How to stay safe online

Information and advice from

Get Safe Online and

BCS - The Chartered Institute for IT

The Golden Rules of Online Safety

Even if you choose to do nothing else, you'll have you a better chance of keeping safe if you observe the following simple 'rules':

Log in

Don't have an account? Create one

Username:

Password:

□ Remember me

Choose, use and protect your passwords carefully

http://www.

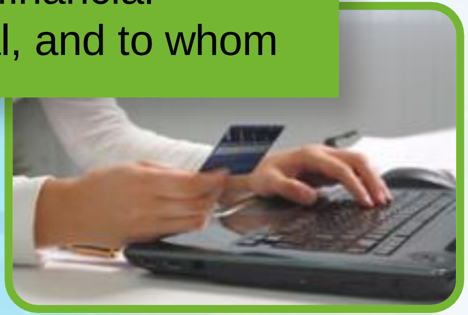
Virus Alert!

Warning! Threat detected!

A malicious item has been detected!

Ensure that your anti-virus/anti-spyware software is always kept up to date and switched on

Be very careful about the amount and level of personal and financial information you reveal, and to whom



How to stay safe online

Protect Your Computer

Protect Yourself

Smartphones & Tablets

Shopping, Banking & Payments

Safeguarding Children

Social Networking

Other Things You May Do Online

Protect Your Computer

Physical security

A computer that's stolen or accessed without your permission can cause a wide range of security, safety and data problems

Keep your PC out of view, lock *it* away when *you're* away

If you're out and about with your laptop, keep it with you at all times

Keep computers out of harm's way, such as water damage and extreme heat

Online security

Viruses, spyware and becoming part of a mass botnet are all risks if you don't follow some simple, common-sense rules

Ensure internet security software is loaded and switched on at all times

Ensure your firewall is switched on at all times

Download and install all software updates – they often contain security fixes

Download and install operating system updates – they often contain security fixes too

Using the internet safely

The internet is a fantastic resource, but careless use can result in financial or identity loss, breaching copyright and emotional upset

Ensure your browser is up to date – otherwise your security could be at risk

Always be cautious when supplying personal or financial details

Make sure home, office or public WiFi is secure before carrying out personal or financial transactions

Viruses & spyware

Viruses and spyware can result in many problems, from inconvenience, through data loss, to fraud and identity theft.

Don’t open attachments in unsolicited emails

http://www.

Virus Alert!

Warning! Threat detected!

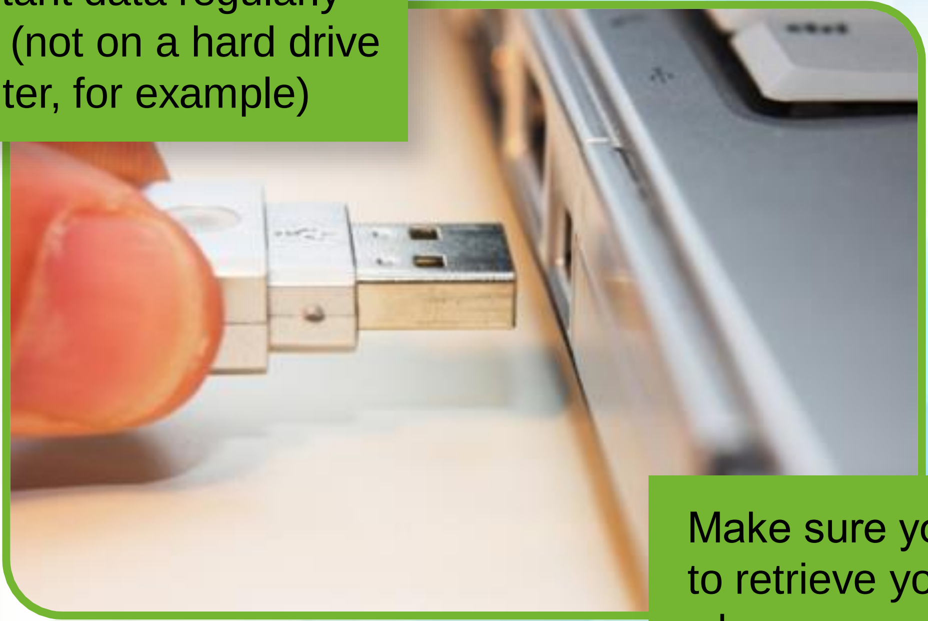
A malicious item has been detected!

Ensure you that you always have up-to-date internet security software loaded and switched on

Backups

If you don't back up your data, you could lose it by a number of means causing inconvenience at best and financial loss at worst

Back all your important data regularly and to a safe place (not on a hard drive next to your computer, for example)



Make sure you'll always be able to retrieve your backed up data whenever you need it

Getting rid of your old computer

Deleting files isn't enough when throwing or giving away your old computer … it could fall into the wrong hands.

Use specialist hard disk erase software, or physically destroy the hard disk so it can't be accessed

Protect Yourself

Public places

Being careful when you use your laptop or mobile device in public places can prevent you from being snooped on – either via WiFi or over your shoulder. It could save your device too.

If you're not sure the wireless network you are using is secure, don't conduct private or financial business online

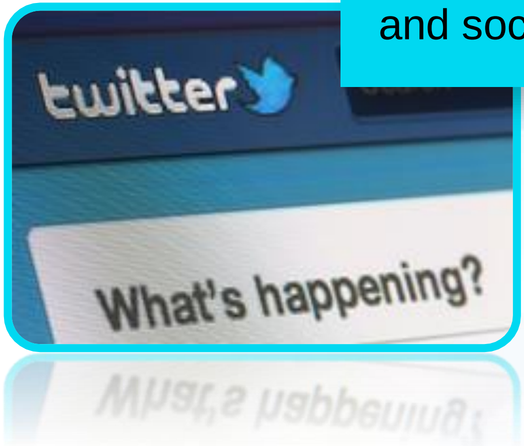
Always keep your laptop, smartphone or tablet with you to avoid loss or theft

When using public computers (such as in an internet café), ensure you leave no trace of your activity

Fraud

Online fraud is very commonplace, and is estimated to cost £765 for every adult in the UK. It takes many forms but can be avoided with some simple precautions and common sense.

Always be vigilant about contact from people you don't know, including via emails and social networking sites



Always remember that if something seems too good to be true … it probably is

Passwords & PINs

Passwords and PINs help you to prove that you are who you say you are, and protect against other people accessing your online accounts, computer and mobile devices.

Always use a password or PIN

Make sure the password or PIN that is very difficult for anyone else to guess or crack

Never disclose a password or PIN to *anybody* else, and don't write it down

Try to use different passwords and PINs for different online accounts and computers or mobile devices

Protect your privacy

Stop and think about how much private information you're revealing in anything you do online. If too much, you could become a victim of fraud, identity theft or abuse.

Never give away more private information than is absolutely necessary. You may not know who is seeing it

Safeguard your identity

Take simple steps to protect your identity, or it could be stolen by criminals and used to defraud you or commit crimes in your name.

Always safeguard personal information online, and on computers and mobile devices

Shred sensitive documents before throwing them away, and lock away bank statements, passports, driving licences, utility bills etc

Think about who you're revealing private or financial information to before you do so

Searching the internet

When you're using a search engine such as Google, Bing or Yahoo!, remember to follow some simple rules to avoid upsetting or difficult situations.

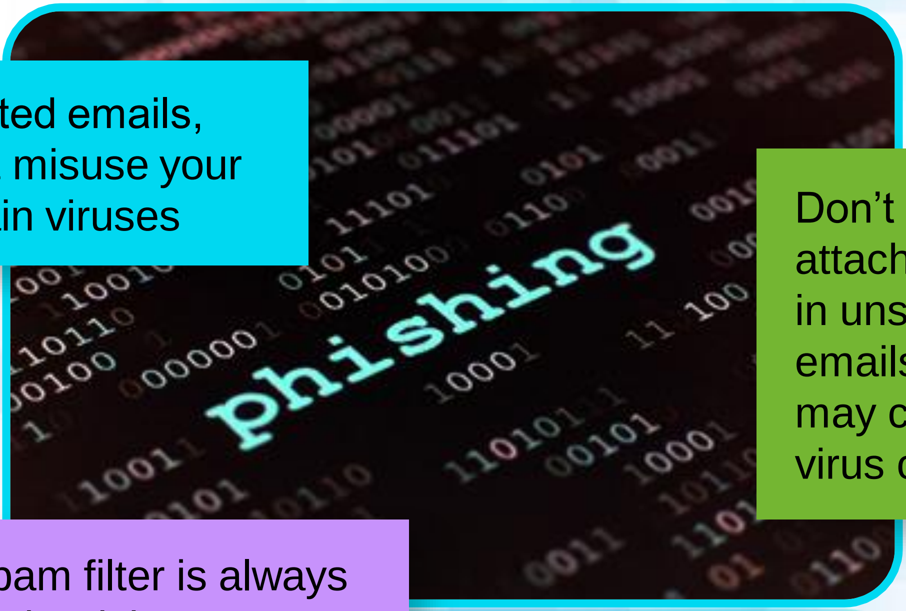
Word your searches as precisely as possible as you'll be more likely to find the sites you want, and less likely to be taken to inappropriate or illegal content

Remember that even 'private' searches are not private, as they are visible to your search engine provider and possibly by others

email

We've all come across emails from people we don't know inviting us to click on a link or open an attachment. Chances are that they are fraudulent.

Don't click on links in unsolicited emails, as they may lead to sites that misuse your personal information or contain viruses



Don't open attachments in unsolicited emails, as they may contain a virus or spyware

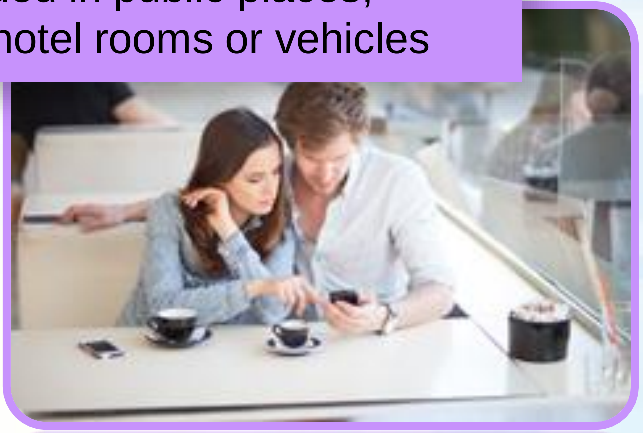
Make sure your email spam filter is always switched on to minimise the risks

Smartphones & Tablets

Take care of your mobile device

It's easy to lose a smartphone or tablet, and they're easy to steal too. It's not just your mobile device, but the information contained on it, that is at risk.

Never leave your device unattended in public places, offices, hotel rooms or vehicles



Always safeguard the information on your device by using a PIN or password

Public places

You can use your smartphone or tablet anywhere, but you do need to ensure your activity isn't being watched over online or in person.

Keep your smartphone or tablet with you at all times to avoid other people seeing what you're doing

Ensure the wireless network you are using is secure

Watch out for people looking over your shoulder

Viruses & spyware

Remember that smartphones and tablets can pick up viruses, spyware and other types of malware too. So make sure they are always protected.

Download a reputable internet security app, especially if your device runs on Android or Windows

Purchase and download apps only from recognised and trusted source

Wireless networks & hotspots

Wireless hotspots in the home, office or public places need to be secure to avoid your private information becoming public, or your connection being used by someone else.

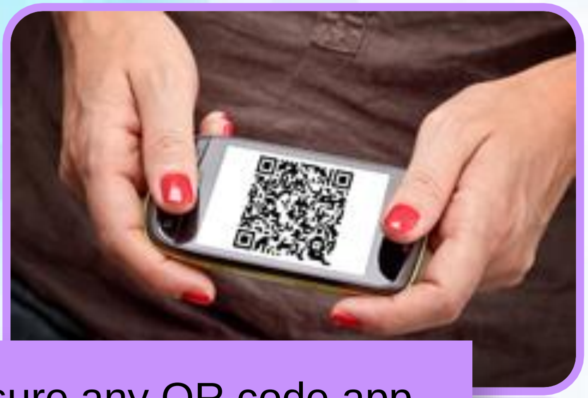
Avoid sending or receiving private information using public WiFi, unless on a secure web page

Check the security settings on your home/business hub/router to ensure security and privacy

QR codes

Easy to use, but because you can't see the website address, you can never be quite sure where you're being taken to.

Don’t enter personal or financial information on a website to which you have been directed from a QR code



Ensure any QR code app you download is from a reputable source

Disposing of your smartphone or tablet

Your mobile device probably holds a lot of personal and financial information such as passwords, emails, bookmarks, browsing history, photos and much more.

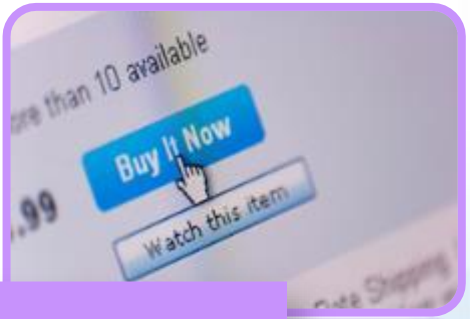
Thoroughly remove all data from your device before disposing of it

This applies even if it's going to someone you know, as you never know where it will end up

Shopping, Banking & Payments

Using auction sites

There are a number of things to consider to ensure you're doing so without risk of losing money or not receiving your goods.



Choose reputable sellers and buyers

When selling, ensure that you have received payment before despatching the goods

Check that the payment website/page is secure before entering your payment details

Using penny auctions

Unlike a normal auction site, you pay all the money that you bid whether you win the auction or not. There is also a risk of being defrauded.

Don't lose track of the amount money you are bidding

Take every precaution to ensure that you will receive the goods you have bid for and that they match the description

Ensure that the site you are using is authentic and secure

Banking

It's very important to exercise care as online banking is a key target for cybercriminals because of the sums of money and potential security lapses involved.

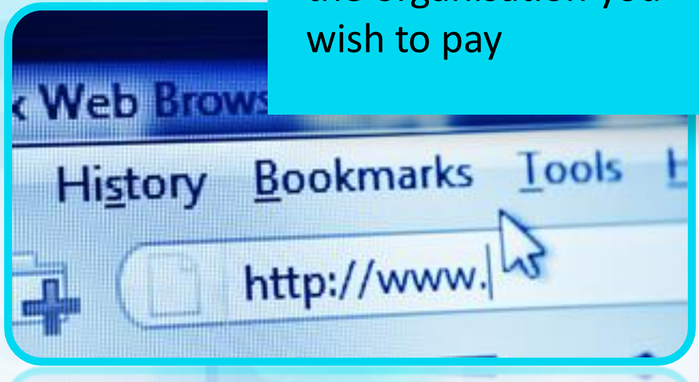
Remember that banks **never** email you requesting you to enter your login details, so never respond to emails that do this

Use strong passwords, different for every account, and ensure that nobody else has access to them

Making online payments

Always exercise care when paying utility, phone and other bills online.

Ensure the payment page is secure before entering your details



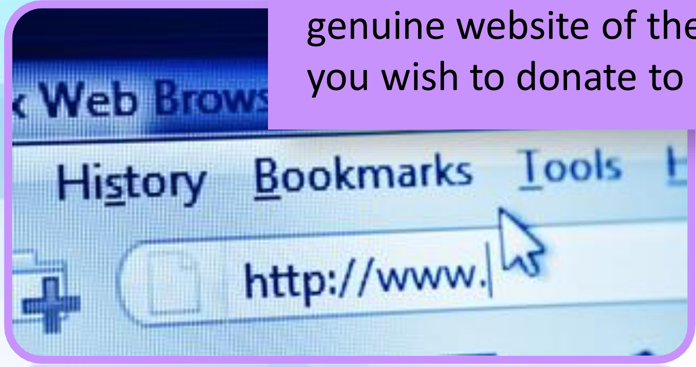
Make sure you are on the genuine website of the organisation you wish to pay

Donating to charities online

Always exercise care when donating to charity online.

Ensure the payment page is secure before entering your details

Make sure you are on the genuine website of the charity you wish to donate to



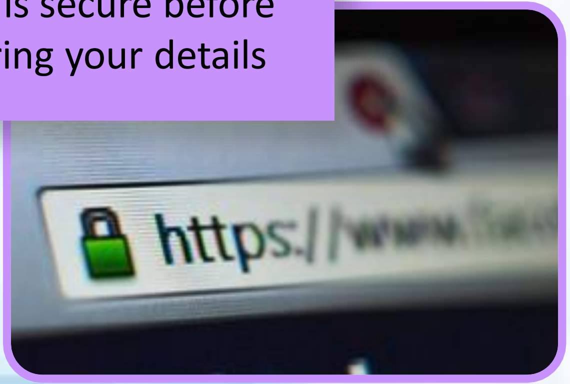
Where possible, donate via dedicated charity sites such as JustGiving, Virgin Money Giving or the Disasters Emergency Committee (DEC)

Shopping

Shopping online is great but also has potential downsides such as payment security breaches, bogus websites and the risk of your purchases not being delivered.

Always choose reputable shopping sites

Ensure the payment page is secure before entering your details



Safeguarding Children

Keeping children safe online

Going online is part of most young people's lives, but unfortunately it can present real risks

Work with children you are responsible for to ensure they know about sensible use of the internet and online risks

Keep yourself up to date with the online risks to children

Take precautions such as parental controls and network-based content filters

Social Networking

Chatrooms

Chatrooms can be fun, but many people you’re chatting with are strangers and the conversations are uncontrolled.

Never disclose personal or financial information

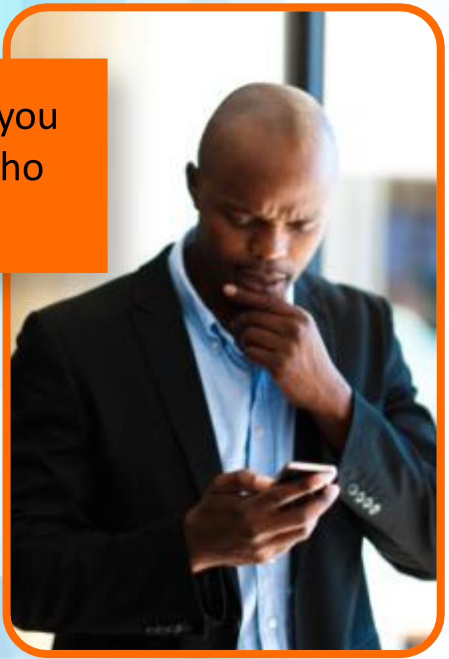
Never write anything libellous, inflammatory or accusatory, and remember that what goes online stays online

Be prepared to encounter strong views and language from strangers

Instant messaging

Instant messaging (IM) is fun and handy but you cannot see the person you’re ‘talking’ to, and it isn’t a secure method of communication.

Never disclose personal or financial information



Be sure that people you are messaging are who they say they are

Social networking sites

Social networking is a great technological advance, but without care it can leave you open to problems such as fraud and abuse.

Remember that what you write online stays online

Never disclose personal or financial information in posts or profiles

Be careful about clicking on links in a post or on a page – they could be harmful

Other things you may do online

Buying medicines and remedies

Many people buy (or are tempted to buy) medicines online, but those obtained from fake or unlicensed sources can be very dangerous, and buying them very expensive.

Consult your doctor or other medical professional for prescription-only medicines rather than purchasing online without a prescription

Buy only from a General Pharmaceutical Council registered pharmacy

General Pharmaceutical Council

Buying & selling vehicles

Unfortunately the motor trade has always been a favourite haunt of criminals and conmen. Being online has simply made it easier for them, so there are precautions you must take.

When buying, always physically view the vehicle, check paperwork and know what you are looking for

Never transfer payment directly into a company's or individual's bank account

When selling, ensure cleared payment is received in full before parting with the vehicle, and never get persuaded into paying any advance 'shipping' fees

Buying tickets

It can be tempting to buy concerts, sports fixtures and other events from unofficial sources including unofficial websites, but this can carry risks such as bogus or non-existent tickets. You can risk not receiving your tickets, refused entry to the event owing to bogus tickets, or payment card fraud unless you obtain tickets from official sources.

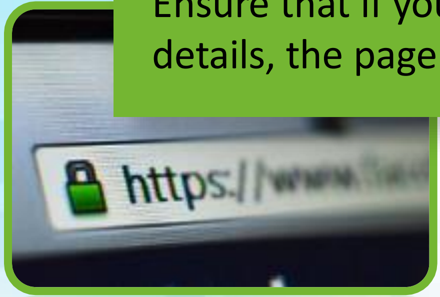
Ensure the website is genuine and secure before entering payment details

Buy tickets only from the venue box office, promoter, official agent or reputable ticket exchange sites

Never transfer payment directly into a company’s or individual’s bank account

Downloading & file sharing

Downloading music, video and other entertainment should always be done from authorised and respected sites, otherwise there are a number of risks.



Ensure that if you enter payment details, the page is secure

Always be certain that the sites you download from are legal and reputable

Be aware of and follow the rules on copyright-protected content, including having to pay for it

Holiday & travel booking

These days, most holiday and travel booking takes place online, but this is a popular target for fraudsters, resulting in financial losses and disappointment.

Never transfer payment directly into a company's or individual's bank account

Do the utmost to ensure that the holiday or travel you are booking is genuine

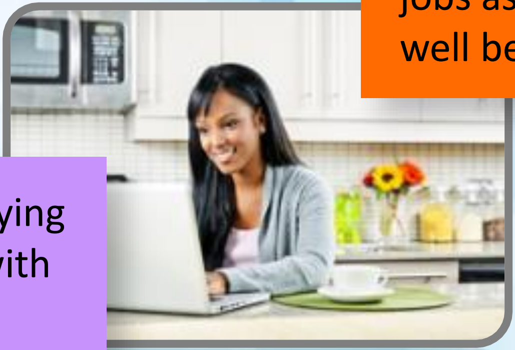
Pay for your holiday or travel by credit card as it provides additional financial protection

Job hunting

With the internet the most common way to find a new job, you need to be aware of associated risks … such as privacy issues, identity theft and financial scams.

Ensure the authenticity of jobsites and think twice about the private information you are divulging when registering or applying

Beware of ads for 'get rich quick' jobs as they could well be a scam



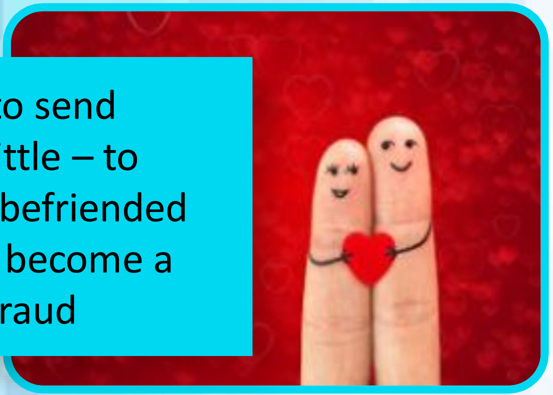
Never be tempted into paying up-front fees associated with getting a new job

Dating

This is a very popular and often successful pastime, but in order to avoid risks, don't let your heart rule your head!

Never disclose private information on online dating sites

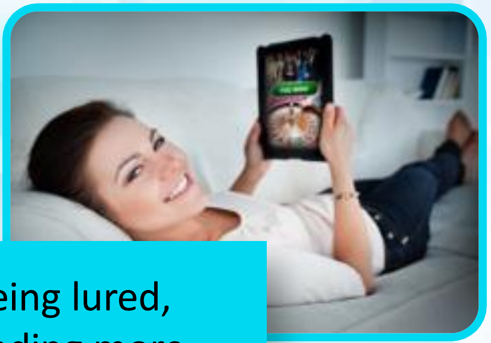
Never be tempted to send money – however little – to someone you have befriended online as you could become a victim of romance fraud



Exercise great caution when meeting someone in person who you have met online, so as not to put your personal safety at risk

Gambling

Online gambling is fast gaining awareness and popularity, which makes it a target for fraudsters and identity thieves.



Always choose reputable gambling and betting sites

Recognise when you are being lured, legally or illegally, into spending more money, such as playing real online games rather than 'play for fun' versions

Exercise responsibility with the sums of money you are gambling

Price comparison websites

You do need to double-check for yourself that you're getting the best deal. You should also be aware that some bogus sites exist for fraudulent purposes.

Ensure your personal data and privacy are protected

Always refer to more than one price comparison site to ensure you are getting the best deal

Renting property

It pays to exercise caution when arranging property rentals and before making any payments, in order to avoid financial losses.

Always view a property and check authenticity of the landlord before paying any money

Always take up references for potential tenants if you are renting out a property

Skype & internet calls

Take some simple precautions to avoid unauthorised access to your personal details, eavesdropping on your calls and having your device infected by malware.

Accept contact requests only from people you know and who would need to communicate with you via Skype or internet call

Never click on links contained in Skype messages, nor in emails claiming to be from Skype or other service providers

Transferring money

You should be aware that legitimate money transfer services can also be used to carry out fraud such as inheritance, romance, overpayment, rental, vehicle or online auction scams.

Never send a money transfer to someone you have not met in person, or that you definitely trust from previous transactions

Always ensure that any cheque you receive from other people is cleared and available before sending repayments – however long this may take

And don’t forget …

- Don’t think “it will never happen to me”
- Don’t get into bad habits, and change your habits
- Don’t take online safety for granted
- Don’t behave online any differently than you would in the ‘real world’
- Don’t forget that ‘online’ means your mobile device too

bcs

The
Chartered
Institute
for IT

GET
SAFE
ONLINE
.org

®

www.getsafeonline.org