police.
✓	Talk to a friend or trusted family member about the people you date online. It is useful to get the opinion of another person; if you are going too fast, or disclosing too much, they can be your sounding board and can warn you.

Action plan to stay safe when using online dating sites:	
Action 1	
Action 2	
Action 3	
Action 4	
Action 5	

Tips for staying safe when meeting a date in person

If you want to meet a person from a dating site face-to-face, you need to continue to be careful and cautious to keep yourself safe. Remind yourself you still haven't met the person. No matter how long you have known the person online, they are still in many ways a stranger to you.

✓	Only meet with the other person when you feel ready. Do not feel pressurised to meet. In fact, if the person is putting you under pressure, it is likely a sign that something is wrong.
✓	Plan your first few dates carefully in advance. Agree with the other person where and when you will meet and stick to the plan.
✓	Arrange your first few dates during the day and avoid dates after dark.
✓	Keep early dates short – agree in advance that the date will be for one hour, for example.
✓	Meet in public and stay in public. A coffee shop is a good place to meet. Make sure there are other people around you at all times.
✓	Make your own way to the date and your own way back home. Avoid accepting a lift if one is offered. If you accept a lift, not only will you be on your own in a car with someone you don't know, but you will also be giving away details of where you live.
✓	Let your friends know. Before you go on a date speak to a trusted friend or family member and arrange to check in with them at an agreed time. Whilst on your date, you can always go to the toilet and message them to let them know you are okay.
✓	Leave the date if it isn't going well. Just make an excuse, get up and leave.

Action plan to stay safe when using online dating sites:

Action 1	
Action 2	
Action 3	
Action 4	
Action 5	

Part 11: Online exploitation and abuse

What is online exploitation and abuse?

Online exploitation and abuse is any type of abuse which happens on the web, be it through social networks, using mobile phones or online gaming. Children and young people are particularly vulnerable to online abuse, however anybody can be a victim. In this section of the module we will look at the different types of online abuse which exists and how you can keep yourself safe.

Cyberbullying:

Cyberbullying is the general term used to describe any bullying which takes place online. Essentially, cyberbullying is any online activity which is carried out with the intention of causing offence, distress or embarrassment. It takes many different forms, including:

- **Tagging without permission**: tagging is a way of connecting an online image with a particular person. Tagging someone's name against an embarrassing or manipulated image without their permission is a form of abuse.
- **Flaming**: this involves posting derogatory or personal comments about another person. This might involve posting false information which damages a person's reputation, or it might be revealing sensitive private information, such as details of a person's sexuality.
- **Sexting**: sexting is the sending of sexual texts or images. Where this is consensual between the individuals concerned then it may not be malicious, although it may still be inadvisable. Where this sort of communication has not been invited, however, then it may be very unwelcome and potentially offensive, alarming or even intimidating.
- **Impersonation**: this involves pretending to be another person and then carrying out actions which are attributed to them. This might then expose the victim to ridicule or the belief that they hold controversial views that they do not, in fact, hold.
- **Online game abuse**: many online games provide forums for players to communicate with each other. Sometimes this communication can become abusive or exploitative.

Trolling:

Trolling can occur in online communities such as chat rooms, blogs and forums. The troll will post comments which are disruptive, offensive or inflammatory with no other real purpose than provoking an emotional response in others. This emotional response is most commonly irritation, but they can sometimes also be upsetting. It is the anonymity that the internet provides that gives the 'troll' a forum to be offensive without any real consequences.

Webcam blackmail:

This is a particularly nasty process that involves a person being lured (usually by someone they have formed an online relationship with) into taking off some or all of their clothes in front of their webcam. The victim is then informed that the video of them without their clothes has been recorded and will be posted online unless they pay a fee. This fee is often a substantial sum of money. Sometimes, rather than requiring a fee to be paid, the blackmailer will threaten the victim into performing intimate acts in front of their webcam. As with Ransomware, even if the blackmailer is paid or their demands are met, there is absolutely no guarantee that they will not continue to blackmail the victim. Indeed, success

is likely to result in the blackmailer continuing, or increasing, their demands. Webcam blackmail can have a devastating impact on victims and in some instances has led to the victim self-harming and even committing suicide.

Revenge porn:

This is the process of making public explicit images of an ex-partner without their consent. The images will usually have been taken during an intimate relationship and will have been understood to be private between the two people concerned. If the relationship ends badly, however, then sometimes, as a form of revenge, one person uploads the private and personal images online. The images may also be tagged with information identifying the victim. As well as a form of emotional abuse and exploitation, this can also become a form of blackmail, where the victim is threatened with explicit images being posted online.

Child sexual exploitation:

Child sexual exploitation is where an individual or group manipulates a child or young person under the age of 18 into sexual activity. Increasingly technology is being used as a tool for child sexual exploitation by involving children and young people in looking at, or being involved in, pornography. 'Online grooming' is a term often used to describe the process whereby children and young people are sexually exploited online. Most commonly, groomers will go to social networks (usually ones used by children and young people) and pretend to be one of them. They may well set up a complete profile as a young person, including pictures. They will seek to gain the trust of the child or young person before steering conversations towards sexual experiences, eventually leading toward asking the other person to send them sexual photographs or videos of themselves. Some may try to arrange meetings. In some instances, the groomer may then blackmail the child or young person, threatening to share the images they have provided. In the same way children and young people may be vulnerable to online grooming and abuse, so might vulnerable adults.

Action plan to reduce the risk of online abuse:

So far in this section we have looked at some of the most common forms of online exploitation and abuse. On the next page are some suggestions as to how you can keep yourself safe. Have a quick look at these suggestions and then complete the sheet on what actions you will take to help you reduce the risk of online abuse.

Remember

Even if you know that the other person is an adult, you should think very carefully before including any sexual content in your online communication. Even if you think you are just flirting harmlessly, there is the risk that the other person may feel intimidated and your behaviour may be regarded as harassment. The best rule of thumb is to avoid sexual content in your online communication.

Any sexual communication with a child is an offence under the Serious Crimes Act 2015. Unless you are certain that the person you are communicating with online is an adult, your interaction should never include sexual content of any kind. Never assume, just because someone says they are an adult, that this is necessarily true – as we have seen earlier in this module, people can pretend to be who they like online.

	Tips to reduce the risk of online abuse
	Cyberbullying and Trolling
✓	Block cyberbullies' and trolls' social media, email and instant messaging accounts
✓	Report cyberbullies and trolls to your internet service provider, mobile phone provider (if in the form of texts or calls) or relevant social media site.
✓	Do not reply to cyberbullies or trolls – this is likely to just make things worse
✓	If bullying or trolling is serious, for example involving threats, then report it to the police
✓	Seek support from friends, family or Transform staff
	Webcam blackmail
✓	Be careful who you accept invitations from or send invitations to on social networking sites – do not accept friendship requests from complete strangers
✓	Make sure you have activated the privacy settings on your social networking accounts. See part 2 of this module for more information on social media.
✓	Remember that whatever you do or say online might remain there permanently – think before you post anything potentially embarrassing
✓	Never let yourself get lured into removing your clothing or performing sex acts in front of a webcam
✓	If you are the victim of blackmail do not respond to the blackmailers demands, but report the incident to the police
	Revenge porn
✓	Remember that even the closest relationship may end in the future
✓	Think very carefully before allowing anybody to take intimate photos or videos of you or taking them of yourself
✓	If you are the victim of revenge porn report it to the police – revenge porn is a crime punishable by up to two years in prison
	Sexual exploitation
✓	Remember – people online may not be who they present to be. Just because someone says they are a young person does not mean this is true
✓	Do not share personal information online – please see part 9 of this module for more details about protecting your identity
✓	Ensure you have effective privacy settings on your online profiles so only friends and family can view them
✓	If you are a parent, make sure that your children are aware of the risks of online grooming and discuss their online experiences with them regularly. You may also want to ensure that parental controls are set on any devices your children use.

To help protect me from exploitation and abuse online I will…	
Action 1	
Action 2	
Action 3	
Action 4	
Action 5	

Remember

Sexual harassment is defined as any unwanted behaviour of a sexual nature which violates your dignity, makes you feel intimidated or humiliated or creates a hostile environment. Sexual harassment can include sexual comments or jokes, emails or texts with a sexual content or photos of a sexual nature.

If you are the victim of sexual harassment, exploitation or abuse online then it is important to remember that it is not your fault and support is available both from Transform staff and from Victim Support. Victim Support can provide emotional support and advice on what to do next. You don't have to report the crime to the police, the service is completely confidential and it doesn't matter how long ago the crime took place. To contact Victim Support:

- Call 0808 168 9111
- Visit https://www.victimsupport.org.uk/more-us/contact-us