Swipe left to romance fraud: Family members of online daters to help protect their relatives

Daters who strike up online relationships between Christmas and Valentines Day tend to be the most susceptible to romance fraud, with a spike of 901 reports recorded by the National Fraud Intelligence Bureau (NFIB) in March 2021.

Despite a peak of romance fraud reports and losses of £8.7 million reported in March, the financial spike came two months later in May 2021 where losses of a staggering £14.6 million were reported.

Criminals often use a range of stories to get victims to transfer them money without it raising suspicion. The stories are often believable, to a certain extent, and something that the victim would find hard to say no to, especially because of their emotional attachment.

Examples of stories include funding travel to visit the victim, money to pay for emergency medical expenses, lucrative investment opportunities and pretending to be military personnel or working overseas.

How to help protect people you know are online dating

- Help your friends and family to ensure they have adequate privacy settings on their social media accounts to ensure strangers don't have access to their personal information.
- Stay in regular contact with your friends and family who are online dating to help spot any changes in behaviour or things that don't seem right.
- Make friends and family aware of the signs of romance fraud so that they are conscious of the tactics criminals use to carry out these scams and reiterate that you should never transfer money to someone that you have never met in person.
- Encourage people to report to Action Fraud and the police if they have become a victim of romance fraud and not to be embarrassed about doing so.

City of London Police would urge anyone who is speaking to people they do not know or have not known for a long period of time to follow the Take Five To Stop Fraud advice.

Take Five to Stop Fraud advice

- **Stop**: Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge**: Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at police.uk or by calling 0300 123 2040.

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.

Online Shopping Fraud: Bogus E-Scooter Sales

Action Fraud received over 350 reports in 2021 about scam websites selling e-scooters.

Victims have reported buying e-scooters online only for the e-scooter to not be delivered. By this point, they're unable to contact the company as the website they made the purchase from has been closed down by its owners. Victims have reported losing over £145,000 to this type of online shopping fraud.

Action Fraud has also received reports of individual sellers offering e-scooters via online marketplaces and social media platforms and failing to deliver them once payment has been made.

We would like to remind the public that whilst the sale of e-scooters is legal, private e-scooters cannot be used in public places or on public roads. They should only be used on private land with the landowner's permission. Those who disregard the law could face fines, seizure of their e-scooter, and points on their driving licence.

What you need to do

- When it's time to pay for your items, use a credit card if you have one. Most major credit card providers protect online purchases. You can also use online payment providers such as PayPal.
- If you're unsure about the legitimacy of a product listing, arrange to meet the seller in person to inspect the item yourself. We recommend that you meet during the day in a busy, public location like a coffee shop.
- Be cautious if a seller asks you for details that are not required for your purchase, such as your mother's maiden name or the name of your primary school.
- If you have visited a website you think is trying to scam you, report it to the National Cyber Security Centre: Report a suspicious website - NCSC.GOV.UK
- If you've lost money to an online shopping scam, tell your bank and report it as a crime to Action Fraud (for England, Wales and Northern Ireland) or Police Scotland (for Scotland).

Apple publishes Airtag safety guide amid harassment and stalking fears

Apple has launched a safety guide after stalking and harassment concerns were raised over the company's Airtag.

The newest product in Apple's line-up, the accessory is a small sensor that can be attached to items such as keys and wallets or placed into backpacks to help find them when lost. Connecting to the Find My app on a user's Apple devices, AirTag and the item they are attached to can then be tracked down.

But there have been concerns that they may be used to track people without their knowledge.

Apple's Personal User Safety Guide gives support for people who are "concerned about or experiencing technology-enabled abuse, stalking or harassment".

The guide gives instructions on what to do if you have given personal information to someone who you no longer trust, or if you're concerned someone who had access to your device or accounts made changes without your permission.

AirTags sends out secure Bluetooth signal that can be detected by nearby devices in the Find My network. These devices send the location of your AirTag to iCloud — then you can go to the Find My app and see it on a map.

Amid privacy fears, Apple launched an Android app at the end of last year to help users scan nearby AirTags or similar item trackers that might be 'travelling' with them without their knowledge.

The Tracker Detect app allows a user to scan for AirTags or compatible devices if they believed someone is using it to track their location.

Warning: Don't fall victim to fraudulent investment opportunities

Investment scams can be hard to spot. Every year, victims lose thousands of pounds to criminals imitating genuine investment firms by clicking on adverts that lead them to fraudulent websites designed to replicate the page of a real investment firm. These imitation websites are known as "cloned companies".

We are working with the National Economic Crime Centre to warn the public about the increasing number of bogus investment websites, as new figures reveal:

- **In the first six months of 2021, £36.2m was lost to 'cloned company' investment scams.**
- **In the first six months of 2021, 1,100 reports were received, equating to an average loss of £47.000 per victim, when investing money in cloned companies.**

What is a cloned company? And how do they target your savings?

They are set up by fraudsters using the name, address and 'Firm Reference Number' (FRN) of real companies authorised by the Financial Conduct Authority (FCA).

The criminals running these scams engage with victims through a number of channels. Often they take out adverts on social media platforms and search engines designed to attract people to click on them by highlighting enticing offers of high returns. The returns being promised by these criminal gangs are often modest so as not to arouse suspicion, but slightly better than the market rate, therefore appealing to those looking for long term, 'safe' investments.

Once a person clicks on the advert, they are taken to an exact replica of a website belonging to a legitimate investment firm. The most sophisticated criminals will even clone the website domain name (i.e., the unique address registered to that site). Once victims have registered their interest, they'll be contacted by the offenders, who often obtain the names of genuine employees at investment firms and create seemingly legitimate company email addresses, but with very subtle changes such as one substituted letter.

TOP TIPS

- Avoid public Wi-Fi for any shopping, banking or entering of any personal information.
- Do not click on links in emails – go directly to the website the email is claiming to be from to verify any details or claim any offer.
- Look for https and either an unbroken padlock, key or the word Secure within the address bar when entering personal details online.
- Strong and unique passwords are key, try using three random words, mixed with CAPITALS, numb3r5 and punc+ua+!on to make your password more secure.

Keep up to date with the latest updates on Community Safety in Warwickshire.

Like us on **Facebook**:
www.facebook.com/SafeinWarwickshire

Follow us on **Twitter**:
@SafeInWarks

Visit our **site**:
www.safeinwarwickshire.com

If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.