Living & Working in a connected world.

A Guide for young people living away from home for the first time.

Spring 2015

SIMS ACCREDITED Support Team

A MEMBER OF UKCCIS
UK COUNCIL FOR CHILD INTERNET SAFETY

Contents.

Introduction.

This guide is meant to be an important help to young people who are leaving school. It does not matter whether you are going to stay living at home, moving away, taking a gap year, or going straight to College or University, or heading off into the world of work.

Good advice is still good advice.

Young people have contributed to the writing of this guide, and it is packed full of useful advice not just for you, but for your family too.

There is not very much in the way of technical stuff in here. E-safety, that is, your safety in living, working and playing in a connected world, is not really about techy stuff. It is, however, about what people **do** online. What you do, what others do, and what potential abusers do.

The word “abuser” in this guide means anyone who wants your identity, or to hack your computer, or may have a sexual interest in you that you do not want. We will use the term abuser for all these things.

We could give you the best advice in the world but it would be useless unless ***you*** do something with it. It is not enough just to read this guide and then forget it. You have to decide what you need to do to stay safe. Then, you need to ***do*** it.

In this guide, there are examples, written in italics, of what has happened to real people just like you when they did not follow the advice. It is not “scare story” stuff, they are ***real*** examples from ***real*** people.

The aim of this guide is not to stop you enjoying and benefitting from the internet. In fact, it is exactly the opposite. We want you to enjoy the fantastic benefits of easy communication, and having fun online.

No matter if you are staying at home when you leave school, going to work, or going to University or college, whether full or part time, taking good e-safety practices with you will keep you safe, as well as your family and friends. If you are living away from home for the first time, you could form an e-safety group at college and make sure they are supporting students well in this essential area of Safeguarding.

This guide contains the latest advice, but remember, e-safety changes all the time.

Enjoy the online world – it’s great – but stay safe.

Technology made simple.

Equipment you will probably have, things you might have…..

Probably have	Possible risks.
Your Mobile phone 	• Phones that do not lock themselves after a period of inactivity are wide open if they are stolen or lost. • Bluetooth networks can be hacked or hijacked unless protected by a strong password. • Your phone SIM card is probably worth more than the phone! Information is valuable. • **4G phones** and service are now coming. 4G offers incredibly fast internet connections over your mobile phone. So fast, in fact, that it is even easier than ever to exceed your bandwidth allowance. Everything comes at a price.
Your Computer/laptop  	• Computers can be stolen. (College halls of residence or student accommodation are not secure.) They need a strong password to protect them. • Disposing of old/unwanted computer equipment, including USB devices is an easy way for an identity thief to read your hard drive or USB disk. One way to prevent this is to physically destroy the hard drive or USB key. • **Essential that you have a good, recognised anti-virus, anti-spyware, anti-malware product installed and regularly updated.** This will probably make your system run a little slower, but it is vital that you have it. Some companies like BT Total Broadband include it as part of the subscription. (At the moment, this is less important for Mac users – but keep your eyes and ears open. • **NEVER let Windows (or any other operating system or web browser) "remember your password."** It is very tempting and there are even products called "Password Vaults" that offer to remember your password for you. Even Facebook now offers the opportunity for you to use your Facebook credentials to access any and all websites you use. **This means nothing more than Facebook have access to all your accounts**. It is a pain having different passwords for different accounts, but if your money or your identity is involved it is absolutely vital for your safety that you have good strong passwords, that you change them regularly and that you NEVER allow a computer or other device to "remember" your passwords for you.
Your MP3 player 	• Some MP3/4 players have access to online purchasing. iTunes for example can be linked to a bank account and music can be purchased through the device itself. If you lose your ipod, anyone finding it has access to your bank account and can buy music that you could end up paying for

Your USB memory key 	• Information contained on these is very useful. • Does your USB memory contain personal information? • Does your USB memory contain personal images? • **Is yours password protected and encrypted? Even using freeware such as Tru-Crypt is better than nothing.**
Your Digital camera/video camera 	• Photographs can be enhanced, changed, and published. • Backgrounds can often yield a huge amount of information. • You do not have to post high-resolution photographs on the internet. • The same goes for video. • **Once you post an image online, you lose control of it forever. It takes less than 8 seconds for a new image to be seen, copied and reposted.** • Some new cameras now automatically upload images to a "cloud" storage. Make sure your camera connects safely so your images can't be lost or hijacked.
Things you might have	
Your wireless network at home 	• Easy to buy and set up. • Needs to be encrypted with a good strong user admin password if you have set one up yourself. (BT Homehubs etc are already encrypted, but beware the hubs that have the admin password printed on the back! Don't put them on window ledges.) • Currently, the industry standard encryption for wireless networks is called WPA-2. WEP and WAP are also available but are far less secure. • If someone DOES hack your wireless network, please make sure your computers have a username and password so that the hacker cannot access them. • It is possible to use someone else's wireless network – **be very careful of this – it may be possible for them to see what is on your hard drive.**
Your Internet games console	• Not all gamers are interested in the game! Some are identity thieves, some are sexual predators. • Young people have found themselves in difficulties from engaging too closely with other gamers. • There is evidence that suggests engaging with violent games a lot can influence your behaviour in the real world. **It can also be addictive.** Employers and universities do not have a lot of time for people who are too tired through playing online games to do their job properly.

	• Some gamers are there to gain your trust, and persuade you to part with information that they can use. • Some gamers may have a deviant interest in you. People have found themselves being stalked both online and in the real world. Play the games, by all means, just don't get too friendly with people you do not know in the real world. • Some game companies do not include all the information on the disc. Some ask you to download items over the internet. This can be expensive if you have a limited bandwidth on your internet account, and **very expensive** if you do it on your mobile phone!
Your Webcam 	• Webcams have a number of myths around them. Here is the reality! i) Video conferences are NOT secure ii) Video streams **can be recorded and then uploaded to the internet**. iii) Not all video cameras have a light on them telling you when the camera is "live". iv) Sometimes, what can be seen in the background of a shot is every bit as important as what is in the foreground. v) Seeing (and hearing) is NOT believing. You have no way of knowing that the other person is not sending you a video stream of someone else. There are also voice synthesizers that are freely available that can change an adult male voice into a female-sounding voice, and visa-versa. Unless you know the person in the real world, you have no way of knowing they are who they say they are online.

Probably have	Possible risks.
Your Bank account 	• Online banking is very good, but your password MUST be different from any other password, and you MUST change it regularly to be safe. • **NO** bank will ever send you an email asking you to "confirm your details". • **NO** bank will ever threaten to suspend your account over the internet.
Your Bank card 	• **PIN numbers are only four digits long. It is easy for someone to read yours.** • Take a good look at each and every cashpoint you use. If you think it doesn't look right, don't use it. • Shield your pin number when you type it in. • Avoid "pattern pins"- such as all four corners of the keypad, or any easily recognisable shape. • **NEVER give your card number, expiry date or cvc**

	on any website that does not begin with https:// • Bank card fraud is one of the highest risks to everyone today, not just young people • **Change your PIN at least every 90 days.** •
Your Online shopping accounts 	• Same username/password for lots of accounts? Change them. **Now**. • Use different passwords for each account, and change them at least every two months. • No matter how you pay, always check that they offer secure payment services. **NEVER enter your credit/debit card into an website that does not begin with Https://** • Avoid letting Internet Explorers **"remember your password."**
Your Membership of websites 	• Same username/password for lots of accounts? Change them. Now. • If your password is weak, it can be hacked and your account can be taken over – with embarrassing consequences.
Your Social networking Sites 	• Governed often by other countries laws. • Terms of use and privacy notices are very hard to read, yet you are giving the site owners rights to use your information. You really should take some time to read them – no matter how boring they are. • It is quite possible that future employers will Google you and have a look at your online presence. • Accepting people onto your contacts lists who you do now know in the real world is always risky. You have absolutely no way of knowing that people are who they say they are. • **Social Networking is NOT about joining people together in Peace, Love and Harmony. It is often nothing more than market research dressed up with a "Friendship" user interface. You should be very careful what information you supply to any social networking provider.** Have ***YOU*** read ***AND UNDERSTOOD*** all the terms, conditions and Privacy Statement of Facebook? No? Thought not.

The same password for many different accounts. 	• By far and away the highest risk that people of all ages have. Remembering complex passwords is not easy. Having the same password for multiple accounts is very high risk. • **As of January 2013, there has been a run of primary email accounts being hacked. Change your primary email account password regularly.**

If you are in college, university or the workplace, remember that access to their ICT facilities is always governed by an Acceptable Use Agreement. In some cases, breaking this agreement may result in you being asked to leave, and could even involve an uncomfortable discussion with external authorities such as the Police.

People can find remembering PIN numbers hard going. It is amazing how many passwords and PIN numbers we need today. It is very tempting to have the same password and/or PIN for lots of different accounts. Tempting, but not very wise!
Joanna found remembering PIN numbers really tricky, so she decided that as no-one would ever use 1234 as a PIN that it would, therefore be safe. No one would ever use that, would they? Joanna lost her bank card and did not notice it was gone for several days. One morning, a letter arrived from her Bank telling her that she was £2000.00 overdrawn.

An E-Safety Consultant writes…
Unfortunately, she did not know that 1234, 4321, 1,3,7,9, or 2,4,6,8, are the PIN numbers that credit/bank card thieves try first. Anything that forms a pattern is a good bet. Be random, and try not to have your date of birth either. Remember, as cameras have got smaller and smaller, it is possible to install one above a keypad. Always cover your hand while entering the numbers, and don't get your card out of your pocket or bag until the last minute. You would be amazed how quickly some people can read and remember a card's details. Always take your cash and card immediately and put it away.

Things you might use	Possible risks.
Open access internet connections  	• Unencrypted wireless networks, and a computer with no password set on it would allow anyone with a wireless enabled device to read your entire hard drive! • Scammers have realised that they can access user information by creating "free" internet sites. **BTFON**, is genuine, but **BTFONERO** is not. The scammers change the names of their fake "hotspots" regularly, and they often copy the design of the real one too. • Technically – it is easy for anyone to set up a fake hotspot. Never connect to a hotspot unless you are ***certain*** it is genuine.

Freeware 	• Rarely, is "freeware" free. Usually there is some form of data miner attached, and/or they want some information from you first. • There are some essential add-ons that ARE free, but ONLY if you get them from the right source. i) Acrobat reader from ADOBE ii) Flash & shockwave players from ADOBE iii) Malicious software removal tool ONLY from Microsoft. • **APPS** have become great ways of earning money – for someone else! Many Apps claim to be "free". They may indeed be free to download, and may even allow you to use them free for a while. What they are less good at is telling you IF there are any charges, and when those charges will start to bite. Always read the Terms of Use for any App you download. If you can't find definite proof that it is and always will be free, then contact the person who is issuing it. If in doubt DON'T download or use it. Some Apps also require access to your contacts lists and address book too.
Add-ons	• Some add-ons you want. Others you don't. Our advice is keep it simple. Install the Google Toolbar if you want to, but you may not want the add-ons that come with it. Whenever you are offered a free add-on, always ask yourself why anyone would offer you something for free, and what is it THEY are getting out of it. Again, there may be lots of boring reading about Terms of Use, or Privacy Statements. Please read it. It matters.
Downloads (Music, games, etc)	• Free may well mean "illegal", and these days, copyright owners are tracking illegal downloads. One family was fined £13,000 for downloading one film illegally. • Some "free" online games carry viruses or data miners. • Some software may be stolen. If you download it, you are an accessory.
Downloads "required" by websites.	• Some websites will insist that "Cookies" are enabled or they will not work. A cookie identifies your computer to the website owner. It is a good idea to clear your cookies out once in a while. Some get there without you knowing! • In the last two years, there has been a sharp rise in websites offering you items that you could easily get from the original source. For example, a PDF reader is available, free of charge, direct from Adobe, yet we have seen many sites offering it, and inviting you to "install our quick downloader" first. • Ask yourself each and every time, **Why does this website want to install something on my PC?** And **Do I REALLY know what this download will do?** Don't forget, people who are up to no good rely on the

	fact that you probably won't ask these questions, or can't be bothered with the reading involved! **You have been warned!**

Why do people do that?

There are many reasons why people write spyware, malware and key logging software.

1) It is relatively easy to do.
2) It is a pain in the ……..
3) They just enjoy messing up other people's systems.
4) They want your money.
5) They want access to your financial potential. (IE Taking out loans in your name, etc.
6) They want YOU. (This is the most extreme end of it.)

High-end, organised crime is probably not interested in you. They want to hit large, wealthy institutions, but think for a moment. A collection of people, perhaps measuring in the thousands, can quickly become a very lucrative source of income.

You do not want to become one of them.

Fortunately, most of the mid-order people who like to scam others are inherently lazy. If you make it difficult for them they will go and try it on somewhere else.

Keeping your identity safe online.

Who you are, and everything that identifies you is the most valuable asset you have.

So,,, a few "house rules"

1) Never disclose any of your identification details unless you are absolutely certain the person asking for them has a right to them and needs them.
2) Have different passwords for all your online accounts, especially those that are linked in any way to money, or buying/selling transactions.
3) Change your Bank Card PIN at least every three months, and preferably more often. If you have more than one bank account, do not use the same PIN for them all.
4) Same with online banking – different usernames – different passwords. Change password often.
5) If you have reason to think someone knows your details who should not know them, **inform your bank/building society immediately, along with any other relevant company such as PayPal, Sainsbury's to you, or whatever. DO NOT DELAY.**

Be mistrusting, rather than trusting, is not a bad place to start! Always ask yourself *why* do they want this particular item of information. Always ask yourself if you *really* know who these people are.

In short, sharpen up your "spidey sense".

Bill went into a local TV shop to buy a television. He had the cash in his hand, and had set his sights on a wide screen, plasma Hi Def, 3D television. The sales assistant asked Bill for his home address, email address and date of birth. Bill knew that the Law states that every new television sale has to record the buyer's home address, as this is used by the TV Licensing Authority to

make sure there is a TV License at the place the television will be use, so he gave that information willingly. He did not, however, see why he should disclose his email address or his date of birth. The shop assistant said it was "company policy". Bill refused to give that information, and left the shop without his TV. He complained to the company head office who then sold him the TV with a £200.00 discount…..and did not record his email address or date of birth.

An e-safety consultant writes….

Well Done Bill.

With the above example, at the very least, Bill would have received unwanted marketing and promotional information from the company. But why did they want his date of birth? They have no possible need for that information, or any right to it. The combination of home address and date of birth is often used by banks and utility companies to verify user identity. All it would take is one unscrupulous employee in the TV company for Bill to find himself in a lot of trouble.

Keeping your images safe online.

Camera technology has come a long way in a very short space of time, as has image manipulation. It is not that along ago where to change an image convincingly, you needed Photoshop, a lot of time, and a lot of skill. Nowadays, it has never been easier to change a photograph – sometimes with embarrassing or perhaps illegal results.

Similarly, most cameras, including even mobile phone cameras are now far higher resolution than ever before. They take images which, on a decent, hi-res monitor can produce massive amounts of detail.

Gillian went on an exchange student visit to Italy. While there, she took a photograph of her room. (Which was not very tidy!) Her mum phoned her the moment she downloaded the photograph from Gillian's Facebook site. The photograph had captured some documents on Gillian's desk, one of which was her bank statement. How many other people might have seen that photograph with the bank details on it?

An E-Safety Consultant writes…

Face & Place information is also a dead give away in some photographs online. People often take photographs while on holiday, and sometimes post them on Facebook. ***This tells people you are not at home.*** *If you do not want just anybody to know where you are living, or where you work or the places you go regularly, think carefully about an image before you post it online. Even images taken in your home can tell people things like whether you have a plasma TV, or a good sound system. Image manipulation has become much easier, and cameras now have very high resolution as standard – at it will only get better.*

Some things you can do…….

1) Only post small, low-resolution images online – it is very difficult to enlarge them and no tiny detail would be visible. They are also not likely to be changed either.
2) If you have built your own website, consider disabling the "right click-copy" function.

3) Think about the most straight-laced person you know in your family. Do not post any image that they might find offensive.

Remember – when you hit that enter button, that image is out there forever. You lose control over it. Even if you delete it from the website, someone may well already have copied it and sent it on to other websites around the world.

Jo was 15. She, like many of her friends is very confident and feels totally in command of her world. She and three of her friends posted topless "selfies" on their Facebook website. Partly, they did it for "shock" value but mostly they did it in the mistaken belief that they could always delete the image, and they mistakenly believed that ***any copies of it would automatically be deleted.***

Jo and her friends were asked to undertake an experiment. First, they were asked to delete the original image. Then, some hours later, they were asked to "Google" themselves.

All three girls found their topless image on a range of websites around the world. Some of the images had also been "tagged" with their names, so they would appear on a search. The girls contacted the websites and asked for the images to be removed, stating they were only 15. While some of the websites complied, (eventually) they are still finding that image online from time to time. And that is without even thinking about the number of printed copies there may be out there.

An e-safety consultant writes *….Jo and her friends had received e-safety training at school – they just didn't believe what they were told. Eventually, Jo's mum and dad became aware of her images online. There are a lot of myths, some of which come from children and young people, while others come from the very people who want to abuse the system. Sentences that seem to apply to everything, such as "If you delete the original, EVERY other image disappears", are rarely true. If it sounds too good to be true, it usually is. Teachers are way too busy to want to give you bad advice, or tell you things that aren't true. It's one thing to test out what you are told, quite another to expose yourself to danger while doing it.*

Future self, future employers.

No short cut here. Your online presence is public property if you do not protect it adequately.

A few facts…..

Future employers can and do Google applicants.
Universities and colleges can and do Google students.
Parents can and do Google children.

In the case of colleges, universities and employers, the reputation of their organisations defines them. Their good standing in their communities is their most important trading asset and they protect it vigorously.

Anna had not been happy at work for a while. Her new line manager was difficult to work with, and generally, Anna did not think much of her employers. Still, it was a job, and it paid the mortgage. One day, after a particularly unpleasant supervision meeting, Anna went home and

wrote on her Facebook wall exactly what she thought about her company, her line manager and the way they did business.

The next day, Anna was suspended for bringing the company into disrepute. As some of the things she had said on her "wall" were not factually accurate, the company decided that they would either accept her resignation, or take legal action against her for damage to their reputation.

Anna resigned, and the company concerned declined to give her a reference.

An E-Safety Consultant writes…

In short, there are laws preventing you from publishing statements that are damaging and/or untrue. They apply to individuals as well as companies. Businesses often have codes of practice they expect their employees to operate.

1) *NO personal comments. About anyone. Ever.*
2) *NO bad language.*
3) *NO racist/sexist or sexual content.*
4) *If you think something is wrong at work, there will be a complaints procedure. Use that – do not post material in the public domain.*

It's not only employers either who take exception to unpleasant comments being made about them. Colleges and Universities can ask you to leave if you bring their reputation into disrepute. Remember, your right to full time education ends when you are 17. Universities do not have to have you there, and there is no right of appeal. If you break their rules, or damage their reputation, you can find yourself off your degree course.

James is 18. He is a hard worker and has done very well in his GCSE examinations. He decided that he wanted to leave school and get a job. Despite his excellent qualifications and application forms, James just was not getting any offers of interviews. Eventually, he became very frustrated and contacted a company he had applied to and asked for feedback. The lady he spoke to was very nice, but pointed him to his Facebook pages. In them, James looked anything but the perfect employee. The site was littered with bad language from both James and his friends, there were photographs of James when he was drunk, and he had said several times that he was "so drunk on Sunday night I couldn't face going to school on Monday."

An E-Safety Consultant writes…

No matter how good the application is, employers do use Google from time to time. You can make your social networking presence work FOR you, by posting material that presents you in a good light. Yes, your social networking is yours to do with as you wish, and yes, you have the right to free speech. You also have the right to silence too! Does your future employer need to see that photograph of you drunk? Do they need to know that James (above) is so unreliable that sometimes he parties so hard at the weekend he is unfit for work?

What does your online presence say about you?

Risks for girls, risks for boys

Time for some plain speaking, and a few facts.

1) There are people out there with a sexual interest in young people of both genders.
2) More girls than boys get targeted in this way, but boys are at risk too.
3) Your online images can be copied, enhanced, changed unless **you** only post low-resolution images online. Even this won't defeat them totally, but it WILL make life much, much harder for them.
4) There are no reputable model agencies out there who would entice you into sending them naked or semi-naked shots "to show producers".

Even though you have now left school and are living on your own, you need to take school of yourself.

There is no end to the tricks those who some people will try. Some of them sound quite plausible, and you may be forgiven for being taken in.

Some of these people want to meet you face to face, others are content with the internet, however, they are highly likely to capture any images you send, and publish them on unpleasant websites without your permission.

They do not care about you at all.

Some people pretend to be of a different gender, and may tell you they are much younger than they are.

Myth 1 Seeing and hearing is believing.

No, it isn't. There is software that is freely available that could make a middle aged male sound like a young girl. Even if you can hear them, you still have no real way of determining their gender.

We all know that there can be delays in video streams, particularly when the internet is busy. Sexual predators know this, and may play you a looped recording that they themselves may have stolen off the internet. Even seeing is not believing.

As of 2016, there is even software out there that can "wrap" a false face around a user's to disguise them. Ralph Feinnes doesn't really look like Voldermort in the real world!

An E-Safety Consultant writes…
Unless you know the person in the real world, you have no way of knowing who they are.

Myth 2 Sexual predators "hit and run".
An E-Safety Consultant writes…
They may, but equally, they may take a long time to build up your trust before they ask to meet you, or ask you to undertake some activity online.

Myth 3 There is a difference between sexual predators, and identity thieves.
An E-Safety Consultant writes…

Not really. Both are committing criminal offenses, and often people offend in different ways. After all, a sexual predator may well already be disguising their true identity, and they will think nothing of trying to rip you off financially as well if they can.

But it's not all about sex. Financial frauds are very common – and young people make easy targets sometimes.

The "courtesy call"

Many adults will know about these! Usually, they happen between 7:00pm and 9:30 and seemingly always start with "Good evening Mr/Mrs. X, this is (whatever company) How are you this evening?" They will then usually ask you to "confirm some details for security purposes."

Why on earth should you? This company, if they are who they say they are phoned you. If anything, you should be asking them to prove who they are. **OF** course, many fraudsters try this one on too.

An E-Safety Consultant writes…

You do not have to confirm your identity to anyone who calls at your door, or phones you. You can always ask them to write to you. If they are who they say they are, they will already have your address. (Even if they read it out to you, do NOT confirm it.)

Edith was 79. One evening, she received a phone call from a very nice young man who claimed to be from British Gas. He told her that her boiler was now considered dangerous and she needed a visit to make sure she was safe. She was asked to "confirm her name and address" which, being trusting, she did. The caller than asked her if there was any time when she could ***not*** *have a visit and Edith told the caller that she would be out all day the following Thursday, but that any other day would be fine. The caller made an appointment for the Friday. On Thursday, Edith's house was burgled.*

An E-Safety Consultant writes…

This could so easily have been avoided. Edith has neighbours who were aware of this type of financial scam taking place. It would have been a good, caring gesture if someone had thought to tell Edith about it.

If you are now living in your first home, you are a neighbour. Not only that, you are a highly knowledgeable neighbour.

It is not only the elderly that have been caught out by "courtesy calls"

*You can register your phone number with the "**Telephone Preference Service**" and this will screen out most UK-based courtesy calls. You can also write to your electricity and gas suppliers asking them not to use your data in this way. Unfortunately, to get round this, more and more companies are using call centres overseas.* ***They are NOT bound by UK regulations***.

You can ask your telephone provider to block all calls from withheld numbers. This can be a pain, as some of your friends may withhold their numbers too. If you start to get a lot of cold-calls, (or even silent calls) you should talk to your telephone provider who may be able to help.

What makes a good password?

Passwords are your keys to your online world. You may well have many different keys to your home, and you need different keys to your online world as well.

Having the same password for many different accounts is a gift to the identity thief.

1) Make a list of **all** the internet accounts you use.
2) Mark those with **any kind of financial activity** in red. (Bank, e-bay, Amazon – any online shopping.)
3) Mark the ones with personal information but no financial activity yellow. (Facebook – Social Networking of any kind – dating websites etc.)
4) Mark the ones with no personal or financial information green.

Use the table below to write down five words in the left column, and then change some of the letters for numbers and punctuation in the right.

Password	How it will look
Coventry	c0v3nt5y

Now we need to think about how to remember your passwords. **Writing them down is no good**. If you are burgled, thieves will look for a list of passwords, and will try them out!

An E-Safety Consultant writes…

"Most people write down clues that will remind them of what their password is.

For example, suppose I use my house number, my mother's middle name, and my house number. I might, therefore, write a "clue" of number-inlawmiddle – number.

That would immediately remind me of

18margaret18

But that is useless to a thief. It is unlikely they would know my mother's middle name, and anyway, I would not use it as all letters as they appear in her name. If I were to use this as a password, it would be something like

18m@rgar3T18

It will take you some time, but playing around until you get a good password formula that works for you is well worthwhile and it will protect you Try to avoid using anything as a password that someone else could easily find out about you."

Finally, change your passwords regularly. Even friends can watch you log on, and can see your passwords.

If you think that a "red" password has been discovered by someone else, then contact the financial organisation concerned, (your bank, paypal, etc) and tell them immediately. They will help you to keep your money safe.

What to do if……..?

We all make mistakes, and even if you are fully clued up into the world of online security, you can still have the awful realisation that you think you have made a mistake or given someone information they should not have. In which case…..

1) If it involves money, contact your Bank and explain the situation to them. They will have seen it before and will be able to help you.
2) IF you are worried about your own personal security or safety, then contact the police.

The important thing here is **DO SOMETHING**.

Who can help, where are they, what will they do?

Who?	When to contact	When
Your bank/building society 	• If you think your contact details have been lost/stolen/disclosed accidentally • If you notice unusual or unauthorised activity on your bank statement. • If you lose your bank card, cheque book or paying in book.	• Immediately!
Police	• If you are worried about your personal safety or security • For advice on making your home or property secure – including security marking • If you think someone is impersonating you online	• **Immediately if you think you are in danger** • As soon as possible when you settle into your new home. • As soon as you think this is the case, taking evidence with you.

	• Http://www.thinkuknow.co.uk • **http://www.ceop.police.uk** **To report abuse, look for this.** 	
Neighbours 	• If you think they might be at risk too – a sudden flood of marketing calls, cold callers, and suspicious activity of any kind. • A lot of neighbourhoods now have "Neighbourhood Watch" organisations. These are set up with the help of the local Police. If your neighbourhood doesn't have one, why not start one yourself? Contact your Local Police Station for advice. • Many Neighbourhood Watch areas operate a "No Cold Callers" policy, and have signs up to inform people of this. • Your Local Authority will have a Trading Standards Department. They are a valuable source of help and advice.	• **Contact your local Police as soon as possible** • Don't underestimate the power of Neighbourhood Watch. Your local community will have a neighbourhood police officer. Talk to them. Invite them to meetings. • Look after any vulnerable people you know about in your community. Good neighbours are people just like you. • Your County Council will have a Trading Standards Department. They too would like to know about rogue traders in your area.
Telephone Preference Service 	• If you start getting flooded out with marketing calls, or if you want to pre-empt that.	• No need to wait until it becomes a problem – you can register as soon as you have your own phone number. • If registering after you have had some calls, it may take a while to take effect. • Does not work with calls from overseas.

Telephone provider (EG BT)	• If you want to have changes applied to your line and for help with malicious calls. • You can have your line set up to reject calls from withheld numbers. • Discuss any problems you are having. They are really helpful.	• At the outset, preferably, but at any time. Again, read the booklet. Some services are free, others will attract an extra charge to your account.

Sarah had just moved into her first flat. About three months later, she started getting phone calls from a withheld number. The phone calls were sexual in nature and Sarah thought that the caller knew her. Each phonecall was more explicit than the last, and each call contained offensive sexual language. One night, the caller asked her to participate in a sexual act with him, and threatened her that if she didn't he would publish some photographs he said he had of her.

Sarah phoned the Police who tracked the number through BT. BT suggested that Sarah should reject calls from all withheld numbers, but also pointed out that some people that she wants to hear from may have their numbers withheld. They told her what to do to get round this problem. The police found the caller, and took action against him.

An E-Safety Consultant writes…

It may sound as if Sarah did the right thing here, and to some extent, she did, however she did not report it immediately, which gave the caller confidence to keep doing it. The situation ended well, but could have been stopped in its tracks far sooner. Imagine the months that went by when Sarah was anxious every time her phone rang in the evening.

Who to Complain to and about what.

Who	About	Contact
Ofcom	• **Television or radio interference.** • **Hostile marketing calls** • **Obscene advertising** • **Nuisance or "silent" calls** **The Telephone Preference Agency can help to reduce the number of cold marketing calls you get.**	**Ofcom** **Riverside House** **2a Southwark Bridge Road** **London** **SE1 9HA** **http://www.ofcom.org.uk** **0300 123 3333 or 020 7981 3040** **-OR-** **The Telephone Preference Agency.** **http://www.telephoneprefence.org.uk** **Wycliff House** **Water Lane** **Wilmslow** **SK9 5AF** **Tel: 01625 545 745** **Fax: 01625 524 510**

		E-Mail: mail@ico.gsi.gov.uk
Ofwat	• **All water companies – anything you feel you are being given misleading advice about or if you cannot resolve your complaint directly with the company**	**Ofwat** **Centre City Tower** **7 Hill Street** **Birmingham B5 4UA** **United Kingdom** **By phone: 0121 644 7500** **By fax: 0121 644 7559** **By email: mailbox@ofwat.gsi.gov.uk** **http://www.ofwat.gov.uk**
CEOP	• **Child Exploitation and Online Protection arm of the Police.** • **For ANY time you think a child is in danger online** • **If you think YOU are in immediate danger, then dial 999** **Your local Police can give you help, advice and support.**	**Child Exploitation and Online Protection Centre** **33 Vauxhall Bridge Road** **London** **SW1V 2WG** **Telephone: +44 (0)870 000 3344** **http://www.ceop.police.uk**
Banks	• **Write your Bank contact details down in your address book. Do NOT write your account details with them!** • **Contact your bank immediately if you think that your account details or account access information may be known to someone else.**	**Your Bank/Building society will have given you their contact details.**

To Sum Up – A Few Facts

- Sadly, there will always be people out there who are up to no good. Most of them will just be a nuisance, but others have more unpleasant intentions in mind.

- Every single person who wants to abuse the internet in some way relies on the fact that people won't talk about it. They like to work in the shadows. Talking about e-safety, no matter how embarrassing is a very powerful weapon.

- Never EVER wait to get help if you think you need it. Banks, Building Societies, Telephone, Electricity, Gas, Water Companies, and the Police, have all decided to work

hard to protect their customers. So, SHOUT FOR HELP IF YOU NEED IT…AND DON'T WAIT!

- Talking to your friends and family may well keep them safe too.
- The bigger the noise we make about e-safety, the fewer places we leave abusers to hide.
- You CAN take a pro-active role in your own safety. You are POWEFUL!
- If a company you are dealing with seems to be taking you for a ride, you can always complain about them.

"Free" services and software are very rarely truly free. Most will want something in return, even if it is only an email address. All services should have a Privacy Notice, telling you what they can or might do with the information you place there.

Image stores that are "free" such as KIK, Imgur and others of a similar nature need to maintain their product, update computers, pay staff etc. This money has to come from somewhere. If they are not charging you, then how are they making their money to cover their costs? If you are using these services to store your images, then how safe are they? When did the site owner last conduct a "Penetration Test"? Was it conducted by a reputable external company? Do they have the results? Will they share them with you?

It is perfectly reasonable to ask them these questions. You can also read their Privacy Notice, although most of these are very lengthy and written in language that is not easy to understand.

An E-Safety Consultant writes…

Sometimes, people breathe a sigh of relief and think e-safety is "done". Unfortunately, this will never be the case. There are so many new devices, new programmes, new operating systems and new methods of connectivity coming along that there is always a need to be careful and protect ourselves.

The three main areas of attack are financial, identity and sexual, although they frequently overlap.

All people who engage in these horrid practices work in shadow and darkness. What they do embarrasses people – and they know it. They know, for example, that it is tremendously difficult to talk about being harmed sexually, or exploited sexually. That is why people tend not to report it when it has happened.

The best thing you can do is talk about e-safety whenever it appears in the news. Every time someone's bank account is emptied, talk about why it happened, and then make sure if can't happen to you or your loved ones. Similarly, sexual predation happens because a sequence of events has occurred. This usually starts by the perpetrator asking unacceptable questions, such as "ASL" (Age sex location) or asking for pictures, perhaps even wanting your SKYPE or mobile phone contact. Why not make yourself a list of questions you will never answer online?

As for "free" services or products, they are rarely free. Every service, piece of software or device had to be invented, designed, refined, and then put on the market. This costs money. Image storage and social networking sites also cost money to run, yet many are offered free of charge

to users, so asking where the operator covers their costs is important. Are they really engaging in market research and using your data or images for this?

The fact is that while there are people out there who are up to no good, ***FAR more good things happen online than bad things.***

We just want to make sure the bad things don't happen to you*.*