FRAUD AWARENESS
FRAUD
NEWSLETTER

GREATER MANCHESTER POLICE

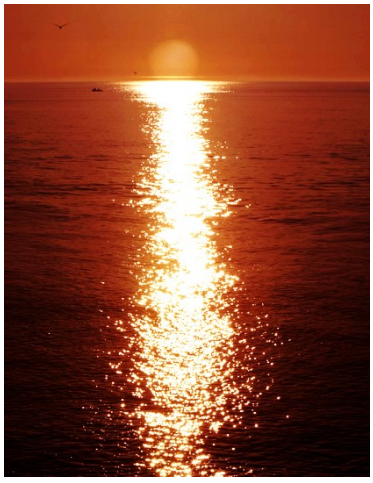
July 2017

Advice to help keep your money safe

Holiday Booking Fraud

Holiday Fraud is when you pay a travel agent or agency, or someone offering short-term lodging for rent online, and find out that the holiday you've booked or parts of it don't exist. A report written by the City of London Police's National Fraud Intelligence Bureau, revealed fraudsters stole £7.2 million from almost 6,000 unsuspecting holidaymakers and other travelers in 2016.

Fraudsters usually use fake online adverts, bogus sales calls, emails and text messages offering cheap rates to tempt you into booking a holiday with them. They may steal images of hotels or rented apartments from other travel websites and pass them off as their own. You're told to pay in cash or via a bank transfer, such as MoneyWise or Western Union, which can be difficult to trace and isn't refundable.



HOW TO SPOT IT:

- You may be contacted out of the blue by a travel agent or company you've never spoken to before, offering a holiday at a suspiciously low price.
- The details, pictures or address of the property or hotel on offer look suspicious, or independent website reviews aren't favourable or don't exist.
- You're asked to pay using bank transfer or cash; be cautious or pay by credit card if you can for extra protection.

HOW TO PROTECT YOURSELF:

- Check the web address has not been altered by slightly i.e. going from .co.uk to .org.
- Do research, don't just rely on 1 review - do a thorough online search to check the company's credentials.
- Check whether the company is a member of a recognised trade body such as ABTA. If you have any doubts, you can verify membership via ABTA online, at **www.abta.com/find-a-member**.
- Paying by direct bank transfer is like paying by cash – the money is very difficult to trace and is not refundable. Wherever possible, pay by credit card.
- Carefully check receipts, invoices & terms and conditions. Be wary of companies that don't provide any documentation. When booking through a Holiday Club or Timeshare, get the contract thoroughly vetted by a solicitor before signing up.

Phishing Scams

Phishing scams are a scammers attempt to trick you into providing them with personal information such as bank account numbers, credit card details and passwords. Scammers usually do this by contacting you out of the blue & pretending to be a legitimate person from a business such as your bank or internet/phone service provider.

They will often contact you via social media, phone calls, text messages and email. For example, emails & messages from the scammers can contain links that lead you to fill a survey with your details to win a non-existent prize or ask you to verify your bank details by providing your bank card details.

Phishing messages/media are designed to look genuine & they often copy their format from the organisation they're pretending to represent i.e a fake website that looks like the real deal, but has a slightly different address. For example, if the legitimate site is 'www.realbank.co.uk', the scammer may use an address like 'www.reall-bank.org'.

HOW TO SPOT IT:

- The scam message doesn't contain your proper name & the message contains spelling & grammar errors, for example 'DeaR CuSt0m3r,.'
- The web address doesn't look like the address you usually used & the site is asking for details the legit site doesn't ask for.
- The message is unsolicited & contains an attachment.
- The senders email doesn't match the name of the company it claims to be from.

HOW TO PROTECT YOURSELF:

- Don't open/save attachments received from unknown senders. If you receive an attachment that you weren't expecting, contact the company to verify the contents or delete it.
- Turn on two-factor authentication – this extra security makes it harder for scammers to access your accounts & information. As a user you would provide 2 authentication factors to verify you are who you say you are before being able to access the account. Lots of banks and social media platforms have this in place to protect you from scammers.
- Secure sites can be identified by the use of 'https:' rather than 'http:' at the start of the internet address, or a closed padlock/unbroken key icon at the bottom right corner of your browser window.
- Never provide personal, credit card or account details if you receive a call. Instead, ask for their name and contact number & make an independent check with the organisation in question before calling back.

TAKE FIVE TO STOP FRAUD

Take Five, stop and think.

If you or someone you know is vulnerable and has been a victim of fraud call GMP on 101 or email GMP Economic Crime Unit at: ActionFraudEnq@GMP.police.uk

If you need to a report fraud or attempted fraud, you can do so by contacting Action Fraud at www.actionfraud.police.uk/report_fraud or by calling 0300 123 2040.

You can also read the latest Action Fraud alerts at www.actionfraud.police.uk/news or by following @actionfrauduk on Twitter.