Be Fraud Smart!
essex.police.uk/befraudsmart
ESSEX POLICE
Protecting and serving Essex

Essex Police Fraud Alert System

15

13th November 2020

ACTION FRAUD WARNS OF RISE IN INVESTMENT FRAUD AS NATION ENTERS SECOND LOCKDOWN

Action Fraud is informing the public of how to protect themselves from investment fraud, after reports spiked following the first national lockdown caused by the coronavirus outbreak.

Pauline Smith, Head of Action Fraud, said:

"The coronavirus outbreak sadly led to many people losing their job or having to manage with a lower income than they were used to. It has also caused a shake up in the economy in general, with interest rates falling, in a similar way to the financial crisis of 2008. All of these factors provide criminals with the opportunity to attract more people with their fraudulent investment schemes."

How to protect yourself from investment fraud:

- **Be suspicious** if you are contacted out the blue about an investment opportunity. This could be via a cold-call, an e-mail or an approach on social media.
- **Don't be rushed** into making an investment. No legitimate organisation will pressure you into making a transaction, or committing to something on the spot. Take time to do your research.
- **Seek advice** from trusted friends, family members or independent professional advice services before making a significant financial decision. Even genuine investment schemes can be high risk.
- **Use a financial advisor** accredited by the Financial Conduct Authority. Paying for professional advice may seem like an unnecessary expense, but it will help prevent you from being scammed.
- **Use the Financial Conduct Authority's register** to check if a company is regulated. If you deal with a firm or individual that isn't regulated, you may not be able to get your money back if something goes wrong and its more likely to be a scam.

Just because a company has a glossy website and glowing reviews from 'high net worth' investors does not mean it is genuine – fraudsters will go to great lengths to convince you they are not a scam.

Remember, if something sounds too good to be true, it probably is.

If you or someone you know is vulnerable and has been a victim of fraud, please call **Essex Police** on **101**
Report fraud or attempted fraud by contacting **Action Fraud** at **actionfraud.police.uk** or call **0300 123 2040**

Keep up to date with fraud and do *even more* Online at essex.police.uk

CALL ESSEX POLICE 101
IN AN EMERGENCY ALWAYS CALL 999

FAKE PAYPAL EMAILS LEAD TO NEARLY £8 MILLION IN LOSSES

Action Fraud is warning people selling items online to be on the lookout for criminals sending fake PayPal emails. Between January and September this year, Action Fraud received over 20,000 reports of fake PayPal emails, resulting in losses of nearly £8 million.

Criminals have been targeting people selling items online, by sending them emails purporting to be from PayPal. The emails trick victims into believing they have received payment for the items they're selling on the platform.

Typically, after receiving these emails, victims will then send the item to the criminal. This leaves them at a further disadvantage having not received any payment for the item and also no longer being in possession of it—for example, one fake email from PayPal claimed the buyer had accidently paid for the item twice. The buyer then asked the seller to wire the overpayment to a bank account in a different country.

If you think you've received a fake email, PayPal offer the following advice:

1. **Log into PayPal:** If you receive a suspicious email, don't act on the message or click on any links. Instead, open your browser, log into PayPal and check for any new activity. PayPal will also email or notify you in the app if you've received any payments.
2. **Check the basics:** Look out for misspellings and grammatical errors, which can be a tell-tale sign of a scam.
3. **Verify an email's authenticity:** Phishing scams will often mimic the look and feel of PayPal emails, and ask you for sensitive information – something that real PayPal emails will never do.
4. **How to spot the difference:** A PayPal email will address you by your first and last name, or your business name, and we will never ask you for your full password, bank account, or credit card details in a message.
5. **Avoid following links:** If you receive an email you think is suspicious, do not click on any links or download any attachments. You can check where a link is going before you click on it by hovering over it – does it look legitimate?
6. **Keep tabs on your information:** Limit the number of places where you store your payment information online by using a secure digital wallet like PayPal. If you are making a purchase online, consider using a protected payment method such as PayPal, so if your purchase doesn't arrive or match the product description, PayPal can reimburse you.
7. **Easiest of all, use common sense:** If a deal seems too good to be true, it probably is! Stay clear of exceptional deals or anything that is significantly reduced in price from what you would expect to pay.

You can forward suspicious emails to **spoof@paypal.com**, without changing the subject line. PayPal will let you know whether it is fraudulent.