‘Friend in need’ scams costs Whatsapp users £1.5 million

A convincing WhatsApp scam where criminals pose as a friend or family member in need has cost victims over £1.5 million this year.
New data from Action Fraud, the national reporting centre for fraud and cyber crime, reveals the continued threat posed by a scam that involves criminals contacting victims on WhatsApp and pretending to be their friend or a family member.

The scam has been reported to Action Fraud 1,235 times between 3 February and 21 June this year, and has cost users a total of £1.5m.
Criminals will typically claim to be a family member and will usually begin the conversation with "Hello Mum" or "Hello Dad".

They will say that they are texting from a new mobile number as their phone was lost or damaged and will go on to ask for money to purchase a new phone, or claim that they need money urgently to pay a bill.

The criminal will supply their bank details for payment, with some coming back on multiple occasions until the victim realises they've been scammed.

How to protect yourself

STOP. THINK. CALL. If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.

You can report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions.

Never share your account's activation code (that's the 6 digit code you receive via SMS)

Action Fraud advises that the public follow the advice of the Take Five to Stop Fraud campaign to keep themselves safe from fraud.

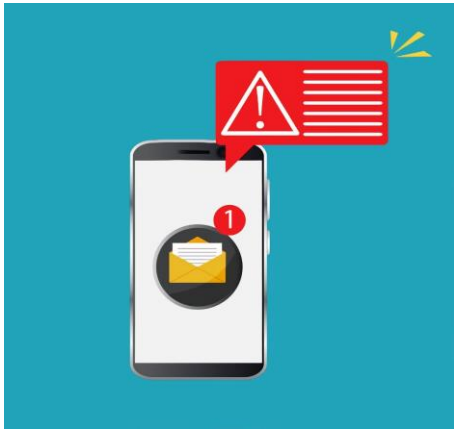
- Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.
- Challenge: Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- Protect: If you think you've been a victim of fraud, contact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

How to report

- You can report suspicious text messages you have received but not acted upon, by forwarding the original message to 7726, which spells SPAM on your keypad.
- You can report suspicious emails you have received but not acted upon, by forwarding the original message to report@phishing.gov.uk.
- If you have provided personal or financial details as a result of a suspicious message, or lost money because of a scam, you should report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040

Beware Bogus ‘OFGEM’ Emails Offering Energy Grants

Warwickshire residents have reported receiving bogus OFGEM emails relating to the £400 energy bill discount some people will receive this coming Autumn. The bogus emails ask residents to provide their personal and financial information to ‘apply’ for the grant. The Government has stated that consumers will see an automatic deduction to their bills and have warned that no household should be asked for bank details at any point. Scammers will use every opportunity to steal personal and financial information, including the cost-of-living crisis.



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.

Young Investors Targeted by Bitcoin Scams

Young Warwickshire residents have reported being scammed after signing up to 'invest' with bogus cryptocurrency trading firms, either online or over the phone.

The fraudsters promote their bogus firms on popular social media platforms. Young investors are offered the opportunity to buy Bitcoin and other cryptocurrencies and are sometimes even given login details to the bogus platform on which they are given the impression that their cryptocurrencies are appreciating in value.

In reality, the fraudsters simply steal their clients' money. No cryptocurrencies are ever purchased and when the clients attempt to withdraw their money, they are usually told they cannot do so unless they send more money to the firm!

In this way people are further scammed.

Warwickshire residents have reported losing thousands to this scam.

Protect your loved ones from callous criminals as new tactics used by courier fraudsters unveiled.

The warning comes as a new list of tactics used by courier fraudsters has been unveiled by the City of London Police.

Typically, courier fraudsters target their victims by claiming to be a police officer or a member of staff from a victim's bank and they often pressure people into making quick financial decisions to assist with fictitious investigations. In 2021 alone, 3,625 people were victims of courier fraud, with loses totalling more than £15.2 million.

An analysis of data from the National Fraud Intelligence Bureau (NFIB) has highlighted four modus operandi (MOs) which are now more commonly being used by fraudsters.

Four common MOs used by courier fraudsters

- **Bank card expiry:** Fraudsters claim to be from the victim's bank and say their card is no longer valid. They ask for the pin number and then send a "courier" to collect the card before using it for fraudulent purposes.
- **Purchasing high end items:** The suspects pretend to be police officers and ask the victim to help with an undercover operation by purchasing expensive items like watches, jewellery and gold. One the item is bought; the victim will hand over the item to the criminal.
- **Counterfeit cash/bank investigation:** A person claiming to be a police or banking official informs the victim that they need to help with a banking corruption investigation. The victim is told to withdraw a large amount of money and the cash is picked up later by a courier to "check for fingerprints or to identify counterfeit bank notes".
- **Computer takeover:** The fraudster telephones the victim, purporting to be from their internet service provider, saying that they have had an issue with their internet connectivity, and they are due compensation. The victim is persuaded to download a remote access application, giving the suspects access to their home computers. The fraudster persuades the victims into thinking that they have been paid too much compensation and the victims then withdraw cash to pay the money back, which is later collected by a courier.

MONTHS TOP TIPS:

Protect yourself from Viruses and Malware:

- Make sure your computer has a firewall and reputable anti-virus software. Without these, your computer has no defence to block infections.
- Take care downloading files. If you don't know someone who's sent you an email with an attachment, or you're not sure about a website offering a file to download, don't do it out of curiosity.
- Browse safely on the web. Get to know the risks and use the same level of caution as you would in the real world.

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

Links to relevant articles:

https://www.actionfraud.police.uk/alert/friendinneed

https://www.actionfraud.police.uk/news/protect-your-loved-ones-from-callous-criminals-as-new-tactics-used-by-courier-fraudsters-unveiled

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.