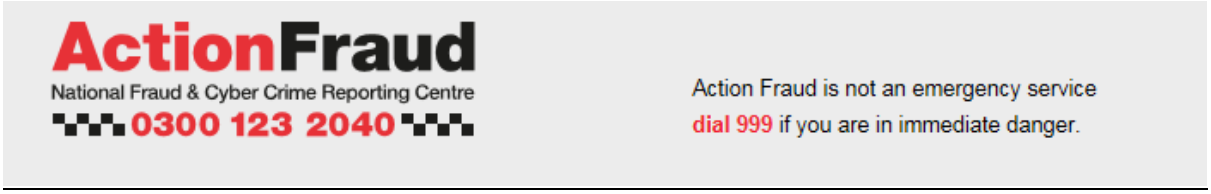
This advice sheet from NHS England South (SW) has been produced with the kind permission of the National Fraud and Cyber Crime Reporting Centre

Recently in the South West, NHS England South SW have received a number of reports from GP Practices regarding patients who have been "cold called" by representatives of various companies. These callers (both by phone and in person), seem to know the patient's medical history and sometimes say that this information has been obtained from the GP Practice. **No GP Practice will ever divulge your medical history.**

If you receive such a call please report it to:

ActionFraud either via the **online fraud reporting form or make your report by calling 0300 123 2040.**



Who is National Fraud Intelligence Bureau?

The National Fraud Intelligence Bureau (NFIB) sits alongside Action Fraud within the City of London Police which is the national policing lead for fraud.

Protect yourself from Fraud

Although fraud comes in many forms, there are some simple steps you can take to protect yourself from the crime.

1. Do not give any personal information (name, address, bank details, email or phone number) to organisations or people before verifying their credentials.

2. Many frauds start with a phishing email. Remember that banks and financial institutions will not send you an email asking you to click on a link and confirm your bank details. Do not trust such emails, even if they look genuine. You can always call your bank using the phone number on a genuine piece of correspondence, website (typed directly into the address bar) or the phone book to check if you're not sure.

3. Destroy and preferably shred receipts with your card details on and post with your name and address on. Identity fraudsters don't need much information in order to be able to clone your identity.

4. Make sure your computer has up-to-date anti-virus software and a firewall installed. Ensure your browser is set to the highest level of security notification and monitoring to prevent malware issues and computer crimes.

5. Sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option while shopping online. This involves you registering a password with your card company and adds an additional layer of security to online transactions with signed-up retailers.

6. If you receive bills, invoices or receipts for things you haven't bought, or financial institutions you don't normally deal with contact you about outstanding debts, take action. Your identity may have been stolen.

7. You should regularly get a copy of your credit file and check it for entries you don't recognise. Callcredit, Equifax and Experian can all provide your credit file. An identity protection service such as **ProtectMyID** monitors your Experian credit report and alerts you by email or SMS to potential fraudulent activity. If it's fraud, a dedicated caseworker will help you resolve everything.

8. Be extremely wary of post, phone calls or emails offering you business deals out of the blue. If an offer seems too good to be true, it probably is. Always question it.

9. If you have been a victim of fraud, be aware of fraud recovery fraud. This is when fraudsters pretend to be a lawyer or a law enforcement officer and tell you they can help you recover the money you've already lost.

10. If you need advice about fraud, call Action Fraud on 0300 123 2040 to discuss your situation with one of our specialist fraud advisers. To report a fraud, you can either use our **online fraud reporting form or make your report by calling 0300 123 2040.**

CLICK HERE to Report Fraud and Cyber Crime | Action Fraud