

# EYES WIDE OPEN

## FRAUD

Many people already know the do's and don'ts of financial fraud and scams – the no one should ever contact you out of the blue to ask for your full PIN or password, or even make you feel pressured into moving money to another account. The trouble is, in the heat of the moment, its easy to forget this. After all, trusting people on their word is something everyone tends to do instinctively. If someone says they're from your bank or trusted organisation, why wouldn't you believe them?

Criminals' use of social engineering tactics through deception and impersonation involving the criminal posing as a genuine individual or organisation and contacting the victim using a range of methods including via telephone, email and text message. Criminals also use social media to approach victims, using adverts for goods and investments which never materialise once the payment has been made.

So when you receive an email, text message or phone call,

**STOP** – Take a moment to stop and think before parting with money or personal information

**CHALLENGE** – Could it be fake? Its ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you

**PROTECT** – Contact your bank immediately if you think you have been the victim of a scam so they can take action to protect your money the contact Action Fraud.

**Action Fraud 0300 123 2040**

**Humberside Police Non-Emergency Number 101**

