

Facebook Fraud Posts 2020

4th February 2020

[#TakeFive](#) 🙌 to learn some fraud facts:

Criminals do not always work alone. They can operate in larger groups working together to strategically target you over a period of time.

<https://www.facebook.com/clevelandpolice/posts/10157715601541855>

11th February 2020

Man Charged with Fraud by False Representation

Officers from Middlesbrough CID have charged a man, 47, with fraud by false representation and he will be appearing at Teesside Magistrates Court today, Tuesday 11th February.

The charge was made after the man allegedly took money off an elderly couple after reportedly claiming to carry out maintenance work at their house in the Brookfield area of Acklam, Middlesbrough.

Anyone with information regarding this incident is asked to contact Cleveland Police on the non-emergency number 101, quoting event number 005664.

For more information regarding cold callers and bogus callers, please visit:

<https://www.cleveland.police.uk/.../fa/fraud/personal-fraud/>

<https://www.facebook.com/clevelandpolice/posts/10157735401191855>

18th February 2020

Romance Fraud Victim Thanks Detective

A detective who worked tirelessly to get a victim's money back after she was defrauded of her life savings has received a heartfelt thank you.

The retired lady from Middlesbrough, was targeted by the fraudster on a dating website and sent him a large sum of money - supposedly to invest in his business.

They kept in contact and, making her believe they were in a relationship, he later persuaded her to send tens of thousands of pounds to be released after claiming he'd been detained and imprisoned in the Middle East while travelling.

She also sent him £1,500 after he appealed to her kind nature, saying it would go to an overseas orphanage project.

Acting Detective Inspector Andy King from Cleveland's Economic Crime Unit came across the fraud investigation last October when reviewing and revisiting local high value cases in an Action Fraud report.

Colleague Detective Constable Rachel Graham said their first objective should be to try to get the victim's money back and she began inquiries, working with other agencies and the victim's bank.

DC Graham referred the lady to Action Fraud which can undertake international fraud investigations and she kept in touch with the victim and her bank locally, offering on-going support and the benefit of her professional expertise and experience.

When the woman finally received a large proportion of her money back last week she contacted DC Graham saying she had "worked a miracle" and was "privileged to have such a wonderful woman on her side taking care of her throughout this whole nightmare."

Inquiries to trace the fraudster are on-going and in the meantime Acting Detective Inspector King paid tribute to DC Graham, saying : "Once again DC Graham has gone above and beyond to support a victim and to contribute to the best possible outcome in this on-going inquiry.

"I would use this case to remind the public that sadly people online are not always who they say they are and alarm bells should ring if someone consistently asks for money - often increasing sums of money. There are fraudsters out there who will take advantage of others' kind and trusting nature and we see time and time again people relieved of huge amounts of cash - which can be extremely difficult to retrieve. We will continue to work with other forces and specialist agencies to locate and arrest the suspect in this case.

"Happily in this case the victim did get a lot of her money back and it was very kind of her to recognise DC Graham's hard work."

Acting Det Insp King gave the following advice on protecting yourself from romance fraud:

- Avoid giving away too many personal details when dating online. Revealing your full name, date of birth and home address may lead to your identity being stolen.
- Never send or receive money or give away your bank details to someone you've only met online, no matter how much you trust them or believe their story.
- Pick a reputable dating website and use the site's messaging service. Fraudsters want to quickly switch to social media or texting so there's no evidence of them asking you for money.

Spot the signs

- You've struck up a relationship with someone online; they're asking a lot of personal questions about you, but they're not interested in telling you much about themselves.
- They invent a reason to ask for your help, using the emotional attachment you've built with them. Your relationship with them may often depend on you sending money.
- Their pictures are too perfect – they may have been stolen from an actor or model. Reverse image search can find photos that have been taken from somewhere else.

<https://www.facebook.com/clevelandpolice/posts/10157756503766855>

(Share) 10th March 2020

See below on behalf of Take Five

...Did you know - in the first half of 2019 a total of £616 million was lost through authorised and unauthorised fraud? Take Five

Did you know that in the first half of 2019 a total of £616 million was lost through authorised and unauthorised fraud?

With criminals becoming increasingly sophisticated, we think it's important that you [#TakeFiveandTellFive](#).

The campaign aims to prevent people from losing money to fraud and scams, like this delivery scam.

Tag someone below who you would like to encourage to take our Take Five Quiz:

<https://quiz.takefive-stopfraud.org.uk/>

<https://www.facebook.com/clevelandpolice/posts/10157816844776855>

16th March 2020

Fraud Prevention Tips in Relation to National Reports of Coronavirus Fraud

City of London Police, the national lead for fraud, have released some figures in relation to fraud linked to coronavirus.

Over £800k has been scammed from victims nationally so far. Ten of the 21 reports were made by victims that attempted to purchase protective face masks from fraudulent sellers.

Fraudsters have also claimed to be from research organisations via email who claim to be able to provide the recipient with a list of coronavirus infected people in their area. To access this information it requires the victim to click on a link, which leads to a malicious website, or they are asked to make a payment in bitcoin to view the list.

Cleveland Police's Economic Crime Detective Inspector, Jim Forster said: "Although we have had no reports of fraud in relation to coronavirus in the Cleveland area, the figures are expected to rise nationally, and the Force would like to take this opportunity to warn people regarding fraud.

"Unfortunately fraudsters take advantage in situations like this and target vulnerable people. We would strongly advise people to follow the below steps which may help to prevent you from becoming a victim of fraudulent crime."

- Watch out for scam messages – do not click on links or attachments from suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details.
- Shopping online – be cautious when shopping online, purchase items from reputable websites or carry out some research first. Ask for advice from a family member or friend if you haven't bought from a particular website before. If you decide to make a purchase, use a credit card, as most major credit card providers insure online purchases.
- Keep software and app updates up to date to protect your devices such as laptops and phones from the latest threats.
- Door to door fraud – Potential fraudsters may knock on your door by offering to help people who are self-isolating by offering to do their shopping. Never hand over your money or bank cards to people you do not know or trust. If someone knocks at your front door claiming to be from a company, first check their ID. If you're not happy, don't let them in. Never call the phone number on their ID card to check them out. Ask the salesperson to

wait outside, shut the door and find the company number on the internet. If they're genuine, they'll understand.

More advice and information can be found on our website:

<https://www.cleveland.police.uk/.../advice-and.../fa/fraud/>

Information regarding coronavirus can be found on the Public Health England website:

<https://www.gov.uk/.../coronavirus-covid-19-list-of-guidance>

<https://www.facebook.com/clevelandpolice/posts/10157834433181855>

23rd March 2020

Please see below on behalf of Action Fraud

Coronavirus-related fraud reports increase by 400% in March

Recently the National Fraud Intelligence Bureau (NFIB) reported a new trend in fraud related to Coronavirus, or COVID-19.

Updated figures show there have been 105 reports to Action Fraud since 1 February 2020, with total losses reaching nearly £970,000.

The first report relating to Coronavirus, or COVID-19, was received on 9 February. There were 20 more reports that month. Since then, there have been 46 reports between the 1 March and 13 March, and 38 reports in just four days (14 March – 18 March).

What scams are we seeing?

The majority of reports are related to online shopping scams where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived.

Other frauds being reported include ticket fraud, romance fraud, charity fraud and lender loan fraud.

Phishing emails

We have also received over 200 reports of coronavirus-themed phishing emails. These attempt to trick people into opening malicious attachments which could lead to fraudsters stealing people's personal information, email logins and passwords, and banking details.

Some of the tactics being used in phishing emails include:

- Fraudsters purporting to be from a research group that mimic the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO). They claim to provide the victim with a list of active infections in their area but to access this information the victim needs to either: click on a link which redirects them to a credential-stealing page; or make a donation of support in the form of a payment into a Bitcoin account.
- Fraudsters providing articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates.

- Fraudsters sending investment scheme and trading advice encouraging people to take advantage of the coronavirus downturn.
- Fraudsters purporting to be from HMRC offering a tax refund and directing victims to a fake website to harvest their personal and financial details. The emails often display the HMRC logo making it look reasonably genuine and convincing.

Superintendent Sanjay Andersen, Head of the National Fraud Intelligence Bureau, said:

“Fraudsters will use any opportunity they can to take money from innocent people. This includes exploiting tragedies and global emergencies.

“The majority of scams we are seeing relate to the online sale of protective items, and items that are in short supply across the country, due to the COVID-19 outbreak. We’re advising people not to panic and to think about the purchase they are making. When you’re online shopping it’s important to do your research and look at reviews of the site you are buying from.”

Graeme Biggar, Director General of the National Economic Crime Centre, said:

“We have already seen fraudsters using the COVID-19 pandemic to scam people looking to buy medical supplies online, sending emails offering fake medical support and targeting people who may be vulnerable or increasingly isolated at home.

“These frauds try to lure you in with offers that look too good to be true, such as high return investments and ‘healthcare opportunities’, or appeals for you to support those who are ill or bogus charities.

“The advice is simple, think very carefully before you hand over your money, and don’t give out your personal details unless you are sure who you are dealing with.

“We are working together across law enforcement, government and the private sector to combat this criminal activity and protect the public. If you think you have been a victim please report to Action Fraud.”

Protect yourself

1) Watch out for scam messages

Don’t click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details.

2) Shopping online:

If you’re making a purchase from a company or person you don’t know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases.

For more information on how to shop online safely, please visit:

<https://www.actionfraud.police.uk/shoponlinesafely>

3) Protect your devices from the latest threats:

Always install the latest software and app updates to protect your devices from the latest threats.

For information on how to update your devices, please visit:

<https://www.ncsc.gov.uk/guidance/securing-your-devices>

For the latest health information and advice about COVID-19 please visit the NHS website.

<https://www.facebook.com/clevelandpolice/posts/10157859590141855>

30th March 2020

Received a suspicious email or text about your bank account or finances? This could be a [#COVID19](#) related scam. Take a look at the Action Fraud

Website at <https://bit.ly/33VI4ON> advice and information on a number of scams you could receive. Cyber Protect UK

<https://www.facebook.com/clevelandpolice/posts/10157886551371855>

(Share) 1st April 2020

! Cyber Crime Warning !

Are you and your team keeping in touch while working from home using @Zoom? Please be aware, cyber criminals are found to be targeting this platform by creating fake websites and posing as the official site.

Please be careful when using this app. If you are affected by fraud or cyber crime, please report to Action Fraud immediately.

<https://www.facebook.com/clevelandpolice/posts/10157892970401855>

6th April 2020

* Cyber Crime Warning Regarding HP laptops *

Do you have a HP laptop purchased in or anytime after October 2012? Your laptop could be at risk due to vulnerabilities in the HP Support Assistant.

Please read the information below from our colleagues at NERSOU. Report any cyber crime or fraud to Action Fraud.

<https://www.facebook.com/clevelandpolice/posts/10157911126761855>

7th April 2020

See below on behalf of Action Fraud.

The police would never send someone to your home to collect money, or ask you to transfer funds out of your account. [#CourierFraud](#)

The police will never send someone to your home to collect money, or ask you to transfer funds out of your account. Don't make life easy for criminals. [#CourierFraud](#)

<https://www.facebook.com/clevelandpolice/posts/10157914165791855>

9th April 2020

Warning from Cleveland Police Cyber Crime team:

Have you received the below email regarding TV license direct debits? Our Cyber Crime team have identified this as a scam.

If you received this email, do not open any links, reply to the sender or provide any personal information.

If you have been affected by fraud or a scam, please report it to Action Fraud.

<https://www.facebook.com/clevelandpolice/posts/10157921358916855>

16th April 2020

Have you received any unexpected emails from Tesco recently? This could be a coronavirus scam. See the below advice from Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10157945994641855>

22nd April 2020

Do you or someone you know have a Nintendo account? Some Nintendo customers have reported their accounts being hacked to our partners at NERSOU.

Please see advice below. Remember, if you are a victim of fraud or cyber crime, please report to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/1015796888361855>

14th May 2020

Have you received any suspicious emails lately?

See below on how to report: Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158048220401855>

15th May 2020

Be aware of fraudulent emails advertising Bitcoin cryptocurrency. Report any suspicious emails to Action Fraud. See below from NERSOU: (image).

<https://www.facebook.com/clevelandpolice/posts/10158051604821855>

28th May 2020

See information below from our colleagues at NERSOU regarding a malicious Android package file disguised as a Covid-19 symptom tracking app.

If you have been a victim of fraud or cyber crime, report it to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158091184616855>

3rd June 2020

Have you received any suspicious emails lately? See information below from Action Fraud on how to report (image).

<https://www.facebook.com/clevelandpolice/posts/10158109111771855>

5th June 2020

***** Economic Crime Unit Recovers over £60,000 Stolen in Mandate Fraud *****

A Cleveland Police investigation has resulted in more than £60,000 being returned to a victim of fraud.

It was reported to Cleveland Police, via Action Fraud, that a business outside of the UK had mistakenly sent more than £62,000 to purchase goods from a UK-based company.

A fraudster was able to trick the business into thinking that they were dealing with the genuine company when they were not, known as mandate fraud.

Mandate fraud is when someone gets you to change a direct debit, standing order or bank transfer mandate, by purporting to be an organisation you make regular payments to, for example a subscription or membership organisation or your business supplier.

Enquires carried out by the Economic Crime Unit led to over £60,000 being located in a bank account. At this time the bank did not know who the money belonged to, but police enquiries were able to trace the money back to the victim and this money will now be transferred back to the victims' business.

Detective Sergeant Andrew King, from Cleveland Police Economic Crime Unit, said: "This is a great result for the victim, who will hopefully now be able to recover financially from the initial loss. Enquiries are ongoing to trace those responsible and bring them to justice. Our detectives' actions have helped return financial security to this business and help them move forward.

"We would like to offer some simple crime prevention advice which could help prevent people and local businesses from becoming victims of crime. Always remember, check it twice or you could be paying the price."

Cleveland Police Economic Crime Unit have offered some crime prevention advice which could help prevent others, and businesses, become victims of mandate fraud. Please see below crime prevention advice:

- Step one: The most important thing you can do is to verify all invoices, emails and requests to change payment arrangements. You can do that by calling the supplier directly using established contact details you have on file.
- Step two: You should also be mindful of how you manage access to sensitive information. Are financial documents only accessible to those employees that require access? Are you mentioning the names of your suppliers in your social media feeds? Fraudsters can use those details to create highly personalised scams.
- Step three: Finally, you should check your bank transactions regularly. If you notice anything suspicious, you should notify your bank immediately.

If you have been a victim of fraud or cyber crime, report it to Action Fraud at www.actionfraud.police.uk

<https://www.facebook.com/clevelandpolice/posts/10158116219371855>

8th June 2020

See information from our colleagues at NERSOU regarding suspicious malware on apps uploaded to the Google Play Store.

If you have been a victim of fraud or cyber crime, report it to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158125152311855>

9th June 2020

See information from NERSOU below regarding an active phishing campaign posing as Amazon. If you have been a victim of fraud or cyber crime, report it to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158128521416855>

(Share) 16th June 2020

See below from Action Fraud regarding criminals targeting snapchat users ... ⚠️ ALERT: Criminals target Snapchat users in extortion scam that threatens to reveal their private photos.

We've had over 300 reports since January. If you've been a victim of an extortion scam, report it to your local police force.

<https://www.facebook.com/clevelandpolice/posts/10158148828336855>

24th June 2020

See important information from colleagues at NERSOU regarding NHS Test & Trace service.
If you receive a fake call, report it to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158173178001855>

24th June 2020

See information below regarding a phishing attack impersonating a LinkedIn notification.
If you have been a victim of fraud or cyber crime, report it to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158173836976855>

29th June 2020

See advice below from NERSOU regarding password security.
If you have been a victim of fraud or cyber crime, report it to Action Fraud

<https://www.facebook.com/clevelandpolice/posts/10158188554826855>

9th July 2020

See information below from NERSOU regarding a Twitter security phishing campaign.
If you have been a victim of fraud or cyber crime, please report to Action Fraud.

<https://www.facebook.com/clevelandpolice/posts/10158220296731855>

10th July 2020

See information below from colleagues at NERSOU regarding Bitcoin investment fraud...
(image).

<https://www.facebook.com/clevelandpolice/posts/1015822233576855>

21st July 2020

See information below on behalf of NERSOU regarding a Facebook scam identifying as Tesco.

If you have been a victim of fraud or cyber crime, contact Action Fraud (image)

<https://www.facebook.com/clevelandpolice/posts/10158252489461855>

27th July 2020

***** Victim of Fraud is Compensated his Life Savings Back Thanks to Partnership Approach to Tackling Fraudulent Crime *****

In 2018, Cleveland Police received a report from Action Fraud regarding a man who had become victim to a Bitcoin scam and had lost his life savings amounting to thousands of pounds.

Thanks to a partnership approach involving Cleveland Police, Victim Care and Advice Service (funded by Police and Crime Commissioner Barry Copping) and the Financial Ombudsman Service, the victim who is in his 70s and is a retired police officer from another Force was compensated 99% of his life savings after two years of enquiries.

Acting Detective Inspector Andy King from the Economic Crime Unit at Cleveland Police said: "This scam was sophisticated and as soon as I read the report, I knew the victim was extremely vulnerable. I visited the victim's home address with Victim Care Officer, Lottie Dixon from VCAS, and it was clear from our visit that his whole world had fallen apart after becoming a victim to this scam so it was really important that we did everything possible to help them.

"Without the dedication from the VCAS team we would not have achieved this result. Lottie is an exceptional member of staff who worked with and supported the victim throughout this whole process, and helped him get his money back after successfully applying for compensation through the Financial Ombudsman Service Scheme."

Speaking of the compensation, the victim said: "I really need to mention the input by Lottie from VCAS into this whole nightmare situation which I am now convinced could happen to anyone.

"I fell for this scheme hook line and sinker, which left me in a depressive state of mind that was hard to accept and live with.

"Lottie gave me the strength to carry on, that no one could say the words that give me comfort in the desperation of being scammed, and somehow she was the light at the end of a tunnel that I worked towards.

"A year passed and I got in contact with the Financial Ombudsman Service, who took over the complaint and registered my official claim for compensation.

"Three weeks ago I was informed that they the FOS upheld my claim and I would be fully compensated for my loss. If it were not for the dedication and sheer persistence by Lottie. I would have given up but she gave me the belief I could come out of this situation with a positive result. Thank you so much Lottie."

Victim Care Officer, Lottie Dixon, added: "It was heart breaking to see the devastating effect this fraud had on the victim, having worked hard all of his life for his savings, to lose them in such a short amount of time with little hope of getting them back.

"Whilst supporting the victim to cope and recover with the impact of the crime, we invited him to speak at our Friends Against Scams presentations about his experience and to help educate people on how easy it can be for anyone to fall victim.

"In doing this he was able to use this negative experience to help others in a positive way. For him to now have been successful in getting this money back is an absolutely amazing result, and I'm delighted for him."

Police and Crime Commissioner Barry Copping who funds VCAS said: "This case demonstrates the power of fantastic victim support, which persists long after the individual

first contacts the police. I met this victim at a number of fraud prevention events and I know the devastating impact the crime had on his life.

“Lottie’s dedication is a shining example of the work VCAS do every day to go the extra mile for vulnerable people and I’m incredibly proud to commission the service.

“It can be rare for victims of serious fraud to recoup their losses in this way and it’s thanks to Lottie that the gentleman involved in this case can put this challenging time behind him and look forward to a more positive future.”

<https://www.facebook.com/clevelandpolice/posts/10158269000566855>

28th July 2020

See information from colleagues at NERSOU regarding a new coronavirus-related phishing scam promising a government-funded tax cut.

Follow the Take Five campaign if asked for your money or information. Report any fraud or cyber crime to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158271890766855>

25th August 2020

See below on behalf of Action Fraud in relation to fake tax refund emails ...

⚠️ Watch out for fake tax refund emails. We’ve had over 150 reports about them within 24 hours.

Forward suspicious emails claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599.

<https://www.facebook.com/clevelandpolice/posts/10158340601861855>

4th September 2020

Help us spread the word about phishing scams this [#nationalfishandchipday](#).


Know someone that’s had their personal information phished? 🐼 Ask them to notify their bank and report it to Action Fraud: www.actionfraud.police.uk [#MulletOver](#)

<https://www.facebook.com/clevelandpolice/posts/10158348308066855>

17th September 2020

! Cyber Crime Warning

See information below from colleagues at NERSOU regarding a spyware which is functioning on third-party app store as 'TikTokPro'.

 If you have been affected by this, please report to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158396067251855>

1st October 2020

 Cyber Crime Warning...

A new phishing campaign has been found to be impersonating a KnowBe4 phishing awareness course via email.

If you have received this email, avoid clicking any links or opening any attachments. Report it to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158429160241855>

8th October 2020

Fall for the person, not the profile – public reminded stay safe online as reports of romance fraud rise 26% in a year

Police forces across the country are working together with partners, including Match Group, to tackle romance fraud, with a combination of awareness raising and enforcement activity, co-ordinated by the City of London Police (CoLP).

The multi-agency campaign, running throughout October, aims to raise awareness of romance fraud and provide clear and unambiguous protection advice to the public, following a 26 percent rise in reports to Action Fraud in the last year.

Romance fraud, or dating fraud, occurs when you think you've met the perfect partner online but they are using a fake profile to form a relationship with you. They gain your trust over a number of weeks or months and have you believe you are in a loving and caring relationship. However, the criminal's end goal is only ever to get your money or personal information.

Between August 2019 and August 2020, Action Fraud received over 400 reports a month from victims of romance fraud in the UK. Losses reported by victims during this time totalled £66,335,239, equating to an average loss per victim of just over £10,000.

During June, July and August 2020, Action Fraud received more than 600 reports per month of romance fraud, indicating people may have met, and begun talking to, romance fraudsters during the national lockdown caused by the coronavirus outbreak.

The top five platforms where victims reported first interacting with the criminal committing romance fraud were Facebook, Plenty of Fish, Instagram, Tinder and [Match.com](#).

As part of the campaign the Match Group, who own OK Cupid, Plenty of Fish, Tinder and [Match.com](#), are running romance fraud protection adverts throughout October on these platforms, to inform their users how to spot the signs of a romance fraud and how to protect themselves online.

Cleveland Polices Economic Crime Inspector Jim Forster said: "Since 1st October 2019 to now, Cleveland Police has received five reports of online dating scams/ fraud.

"Three of the victims were elderly and two were aged in their 30s. Each of the victims were scammed out of money, ranging from £50 to over £100k.

“Romance fraud is a devastating crime that can leave victims feeling heartbroken for a person they believed they had grown close to and embarrassed to tell people about what happened. Financially, some people have also been left with a huge loss.

“As a Force we fully support this campaign so that as many people as possible become aware of how easy it is to be targeted and how sophisticated this level of crime can be.

“Some people aren’t always as they seem and there will be individuals out there who will play on people’s emotions and vulnerabilities and will target them for money. It is vital that the public are aware of the warning signs (detailed below) to help prevent more people from becoming a potential victim.”

- Avoid giving away too many personal details when dating online. Revealing your full name, date of birth and home address may lead to your identity being stolen.
- Never send or receive money or give away your bank details to someone you’ve only met online, no matter how much you trust them or believe their story.
- Pick a reputable dating website and use the site’s messaging service. Fraudsters want to quickly switch to social media or texting so there’s no evidence of them asking you for money.

Spot the signs

- You’ve struck up a relationship with someone online; they’re asking a lot of personal questions about you, but they’re not interested in telling you much about themselves.
- They invent a reason to ask for your help, using the emotional attachment you’ve built with them. Your relationship with them may often depend on you sending money.
- Their pictures are too perfect – they may have been stolen from an actor or model.

Reverse image search can find photos that have been taken from somewhere else.

<https://www.facebook.com/clevelandpolice/posts/10158445330481855>

9th October 2020

Colleagues at NERSOU are raising awareness to vulnerabilities in Android security.

See information below regarding products affected.

If you have been a victim of cyber crime or fraud, report it to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158447919136855>

14th October 2020

On the final day of Prime Day, colleagues at NERSOU are warning of an Amazon-themed phishing campaign.

The phishing campaign impersonates Amazon with "returns" and "order cancellations" in relation to Prime Day.

If you have been impacted by this, please report to Action Fraud (image).

<https://www.facebook.com/clevelandpolice/posts/10158459766621855>

27th October 2020

Fall for the person, not the profile – public reminded stay safe online as reports of romance fraud rise 26% in a year.

Cleveland Police is supporting a national romance fraud campaign to remind & show people how to stay safe online from scammers.

Police forces across the country are working together with partners, including Match Group, to tackle romance fraud, with a combination of awareness raising and enforcement activity, co-ordinated by the City of London Police (CoLP).

Read what our Economic Crime Insp Jim Forster has to say about the figures here:

<https://rb.gy/nle9qx>

Action Fraud

#lovenotlies

<https://www.facebook.com/clevelandpolice/posts/10158489077066855>

9th November 2020

See below from Action Fraud regarding PayPal scams ...

!! We are warning people selling items online to be on the lookout for criminals sending FAKE PayPal emails.

For more information on how to protect yourself:

<https://www.actionfraud.police.uk/.../fake-paypal-emails...>

<https://www.facebook.com/clevelandpolice/posts/10158520158421855>

9th November 2020

Action Fraud warns of rise in investment fraud reports

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

Between September 2019 and September 2020, Action Fraud received just over 17,000 reports of investment fraud, amounting to £657.4m in reported losses. However, reports spiked in May, June, July, August and September 2020 as the nation adjusted to life after lockdown.

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.

“Preying on people when they are at their most vulnerable really shows how low these criminals will stoop to make a profit for themselves. That is why we are working hard with our law enforcement colleagues, and partners in the finance industry, to tackle investment fraud and empower the public to spot a scam.”

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 think you've been a victim of an investment fraud, report it to Action Fraud online at www.actionfraud.police.uk or by calling 0300 123 2040. For more information about investment fraud, visit www.fca.org.uk/scamsmart.

<https://www.facebook.com/clevelandpolice/posts/10158519841366855>

18th November 2020

RE-APPEAL: WARNING OF COURIER FRAUD

As we repeat our warning about courier fraud, a detective from our Organised Crime Unit has spoken on

[BBC Radio Tees](#)

today.

You can hear the interview at around 2 hours 15 minutes on the link below.

<https://tinyurl.com/y4336gf9>

We are reminding people to please be aware of "courier fraud" and alert any friends and family, especially if elderly and vulnerable.

Nationally and locally, vulnerable elderly people have been targeted for money by phone.

Victims are usually contacted by someone who is impersonating a police officer, telling them they've been victim of a fraud and that an investigation's ongoing.

The caller then asks for personal details and cash withdrawals, claiming they will return the money once the investigation is over.

Officers are urging people to never provide any personal details or financial information to anyone they do not know and reminding them that police and bank officials would never ask anyone to withdraw money.

If in doubt hang up, however credible the call may seem.

If you believe you've been victim of courier fraud, please report to Cleveland Police via the 101 number quoting Ref 187803

<https://www.facebook.com/clevelandpolice/posts/10158540850636855>

20th November 2020

Warning - Computer Service Fraud

We are seeing a rise in computer service fraud in the Cleveland area, this is where a scammer takes over your computer remotely.

The most common way for this to happen is a phone call from what you believe is a legitimate company such as Microsoft or Virgin Media, advising there is a problem with your computer or broadband and could you open the file they have sent so they can fix the problem.

The file contains a Remote Access Trojan, which allows them to take control of your computer, you may see them going into files and making code appear on your screen looking very official. They may then charge you a fee for their service.

Now the RAT is on your computer they can then access it again whenever they choose to, giving them plenty of time to go through your personal files, access stored passwords or gain entry to accounts you hold.

Keep yourself safe by not responding to unsolicited calls or emails, if you get a call asking you to do anything to your computer, hang up, wait a few minutes to ensure the line is not still connected and ring the company direct on a number you know to check if it was them. Never click on unknown links on emails or texts and keep your antiviral software up to date and run regular scans.

<https://www.facebook.com/clevelandpolice/posts/10158544945706855>

4th December 2020

Confirmation of Payee is a new way of checking account details to give customers greater assurance that they're sending payments to the intended recipient; another measure to help combat fraud and scams.

When a customer sets up a new payee or amends an existing payee's details, banks that use the system will check if the name supplied matches the account details entered.

If you've been urged to proceed with a payment where the details don't match, **#Stop** – don't feel pressured to continue.

#TakeFive to contact organisations directly using details that you know to be genuine in order to confirm any requests.

#Protect If you think you've fallen for a scam, contact your bank immediately on a number you know to be correct, such as the one on the back of your debit or credit card and report it to Action Fraud: <https://www.actionfraud.police.uk/>

<https://www.facebook.com/clevelandpolice/posts/10158576799191855>

8th December 2020

URGENT! Please speak to older friends and relatives about courier fraud

Last month we issued a number of warnings about courier fraud, where people are targeted by callers claiming to be from "the police", "the fraud squad" or their bank, asking them to withdraw large sums of money which a courier will then collect.

Sometimes they ask people to do bank transfers of large sums of money.

The very convincing cold callers often phone several times a day and manage to convince people they need to co-operate, telling them they've been affected by fraud and are therefore part of an on-going investigation. They even give them a "crime number" to make it seem even more realistic

We're sorry to say we've had several further reports of people in our area being targeted by these highly organised criminals and we'd urge everyone to remind their older or more vulnerable friends and relatives that police or your bank would never phone you asking you to withdraw money.

Anyone who receives a phone call from someone claiming to be police or a bank and asking about money should hang up immediately and inform a trusted friend or relative.

Cleveland Police is working with forces and financial institutions nationally, as well as the National Crime Agency and NERSOU (the North East Regional Special Operations Unit) to counter this activity.

After recent appeals and further investigation by Cleveland detectives, two men (age 22 and 24) were recently arrested in London by our NERSOU colleagues

They were questioned on suspicion of conspiracy to defraud (including alleged incidents in Cleveland) and released under investigation while inquiries continue.

Detective Inspector Jim Forster of Cleveland Police's Economic Crime Unit said: "These despicable criminals have conned 320 people nationwide in just the last month and that's only the people who police know about. Some people are too embarrassed to admit they've been scammed while some simply believe that they were helping police or banks to fight fraud, which is ironic and very sad.

"My message is simple – police and banks would never phone anyone and ask them to take money out of their accounts.

"I'd urge everyone to talk to their older family members or friends who may not have seen our messages on social or traditional media. Please, make them aware and help us to protect them."

<https://www.facebook.com/clevelandpolice/posts/10158585612896855>

14th December 2020

Revealing too much information on social media could lead to [#identitytheft](#). Be mindful of what you share online as your identity and personal information are valuable.

Criminals can use them to open bank accounts, get credit cards/loans and even apply for documents such as passports and driving licenses in your name.

You can request a copy of your personal credit report from a credit reference agency to check if it includes items you don't recognise.

If you think your identity has been used by someone else, contact your bank immediately and report it to Action Fraud (image). Read more here <https://tinyurl.com/y2azz9fx>

<https://www.facebook.com/clevelandpolice/posts/10158600030481855>

14th December 2020

Another case of courier fraud has unfortunately been reported in our force area in the last few days.

Police received a call from Barclays Bank in Hartlepool on Friday afternoon after staff made routine checks when a customer attempted to withdraw thousands of pounds.

They contacted officers who spoke to the gentleman (who's in his 70s) and he confirmed he'd had a call on his mobile phone from very convincing fraudsters, telling him he was victim of a scam which was being investigated by police, but that they would need him to withdraw cash to help their inquiries.

The callers phoned the man to ensure he was on his way to the bank, and again while in the premises however thanks to the swift action by staff, no money ended up in the scammers' hands.

We would again appeal for everyone to speak to older or more vulnerable friends and relations about courier fraud and to stress our simple messages:

- Police or banks would NEVER ask you to withdraw cash to give a courier to pick up.
- If you receive an unexpected call where someone asks for your bank details or for you to remove cash, put the phone down and tell a trusted family member or friend.

Cleveland Police continues to work with forces and financial institutions nationally, as well as the National Crime Agency and NERSOU (the North East Regional Special Operations Unit) to counter this activity and a number of arrests have been made in connection with this kind of fraud.

<https://www.facebook.com/clevelandpolice/posts/10158599952856855>

15th December 2020

WARNING Following another Case of Courier Fraud Reported to Cleveland Police

Police received a call from Yorkshire Bank in Hartlepool yesterday, Monday 14th December after staff made routine checks when an elderly customer was contacted over the phone and asked to transfer cash by fraudsters.

Thankfully due to the banks protocol no money was handed over and the incident was reported to police.

We would again appeal for everyone to speak to older or more vulnerable friends and relations about courier fraud and to stress our simple messages:

- Police or banks would NEVER ask you to withdraw cash to give a courier to pick up.
- If you receive an unexpected call where someone asks for your bank details or for you to remove cash, put the phone down and tell a trusted family member or friend.

Cleveland Police continues to work with Forces and financial institutions nationally, as well as the National Crime Agency and NERSOU (the North East Regional Special Operations Unit) to counter this activity and a number of arrests have been made in connection with this kind of fraud.

<https://www.facebook.com/clevelandpolice/posts/10158601575711855>

17th December 2020

Officers Prevent Victims from Being Scammed of Savings Amounting to Over £130k

Officers from the Incident Response Team and Economic Crime Team have prevented victims from the loss of £135,000 in courier fraud scams thanks to banking protocols.

In the last month the Force has received over 30 courier fraud reports. This type of fraud is when people are targeted by very convincing callers claiming to be from the police, the bank or the 'fraud squad' and asking them to withdraw large sums of money.

Unfortunately a couple of people fell victim to the scams but most potential victims spotted the scam for what it is and ended the call and others were stopped by police or banks.

Detective Inspector Jim Forster of Cleveland Police's Economic Crime Unit said: "Courier Fraud is a particularly nasty crime that strips people of their savings. The average victim age in our area has been 71 years old.

"The banking protocol is an important part of preventing this type of crime. When banking staff become suspicious of a transaction they will, if required, call the police to try and prevent the transaction.

"In recent weeks, several victims have had their savings protected by the banking protocol, amounting to over £135,000.

"Officers from the Economic Crime Unit have been visiting all the banks across the Force area to reaffirm how important it is to call us for any suspicious transactions.

"Anyone who receives a phone call from someone claiming to be police or a bank and asking about money should hang up immediately and inform a trusted friend or relative.

"I want to make it clear that police and banks would never phone anyone and ask them to take money out of their accounts.

"I'd urge everyone to talk to their older family members or friends who may not have seen our messages on social or traditional media. Please, make them aware and help us to protect them."

If you believe you have been a victim of courier fraud please contact Cleveland Police on 101.

<https://www.facebook.com/clevelandpolice/posts/10158606384906855>

21st December 2020

Officers investigating alleged fraud incidents have arrested a 22 year old man. The incidents were reported to have taken place on Wednesday 16th December when it is claimed that distraction techniques were used to gain large sums of cash as refunds in a dry cleaners and a pharmacy in Middlesbrough.

The man remains in custody awaiting questioning by detectives and inquiries are ongoing.

<https://www.facebook.com/clevelandpolice/posts/10158615855486855>

21st December 2020

Christmas is not only the nation's favourite time of year but also a favourite for criminals. 🌲
If you receive an unexpected call from a trusted organisation informing you of outstanding debt/bills that need to be settled through the purchase of gift cards/vouchers [#TakeFive](#) 🙌
Criminals will often use urgent language and time pressure to convince you to act quickly and relay the serial number listed on the back of gift cards/vouchers.

Remember: Only use gift cards/vouchers for purchasing goods and services directly from the named retailer.

If you think you've fallen for a scam, contact your bank immediately on a number you know to be correct such as the one listed on the back of your debit/credit card and report it to Action Fraud (image). For more information : <https://tinyurl.com/y8lpzvoy>

<https://www.facebook.com/clevelandpolice/posts/10158616331016855>

23rd December 2020

A police officer will NEVER ask you to hand money over to them to support an investigation, or ask you to transfer money to a safe account for fraud reasons. [#TakeFive](#) to stop courier fraud. [#FraudFreeXmas](#)

<https://www.facebook.com/clevelandpolice/posts/10158618234941855>