Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Friday 29th May 2020

Today's topic is 'Investment Scams'.

The first recorded financial fraud in 300 BC, was Hegestratos who insured his ship's cargo, then sold it and planned to sink the empty vessel, claiming the money for the 'lost' cargo. In today's world, modern fraudsters such as Bernie Madoff, Jordan Belfort (the Wolf of Wall Street) and the 'Missing Crypto Queen' Dr Ruja Ignatova, ply their trade, swindling the unwary.

The current economic climate has seen the Bank of England drop base rates to historic lows, meaning savings pay less interest. People facing an uncertain financial future are looking for ways to bolster their finances and may turn to online investment opportunities to supplement their income. Online investors need to be aware of the potential dangers.

Fake investment websites: A well-crafted website can be difficult to distinguish from a legitimate one. Many are well formatted and sophisticated, containing convincing pitches for unique investment opportunities. These sites encourage visitors to leave contact details, in order to receive glossy investment brochures or a telephone appointment with a financial advisor. Whilst these processes appear genuine, they are designed to steal your identity and money.

Unsolicited emails: Fraudsters will offer money making opportunities such as shares, bonds, property investments, online trading, binary options, and cryptocurrency investments all offering great returns.

Investment cold callers: They usually contact victims out of the blue, sounding like a professional stockbroker and offering investment opportunities that seem too good to be true. Fraudsters may 'spoof' a phone number to convince a target they are from a legitimate investment or pension company. They promise free research reports, special discounts and 'secret' stock tips. In reality, they are cold calling as many people as possible, persuading them to invest, using hard-sell techniques, scare tactics and emotional manipulation.
The fraudsters try to pressure victims into making rushed decisions to part with sensitive data or money. Once the fraudsters have squeezed whatever money they can from investors, they quickly disappear.

Top tips for staying safe:

- **Check for FCA authorisation:** If a UK firm or individual does not appear on the Financial Services Register, it could be a scam, always check.
- **Real or fake:** Make sure it is the genuine firm by calling the switchboard number, listed on the FCA Register. Scammers can pretend to be any company.
- **Telephone Preference Service (TPS):** Register with the TPS to prevent unwanted sales calls.
- **Reject unexpected offers:** If you're contacted out of the blue about an investment opportunity, chances are it's a high-risk investment or a scam. The safest thing to do is to hang up and/or ignore unexpected offers by email or text.

- **Links**: If you receive a suspicious email or text message, never click on links or download attachments.
- **Guard your digital footprint**: Check online privacy settings for accounts created. Use the 'contact us' part of any web page to remove personal data. Under GDPR guidelines, you have the right to be 'forgotten'.

Hot topic

Bitcoin investment: Emails are advertising investments in Bitcoin platforms to 'take advantage of the financial downturn' and help people recover from bankruptcy. A link in the email claims to take recipients to a website, explaining how Bitcoin trading platforms work. This link will steal credentials and/or get the recipient to download a virus.

A phishing email, claiming to be from a researcher at A-Z Pharmaceuticals – a company in the UK - is asking recipients to invest money/sponsor/donate as a result of the outbreak. The money is purported to be for the manufacture of cancer treatments, related medication, and an animal vaccine and claims the recipient will have a major share in the profits.

Email purporting to be from Amazon, is asking customers whether they would like to apply to the Amazon Grant relief fund, to receive up to £1,000. They claim this fund is administered by the Emergency Assistance Foundation Inc. and is targeting individuals self-isolating due to COVID-19. The recipient is asked to click on a link if they wish to apply, this link has been checked and the results confirm it is designed to steal credentials.

Cyber criminals are now concentrating their efforts on disrupting healthcare entities, pharmaceuticals, local governments, medical researchers and academics and their supply chains. COVID-19 intellectual property could be of great value to cyber criminals.

Reporting

Reporting to Action Fraud can be done online or by calling 0300 123 2040.
To report offers of financial assistance from HMRC, contact phishing@hmrc.gov.uk.

This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.