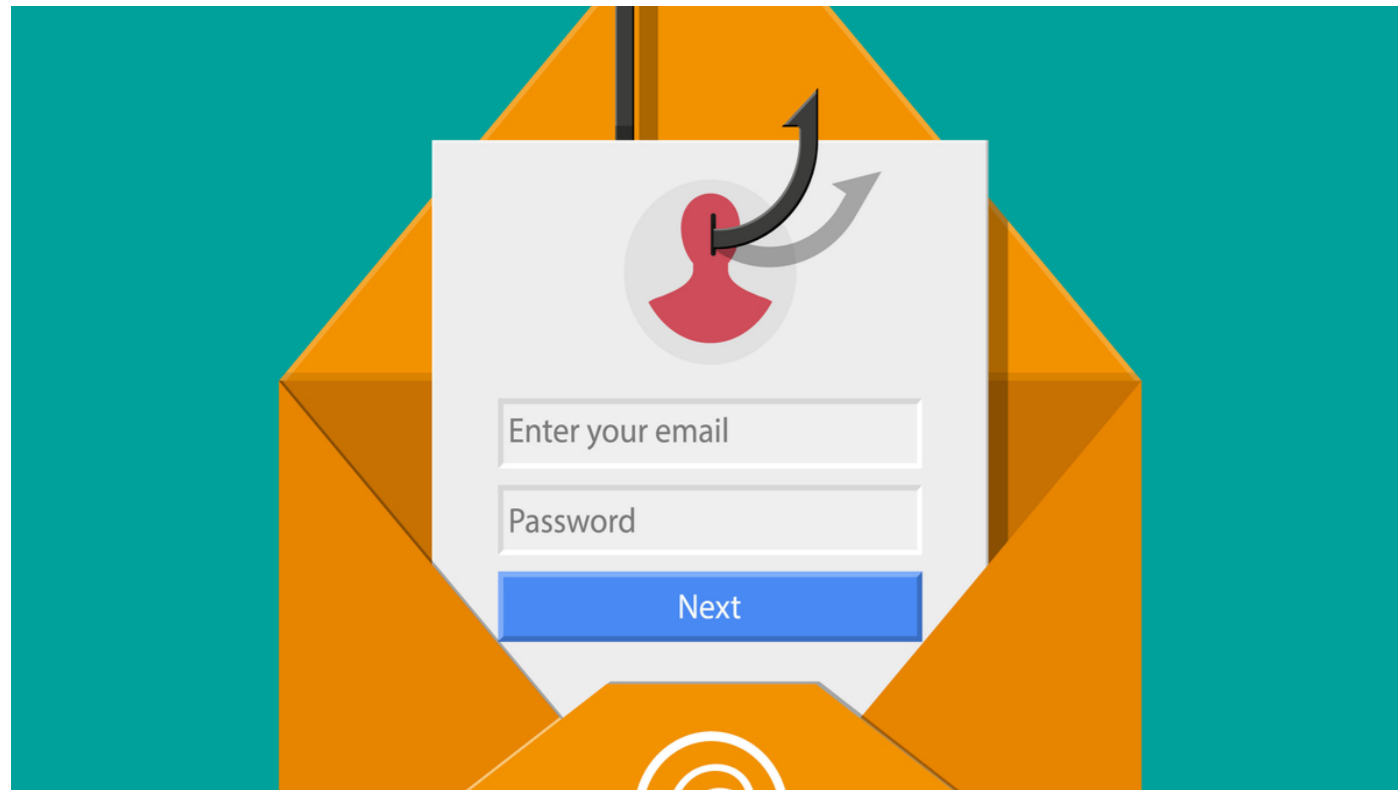


Instagram Phishing



In the context of Instagram, someone might send you a suspicious message or link that asks for personal information. These messages could try to scare you by claiming your account will be banned or deleted if you don't follow their directions.

Another phishing method on Instagram could be through spoofed login page in fake apps or websites. These apps might promise to manage a users social media account.

How to avoid getting phished?

- Look out for suspicious emails or messages
- Don't click suspicious links
- Don't respond to these emails
- Create a secure password using **ThreeRandomWords** and a combination of numbers, symbols and cases
- Turn on **two-factor authentication**



Recovering a hacked account

- Update your devices
- Contact your provider
- If your email account was hacked
- Change passwords
- Set up two-factor authentication
- Notify your contacts
- If you decide to make a new account, be sure to notify your contacts
- Contact Action Fraud

Reporting


If you think your online account has been hacked **report it.**



Action Fraud is the main fraud and cyber crime reporting service in the UK. You should also report to the social media account provider.



Suspicious Email and Text Reporting

 7726

 report@phishing.gov.uk