Is someone using your pictures to catfish? Your rights when it comes to fake profiles and social media stalking

October 18 2023, by Rachel Maguire and Aislinn O'Connell

Credit: AI-generated image (disclaimer)

If you've ever used a dating app, you've probably experienced the disappointment of meeting someone who doesn't look quite like their photos. You may have even been a victim of catfishing, where someone creates a fake identity to deceive or scam others online. But what if

someone uses your photos to catfish someone else?

Setting up a social media account or dating profile is as easy as entering a name and email address. Platforms do very little to verify users' identities, making it easy for someone to scam you, harass you—or pretend to be you.

There is very little known about how many online accounts are fake. What we do know is that many of these fake profiles use images from real people—often an unsuspecting third party's public social media account. This, of course, can cause problems for the person whose photo is used. Their face is now attached to online behavior that may be illegal, dishonest or just plain embarrassing.

Fake profiles can also include the personal contact details of an innocent third party, a form of doxing (revealing identifying or personal information about someone online) that can lead to unwanted calls, texts, emails, or even in-person visits and violent attacks.

Can the law help?

Unfortunately, if a fake account is using your image or contact details, there are not always reliable legal protections to help you stop it.

There are some relevant criminal offenses in the UK, but they can be difficult to investigate and prosecute. For example, if the profile is being used to carry out a financial scam, it might be fraud. Doxing that results in the target being bombarded with unwanted messages could be stalking or harassment.

There is also a communications offense that criminalizes knowingly sending false messages or persistently using the internet to cause someone annoyance, irritation or needless anxiety. New online safety

laws could make it harder to establish criminality for this, by requiring proof that the perpetrator intended to cause the target physical or "non-trivial" psychological harm.

Other legal options include suing whoever set up the fake account. There are potential civil claims in harassment, defamation or copyright law. However, this is expensive, time-consuming and reliant on being able to identify the account holder, which is not straightforward. Perpetrators may be located in a different country, so outside of court jurisdiction—if they can be tracked down at all.

If you think that a crime has been committed, contact the police for their advice, particularly if you think that you know who is behind the account. Evidence is vital, so make sure you take screenshots before you do anything else.

What platforms can do

Asking the platforms to remove fake profiles may be your best option. If the account is using photographs that you took yourself, one of your most effective legal protections will be copyright law. Platforms are not generally liable for the content posted by users, but if you use their tools to report copyright infringement, they will take it seriously.

You can also report fake accounts using websites' own tools. This can sometimes turn into a game of fake profile "whack-a-mole", as new accounts spring up as soon as one is shut down. Additionally, platform responses to such reports have not always been adequate.

A new law might help. Under the online safety bill, which is awaiting royal assent, platforms must take steps to prevent users from encountering "priority illegal content" that amounts to certain criminal offenses, including stalking and harassment. This legal obligation should

make platforms more proactive about addressing these types of harms.

The new law will also require the largest and riskiest platforms (such as the main social media sites) to offer users a way to verify their identity. Verified users will also be able to block non-verified users from seeing their content, reducing the risk of unknown users accessing their photographs and personal information.

How to protect yourself

1. Make a report

Use platform reporting tools to request that profiles are taken down. Speak to the police if you think a crime such as fraud, stalking or harassment has taken place, and take screenshots of messages or false accounts as evidence.

2. Tell your networks

Let your friends and family know that you have come across a fake profile using your information. If they know it is out there, they are less likely to think it's you. Consider agreeing code words so that friends and family can check it is really you, and not a scammer, before sharing personal or financial information via messaging apps.

3. Protect your images

This is certainly not foolproof, but adding a watermark to photos, such as your social media handle, can reduce their appeal to fraudsters.

4. Review your privacy settings

It is not always feasible or desirable to have a private account, but make sure you have made conscious choices about your online privacy, rather than relying on default settings.

Provided by The Conversation