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

FRAUD AWARE

SPRING 2021

FRAUD AND YOU

Fraudsters invest a lot of time and effort into making their scams believable, and while some frauds can be easily spotted, there can be occasions where you may not spot a fraud until it is too late.

The best way to frustrate the fraudster is to be aware of the scams they operate. This booklet is designed to help you avoid falling these pitfalls by giving you the information to spot and protect yourself from those frauds and scams.

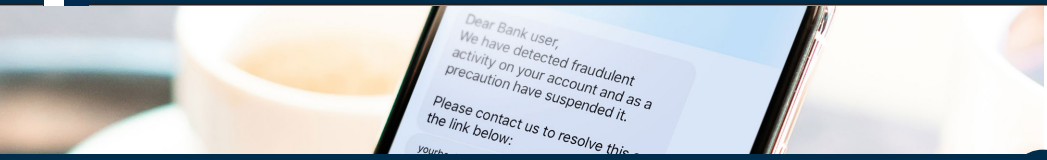
But if you are unfortunate to fall victim to fraud, please report it to the police, help us to catch them and to also make sure that it doesn't happen to anyone else.

Fake Emails, Texts & Phishing | *Suspicious Phone Calls* | *Online Shopping Fraud* | *Investment Fraud* | *Romance Fraud*

Uttlesford CSP Uttlesford Community Safety Partnership

kindly funded by the Uttlesford Community Safety Partnership

ESSEX POLICE
Protecting and serving Essex



Fake Emails, Texts & Phishing

What are they?

Phishing is where criminals send an email to a vast number of email addresses, in order to trick people into giving out their personal data.

Smishing uses the same principle but using SMS text messages. Recently we have seen examples of both phishing and smishing where criminals have pretended to be the NHS offering COVID vaccinations.

What are the signs?

'Dear Customer' – be suspicious of any emails that are not addressed to you by name.

Spelling and grammar – be suspicious of emails that contain poor spelling and grammar, including looking for random 'cApitAls' and 'Sp(e)llings'.

Unexpected contact – be suspicious if organisations such as 'the bank' contact you out of the blue and ask you to confirm your personal details.

What can I do?

Check the sender – hover your mouse over the email address (or click and hold on a mobile device) to see the true sender. It is also possible to 'spoof' phone numbers, so be alert to any messages you receive.

Never click the link – phishing/smishing relies on you clicking a link that takes you to the malicious webpage. This site may harvest your personal data or download viruses and malware which can damage your device or your network.

If unsure, check with the company – if you are still unsure whether the email is genuine, check the company website or contact them using a trusted number (never use a number supplied by the email). Genuine companies will have no issues with you confirming whether an email is real.

You can also forward suspicious emails to **report@phishing.gov.uk**

Suspicious Phone Calls

What are they?

Criminals often make contact with potential victims via the telephone. There are a number of different types of telephone fraud, including computer software service fraud (where the criminals pretend to be from Microsoft to help you 'fix' a problem with your computer) and courier fraud (where criminals pretend to be from the police or the bank to trick people into handing over money or bank cards).

What are the signs?

Unexpected contact – be suspicious of calls that you were not expecting. Would you expect that organisation to contact you out of the blue?

Requesting personal details – be suspicious of calls requesting personal or financial details. The police or bank will never request that you disclose your PIN number or transfer your money to a 'safe' account.

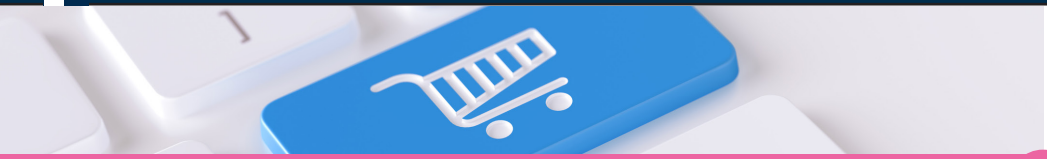
Pressure – be suspicious of callers that are aggressive or try and pressure you into making a decision whilst on the phone. This is the criminals trying to rush you into making a decision that benefits them.

What can I do?

Hang up – if you are unsure whether the call is a scam, simply hang up the phone. If you want to check with the company to see whether the call was genuine, call back using a trusted number (never use contact details provided by the caller). Ideally, use a different phone but if this is not possible, wait for five minutes to ensure the call has fully disconnected, or unplug the phone first.

Get a call blocker – contact your phone provider to see what call-blocking services they offer. There are also other products available on the market that will screen your calls even more vigorously.

Talk about it – if you have received a suspicious phone call, speak to friends and family before making any decisions. Often having a second opinion will confirm or deny your suspicions and help you protect yourself.



Online Shopping Fraud

What is it?

As more people have become reliant on online shopping throughout the COVID-19 pandemic, more people have fallen victim to online shopping fraud. Where individuals have sold items on auction sites or social media, this includes sellers not receiving payment and buyers receiving different items or no items at all. Items include anything from puppies to motorhomes which are either misleadingly advertised, or simply don't exist.

What are the signs?

Requests for money up front – be suspicious of requests for money or large deposits before being allowed to see the item, especially pets – ensure you have been allowed to see the animal in person (or at least on a video call) before agreeing to pay a deposit.

Unbelievable offers – be suspicious of rock bottom prices for must-have items. Scammers will try and lure you in with irresistible prices or discounts. If it seems too good to be true, it usually is!

Requests you pay by bank transfer – be suspicious of sellers requesting that you pay via bank transfer. Bank transfers are not covered by the same protections as credit card and PayPal payments, meaning you're unlikely to get any money back if things go wrong.

What can I do?

Do your research – know what the recommended price of the item is so that you know whether a price seems too good to be true. Check the buyer/seller's reviews and make sure you are buying from a genuine and trusted website.

Selling an item – make sure you receive proof of payment before posting the item. Take a picture of the condition of the item prior to posting to prevent fraudulent damage claims.

Make secure payments – ensure you use the recommended and trusted payment platforms. Don't make payments over public WiFi or WiFi with no password protection as criminals can intercept your payment details.

Investment Fraud

What is it?

Investment fraud is when criminals contact you to encourage to you make a 'high returns' investment in a product. Often, people are encouraged to invest increasing amounts of money, to later discover that the product is worthless, or worse, does not exist. Criminals will use convincing websites and brochures to try and convince you that they are legitimate. Investment scams can come in a number of forms including diamonds, cryptocurrencies (including Bitcoin), fine wines and time shares.

What are the signs?

Unexpected contact – be suspicious if you are contacted out of the blue, either over the phone, via social media or email.

Time pressure – be suspicious of 'time limited offers' or discounts that pressure you to make a decision then and there.

Unrealistic returns – be suspicious of adverts that promise 'guaranteed returns'. In the world of financial investments, there's no such thing!

What can I do?

Check if the firm is authorised – check the Financial Conduct Authority (FCA) register to see if the company is authorised and check their Warning List for firms to avoid. If you use an unauthorised firm, you are unlikely to be able to get your money back if things go wrong.

Get impartial advice – making an investment is a big financial decision! You should consider getting impartial financial advice from a regulated financial advisor or approved sites such as the Money Advice Service.

If you're suspicious, report it – don't allow yourself to be pressured into making a decision. If it sounds too good to be true, then it usually is! Allow yourself time to do all the research you need to do, and if you're still not sure then report to the FCA.

Romance Fraud

What is it?

Romance or dating fraud occurs when you think have met the perfect partner through an online dating website, dating app, or social media but the other person is using a fake profile. Once the fraudster behind the profile is confident that they've gained your trust, they will invent a problem and ask for your help by sending them money. They might even get you to use your bank account to launder criminal funds.

What are the signs?

Difficulty meeting in person – be suspicious if they make excuses for why they can't video chat or meet in person. They might also be 'working overseas' or in a foreign military.

Requesting money – be suspicious of any money related requests. They could be asking for money in an emergency or requesting that you transfer some money on their behalf.

Keeping the relationship secret – be suspicious if they ask you to keep your relationship 'private' and insist that you don't discuss it with anyone. Being in a relationship should be a wonderful thing that you want to share with your friends and family!

What can I do?

Stay on the platform – most romance fraudsters will quickly try and move the conversation to other platforms such as Whatsapp because they offer less regulation and more encryption options, meaning there is less evidence of their requests for money.

Avoid giving out personal details – be conscious of the details that you provide on your dating profile such as name, date of birth and home address, as this can easily lead to your identity being stolen.

If you're suspicious, report it – if their profile pictures seem a little too good to be true, consider doing a reverse image search on Google to check that they haven't been stolen from another profile. If they have, or they have made a request for money, then report the profile to the dating site.

Need to contact Essex Police about something that's a non-emergency?

Now there's a quick online alternative to calling 101 or visiting a station - DIGITAL 101

Digital 101
essex.police.uk

Do it online at:

essex.police.uk

REPORT

- Crime
- Road traffic incident
- Anti-social behaviour
- Missing person
- Fraud
- Civil disputes
- Lost or found property
- Lost or stolen vehicles

REQUEST

- A collision report
- Intellectual property (IP) licence, such as the use of the Essex Police crest
- Your fingerprints
- Information: about the police, yourself or someone else

APPLY OR REGISTER

- Careers
- Charity collection licences
- Compensation for victims of crime
- Firearms, shotgun or explosives certificate
- Register an as overseas visitor
- Attend a misconduct hearing

LIVE CHAT

- Live Chat is now available on our Essex Police website
- It's a new way for the public to contact us and ask questions directly on your computer, tablet or mobile phone.

TELL US ABOUT

- Possible terrorist activity
- Something you've seen or heard
- An existing case or report
- An event or procession
- Filming

YOUR AREA

Find out more about what's going on in your local area, including:

- Your local policing team's day-to-day activities
- Crime statistics
- Meetings
- Prevention advice
- and more

FEEDBACK

- Thanks
- Complaints
- Feedback about the website

Digital 101
essex.police.uk

ESSEX POLICE
Protecting and serving Essex

HELPFUL TIPS

TAKE FIVE TO STOP FRAUD

1. **The best way to avoid frauds and scams is also the simplest too - don't engage with anyone or anything you think is even slightly suspicious.** Don't reply to that message, don't continue that call or conversation - ignore them, delete the email, hang up the phone, close the door. **Now you're stopping fraud in its tracks.**

2. **MY INFO? MY MONEY? I DON'T THINK SO!**

   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.

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

   CHALLENGE - make sure your doors & windows are locked shut, some scammers work in pairs with one distracting you while another goes through the back door.

   PROTECT - Put the chain on your front door before opening it to callers. Check on the caller though a door spy-hole or window.

   Want to know more? Visit **takefive-stopfraud.org.uk**

3. **Organisations such as banks or utility providers will never ask you for your full password or PIN**, only parts of it. If they ask for more, it's suspicious. Banks / building societies or Police will never come to your home to confiscate your cards or to collect cash or a 'payment' of any form.

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

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk