



**National
Online
Safety**

Publish date: 13/02/19

WARNING!

Catfishers will
target **ANYONE**
OF ANY age

What parents need to know about

CATFISHING

In this technological era, making friends online and communicating with them are normal parts of life. Unfortunately, there are people out there who may try and exploit your trust. Catfishing is when someone creates a fake online profile to trick people into thinking they are somebody else. They assume a fake identity and goes the extra mile to make their victim believe that they are exactly who they say they are.

1 new friend request

WHY DO PEOPLE CATFISH?

The term 'catfish' was coined in a 2010 documentary about a man who developed an online relationship with a woman, only to discover the person he thought he was communicating with was someone else. Catfishers make up life stories and use photographs of unsuspecting victims to create fake identities. They will share life experiences, jobs, friends and photographs to the fake accounts. The aim of the perpetrator may be to lure victims into a sexual relationship, but they can also be part of social engineering to trick people out of money. After building up trust and developing an online relationship, a catfisher may ask for cash for a loan, money for travel, or some other form of payment.

OTHER CONCERNS & WORRIES

Catfishing can escalate very quickly. As someone executing a catfishing scam is looking to achieve a goal - whatever that may be - they are likely to want to get things moving as quickly as possible. The victim may be encouraged to develop a relationship faster than they are comfortable with. In addition to this, people who create fake identities could also be taking the victim's photos and pretending to be them. It is common for fraudsters to post pictures stolen from social media sites, including Facebook and Instagram.

HOW TO SPOT CATFISHING

Profile pictures and other photos that are posted can be big indicators. To avoid revealing their real identity, a catfisher may use 'stock' images of models, other people's photos or photos in which it is difficult to see their face. They may try to limit chat to text-based messaging and anything involving video is likely to be shunned for fear of revealing their true identity. Through the course of conversations, there may be inconsistencies with what is said, or instances of people being very vague in response to specific questions about themselves.



Top Tips for Parents

MONITORING & CONVERSATION

Encourage your child to talk to their trusted adults about anything that has made them feel uncomfortable online, particularly if someone they don't know has contacted them. Remind them that they should not accept friend requests or communicate with anyone they don't know online, and to ask a parent or carer if they are unsure. It is also very important to closely monitor their internet usage so you are aware of who they are communicating with, especially if they are being secretive. Have regular and honest conversations with your child about what is safe to share with people online; the importance of keeping private information private; and that anything that could identify them should not be shared online.

PRIVACY & SECURITY

Go through your child's security and privacy settings thoroughly to ensure that their online profiles are set to private. This means that only friends can see their profile and can contact them. It may also be a good idea to check through your child's friends list with them - do they know and trust everyone on the list? In some cases it's difficult to stop young people from talking to new people. In these circumstances, encourage your child to be curious and ask lots of questions rather than rely on the information given in someone's online profile. Do they have any mutual friends? If not, how did that person find them and why did they reach out? It's vital that they know never to arrange to meet up with people they meet online, and never to send money to them - either their own, or from your account.

BE ALERT & REPORT

Make sure that you and your child is aware of how to report and block accounts on all platforms that the child uses. You can report fake accounts and block users to prevent them from viewing your child's profile. If you are concerned that someone is using your child's photographs for their own benefits, you can check by using Google image search. You can upload a photograph and Google will show related images used on other websites. This will show you if anyone else is using photos that your child has previously shared online. If this is the case, you need to report the user directly to the platform. If you suspect that any fraudulent, illegal or inappropriate activity has taken place, you should report to the police immediately.

SOURCES:

<https://www.thesun.co.uk/news/4303893/student-17-catfished-facebook-year/>
<https://www.thesun.co.uk/fabulous/1754916/catfishing-meaning-identity-steal-online-dating-law/>