PERSONAL ONLINE SAFETY,
A GUIDE.

Lycetts | Insurance Brokers and Financial Services

ARE YOUR PERSONAL DETAILS SAFE?

Since the COVID-19 pandemic and the resulting lockdown, many clients are now facing an ever-increasing threat of online fraud. They are also facing evolving threats from fixated individuals to political activists with links to extreme movements. We have compiled a series of steps which can be taken to mitigate against the treats and limit over-exposure.

DOXING - WHAT IS IT?

Doxing is the practice of using the Internet to harvest someone's personal information, and then to consolidate and release that information online. It can be used to incite harassment by disclosing an individual's contact details and address, or to humiliate and discredit a victim by disclosing sensitive or intimate information.

There are a few more toxic practices online than just doxing, though unfortunately it is becoming all too normal. It is used to devastating effect to harass, intimidate and humiliate victims.

PROTECTING YOURSELF FROM DOXING

We advise that individuals assess their online footprint and understand what exactly is publicly accessible. It is easy to build a picture of your online footprint and find out exactly how exposed you might be. Furthermore, it is possible to request that information related to you is removed from certain websites.

- **192.com:** There is a good chance that your address will be linked to your name if you search yourself on the electoral role website 192.com. If you find information that links yourself or immediate family members to your address, you can complete an online CO1 form on behalf of yourself or members of your immediate family with no cost. The information should be removed from the website within 24 hours of receiving the form.
- **Companies House:** If you are a company owner, shareholder or director and your home address is disclosed on the company's Companies House profile, you can have the address provided on the website changed to an alternative address. We recommend that the address is changed to that of your accountant. This can be done by paying a £32 fee and completing an SR01 form. Added to this, if and when you decide to create a new company, we recommend that you list the company address to that of an accountant or company secretary.
- **Planning Applications:** All planning applications for properties are available in the public domain for viewing online and cannot be removed. We therefore recommend that any future planning application that you submit on your property should be named under your architect or interior designer.

We all have the right to be forgotten on Google. The right to be forgotten allows you to compel a search engine to de-list website links from search results for your own name. Search for 'Personal Information Removal Request Form' on Google. On the form, Google will ask you to provide each website link or URL where you traced personal information and ask for the reason why you want it removed. You can submit the form on behalf of yourself, a family member, a client or a friend. The form can be submitted at no cost.

BE VIGILANT WITH SOCIAL MEDIA ACTIVITY

Maintain good discipline on your personal social media accounts as well as that of your children in order to prevent burglars from being able to use them to gather intelligence. Burglars very often conduct reconnaissance on social media to choose their victims, learn more about patterns of life and gather information on potential assets to steal.

- Look for any historic social media accounts or email accounts that are no longer active and delete them. Social media accounts can often be forgotten about and may contain contact details or historic posts that are visible to anyone online.

- If you use multiple platforms online, have a username unique to each account rather than using the same username on each. This will mean that even if you are traced to a social media account on a particular platform, then the username on the account cannot be used to trace your accounts on other platforms.

- Good social media discipline involves managing who can view real time information about your movements, particularly if you are about to embark on a holiday.

- If you post images of luxury possessions on social media, such as photographs of cars or jewellery items, make sure that the settings on that social media account are private so that only approved individuals or accounts will be able to view these posts.

- It is unrealistic and naïve to ask people to refrain from using social media altogether, particularly if they are active users. However, the following steps are recommended to mitigate the risk of hostile reconnaissance:

Instagram: Set your Instagram account to ‘Private’ then only your approved followers can see your posts and Instagram story.

Snapchat: By default, only friends you’ve added on Snapchat can contact you directly or view your story.

Facebook: Set your Facebook account so that only friends can view your profile. Furthermore, before you post a Facebook story, click the audience selector next to ‘your story’ in the bottom right and select to share with ‘Friends’.

PROTECTION FROM ONLINE FRAUD

The unprecedented changes in lifestyle resulting from the COVID-19 pandemic have contributed to a major rise in incidents of fraud.

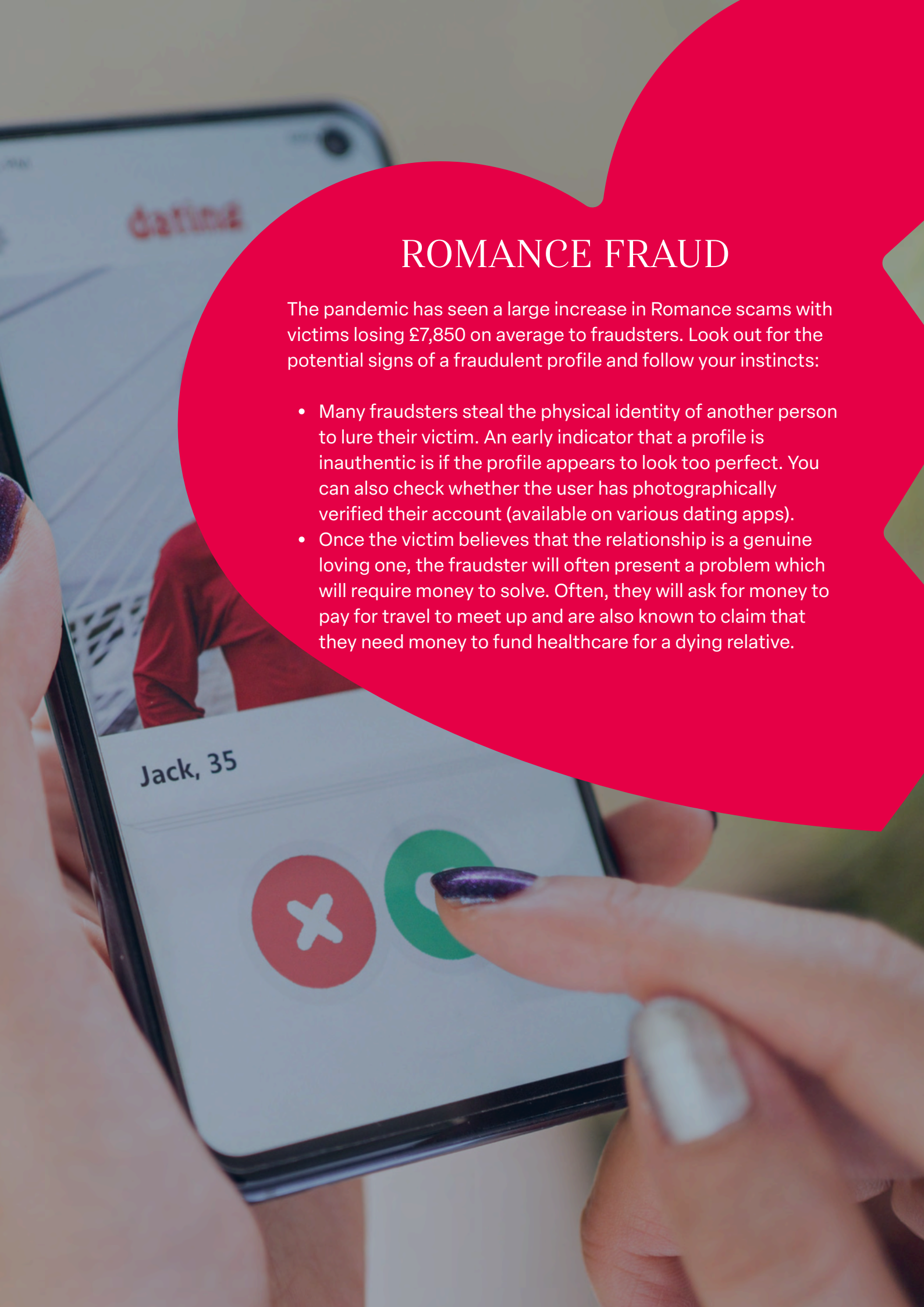
You should always destroy and preferably shred receipts with your card details on and post with your name and address on. Identity fraudsters don't need much information in order to be able to clone your identity.

Here are some of the common threats that have soared during the pandemic, and how to recognise and avoid them.

PHISHING ATTACKS

These attacks occur in the form of seemingly legitimate emails to victims, which are of course malicious and designed to lure victims into engaging with them and infecting their computers. Be aware of the following tricks and trust your instincts when recognising an attack:

- Be alert if you receive an email that does not seem right. A classic example is an email claiming to come from websites such as Amazon and advising you that an expensive item that it is claimed you have just paid for is about to be delivered to an unfamiliar address and offering you a hyperlink to click on.
- Look for other signs that the email sender is not authentic. Poor spelling or company branding and icons that appear out of place or size are common good indicators.



ROMANCE FRAUD

The pandemic has seen a large increase in Romance scams with victims losing £7,850 on average to fraudsters. Look out for the potential signs of a fraudulent profile and follow your instincts:

- Many fraudsters steal the physical identity of another person to lure their victim. An early indicator that a profile is inauthentic is if the profile appears to look too perfect. You can also check whether the user has photographically verified their account (available on various dating apps).
- Once the victim believes that the relationship is a genuine loving one, the fraudster will often present a problem which will require money to solve. Often, they will ask for money to pay for travel to meet up and are also known to claim that they need money to fund healthcare for a dying relative.

MINIMISE YOUR CYBER - ATTACK EXPOSURE

There are two main goals of cyber-attacks - to disable the target computer or attacks where the aim is to get access to the target computer's data and gain admin privileges on it.

Due to coronavirus, people have been spending more time online this year. This presents more opportunities for hackers to carry out cyber-attacks. They often do this by targeting people and businesses using:

- email and website scams
- malware - software that can damage your device or let a hacker in

If hackers get into your device or accounts, they could access your money, your personal information, or information about your business.

YOU CAN IMPROVE YOUR CYBER SECURITY BY TAKING SIX ACTIONS:

1. Use a strong and separate password for your email to all your other accounts such as banking and social media
2. Create strong passwords using 3 random words
3. Save your passwords in your browser to make sure you do not lose or forget your passwords and to protect you against fake websites
4. Turn on two-factor authentication (2FA) to stop hackers from getting into your accounts, even if they have your password. Some online banking uses 2FA automatically. It does this by asking for more information to prove your identity, such as a code that gets sent to your phone
5. Update your devices regularly with any software and security upgrades
6. Back up your data on another device or use cloud storage

HOW CAN WE HELP

ONLINE DATA ASSESSMENTS

In partnership with Blackstone Consultancy, we can conduct clients' data scrapes when required. These are conducted by analysts who are experienced at gathering as much information as is available about a client from their online footprint and discovering where potential online exposures exist. The client's online footprint will be analysed along with immediate family members and home address. A report then outlines where any online exposure exists and how it can be removed or managed.

RESIDENTIAL RISK ASSESSMENTS

Blackstone Consultancy also undertake residential risk assessments of clients' properties across Europe, both when clients want to proactively enhance their security and post burglary.

These assessments identify the true risk faced and provide a range of measures which can be implemented to reduce risk. Should either of these services be of interest, please do let us know.

CYBER INSURANCE PROTECTION

We can also offer advice on how to react and deal with the growing threats and subsequent impact of cyber-attacks. Our cyber insurance policies evolve with the fast changing and highly disruptive environment so that you are properly protected.

For a complimentary review of your insurance needs, highlighting any gaps or unnecessary cover, please contact us.

0191 232 1151

lycetts.co.uk

info@lycetts.co.uk

Lycetts | Insurance Brokers and Financial Services

Proudly part of the BENEFACT GROUP