Lancashire Constabulary are committed to keeping the residents of Lancashire up-to-date with the latest frauds that we see being reported to us on a daily basis. We hope that this article helps you avoid becoming a victim to one of them:

EMAIL SCAM

This particular scam email popped into my personal inbox one morning this week, informing me that there'd been a problem with my TV licensing direct debit and to click the link to access the details. It had the right logos, but being suspicious of everything that comes into my inbox, I forwarded it on to report@phishing.gov.uk.

Unfortunately, that same afternoon I had a conversation with a victim who had gone onto the link and had several accounts hacked. As well as the financial loss, victims suffer a great deal of stress and anxiety having to report it several times and generally dealing with the repercussions from it, which can be traumatic. If in doubt – don't!

AMAZON PRIME SCAM CALL

Thanks to COVID, most of us use Amazon at some point now. This scam call will come from an unrecognised number. When you answer, the fraudster will tell you that your Amazon Prime subscription is increasing in price or is about to expire.

If you say that you want to cancel your subscription, you'll be put through to another fraudster. They will tell you that you need to download remote access software (typically the app 'AnyDesk'). This is a genuine program that fraudsters sometimes look to exploit as a vehicle for their scams.

Once you've downloaded the program, you'll grant the scammer access to your device - allowing them to steal your personal information or install malware. Always say that you'll phone the organisation direct, who the criminal purports to be from and hang up. Wait for at least 5 minutes before making a call to ensure that the previous call has disconnected.

Saga has confirmed that a data breach has exposed some customers' addresses and partial bank card numbers. Watch out for emails asking you to update your payment details.

TOP 5 TELEPHONE SCAMS:

- Being called by so-called Microsoft Windows Support saying your computer has a virus and they need your passwords to fix it. **Don't ever give anyone your computer passwords.**
- Someone claiming to be from your bank or HMRC saying there's a problem with your account or tax bill and they need your security details. **A bank or HMRC will never ask for your details.** HMRC now have a fraud hotline **0800-788-887 8am-8pm 7 days, 365 days a year.**
- An offer of an unmissable bitcoin investment or the chance to access pension savings early. If it seems too good to be true – then it generally is! Always use bonafede investment organisations. If in doubt watch this video On the hunt for the businessmen behind a billion-dollar scam - BBC News
- Being told you have won a large prize and being asked to pay a processing fee or to call a premium rate line to claim your prize. **There is no prize ☹.**

BUYING NON-EXISTENT VEHICLES FROM ON-LINE MARKET PLACES

Even when you carry out due diligence it's difficult to be certain that you're buying a legitimate item from the supposed seller. So,

- When it comes to making online purchases from small, unknown retailers or via social media, it's important to fully research the company or seller. Can they prove that they own the vehicle?
- Check the company's website for spelling and grammatical errors. If you're encouraged to send money by bank transfer rather than paying by credit or debit card, this could be a sign of a scam.

- Keep an eye out for common tactics such as time-limited offers and above all, be on your guard against deals that suck you in. **STOP – THINK – CHECK!**

Please report all fraud to Action Fraud 0300 123 2040 or online actionfraud.police.uk.

You can make a non-urgent report to Lancashire Police by calling us on 101 or online at https://doitonline.lancashire.police.uk.

Follow us on Twitter for all the latest posts @LancsFraudCyber

Stay safe.

Best wishes,
The Fraud Triage Team