babcock™

Keeping Yourself Safe

As part of your Babcock training programme, you will be asked to use the internet for research and assignment purposes. We would also like to communicate and support you via e-mail and text between visits. For this reason and as part of our duty of care to all learners, it is very important to us that we provide you with the knowledge and tools to help keep you safe on-line and to support you if things go wrong.

Today's Online World

With the freedom of online communication comes the increased opportunity for criminal activity. For many, these incidents are just frustrating and can be remedied, but for others online bullying and other criminal and fraudulent activities can be very serious, sometimes with tragic consequences.

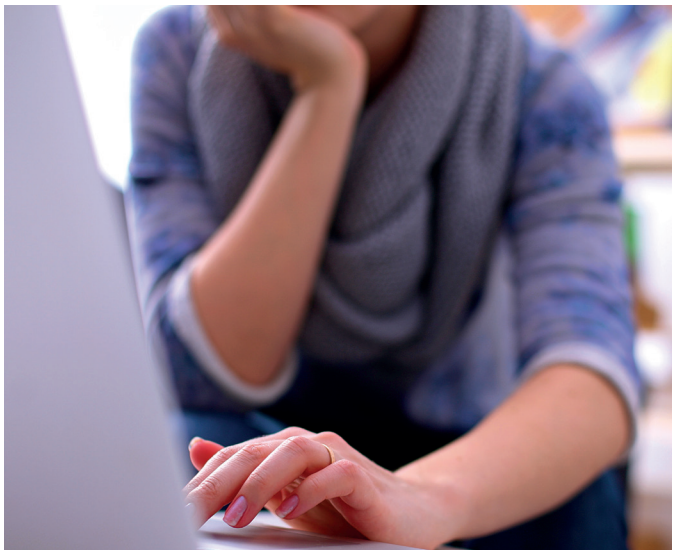
The key thing to remember is that no one is immune, so it is very important that you are constantly alert and always observe the basic principles for keeping safe online.

Phishing

Phishing involves the sending of bogus emails, instant messages, text messages or letters to numerous randomly generated addresses, each containing malicious attachments and/or website links.

On opening or clicking, the unsuspecting person is usually directed to a hoax website where login or other personal details may be requested. Once inputted, criminals then use this information to commit crimes such as identity theft and fraud. In addition the person runs the risk of their computer or smartphone being infected by viruses.

Often the communications are very convincing and appear to come from a legitimate source including high street banks, building societies and online retail outlets.



Recognising a Phishing Message

Legitimate organisations, including banks and other financial institutions, will never ask their customers for passwords or any other sensitive information using email or by asking them to click on a link to visit a website.

Criminals/fraudsters rarely know your name so will address you in generic terms, for example 'Dear Valued Customer'.

To get around spam filters, phishing emails often include strange 'spe11ings' or 'cApitALs in the 'subject' box and spelling or grammatical errors in the email contents.

Responding to a Phishing Message

When responding to emails or phone calls, never give out your login or personal details.

If you detect a phishing email, mark the message as spam and delete it to make sure it cannot reach your inbox in future. Your employer may have further guidance on what to do in this situation and who to report it to so please check with your line manager or IT department.

Never respond to a message from an unknown source as this provides verification that your e-mail address is active, allowing further malicious emails to be targeted. Take care not to open any attachments or click on embedded links.

If you have lost money or information or your computer has been taken over by a phishing or malware attack, talk about it to someone you trust and report to ***Action Fraud*** or your local police.

Identity Theft and Identity Fraud

Identity theft is the term used when criminals, in particular, fraudsters, access sufficient personal information about a person's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud.

Identity theft and fraud is most commonly used to:

- Open bank accounts and obtain credit cards, loans and state benefits.
- Take over existing accounts.
- Order goods and set up contracts, in particular for mobile phones and expensive online purchases.
- Obtain genuine documents such as passports and driving licences.

Being a victim of identity theft and fraud can be very traumatic and can have a serious impact on your personal finances, i.e., making it difficult to obtain loans, credit cards or a mortgage.

Keep yourself safe by:

- Checking your bank statements carefully and report anything suspicious to the bank or financial service provider concerned.
- Don't leave things like bills lying around for others to look at and always shred any personal information prior to disposing of it.
- If you're expecting a bank or credit card statement and it doesn't arrive, tell your bank or credit card company immediately.
- If you move house, ask **Royal Mail** to redirect your post for at least a year.
- Do not share account information with anyone including family and friends.
- Have up to date and effective antivirus/antispyware running on your computer.
- Never give out private and personal information data in response to an email, text, letter or phone call unless you are certain it is a genuine request.
- Be aware of people looking over your shoulder when you are entering private information on a computer, /tablet or ATM.

Shred documents that show your personal information.

If you think your identity has been stolen:

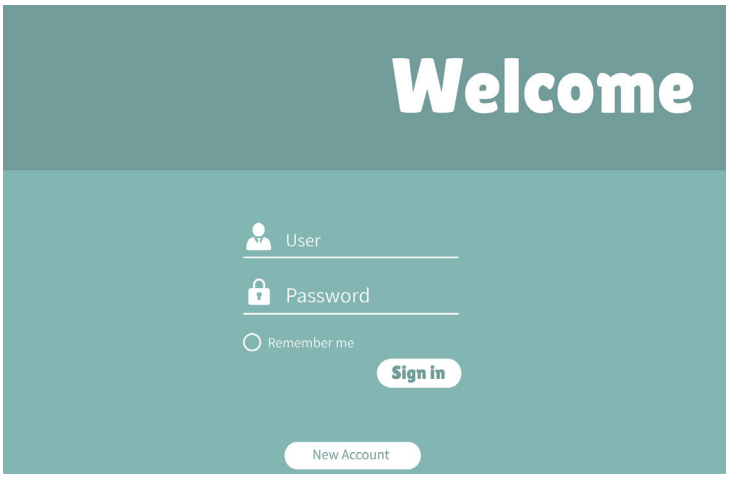
- Take immediate action to minimise the impact of the theft.
- Contact any affected websites and advise them about the problem and change your password on other websites in case your information has been compromised there.
- Tell your bank, building society, credit card company etc and get advice on freezing accounts and getting new cards, passwords and PINs etc.
- Check your other personal information, such as addresses, to make sure it is still correct where it is used.
- Report all lost or stolen documents (passports, driving licences, credit cards etc) as soon as possible to the relevant issuing authorities.
- Change any compromised PINs.

Passwords

Passwords are the most common method to prove your identity when using websites, email accounts and your computer itself. Strong passwords are essential to protect your security and identity.

If someone else knows your passwords they can impersonate you to commit fraud and other crimes, such as:

- Accessing your bank account.
- Accessing private information on your computer.
- Buying items online with your money.
- Sending emails in your name.
- Impersonating you on social networking and dating sites.



Don't use the following as passwords:

- Your username, actual name or organisation name.
- Family members' or pets' names.
- Yours or your family's birthdays.
- Favourite team or other words easy to work out with a little background knowledge.
- The word 'password'.

Some advice on passwords:

- Never disclose your passwords to anyone else.
- If you think that someone else knows your password, change it immediately.
- Use a different password for every website. If you have only one password, a criminal simply has to break it to gain access to everything.
- Don't write down your passwords.
- An alternative to writing down passwords is to use an online password vault or app.

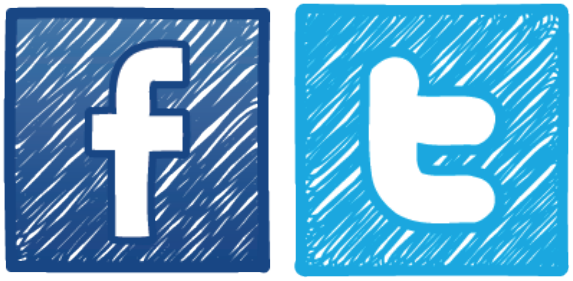
Social Media Networks and Gaming Sites

The use of social media including online gaming networks has seen a huge growth and for many is now part of the way we live and communicate. However, becoming part of a network of millions of people you don't know can carry risks, with people and criminal groups, potentially looking to use the information you and your friends post for more sinister reasons.

Social media can bring so many benefits but it is important to also be aware of the risks:

- Disclosure of private information by either your or friends/contacts.
- Bullying.
- Cyber-stalking.
- Online grooming and child abuse.
- Coming across comments that are violent, sexual, extremist or racist in nature, or offensive activities and hateful attitudes.
- Friends, contacts and companies posts encouraging you to link to fraudulent or inappropriate websites.
- People trying to persuade or harass you into changing your basic beliefs or ideologies, or adopt an extremist stance.
- People hacking into or hijacking your account or page.
- You or your family posting that you're away or going on holiday thus advertising that your home is empty and leaving the way open for burglars.

It is important to check the privacy settings for all social networking sites that you use as many are different and could result in you sharing posts and photographs with a far wider audience than you intended.



Remember
Never share or post anything without the owner's consent.

Reputation – What you post online can remain accessible for a long time, so stop and think before you post anything that may cause you or your family and friends' future embarrassment and distress. Never share or post anything without the owner's consent. Remember that many companies routinely view current or prospective employees' social networking pages, so be careful about what you say, what pictures you post.

Identifying info – Choose a profile picture that doesn't give away personal information such as where you live or where you go to work.

Keep your personal info safe – don't share or post your address, phone number and never give any information to anyone you don't know and trust.

Remember virtual friends are not the same as 'real' friends – be mindful of whom you are speaking or chatting online to and be cautious about any requests they make and the messages they are giving out – are you really happy with what you're hearing or being asked to do? If in any doubt, stop the conversation and speak to someone you trust.

Online Bullying

Sadly, with more of us now using social media and chat sites, incidents of online bullying, also known as cyberbullying, have seen a significant increase.

Bullying is the act of someone or a group of people upsetting, humiliating or hurting another person either face to face or via digital technology. Online bullying can happen to persons of any age and background and occurs via:

- Networking and gaming sites
- Email
- Texting

Unlike face to face bullying, the perpetrator is usually always anonymous, so could be anyone the person knows or someone they meet or pass every day in the street or work. If you are receiving upsetting or unwanted messages, you can either block individual users if this service is available or report them to the network provider.

Save the evidence. This will help you explain to people what is happening. Take screenshots, save the messages. Don't delete anything, but don't reply either. Retaliating can often make the situation worse and may end up with you getting some blame. There isn't a specific online bullying law in the UK, but some actions can be criminal offences under different laws.

If you are affected by online bullying here are a few things that you can do:

- Talk to a friend, family member or other trusted person about what is happening and how it makes you feel.
- Report serious bullying such as threats of physical harm or abuse, to the police.

Warning: Individuals have been prosecuted for abusive behaviour towards others on social networking sites. We are all very different and what makes one person laugh may be considered very hurtful to others. Don't post anything that you wouldn't be comfortable saying to a person's face.

Grooming

Grooming is a process by which someone builds an emotional connection with predominantly a child, young adult or vulnerable person, to gain their trust for the purposes of sexual abuse or exploitation. Groomers can be male or female and any age and often know the victim. However, for many victims the groomer is a total stranger. They may not even target a particular victim, but instead use social networking sites, instant messaging apps., including teen dating apps., and online gaming platforms to send messages to hundreds of young people and then just wait to see who responds.

Increasingly, groomers are persuading their victims to take part in online sexual activity. Once a victim is selected, they make contact, usually hiding their own identity and taking on the persona of a 'friend'. They will then start to build a relationship.

When sexual exploitation happens online, victims may be persuaded, or forced, to: send or post sexually explicit images of themselves, take part in sexual activities via a webcam or smartphone, or have sexual conversations by text or online.

Remember
You should never feel pressured into anything, including sending intimate photos, even if it seems as though everyone else is doing it.

Be aware, as soon as content is sent or posted publicly it's no longer in the sender's control and can be viewed by anyone, even potential employers.

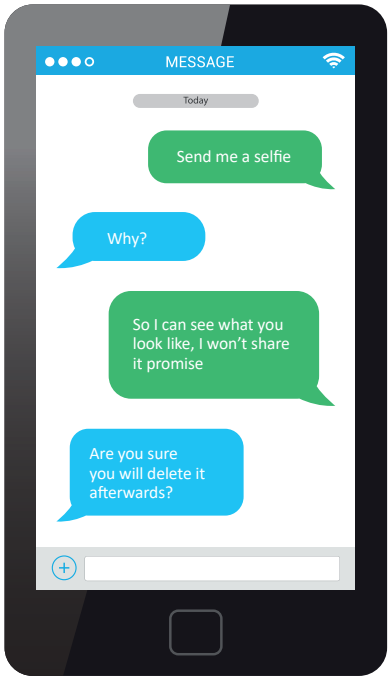
If victims threaten to report the abuse, groomers often turn to blackmail and threaten to send images, video or copies of conversations to the victim's friends and family unless they continue to take part in other sexual activity.

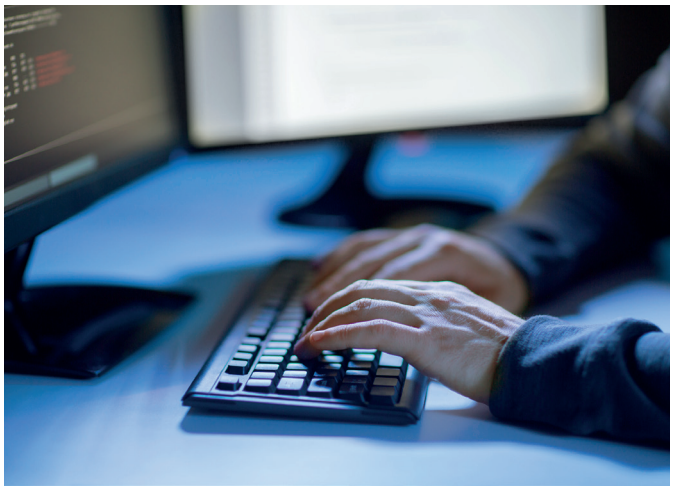
Sexting

Sexting - This is when a person takes indecent images or video of themselves (and sometimes even of friends) and sends it to a friend or boy/girlfriend via their phone or publishes it on the internet or on social networking sites.

At the time this activity may seem like 'harmless' fun and even a good way to get themselves liked or to show someone they like them. For others it may make them feel more sexually confident or grown up.

However, the most common reasons are peer pressure from partners and friends and online grooming by strangers. It is illegal and a serious criminal offence to take, hold or share "indecent" photos of anyone under the age of 18. The maximum penalty is 10 years in prison.





Revenge Porn

Revenge Porn is the illegal sharing of private sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress. The images are sometimes accompanied by personal information about the subject, including their full name, address and links to their social media profiles.

The offence applies to both online and offline images e.g., the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image.

In February 2015, 'revenge porn' became a criminal offence in England and Wales and if convicted, could result in a two years in prison. Stop and think - What happens if a relationship breaks down? Could you still trust your ex partner/friend not to publish an image out of anger and upset? If they do, it can be in the wider public domain within minutes.

If you're worried that you might have shared too much, check out this great guide from the UK Safer Internet Centre, ***'So You Got Naked Online'***, which will help you figure out if you want or need to do something.

Radicalisation and Extremism

In the UK we have the right to express our viewpoints and to act how we want, providing our actions are kept within the law. For example, if you feel strongly that closing or removing a local facility or service is wrong, under our 'freedom of speech', you can protest about it. However, as soon as you use threatening or violent language or behaviours or participate in the destruction of other people's property, this becomes illegal and could then lead to prosecution.

Online Radicalisation

A worrying new threat affecting people from any background, any community, or any religion, is the increasing use of the internet and social media to entice allegiance to extremist groups and to adopt increasingly dangerous political, social, or religious ideals, often referred to as radicalisation. For some, as we often see in the news, this can lead to horrific criminal and terrorist actions, both in the UK and abroad.

If you are concerned that you or a family member/friend are being radicalised and coerced into taking part in extremist and criminal acts, please share it with someone immediately. Your local police will be able to provide specialist support.

Extremist groups target individuals or groups of people who could be easily radicalised, usually based on their experiences, state of mind and/or upbringing. Often these people are vulnerable and the internet provides an ideal platform to create interest and to communicate with them; with the objective of grooming them into a system of extremist radical beliefs. The internet enables large numbers of people to be reached, in a wide geographic area, and with little effort by the extremists.

Radicalisation can be really difficult to spot. It is important to look out for any signs.

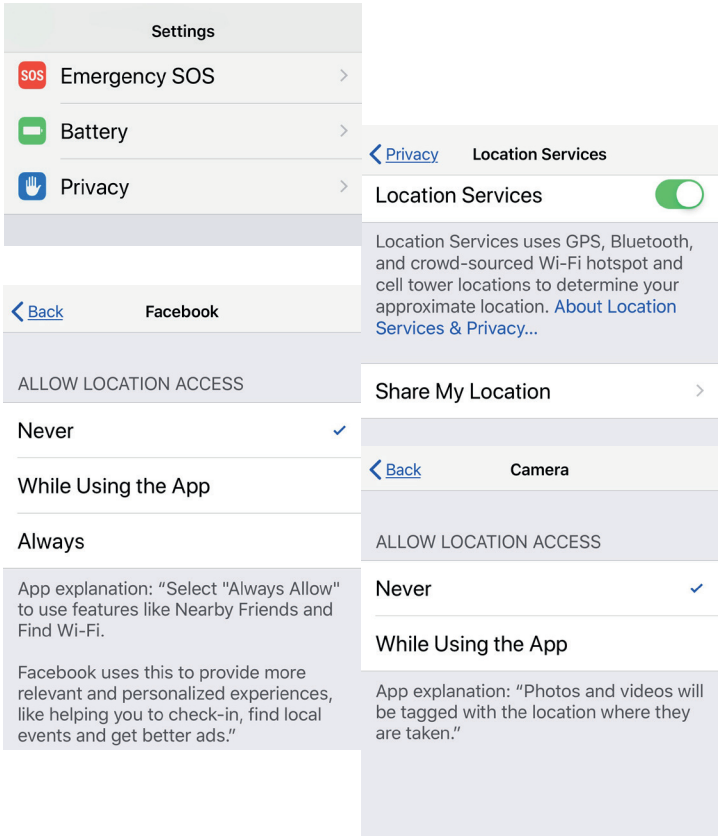
Social media and chat rooms are used by extremists to research and seek out vulnerable people with the potential for radicalisation. They are easy to identify from their profiles, posts/tweets, photos and lists of friends.

So how can you guard against this?

- If you have family members, friends or others that you think may be susceptible to radicalisation, keep an eye on them.

  Look out for:

  - Changes in behaviour.
  - Withdrawal or introvert for no apparent reason.
  - Changes in their beliefs.
  - Them making unusual travel plans.
- Report attempted or actual radicalisation immediately including material promoting terrorism or extremism.



Remember
Geotag settings are generally built into the device or app and can default as 'on' without asking for your consent first.

Geotagging

Geotagging is powered by the global positioning system (GPS) or satellite positioning used by a device and/or app.

Your geographical location is embedded as 'metadata' such as place co-ordinates (latitude and longitude), bearings, altitude, distances, or even place names and associates this data with the digital information you are sharing online, such as a photo, video; or when you 'check in' or post that you're doing a particular activity; e.g. out for a meal, at home, at work, on holiday, gone to the gym, bored or had a row with parents etc.

Use of online maps, finding a nearby shop, or locating friends etc. are all good examples of legal ways we can utilise geotagging.

However, criminals can learn patterns. This is called cybercasing and it refers to how geotagged text, photos and videos can be used by criminals for burglary, identity theft, stalking and cyberstalking and grooming including radicalisation. If you 'check-in' or post at the same coffee shop or gym at the same time on specific days, someone could determine your routine and exploit that information to their advantage. Paedophiles stalking children want to see photos and can learn where they live, what school they go to, what parks they frequent, and what interests they have.

Aside from any visible landmarks in a photo, criminals may also note from a photo you took in your home what valuables you own and can simply wait for you to post a photo whilst no-one is home, all using the geotag data you have inadvertently supplied.

Research how to switch your location setting(s) to 'off', as each device and app may have different privacy systems. Also, check your family and friends' privacy settings as they may be inadvertently sharing not only their own; but your location too, which could potentially be seen by criminals. And, ask yourself, do you really know the 100+ so called 'friends' you have on social media that you're sharing all this personal information with?

Tips for Staying Safe Online

1. **Never give out your password** and adopt the 8 + 4 Rule. This rule helps you to build strong passwords. Use at least eight characters with one upper and one lower case, a number and a special character like an exclamation mark. The more random the password the better.

2. **Protect your identity.** Keep your privacy settings as high as possible and don't share personal information online such as your address, email address or mobile number. If you are using social media check your privacy settings and make sure only friends can see your posts.

3. **Be aware of your digital footprint.** Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it, it's not just yours anymore.

4. **Think before you post.** Social media and some websites are great for airing your opinions. Remember the potential damage that can be done with the incorrect use of social media both in and out of work. Nearly all organisations will have a social media policy – check if yours does and make sure you adhere to it.

5. **Know who you're dealing with.** Many people only meet up with or chat with people they know in person, and that's a sensible approach. But if you do meet people you don't know, use the same caution that you would offline. Always remember people may not be who they say they are, so be mindful about what you say about yourself.

6. **Practice safe surfing & shopping.** When shopping online, or visiting websites for online banking or other sensitive transactions, always make sure that the sites address starts with "https", instead of just "http", and has a padlock icon in front of the website address. This indicates that the website is secure.

7. **Boost your network security.** Make sure that your connections are secure. When at home or work, you probably use a password-protected router that encrypts your data. But, when you're out and about, you might be tempted to use free, public Wi-Fi. The problem with public Wi-Fi is that it is often unsecured. This means it's relatively easy for a hacker to access your device or information.

8. **Keep up to date.** Keep all your software updated so you have the latest security patches. Turn on automatic updates so you don't have to think about it, and make sure that your security software is set to run regular scans.

9. **Use a firewall.** This is an electronic barrier that blocks unauthorised access to your computer and mobile devices; this will help to ensure that your documents, files and information are safe. You should always use comprehensive security software, and make sure to back up your data on a regular basis in case something goes wrong.

10. **Protect your mobile life.** Mobile devices can be just as vulnerable to online threats as laptops and computers. In fact, mobile devices face new risks, such as risky apps and dangerous links sent by text message. Be careful where you click, don't respond to messages from strangers, and only download apps from official app stores after reading other users' reviews first. Make sure that your security software is enabled on your mobile, just like you would on your computer and other devices.

11. **Click smart.** Many of today's online threats are based on phishing. This is when you are tricked into revealing personal or sensitive information for fraudulent purposes. Spam emails, phony "free" offers, click bait, online quizzes and more all use these tactics to entice you to click on dangerous links or give up your personal information. Always be wary of offers that sound too good to be true, or ask for too much information.

12. **Keep your guard up.** If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website and tell a trusted suitable person immediately.