

Coronavirus Vaccine Scam Warning



Coronavirus vaccine scams

OFFICIAL

Coronavirus vaccinations are free of charge. The NHS will never:

- ask for your bank account or card details
- ask for your PIN or banking passwords
- arrive unannounced at your home to administer the vaccine
- ask for documentation to prove your identity, such as a passport or utility bills

The vaccine is only available on the NHS and is free of charge.

If you receive an email, text message or phone call purporting to be from the NHS and you are asked to provide financial details, or pay for the vaccine, this is a scam.

A Practical Guide to Romance Fraud

[A new booklet](#) has been developed by Thames Valley Police's Economic Crime Unit alongside Dr Elisabeth Carter, Senior Lecturer in Criminology and Forensic Linguist at the University of Roehampton

It explains the clever tactics used by romance fraudsters who are masters of manipulation and will go to great lengths to create a false reality in which an individual feels that they are making reasonable and rational decisions.

Staying Safe from ROMANCE FRAUD

A practical guide highlighting common tactics used in romance fraud. Safeguarding through knowledge and empowerment.



The booklet also dispels the myths of shame and embarrassment often associated with this crime by highlighting the link to coercive control.

Safer Internet Day 2021

Get involved in the day
We have films, free resources, top tips, a quiz, posters and more.

saferinternetday.org.uk

[Safer Internet Day](#) is on 9th February 2021. This theme will be: An internet we trust: exploring reliability in the online world. With many young people now learning from home UK Safer Internet Centre have produced four documents to help educators engage young people in the celebrations for Safer Internet Day.

National Insurance Scam Phone Call

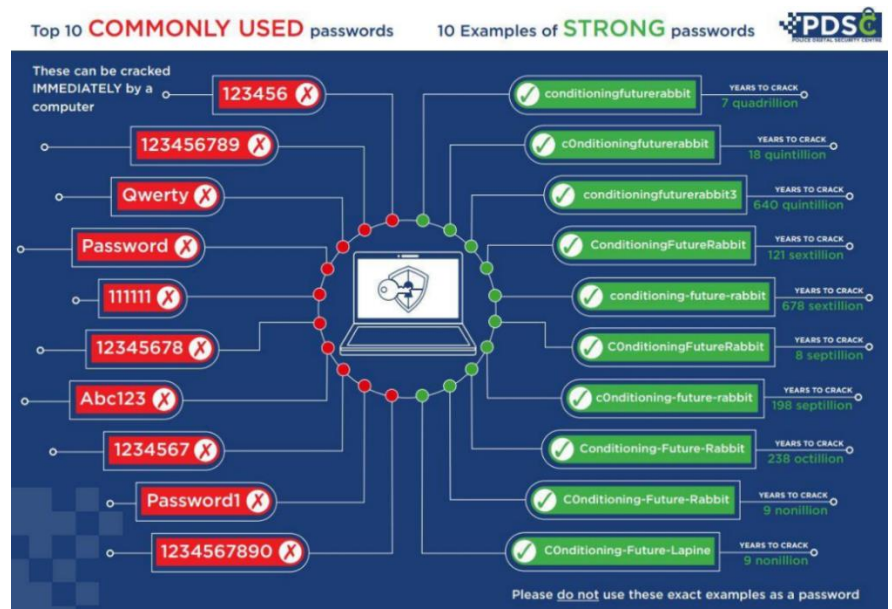
Action Fraud is warning the public about a [National Insurance scam](#). Victims have reported receiving an automated telephone call telling them their “National Insurance number has been compromised” and in order to fix this and get a new number, the victim needs to “press 1 on their handset to be connected to the caller”.

You can report a scam call to Action Fraud via [the website](#) or by calling 0300 123 2040. Additionally, if you’ve received a suspicious phone call, you can help the HMRC’s investigations by providing your phone number, the caller’s phone number, the date and time of the call and a brief description to phishing@hmrc.gov.uk



Protect your online accounts: Use strong passwords

Passwords are essential to the security of online accounts. Cyber criminals have developed techniques to break-in to online accounts and act as the authorised user. These attacks are successful when users create weak passwords or utilise common techniques. Strong, unique passwords can combat these attacks. Please see the [Police Digital Security Centre](#) for further details.



Two-factor authentication to further protect your passwords



Two-factor authentication (2FA) can be enabled on important online accounts to protect them. Action Fraud say it is the single best thing you can do to improve the security of your most important accounts such as emails. It can protect the account even if the password has been stolen such as in cases of a data breach. It is an additional layer of protection for your accounts.