

# **‘Dear Mam’ ‘Dear Dad’ WhatsApp & SMS Fraud Scam**





# How it works

**The 'Dear Mum' or 'Dear Dad' scam involves fraudsters posing as family members in order to manipulate victims into transferring money**

Parents are targeted by criminals pretending to be one of their children, saying they are texting from a new number as their phone has been lost or damaged



They typically begin the conversation with "Hello Mum" or "Hello Dad" and then ask for their parents to transfer them money urgently as they need to buy a new phone or pay a bill

Typically, the conversation on WhatsApp, or via text message, is started by an automated bot, and then forwarded to a human who can communicate with the victim if they engage.

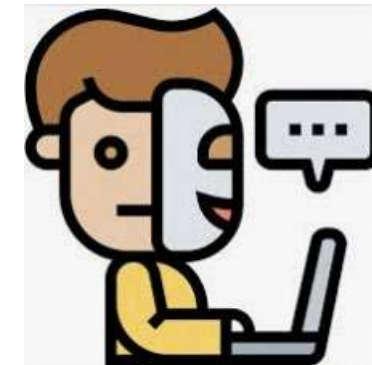
Some can take weeks because they believe that, if they can really dupe those people, it might be worth it!!



# How it works

## Impersonating family members is a new tactic by criminals to undermine people's mental safeguards against being defrauded

These scammers believe if you can add the psychological element into a scam, they work far better than the previously used phishing emails thrown out as a net



When you are being called **Mum** or **Dad**, that is what many people would have in their phonebook. Preying on the heartstrings by saying they have lost their phone – it fits in with what is very likely

It is easy for criminals to obtain a database of names, phone numbers and dates of birth through the dark web and social media channels





# Message examples via WhatsApp

## New Phone





# What to do!

WhatsApp is designed to protect people from unwanted contact, which is why, whenever you get a message from someone who isn't in your contacts, it should ask if you want to block or report them.

**NEVER EVER** take payment instruction from someone who is requesting payment via WhatsApp / SMS or any social media message without verifying in person

**NEVER EVER** click on any links asking you to confirm your account details or personal security information

Your Credit Union will **NEVER EVER** ask you to disclose your personal details via SMS or email

Be **WARY** of any number that is not already in your contacts, and to try the original stored number of the person who is apparently making contact

Immediately **BLOCK** the sender and report messages to the Guards

If in doubt, temporarily **SUSPEND** your Current Account debit card until you have verified all your debit card transactions

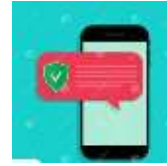




# Staying Safe Tips



## Stay Safe



Messages from unknown numbers asking for money are usually malicious.

Confirm your contact via another method before acting on any payment instruction.

Activate WhatsApp 2-step verification. Once enabled, they send a code to the default device when someone tries to log in from a different one

Take a closer look at the language being used, does it sound familiar?

Are there unusual spelling or grammar mistakes?



## Watch Out For



You get a WhatsApp / SMS message from an unknown number saying they are a friend using a different number

Messages start friendly but quickly turn into talking about money



They may ask you to transfer money to a 'safe account'

They don't answer calls if you attempt to contact them