

Resource 3: Top Tips for Avoiding Social Engineering and Cybercrime



01	Get a second opinion if an offer, competition or giveaway is too unrealistic.
02	Avoid rushing or being pressured to act urgently, particularly if there is pressure to reply or give information in a short time period.
03	Think about the information being asked to handover; why might a legitimate company want or need this?
04	Trust instincts – if something doesn't seem right, don't be embarrassed to refuse to give over information or to leave the conversation.
05	Check who sent the email or verify the caller; if it's genuine, they won't mind if someone checks and uses the general email address or phone number.
06	Check who the email is sent to and question where it came from.
07	Be aware of companies or contacts that are not familiar; use a search engine to check they are genuine.
08	Do not click on any links or open any attachments without doing some research first.
09	Be cautious with social media, keeping privacy settings high, not over sharing personal information and being wary of clicking links.
10	Protect devices by making sure anti-virus software is installed and is regularly updated. Have strong and varied passwords for the different services used online.