TOP TIPS FOR FIGHTING CYBER CRIME AND FRAUD

01	If an offer, competition or give-away seems too good to be true, it probably is!
02	If a lot of pressure is involved, particularly pressure to reply or give information in a short time period, this is a key indicator of a scam
03	Think about the information you are being asked to handover; why might a legitimate company want or need this? Also be aware of information that quizzes or competitions on social media ask for; they are a way of gathering people's personal information.
04	Trust your instincts; if something doesn't seem right, don't be embarrassed to refuse to give over information or to exit the conversation
05	Check who sent the email; if the email claims to come from a company then it should have an official email address, not an individual person. Verify the caller; if it is a genuine call from the police, the bank or a company they won't mind if someone hangs up and calls them back.
06	Check who the email is sent to; if your name is not included at the start of the email, and instead your email address or username is used, this is unlikely to be a genuine email
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. If the email is presenting a genuine offer, it can be accessed through the company's website rather than the email they send. hovering over hyperlinks will show the web address it links through to.
09	Beware of social media! Lots of scams on social networking sites are about gathering 'likes' and 'shares' which reveal personal information – keep privacy settings high, don't over share personal information and beware of clicking links
10	Protect your technology by making sure antivirus technology is installed and that it is regularly updated. Use strong and varied passwords for different devices and sites.