Market Field School

Online Safety Newsletter Autumn 2022

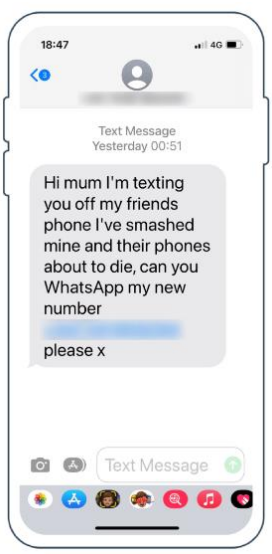
Hi Mum WhatsApp Scam

We have recently become aware of an increase in a phishing scam, often known as 'Hi Mum'. The scam involves the impersonation of friends or family members and can be conducted through text message or an instant messaging service, such as **WhatsApp.**

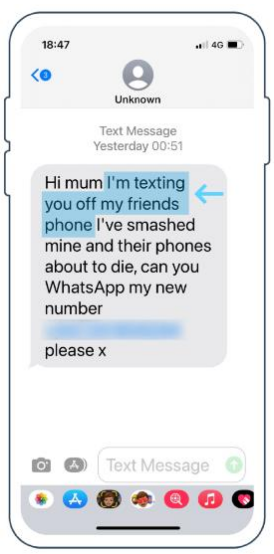
What Is The 'Hi Mum' Scam?

- Potential victims are contacted by a scammer posing as a family member or a friend. This is usually done via a messaging service like WhatsApp.
- The scammer will claim that they have lost or damaged their phone (this explains why they're contacting from a different number).
- After a few messages have been exchanged in order to build a rapport, the scammer will ask for personal information. This might be photographs (for their social media profile) or money to urgently help pay a bill, a contractor or to replace their phone.
- These requests continue the ruse of a lost or broken phone, with the justification that the funds are needed because they can't access their online banking temporarily.
- The 'end game' for the scammers is to access your banking and/or private information, which they can then use for their own financial gain.

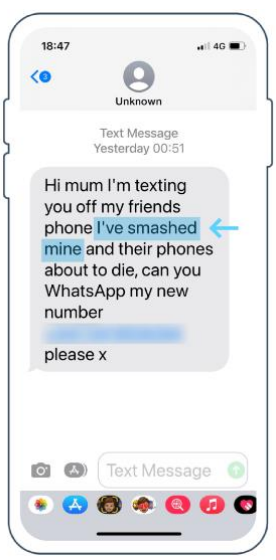
Top 3 signs to spot the 'Hi Mum' scam



1. Unknown Number



2. Instead of using a name, writing 'It's me' or not stating who it is



3. Saying their phone is lost or broken

What To Do If You've Been Targeted

Firstly, directly contact the person they are claiming to be. Ask if they have messaged you from a different number. If they haven't and you haven't yet sent any personal or private information to the scammer, you should block and report the scammer.

Never directly respond to the scammer. They may sell your details to other scammers who will bombard you with spam messages or calls.

Note the number that the scammer is contacting you from and any other information, such as a profile photo. If you can, take a screenshot – this will be helpful information to include when reporting the scammer. You can report the phishing scam to the National Cyber Security Centre (NCSC).

If you have already given the scammer information, here's the next steps you can take:

- **Phone the police.** Contact the non-emergency number 101 and report the scam to the police.
- **Change your passwords**. As soon as possible, change all passwords for accounts that have been compromised, as well as accounts that use similar account login details and passwords.
- **Cancel your card.** Get in touch with your bank immediately and cancel your card. If you have internet banking set up, you may be able to do this online.
- **Go offline.** Take your device offline so you won't inadvertently send phishing links from your device to others. If you suspect you're a victim of a ransomware attack, take your device offline and save as much as you can to a USB stick.
- **Report the phishing scam to NCSC.**

Netflix

Did you know that Netflix have parental controls available so you can restrict what your child is watching to suitable content only? You can set up a profile for your child and then set a maturity level to restrict titles to an age rating (for example 12+ or 15+). You can learn how to set up profiles here: https://help.netflix.com/en/node/264

In addition, you can block/unblock specific TV shows and movies for your child. Find out here: https://help.netflix.com/en/node/114276

Gaming Communities

Have you heard of Gaming Communities? These are online places where players can meet to chat about different games.

Parent Zone have published this useful article discussing what they are, the risks and what parents do. You can read the article here: https://parentzone.org.uk/article/gaming-communities

Sexual Harassment

Talking to our children about online sexual harassment can be difficult which is why the Children's Commissioner have produced a guide to help you. The guide focuses on several topics that can often be difficult to talk about with our children such as body image and peer pressure.

Through the work of the Children's Commissioner, they found that we should start these conversations early, introducing topics in an age appropriate manner before a child is given a phone or a social media account (often around the age of 9 or 10). The guide is a 'starting point' and includes further links to other resources, young peoples' views and top tips from 16–21 year-olds. The guide and further information can be found here:

https://www.childrenscommissioner.gov.uk/report/talking-to-your-child-about-online-sexual-harassment-a-guide-for-parents/

Online Challenges/Hoaxes

"The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children and young people to be spread quickly. You should carefully consider if a challenge or scare story is a hoax. Generally speaking, naming an online hoax and providing direct warnings is not helpful. Concerns are often fueled by unhelpful publicity, usually generated on social media, and may not be based on confirmed or factual occurrences or any real risk to children and young people."

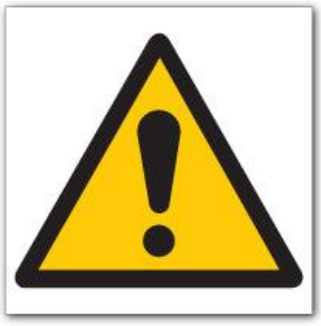
https://www.gov.uk/government/publications/harmful-online-challenges-and-onlinehoaxes/harmful-online-challenges-and-online-hoaxes [Accessed 27.6.22].

Reassure your child that challenges that suggest that bad stuff will happen if they do not complete the tasks are not real.

It is important to talk to your child about hoaxes and challenges that may appear on the internet. Some challenges are fun and provide no risk, however there will be challenges that are risky/dangerous. Your child may see others complete certain challenges online without being harmed and therefore may want to repeat them and not weigh up the potential risks to themselves. Make sure they know that they should talk to you about what they see online, particularly if they plan to try a challenge or if something scares or upsets them.

The following links will provide you with further information as well as content to help you talk to your child:

- https://www.thinkuknow.co.uk/parents/articles/theres-a-viral-scare-online-what-should-i-do/
- TikTok have produced this resource to help you talk to your child about challenges and the potential risks: https://www.tiktok.com/safety/en-sg/online-challenges/



Social Media: harmful content

Report harmful content provide links to the advice sections from several social media platforms: https://reportharmfulcontent.com/advice/advice-for-parents/

Useful sites

- UK Safer Internet Centre provide tips, advice, guides and other resources to help.
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- National Online Safety | Keeping Children Safe Online in Education has lots of free parent/carer guides on a variety of topics.
- Childnet — Online safety for young people provides lots of helpful information about online safety.