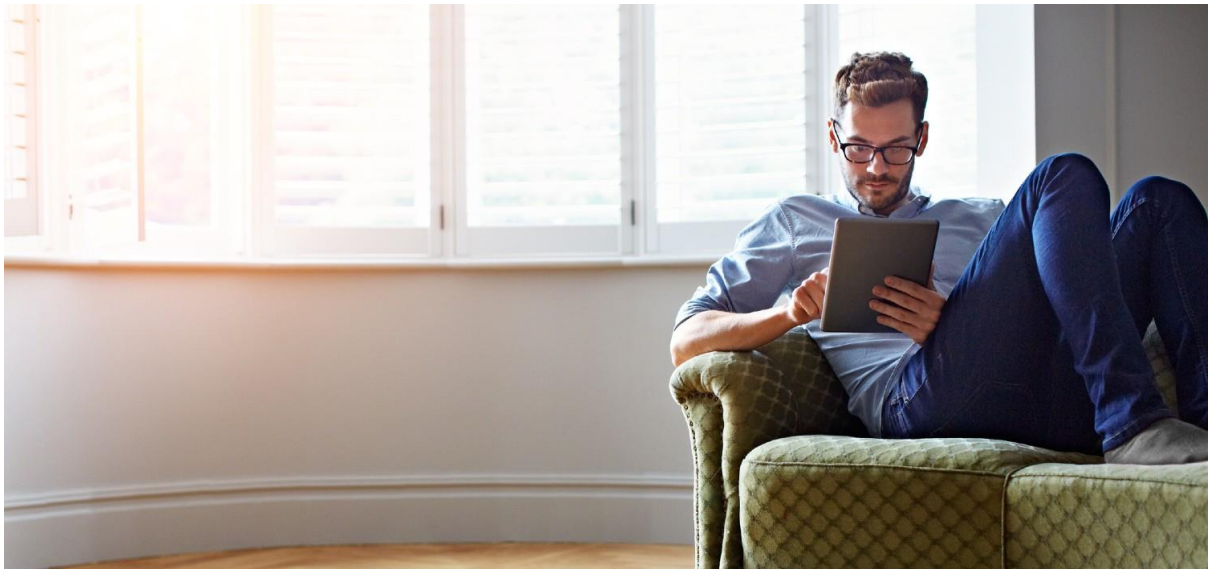
How to stay safe online during isolation?



As we continue our time in quarantine, and with most children now being home-schooled, screen time is on the rise for parents and children alike.

We are now a nation that is functioning online; from shopping for essentials, home schooling the kids, keeping in shape or communicating with our loved ones - which is why it's never been more important to pay attention to our safety and security online.

Online scammers and cyber-criminals are more prevalent and sophisticated than ever, exploiting the current situation and using a variety of tricks that can easily fool us into visiting fake sites or opening phishing emails.

Be aware of phishing emails

One of the most common forms of cybercrime is the creation of bogus and imitation emails, often with links claiming to have important updates. If you receive an email asking you to provide any personal security information, give your login credentials or login to a site which is not the usual website address or does not have 'https://' then you should report it to the company the Email is trying to imitate and then delete it.

Do not respond to these emails or click on any links. It is important to remember that official sources (including your bank) should never ask you to supply personal information from an email.

Never give out your personal details

Be wary of anyone who asks you for your personal information, however official it may seem. Banks will never call or email asking for your Card details, PIN or password. If you do receive a call asking for your personal details, simply end the call and notify your Bank directly, or call your bank back on the number from the back of your card.

Use strong passwords on any online accounts

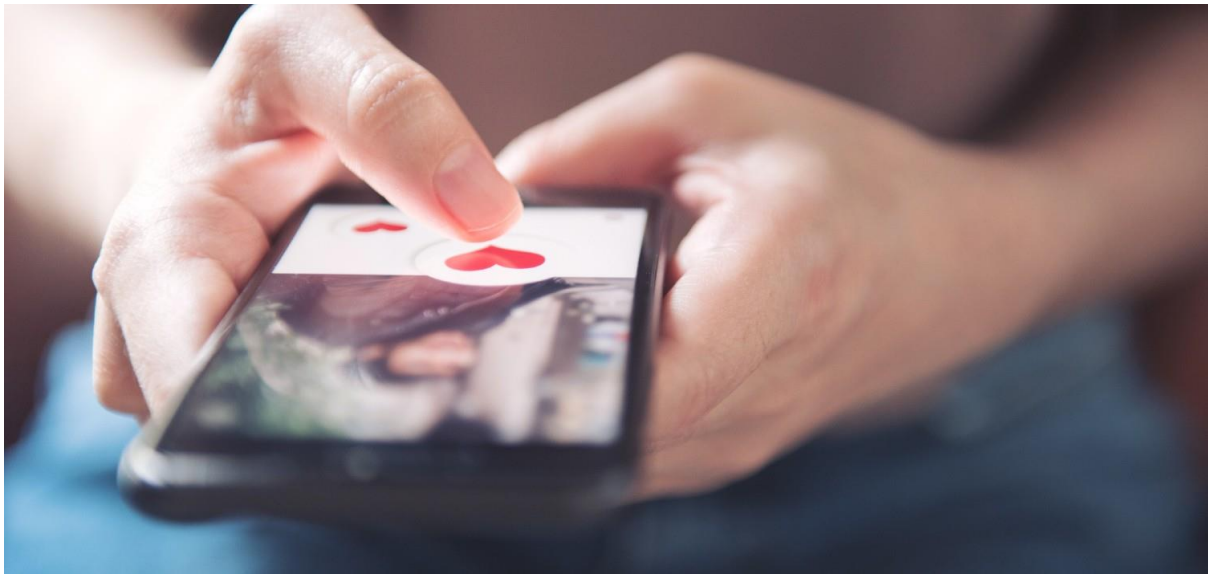
It's easy to choose a memorable password, however, the best password is one that's impossible for anyone to guess.
We recommend you change your password frequently and do not use the same password for every account.

Your password should contain a minimum of 8 characters including at least 1 upper case letter, 1 numerical digit and 1 special character (?!£$%). This will ensure your account is as secure as possible.

Be vigilant on social media

Stay smart when posting or interacting on social media - remember, everything you post on the internet could be public and permanent.
Our timelines are filled with family and friends, so they are more trusting of the content that is shared with them. Hackers often take advantage of this trust by cloning accounts and reaching out to all the cloned account's contacts.
Be sceptical of accounts or messages that seem outside of the norm, as they are likely a scam or a phishing attempt.

Be aware of romance scams



Millions of people turn to online dating apps or social networking sites to meet someone, but instead of finding romance, in some cases, they may find a scammer trying to trick them into sending money.
The scammers create fake profiles online and strike up a relationship with their targets to build their trust, sometimes talking or chatting several times a day.

They then make up a story and ask for money, usually via an international transfer, with prepaid cards or with gift cards because they can get cash quickly and remain anonymous.

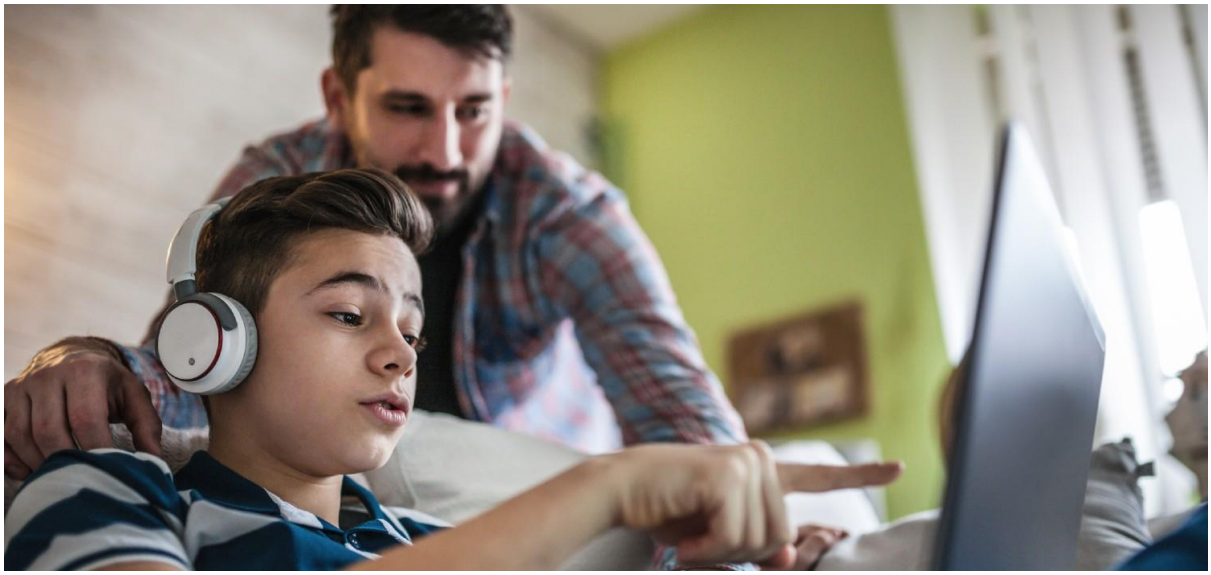
Look out for bogus websites

Double check the URL of the site you are visiting, especially if you arrived at through a link in an email. Most organisations will never ask you to link through to a site which is not their standard URL or log into your account which is not https:// encrypted. You should always see this in the browser address window with a padlock icon being displayed. This confirms the page you are visiting is secure.

Use store apps when shopping on mobile devices

It is difficult, if not impossible, to do all of the standard safety checks you would do on a computer (checking links, checking browser connections) on a mobile device's web browser.
The safest way to shop on a mobile device is to use the store's own app — downloaded from an authorised app store — and use your mobile phones network or a secure Wi-Fi network.

Top 5 tips for keeping children safe on the internet



Children are likely to be completely unaware of what viruses, phishing, social network bullying and online fraud is, or the harm it could potentially bring. That’s why it’s our jobs to educate them on the importance of staying vigilant online. Here’s our top tips:

1. **Have open discussions with them**
2. **Set parental locks**
3. **Check the device privacy and location settings**
4. **Set specific time slots**
5. **Be social savvy yourself**

Keep your eyes peeled for our more detailed article on keeping the kids safe online. The internet is a wonderful place that can educate, entertain and ease us into this indoor lifestyle. However, we must stay vigilant when surfing the net, to ensure that we avoid any online scams or fraudulent activity.