NORTH WEST REGIONAL ORGANISED CRIME UNIT

Beware of online scams & fraud during the COVID-19 outbreak

Criminals are using the Covid-19 pandemic to scam the public **- don't become a victim.**

Law enforcement, government and private sectors partners are working together to encourage members of the public to be more vigilant against fraud, particularly about sharing their financial and personal information, as criminals seek to capitalise on the Covid-19 pandemic.

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment.

1. **STOP**: Taking a moment to stop and think before parting with your money or information could keep you safe.

2. **CHALLENGE**: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

3. **PROTECT**: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

4. Your bank or the police will **NEVER** ask you to transfer money or move it to a safe account.

Online Shopping Fraud

Seek advice: If you're purchasing goods and services from a company or person you don't know and trust, carry out some research first, and ask friends or family for advice before completing a purchase.

Scam messages: Be wary of unsolicited emails and texts offering questionably good deals, and **never** respond to messages that ask for your personal or financial details.

Payment Method: Avoid paying for goods and services by bank transfer as that offers you little protection if you become a victim of fraud. Instead, use a credit card or payment service such as PayPal.

If you have made a payment: *Inform your bank as soon as possible,* they can help you prevent any further losses. Monitor your bank statements regularly for unusual activity.

Computer Software Service Fraud

Installing software: Never install any software, or grant remote access to your computer, as a result of a cold call.

Financial Details: Genuine organisations would **never** contact you out of the blue to ask for financial details such as your PIN or full banking password.

Tech Support: If you need tech support, ask your friends or family for recommendations and look for reviews online first. Don't contact companies promoting tech support services via browser pop-ups.

If you have made a payment: *Inform your bank as soon as possible,* they can help you prevent any further losses. Monitor your bank statements regularly for unusual activity.

If you have granted remote access to your computer: Seek technical support to remove any unwanted software from your computer. Ask your friends or family for recommendations and look for reviews online first. Don't contact companies promoting tech support services via browser pop-ups.