Stay Safe Online:

Scam Awareness after Brain Injury

Introduction

Recovering from a brain injury can bring about unique challenges, including changes in cognitive function such as memory, attention, and problem-solving skills. These changes may make it difficult to recognise potentially fraudulent situations, which is why scammers often target people in vulnerable positions.

The goal of this booklet is to empower you with knowledge and tools to protect yourself.

Let's take the first step towards enhanced safety by understanding the landscape of scams and how they might affect you.

What are scams?

Cyberscams are tricks that happen on the internet, through texts, phone calls, emails, and social media.

Scammers are skilled and manipulative; they read from scripts, and often deceive people with their clever tactics. On top of that, technology moves fast and it is difficult to keep up with safe practices.

In 2021, more than two thirds of adults in the UK were targeted by a scammer.

Why are scams bad?

A scam is bad because it means someone is trying to trick you or take advantage of you. Here are three problems scams might cause:

- **Losing money:** Scams often trick you into giving away your money. This can mean you might not have enough money left for important things like rent, food, or bills.
- **Feeling upset:** Being scammed can make you feel very sad, confused, or embarrassed. It can be very upsetting to lose money or trust in others.
- **Harder to trust people:** After being scammed, you might find it hard to trust others, even people you meet who are not trying to

scam you. This can make it difficult to enjoy talking to new people or trying new things.

Why brain injury increases scam risks

Individuals recovering from brain injuries often face unique challenges that can unfortunately make them more susceptible to scams. Understanding these vulnerabilities is crucial in developing strategies to protect yourself.

Here are reasons why those with brain injuries might be at a higher risk:

- **Impaired judgment:** Brain injuries can impair judgment, making it harder to discern legitimate offers from scams. This can lead individuals to mistakenly trust fraudulent schemes.

- **Memory issues:** Memory loss is common after a brain injury, which scammers exploit by contacting victims repeatedly or altering their deceptive offers to appear more believable.

- **Reduced executive functioning:** Brain injuries can weaken the ability to organise and prioritise, leaving individuals overwhelmed by information and more prone to making hasty decisions without proper evaluation.

- **Increased emotional vulnerability:** Brain injuries may disrupt emotional control, increasing susceptibility to emotionally charged scams that urge you to act quickly.

- **Social isolation:** Recovery often leads to reduced social contact, which scammers exploit by offering fake friendships or support to manipulate victims' emotions.

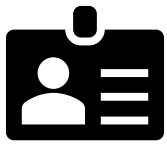
- **Spending a lot of time online:** The more you're online, the more you might run into scams. If you use the internet a lot, you might start ignoring the warning signs of scams without realising it.

- **Dependency on others:** Increased reliance on help post-injury can make individuals targets for scammers posing as support professionals or advisors to gain trust and access finances.

Red flags of scams

Being aware of the common warning signs can help you avoid falling victim to scams. Here are essential red flags to watch for:

1. **Sense of urgency:** Scammers pressure you to act quickly with statements like "Act now!" or "Limited time offer!" This tactic is designed to prevent you from thinking critically or seeking advice.
2. **Too good to be true offers:** Extreme bargains or unexpected large sums of money for minimal effort should raise suspicions. If an offer seems too good to be true, it likely is.
3. **Requests for personal information:** Be cautious if you're asked for sensitive information such as:
    a. your birthday,
    b. user name and passwords,
    c. national insurance numbers,
    d. bank details,
    e. passwords,
    f. names of pets, the school you attended, or your mother's maiden name.



4. **Unsolicited contact:** Unexpected calls, emails, or messages, particularly from strangers or from abroad (watch for international codes like +44 for the UK), can be red flags.
5. **Suspicious payment methods:** Scammers often prefer untraceable payment methods such as wire transfers, cryptocurrencies, or gift cards (like iTunes vouchers).
6. **Poor grammar and inconsistencies:** Errors in communications or inconsistencies in language that don't fit the individual's supposed background might indicate a scam.
7. **Avoidance tactics:** Be suspicious if someone avoids meeting in person or video calls by claiming their camera or internet is broken, especially if they also have dramatic excuses like financial troubles or family emergencies.
8. **Unusual requests:** Be sceptical of requests to perform tasks that a stranger could do themselves, such as opening a bank account, buying a mobile phone, or shipping parcels.
9. **Impersonation:** Be wary of anyone claiming to represent reputable organizations without proper verification. Always check their credentials through official channels.

Trust your gut feeling. If something feels off about a person or situation, it's worth taking a closer step to verify the details before proceeding.

Preventing scams

Protecting your personal information and financial details is crucial to avoid falling victim to scams. Here are some strategies to safeguard your sensitive data:

Protective measures

1. **Strong passwords:** Use complex passwords that include a mix of letters, numbers, and symbols. Avoid writing them down.
2. **Two-factor authentication:** Enable two-factor authentication on all accounts that offer it. This adds an extra layer of security by requiring a second form of identification beyond just your password.
3. **Secure networks:** Only enter sensitive information when connected to secure Wi-Fi networks. Avoid using public Wi-Fi for financial transactions or accessing sensitive accounts.
4. **Check bank statements:** Regularly check your bank statements and credit reports for unauthorised transactions or changes.
5. **Adjust privacy settings**: Adjust the privacy settings on your social media and other accounts to control who can see your information.
6. **Regular updates:** Keep your software, apps, and devices updated. Updates often include security patches that protect against new threats.
7. **Keep track**: Occasionally search for your name online to see what information is available about you and take steps to remove anything you don’t want public.
8. **Clean up**: Delete old accounts you no longer use and clear your browsing history regularly.
9. **Meeting up safely:** If you make a friend online and decide to meet, choose a public place and always tell someone where you're going.

Security best practices

1. **Educate yourself and family:** Stay informed about the latest scam tactics. Educating yourself and family members can help you recognise and avoid new scams.

2. **Shred sensitive documents:** Shred documents that contain personal information before disposing of them to prevent dumpster divers from getting your data.
3. **Verify sources:** Before responding to any requests for personal information or money, verify the legitimacy of the source. Contact the organisation directly using a trusted number or website.

How to stop a scam

Anyone can be tricked by a scam. There's no reason to feel embarrassed if it happens to you.

Once you've lost money to a scam, it's usually hard to get it back. But you can do things to stop losing more money.

First, make sure you:

- **Don’t talk to the scammer anymore:** Cut off all contact right away.
- **Stop sending money:** The scam ends when you stop the money.
- **Talk to someone you trust:** Tell a friend or family member what’s happening. They can help you figure out what to do next.
- **Call your bank or payment service:** Let them know about the scam as soon as you can. They might stop more money from going out or close your account to keep it safe.

Next, protect your information:

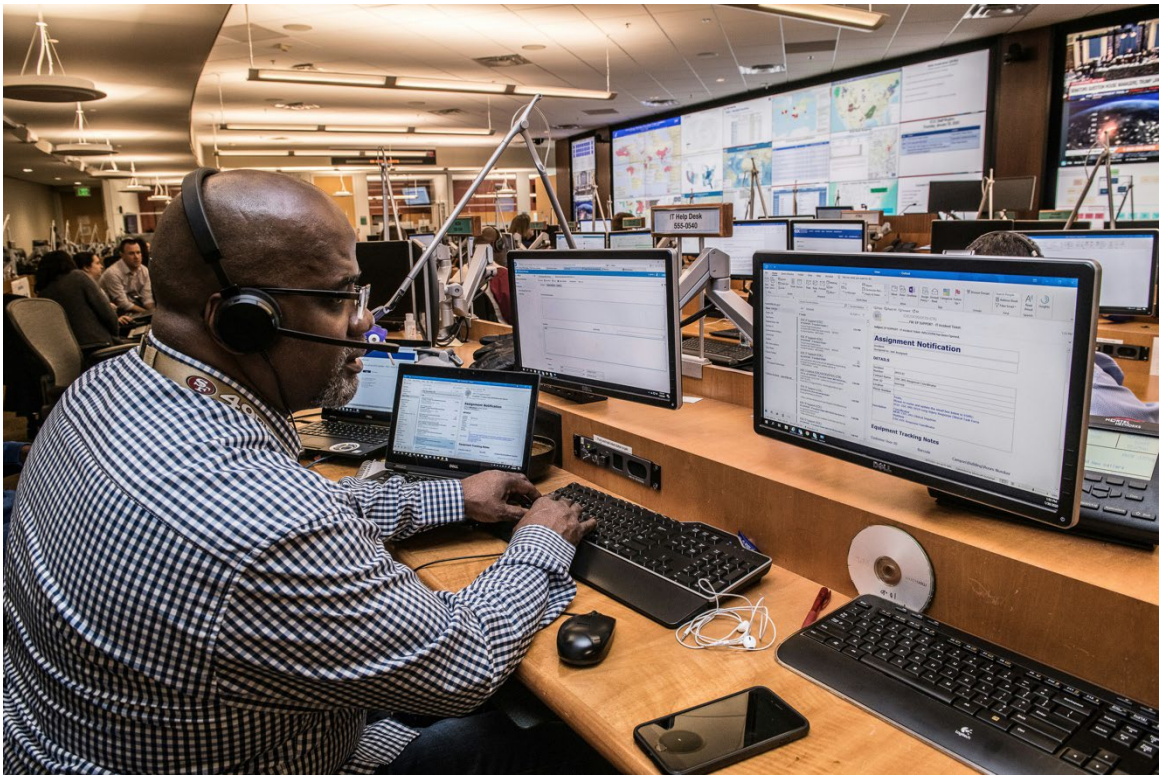
- **Change your passwords:** Make new passwords for things like your bank account, email, and social media.
- **Block the scammer:** Block their phone number and social media so they can’t reach you.
- **Check your privacy settings:** Make sure your social media profiles are set to private.
- **Make your phone safer:** Use security apps on your phone that stop scams.

Finally:

- **Use a scam detection app**, such as Truecaller or Bitdefender, which can help identify and block scam calls and texts.
- **Report the scammer** on the platform they contacted you on to help prevent them from scamming others.

Who to contact if you have been scammed

- If you **feel threatened or unsafe**, dial 999.
- If the **scammer is in your area or** you **transferred money to the scammer in the last 24 hours**, tell the police immediately by calling 101.
- **Action Fraud:** You can report fraud or cybercrime by calling 0300 123 2040 Monday to Friday 8am - 8pm. You can also report it any time of the day or night using an online form.
- **Advice Direct Scotland's Consumer Service:** Report the scammer to Advice Direct Scotland's consumer service. They will give you advice on what to do next and report the scam to an authority: www.advicedirect.scot
- **Your bank:** If you've noticed any unusual activity with your bank account, call the centralised number **159** or the phone number on the back of your bank card.



Coping with being scammed

It is understandable for you to feel shocked, angry, or embarrassed as a result of being scammed.

Recognising that you have been scammed is a crucial first step towards regaining control and preventing further damage.

Talking about what happened with trusted friends or family members can really help. You could speak with your doctor, who can refer you to a mental health support worker, or reach out directly to a counselling or support service:

- **Think Jessica:** If a scam has made you feel anxious, fearful or guilty. They provide emotional and practical help to victims of crimes and scams.
- **Samaritans:** You can call their helpline on **116 123** if you feel low or anxious and need someone to talk to.

Going through a scam doesn't have to be all bad; there are silver linings too. Overcoming a scam can make you feel empowered and turn a negative into a triumph. It teaches you to trust your instincts, making you more cautious and wiser in the future.