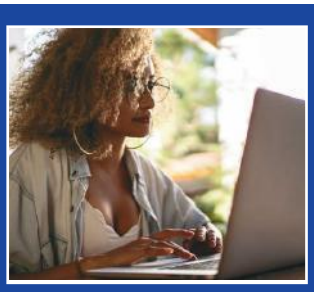


Your router could be a risk - P2-3

Register your cat converter - P5

Fly away but keep to the rules - P6-7

Stay alert to the holiday scam - P13

CWM

JUNE 2021

COMMUNITY WATCH MAGAZINE ESSEX

P11: SEE OUR SUMMER GUIDE FOR KEEPING YOUR HOME SECURE

Right of reply

■ BT GROUP AND EE

"The vast majority of our customers are using our BT Smart Hub 2 or EE Smart Hub. We want to reassure customers that all our routers are constantly monitored for possible security threats and updated when needed. These updates happen automatically so customers have nothing to worry about."

■ VIRGIN MEDIA

"We do not recognise or accept the findings of the Which? research – nine in ten of our customers are using the latest Hub 3 or Hub 4 routers. We have robust processes in place to protect customers by rolling out security patches and firmware updates as well as issuing customer communications where necessary."

■ TALKTALK

"These routers make up a very small proportion of those in use by our customers. Customers using all of these routers can change their passwords easily at any time."

■ PLUSNET

"We want to reassure customers that all our routers are constantly monitored for possible security threats and updates with firmware. These updates happen automatically so customers have nothing to worry about. If a customer has any issues, they should contact us directly and we will be happy to help."

■ VODAFONE

"All new Vodafone routers have device specific passwords. We stopped supplying the HHG2500 router to customers in2019. Customers who still have the HHG2500 router will continue to receive firmware and security updates as long as they have an active customer subscription. Customers who haven't already changed their password should do so, following these instructions."

Is your router safe or are you at...

MILLIONS of internet users could be at risk of hacking attacks due to using outdated routers from their broadband providers that have security flaws, a Which? investigation has found.

Households across the country are using their home broadband more than ever, to work, educate their children or keep in touch with loved ones.

But many are unaware that old equipment provided by internet service providers (ISPs), including EE, Sky, TalkTalk, Virgin Media and Vodafone, could be putting them at risk of hackers spying on what they are browsing or even directing them to malicious websites used by scammers.

Which? investigated 13 old router models and found more than two-thirds, nine of them, had flaws that would likely see them fail to meet requirements proposed in upcoming government laws to tackle the security of connected devices. The legislation is not yet in force and so the ISPs aren't currently breaking laws or regulations.

The Brightbox 2 router

The consumer champion's lab testing identified a range of issues with the routers. These security risks could potentially affect around 7.5 million people, based on the number of respondents who said they were using these router models in Which?'s nationally representative survey.

Around six million people within this group of users could be using a router that has not been updated since 2018 or earlier. This means the devices have not been receiving security updates which are crucial for defending them against cyber criminals.

The problems uncovered by Which?'s lab tests on the old router models that failed were:

■ Weak default passwords, which in certain circumstances could allow a cyber criminal to hack the router and access it from anywhere;

■ a lack of firmware updates, which are vital for both security and performance;

■ a local network vulnerability issue with the EE Brightbox 2. This could give a hacker full control of the device, and for example allow them to add malware or spyware, although they would have to be on the network already to attack.

The survey also suggested that 2.4 million users haven't had a router upgrade in the last five years.

Which? is concerned that many customers are being left using old kit, often with no guarantee of an upgrade, and is encouraging consumers in this position to talk to their broadband provider about getting an upgrade.

In contrast to the other ISPs, the old BT and Plusnet routers Which? tested all passed the security tests – researchers didn't find password issues, a lack of firmware updates or a local network vulnerability with these devices.

When Which? contacted the ISPs with its findings, most of them said that they monitor for security threats and provide updates if needed. BT Group told Which? that older routers still receive security patches if problems are found – although Which? did find an unfixed vulnerability on the EE (part of the BT Group) Brightbox 2 router. Aside from Virgin Media, none of the ISPs Which? contacted gave a clear indication of the number of customers using their old routers.

Virgin said that it did not recognise or accept the findings of the Which? research and that nine in 10 of its customers are using the latest Hub 3 or Hub 4 routers.

However Which? notes that Virgin was counting just paying account holders, whereas Which?'s survey was of anyone using routers within a household.

Continued page 5

...risk from hackers who steal your ID?

Check the right route to safety

From page 4

Which? believes that ISPs should be more upfront about how long routers will receive firmware and security updates – one of the requirements of proposed government laws to tackle unsecure devices – and encourage people to upgrade devices that are at risk.

As part of its proposed legislation to tackle unsecure devices, Which? is also calling for the government to ban default passwords and also prevent manufacturers from allowing consumers to set weak passwords that may be easily guessable and hackable.

The consumer champion also believes broadband providers should be ready to respond when security researchers warn them about possible issues – and should make it easy for researchers to contact them. Only Sky, Virgin Media and Vodafone appeared to have dedicated web pages for this.

Consumers with routers that are five years old or more should ask their provider if the device is still supported with security updates and if it is not they should ask for an upgrade.

Kate Bevan, Which? Computing editor, said: "Given our increased reliance on our internet connections during the pandemic, it is worrying that so many people are still using out-of-date routers that could be exploited by criminals.

"Internet service providers should be much clearer about how many customers are using outdated routers and encourage people to upgrade devices that pose security risks.

"Proposed new government laws to tackle devices with poor security can't come soon enough – and must be backed by strong enforcement."

A significant problem uncovered by Which?'s lab tests on the old router models was weak default passwords – with more than half (seven out of 13) of the old routers having this flaw that could allow a cyber criminal to hack the router and access it from anywhere. This issue affected TalkTalk, Virgin Media, Vodafone and Sky models.

A lot of consumers leave default passwords unchanged on their equipment because they are not aware of the security risks of doing so, potentially leaving them exposed to hackers.

Another issue exposed by the lab tests was a lack of firmware updates, which are vital for both security and performance. More than half (seven out of 13) of the routers had not been updated since 2018, for some this went as far back as 2016.

Which? also found a local network vulnerability issue with the EE Brightbox 2, which has not yet been fixed.

The government is planning a new law to make sure virtually all smart devices meet new requirements:

- Customers must be informed at the point of sale the duration of time for which a smart device will receive security software updates
- A ban on manufacturers using universal default passwords, such as 'password' or 'admin', that are easily guessable

Manufacturers will be required to provide a public point of contact to make it simpler for anyone to report a vulnerability.

Which?'s advice on how to change your router password: **which.co.uk/routerpasswd.**

Further details on the routers Which? tested:

Weak passwords - devices affected:
TalkTalk HG533
TalkTalk HG523a
TalkTalk HG635
Virgin Media Super Hub 2
Vodafone HHG2500
Sky SR101
Sky SR102

Lack of updates - devices affected:
Sky SR101
Sky SR102
Virgin Media Super Hub
Virgin Media Super Hub 2
TalkTalk HG523a
TalkTalk HG635
TalkTalk HG533

Network vulnerabilities:
EE Brightbox 2

The three routers that passed the security tests:
BT Home Hub 3B
BT Home Hub 4A
BT Home Hub 5B
Plusnet Hub Zero 2704N

Drug gang jailed

■ THE ringleaders of an organised crime group which supplied drugs to county lines gangs have been jailed for a combined total of more than 40 years.

Christopher Golding headed up the Harlow-based network, which smuggled cocaine in containers through ports before selling it on to gangs supplying west Essex, Hertfordshire, Kent, London and Suffolk.

The operation was estimated to have earned them at least £500,000 which was stashed in Bitcoin or laundered through the pub Golding ran as a licensee.

Golding was given a 12-year prison sentence; Stuart Thurgood was handed eight years in jail; Lee Wilkinson was sentenced to six years and eight months; Adam Dalby recieved a sentence of six years and eight months; David Wilkinson was given four years and eight months in prison; Robert Aldred was jailed for two years and eight months; Algirdas Gustaitas was sentenced to two years and four months; Lee Collet was given a two year sentence.

Mobile shutdown

■ ELEVEN phone numbers used by drug dealers in west Essex have been shut down as part of a police operation.

Operation Raptor, an Essex Police team dedicated to dismantling drugs gangs, applied for the orders after identifying phone numbers offering cocaine and cannabis for sale in Thurrock and Brentwood.

Working with the telephone network companies and courts, it secured the Drug Dealing Telecommunications Restriction Orders at Clerkenwell and Shoreditch County Court.

Let us spray to keep churches protected

Churches and historic books are being safeguarded using unique forensic mark-

ONE of the world's leading forensic marking companies are being touted by foreign leaders to ensure that priceless antiquities across the globe are protected from international criminals.

SelectDNA, recognised as pne the best in their field, has established a reputation globally that makes the recovery of stolen items easier once they have been invisibly marked.

While SelectDNA contains a unique DNA code that can be registered to a specific museum or heritage site or property and can be easily applied to exhibits as it is almost invisible on application and is compatible with virtually all types of materials and surfaces.

In the event that a marked exhibit is stolen and recovered by police, it could be quickly traced back to the museum via the DNA code.

A Bronze-age village in County Durham has had priceless artefacts DNA-protected; and the Church of England has protected altarware dating back to medieval times with it.

Rare books in the United States, which are considered among the globe's most prized and valuable literary works, have also been forensically marked by SelectDNA to help a leading antiquarian rare book gallery with authentication and inventory management.

SelectaDNA has been used to mark priceless exhibits at a number of museum and heritage sites following its success in reducing theft in residential property marking schemes.

It has been used to help catalogue items at the Natural History Museum in London and has been applied to the prestigious collection of cars at the world-famous National Motor Museum at Beaulieu and also at the Goodwood Motor Museum.

Historic England have also used SelectaDNA to forensically protect ancient marine wreck sites from theft and damage; while secret bunker sites at Portadown in Northern Ireland and Skelmorlie in Scotland, which were originally used at the height of the Cold War, and are now visitor attractions with on-site museums have marked all their irreplaceable monitoring equipment for posterity.

Be smart to beat the thieves

CATALYTIC converter theft is a booming criminal enterprise and is one of those crimes that can happen while you are shopping or when your are asleep.

You won't even know yours has been stolen until you start the engine and it sounds louder than usual.

Thousands are stolen every year because they contain precious metals that have shot up in value in recent years, giving them a high scrap metal value.

However did you know that although police seize thousands of suspected stolen catalytic converters during raids on scrap metal yards, they can't prove them stolen and are forced to return them to the dealer.

But that has now changed. In partnership with the police and Toyota, the National Database for Catalytic Converters has been created.

It means in just 10 minutes you can register your catalytic converter and if it gets stolen the police have more chance of recovering your property.

Toyota has joined forces with police to create the new national database and with SmartWater to uniquely mark exhaust systems..

The database will be operated by the Centre for Infrastructure and Asset Protection (CIAP), an intelligence unit made up of analysts who are accredited Police contractors, tracking organised crime gangs around the UK.

They work with police on the NICRP to reduce and tackle crime and the method of registration is to mark the catalytic converter with a uniquely formulated SmartWater® solution, a special liquid designed to withstand the heat of an exhaust.

It has a unique forensic code embedded within it, which is registered against the registration number of the vehicle and simply painted all over the catalytic converter by a trained auto technician.

It glows bright yellow under a special UV light that has been provided to the police and it only needs a speck to identify the vehicle of origin. If the thieves try to remove the solution, they're spreading incriminating evidence all over their hands, clothes and location.

SmartWater have agreed with the police to provide them with free access to the database, forensic analysis and expert testimony in support of prosecutions.

Superintendent Mark Cleland of British Transport Police, said "The National Infrastructure Crime Reduction Partnership coordinated Police and partners across the UK in a week of action to target catalytic converter crime.

"With over 1000 stolen catalytic converters recovered, 60 arrests and nearly a 1000 site visits, we managed to reduce catalytic converter crime nationally by 50% during that period.

"One key element of the operation was the use of forensic marking as an option to prevent crime in the first place.

"Toyota led the way on this approach through a partnership with CIAP to roll out marking in line with our 'Protect, Mark, Park' approach and our advice to forensically mark and register your property to help protect it, prevent crime and trace it should the worst happen."

Rachael Oakley, head of CIAP, added: "This latest spike in catalytic converter thefts represents a considerable issue for police, as a lack of clear distinguishable marks and traceability mean it is difficult for officers to prosecute.

"However, the creation of the national database, thieves will now be held to account for their actions and offences will be traced, sending out a powerful deterrent message."

Get ready for...

SINCE 17th May 2021 the UK Government has allowed travel abroad, although for most destinations, this is for essential travel only. If you do decide to travel, this article offers advice on what to do before and after your trip.

Traffic Light System Explained
The UK Government has categorised countries as either being red, amber, or green. The traffic light systems outlines what you will need to do on your return to the UK.

Green – You will need to take a **COVID-19** test before you fly back to the UK. Accepted tests include PCR, LAMP, and rapid antigen (also known as lateral flow). You will also need to take a PCR test 2 days after you return. You will not be required to quarantine unless you return a positive test.

Amber – You will need to **quarantine at home** for 10 days on your return to the UK. You will need to take the same tests outlined in the green section above as well as another test 8 days after you return. There is the option to pay for an additional private test on day 5 of your return to end your quarantine early. This is called **test to release.**

Red – You will need to stay in a **quarantine hotel** for 10 days on your return, as well as take tests as outlined in the amber section above. There is no option to test to release from a red list country. The cost for hotel quarantine is currently £1750 per person.

All passengers regardless of where you are travelling back from will need to complete a **Passenger Locator Form** before you return to the UK.

The Government is reviewing the status of countries every three weeks so it is essential to check the Government Website **gov.uk** before you travel so you understand what will be required of you when you return as this may have changed since you booked your trip.

It is also essential check the advice of the Foreign, Commonwealth and Development Office (FCDO) **gov.uk/foreign-travel-advice** before you travel to understand what restrictions are in place in the country you are visiting.

Continued page 7

Follow us on Facebook and Twitter for useful leaflets to share with your friends and family. Don't take chances, follow our advice and stay safe.

...take-off but follow the advice

Check your passport is up to date before you leave

From page 6

It may be that you will be required to quarantine on your arrival and some countries require you to provide a negative test result before travel but the rules can be different depending on where you go.

You will also need to check which test you need to take as some popular destinations will only accept PCR tests which are more expensive. Each countries requirements can be found on the above FCDO site.

.

Other helpful Advice

Take out comprehensive travel insurance as soon as you book your trip. Many new policies now offer protection against cancellation if you are unable to travel due to Coronavirus, as well as covering medical expenses should you fall ill while you are away.

Check your passport. Now that we have left the EU you will require at least 6 months validity on your passport to enter an EU country. Also check if your EHIC card is still in date. If it is not you will need to apply for a **GHIC card.**

Be aware that travelling through airports and ports will be different. You will be required to wear face coverings and practice social distancing. Restaurants may be closed and food onboard your plane may not be available.

Changes to Holidays Already booked

If you already have a holiday booked and advice from the **Foreign, Commonwealth and Development Office (FCDO)** is not to travel to that country you will be entitled to claim a full refund or re-book your holiday.

Complete the Passenger Locator form on leaving

Please note that the requirement to quarantine on your return from holiday from an Amber list country, does not fall into this category and if you wish to cancel a holiday because you do not wish to quarantine on your return, cancellation charges may apply.

Many travel companies are willing to be flexible, so speak with your travel provider at the earliest opportunity should you have any concerns.

We hope the above information is useful, but if you would like more detailed advice on your individual circumstances, please contact the Citizens Advice Consumer Helpline on **0808 223 1133** or visit their website at **www.adviceguide.org.uk.**

Remember you might have to go into quarantine

To find a reputable trader approved and vetted by Trading Standards visit **www.buywithconfidence.gov.uk**

For general help and advice or to report a problem with a trader you can telephone the Citizens Advice Consumer helpline on **0808 223 1133**

BUY WITH CONFIDENCE TRADING STANDARDS APPROVED
buywithconfidence.gov.uk
ESSEX TRADING STANDARDS

Buy With Confidence

The only nationally available business approval scheme that's owned, controlled and operated by Trading Standards services

It can be difficult to know who to trust. That's why Trading Standards created Buy With Confidence. Fully trained Trading Standards professionals independently check, vet and monitor businesses, who will treat you fairly.

So, whether you need a plumber, electrician, roofer or anything else, visit **BuyWithConfidence.gov.uk** to find Trading Standards Approved businesses you can trust.

BUY WITH CONFIDENCE
TRADING STANDARDS APPROVED

buywithconfidence.gov.uk
ESSEX TRADING STANDARDS

Mobile packages could be a scam

CIFAS, the UK's leading fraud prevention service, is issuing a warning about a scam which could see victims hand over personal details and have mobile phone contracts set up without them receiving the phone they are promised.

Telecoms providers are reporting a number of phone users receiving calls from scammers offering deals on the latest phone models.

After the victim agrees to the contract and provides personal details, and in some instances also makes an upfront payment, they receive confirmation that their order has been placed. These are then followed by texts from a delivery company to let them know their order is safely on its way.

When the phone is received, it's not the model the victim was expecting, as the scammer has used the victim's details to apply for a cheaper model at the price the victim was expecting to pay for the more valuable handset.

Minutes after the delivery, the fraudster calls the victim to advise the incorrect phone has been sent and asks for the phone to be returned to an address in return for the correct model.

The new phone never arrives, and when the victim calls the real mobile phone network, they are told the address they returned the phone to is not an official company address.

This scam is designed to both steal the personal and financial details of victims, as well as provide the scammers with a handset which could be sold for a profit or used to commit further criminal activities.

Cifas is reminding consumers to remain vigilant when receiving unsolicited calls and to look out for the following warning signs:

Pay attention to the phone call – calls from scammers will often be poor quality

Check the transaction with your bank or on your banking app – the payment should show as a telephone purchase to the company you were speaking to. If the transaction appears as an online purchase, or is sent to a name other than the company you were dealing with, this could be an indication of fraud

Be cautious if you receive a call telling you the wrong phone has been sent – it is unlikely that a genuine company will call and advise this is the case

Expect a prepaid envelope to return the phone to the company – if you are asked to send the phone back then question who you are speaking to, and remember that a genuine company will normally send you a prepaid envelope.

Phone users contacted about similar offers should hang up and call their network provider using the phone number available on their official website to ensure the call is genuine.

Users should also call the phone company if they have received a call advising the wrong package has been sent and are asked to return it to an address.

Upon return of the phone to the correct address, the phone company will cancel any contract set up in the victim's name under their customer money back policy.

Anyone that believes they have been a victim of a scam must tell their bank or credit card supplier immediately and report the incident to Action Fraud or Police Scotland. Victims may also consider adding their details to the Cifas National Fraud Database to help protect themselves against further use of their identity without their knowledge.

Mobile phone operators are engaging with each other and Cifas to gather intelligence, drive involvement with law enforcement and raise awareness of this scam.

Continued page 10

From page 9

It is believed there are potentially thousands of victims of this scam, with losses reaching into the millions. The respective fraud teams at each mobile phone operator are continuing to identify fraudulent applications and are cancelling orders prior to delivery.

Cifas, the UK's leading fraud prevention service, is issuing a warning about a scam which could see victims hand over personal details and have mobile phone contracts set up without them receiving the phone they are promised.

Telecoms providers are reporting a number of phone users receiving calls from scammers offering deals on the latest phone models.

After the victim agrees to the contract and provides their personal details, and in some instances also makes an upfront payment, they then receive confirmation that their order has been placed. These are then followed by texts from a delivery company to let them know their order is safely on its way.

When the phone is received, it's not the model the victim was expecting, as the scammer has used the victim's details to apply for a cheaper model at the price the victim was expecting to pay for the more valuable handset.

Minutes after the delivery, the fraudster calls the victim to advise the incorrect phone has been sent and asks for the phone to be returned to an address in return for the correct model.

The new phone never arrives, and when the victim calls the real mobile phone network, they are told the address they returned the phone to is not an official company address.

CIFAS warning that could save you from heartache

This scam is designed to both steal the personal and financial details of victims, as well as provide the scammers with a handset which could be sold for a profit or used to commit further criminal activities.

Cifas is reminding consumers to remain vigilant when receiving unsolicited calls and to look out for the following warning signs:

■ Pay attention to the phone call – calls from scammers will often be poor quality

■ Check the transaction with your bank or on your banking app – the payment should show as a telephone purchase to the company you were speaking to. If the transaction appears as an online purchase, or is sent to a name other than the company you were dealing with, this could be an indication of fraud

■ Be cautious if you receive a call telling you the wrong phone has been sent – it is unlikely that a genuine company will call and advise this is the case

■ Expect a prepaid envelope to return the phone to the company – if you are asked to send the phone back then question who you are speaking to, and remember that a genuine company will normally send you a prepaid envelope.

Phone users contacted about similar offers should hang up and call their network provider using the phone number available on their official website to ensure the call is genuine.

Users should also call the phone company if they have received a call advising the wrong package has been sent and are asked to return it to an address.

Upon return of the phone to the correct address, the phone company will cancel any contract set up in the victim's name under their customer money back policy.

Anyone that believes they have been a victim of a scam must tell their bank or credit card supplier immediately and report the incident to Action Fraud or Police Scotland.

Victims may also consider adding their details to the Cifas National Fraud Database.

Head of Fraud Intelligence for Cifas, Amber Burridge, said: "Criminals have increasingly turned to phone fraud to target victims. These scams often involve the promise of a new phone or item of technology.

"I would urge anyone receiving these calls to take a moment to stop and think about the consequences of parting with their personal and financial information. Challenge anything that seems suspicious. If you are a victim

A CIFAS case study

IN a similar scam technique Amy, 54, received a package including an iPad and a SIM card. While Amy was out of the home, she called the provider to let them know she hadn't ordered the item and was advised by the provider to not give the package to anyone until she had heard back from them with further instructions.

However, by the time she had contacted her family at home to convey the message, another courier had already arrived advising the device was to be recollected as it had been delivered to an incorrect address.

Unaware of the conversation Amy was having with the provider, a family member gave the package back to the courier who was dressed in the correct uniform and had presented identification.

This was an incredibly stressful experience for Amy whose business had been impacted by the pandemic and had reduced her income. The thought of criminals using Amy's personal details to create accounts in her name was particularly worrying.

Amy contacted Action Fraud to report the incident, as well as her bank to cancel her card, and took out a Cifas Protective Registration marker to protect herself from identity fraud.

*details of the victim substituted to protect their identity

Burglars don't go on holiday

JUST because it's the summer and your area may have one of the lowest rates of burglaries, remember criminals do not take seasonal holidays.

Police say thefts can increase during the summer months as thieves gain access to properties through insecure doors and windows.

According to a recent Crime Survey for England and Wales, burglars got inside homes through an unlocked door 21 per cent of the time and through an open window 11 per cent of the time.

Officers say locking windows and doors, making sure all valuables are out of sight and tidying away tools, can significantly reduce the chances of a home being broken into.

A police spokesman said: "It's been a strange 12 months so far and understandably, people are excited to make the most of being able to see friends and family again, spending time outside and even going away.

"However, with this, burglars may take advantage of people leaving their homes empty, especially in the warmer weather.

"Any burglary can be devastating for the victims – or, at the very least, cause huge inconvenience – so it's important that residents do everything possible to keep the burglars at bay.

"Good-quality doors, windows and locks are excellent deterrents, but there's even more you can do to stop burglars in their tracks."

These are the ten steps to improve home security this summer

* **Keep them out of view:** Make sure all valuables and keys, including car keys, are out of sight and away from the view of windows and the letterbox – remember a device could be used to hook keys through the letterbox.
* **Keep them locked:** Leaving ground floor windows, doors and patio doors open in the summer can give burglars the perfect opportunity. If you are upstairs, out of the room, or in the garden, even just for a few minutes, keep them locked and help shut burglars out.
* **Pay attention:** Pay particular attention when you're outside in your garden, as you may not be able to see or hear someone entering your home.
* **Tidy away tools:** Ensure sheds, garages and outbuildings are locked and secure at all times – tidy away power tools and garden equipment after you've used them, don't leave them outside where they could be used to break into your home.
* **Burglar-proof your bikes:** Secure bikes at home by locking them to an immovable object inside a locked shed or garage.
* **Check access to windows:** Burglars often target windows as they generally offer easier access than doors. Take a good look at your windows from the outside and remove potential access points where you can. Are there walls, bins or garden furniture that could be used to reach windows?

* **Give burglars nowhere to hide:** Burglars don't want to be seen or heard and if they think they'll be noticed by a neighbour or passer-by, they'll probably move on. Cut back hedges at the front of your property to allow for a clear view over the top and don't provide cover for anyone wishing to hide and make sure your security lights are working.
* **Gates and fences:** Make sure the fences around your garden are in good condition, especially rear fencing and ensure side gates are locked to prevent access to the rear of the property.
* **Going away or on holiday?** Get a trusted neighbour to keep an eye on your property and leave radios or lights in your house on a timer to make the property appear occupied.
* **Property marking:** Mark your property and check to see if the police offer free property marking in your area.

ESSEX CRIME AND COMMUNITY NEWS

Guilty of murder

TWO teenagers have been convicted of the murder of Lee Chapman in Southend have been jailed for life. Lamar Davis and a 17 year-old boy, who cannot be named for legal reasons, were found guilty of murdering twenty-six year-old Lee who was stabbed multiple times in what was described as a "frenzied attack" in Cromer Road in March last year. **FULL STORY**

32 year sentence

TWO men have each been jailed for life, with a minimum of 32 years, for murder and another four men have each been given a jail sentence of 13 years for their part in an aggravated burglary at the property in Tintern Avenue, Westcliff, in which Asqeri Spaho, 25, died. **READ MORE**

Sex pest jailed

BHUSAN Chettri has been jailed after posed as a 16-year-old boy on social media to speak to what he believed was a 12-year-old girl and encourage her to have sex. Over the course of a month, he sent her sexual images and arranged to meet her to engage in sexual activity. **FULL STORY**

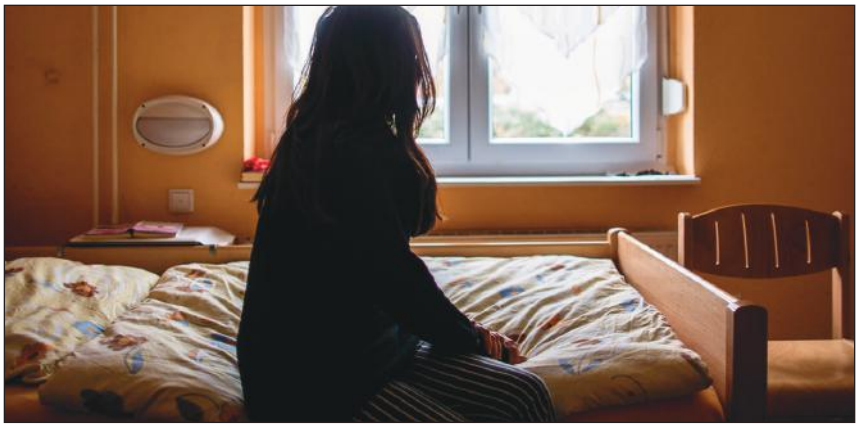
Jail for drugs boss

THE ringleader of a multi-million pound drugs ring, his girlfriend and two associates have been jailed after officers dismantled an organised crime group. Abdul Hamid, who got 18 years, ran the Tariq drug line selling cocaine mainly in Chelmsford, Maldon, Heybridge and the Dengie Peninsula. **READ MORE**

Wine shop robbery

A WOMAN has been jailed for four years after attacking a shop worker while armed with two knives during an attempted robbery. Police also secured a restraining order, which bans Justine Roberts from entering Benfleet Wine where she carried out her crime. **FULL STORY**

Cash support for the survivors of abuse



SURVIVORS of sexual violence and domestic abuse will benefit from extra support thanks to £500,000 Ministry of Justice funding being awarded to the Police, Fire and Crime Commissioner for Essex.

The money, an increase to the 2021/22 Victim's Grant, will fund 4.5 Independent Sexual Violence Advisors and 11 Independent Domestic Violence Advisors for a year, with the indication the funding will be granted again next year for a further 12 months.

The advisors will be employed by Synergy Essex, Changing Pathways, Next Chapter and Victim Support and will work across greater Essex. Some posts will focus on supporting children and young people, those with complex needs and the LGBT+ community.

Roger Hirst, Police, Fire and Crime Commissioner for Essex, said: "Protecting those most vulnerable from harm and breaking the cycle of domestic abuse is so important. This money will make a huge difference to the services and support that we provide in Essex.

"We work hard across the county with our partner agencies to encourage survivors of domestic abuse and sexual violence to come forward. Investing in specialist support services like these will help survivors to move on and bring offenders to justice."

The PFCC has a responsibility to commission services to support victims of crime. The Commissioner places supporting victims at the heart of everything he does.

To support this, the Ministry of Justice provides a Victims' Grant which is used to commission Domestic Abuse, Sexual Abuse, and all other crime support services.

In May 2020, the Ministry of Justice secured £28 million from the Treasury to support services as they responded to the impact of COVID-19 and the public health restrictions that had to be put in place.

In Essex, the PFCC was successful in obtaining and distributing £717,273 of available funding. The funding awarded previously expired at the end of March this year.

Since this first round, the Ministry of Justice have announced further funding of £40m for victims. Support services have continued to remain open, responding and providing vital support to the victims of Essex throughout the pandemic and to ensure support continues to be available in 2021-22Essex funding is outlined below:

2021/22 Victims Grant Details:
Domestic Abuse £287,115
Sexual Violence £139,778
ISVA/IDVA Funding:
£500,820 for 2021/22
£554,023 for 2022/23

Jetaway is a charter for crooks

EVERYONE is dreaming of sun, sand and sangria after more than a year virtually prisoners in our own homes.

Now Action Fraud, the national reporting centre for fraud and cyber crime and ABTA, The Travel Association, are reminding the public to think twice before handing over their money and personal information when booking holidays this year.

In previous years, criminals have targeted unsuspecting holidaymakers booking airline tickets, holiday accommodation and religious pilgrimages.

Pauline Smith, Head of Action Fraud, said: "We are all more eager than ever to go on a holiday and relax with family and friends after the year we've all had.

"However, the surge in holiday bookings provides criminals with an opportunity to defraud innocent people out of a well-deserved break and their hard-earned cash.

"Criminals are increasingly using more sophisticated ways to trick their victims, which is why it's important that we all do our research when making travel arrangements."

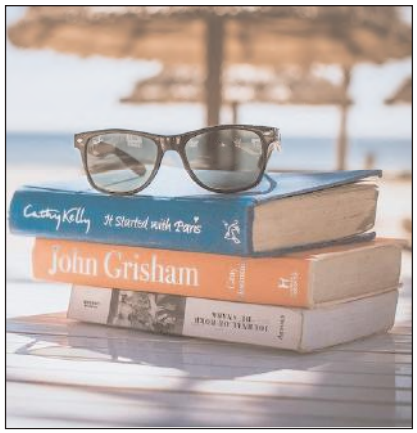
What is holiday fraud?

Holiday fraud can vary from fake accommodation listings advertising hotels, and self-catering properties that don't exist, to "too good to be true" offers with flights being particularly targeted.

"Criminals can approach you over the phone, via text, email and social media, offering incredibly cheap deals to tempt you into booking a holiday with them. In reality, the holiday you've booked, or parts of it, doesn't exist.

Tops tip to avoid falling victim to holiday fraud

- **Stay safe online:** check the web address is legitimate and has not been altered by slight changes to a domain name – such as going from .co.uk to .org.
- **Do your research:** don't just rely on one review – do a thorough online search to ensure the company is credible. If a company is defrauding people, there is a good chance that consumers will post details of their experiences, and warnings about the company.



- **Look for the logo:** check whether the company is an ABTA Member. Look for the ABTA logo on the company's website. You can verify membership of ABTA online on their If you're booking a flight and want more information about ATOL protection, or would like to check whether a company is an ATOL holder, visit the CAA website.
- **Pay safe:** wherever possible, pay by credit card and be wary about paying directly into a private individual's bank account.
- **Check the paperwork:** you should study receipts, invoices and terms and conditions, and be very wary of any companies that don't provide any at all.
- **Use your instincts:** if something sounds too good to be true, it probably is.
- **Get free expert advice:** for further advice on how to stay safe when booking or researching travel online, go to Get Safe Online.

For a full list of tips to avoid becoming a victim of fraud, please visit https://www.abta.com/tips-and-advice/planning-and-booking-a-holiday/how-avoid-travel-related-fraud.

If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

ActionFraud

Advice Directory

Everywhere you go criminals are ready to steal your money, in many cases your life savings. They pose as police officers, bankers, roofers, builders, energy suppliers and other utility companies.

Some even contact you on the internet from far flung countries posing as foreign officials or

Telephone scams

A PHONE scam is when someone calls pretending to be someone else, such as the police or your bank. They do this so that they can trick you into revealing personal details, withdrawing money or transferring money to a fake account.

Follow our advice

■Always stay alert when someone you don't know calls you – no matter who they claim to be or what number is showing on the caller display.

■If in doubt, call back on a phone number that you know is official. You can usually find this on the company's website or on your statement or bills.

■If you get an automated call from a fraud-detection service, use our telephone number checker to check the number you've been asked to call is genuine

■If you run a business, look out for fraudsters impersonating your customers or suppliers. They may ask you to make a payment or change payment details. If you're suspicious, call them back on a number you're sure is genuine

■Never share your PIN, PINsentry codes, passwords or other confidential information with someone who calls you – if someone does ask for this information, end the call.

■Never enter your PIN into a telephone – it won't be kept secret from the caller

Treat all unsolicited calls with caution.

Remember, banks and the police will never ask you to transfer money, buy high value goods, or hand over cards or money.

Avoiding card scams

■ALWAYS shield your PIN when you're using your card

■Don't let anyone distract you when you're using your card in a shop or at a cash machine, even if they appear to be helpful

■Be wary if someone is looking over your shoulder, or saying something to distract you, as they may be trying to get your PIN or card

■Don't use a cash machine if it – or anyone around it – looks suspicious

■Sign new bank cards as soon as you get them and keep them in a safe place

■Never let someone take your card away to process a transaction

■Never hand your card over to anyone that comes to your door

■Never write your security or card details down in a way someone else might recognise

Check your card expiry dates and call us if a new card hasn't arrived when it should

■If you live in a property where other people have access to your mail, it may be better to collect new cards from your local branch

Report any lost or stolen cards immediately

Text scams

A TEXT message scam is when someone sends you a text asking you to call a telephone number, click on a link or to send security details.

The message might appear to be from a bank or someone you trust because fraudsters are able to spoof genuine telephone numbers to hide the true identity of the sender.

Our advice

■Never share personal or security information on a website you've been sent by text

■A bank will never text you asking you to confirm your account or security details

■Banks will never text you a link that goes straight to the online banking log-in page.

■They will never text or call to ask you for your card details, PINs, PINsentry codes or passwords

■They will never email you asking for confirmation of a recent transaction or call to get you how to respond to a confirmation text message.

Email scams

AN email scam is an unsolicited or trick email designed to look like a genuine company and make you hand over money or reveal personal details. Stay vigilant when emailing – especially if you're sending people personal details or organising financial transactions.

■Never share personal or security information via email, web chat or on a website that's been sent to you via email. Banks will never text you a link that goes straight to the Online Banking log-in page

■Act with care when clicking links or downloading attachments from unsolicited emails

■Check a website is secure before you enter any account or card details. Look for the `https' at the start of the web address and the padlock or unbroken key icon next to the address bar

■Keep your internet security software up to date, and run regular scans and system updates. If you use Barclays Mobile Banking or Online Banking, you can download Kaspersky security software for free

■If you're sending money using an account number someone has sent you by email, call them to double check it's correct and hasn't been intercepted

Distraction scam

A DISTRACTION scam involves someone trying to distract you while you're at a cash machine in order to get your PIN, card or money.

■Don't let anyone distract you when you're at a cash machine

■Cover your PIN when you pay in shops or go to a cash machine

■Ignore people who speak to you when you're at a cash machine – even if they appear to be helpful

■Don't use a cash machine if it, or anyone around it, looks suspicious

■Call your bank straightaway if you think your card, PIN or other security details have been compromised.

Vishing

VISHING is similar to phishing but involves a phone call from a fraudster who will come up with a plausible story to try to get you to share your information.

For example, the fraudster may say they're from a satellite TV provider, phone or utility company and offer you a refund.

To process the refund, they'll ask you to input your debit card into your PINsentry card reader and give your authorisation codes.

They'll then use the codes to make fraudulent online banking payments from your account.

Fraudsters also call pretending they're the bank or the police and tell you there's a problem with your debit or credit card.

They may ask you to key your card PIN into the phone and tell you they are sending a courier to collect your card.

Alternatively, they may ask you to withdraw funds or buy high-value items and hand them to a courier to help in an investigation, or even try to convince you to transfer funds to a new 'safe' account.

Security tips

■Never share your PIN, PINsentry codes or passwords with anyone who contacts you

Banks and the police will never ask you to hand over your PIN, cards or cash, or buy high-value items or transfer funds to a new account. If someone calls asking you to do this, ring off immediately.

■Don't rely on the caller display on your phone to confirm a caller is genuine – fraudsters can

Government agents claiming they have millions of pounds for you providing you can hide their money away from officials.

Others knock on your door offering to carry out building work then disappear with your money without completing all the work. Follow our advice so you don't become a victim.

Advice Directory

ActionFraud

items or transfer funds to a new account. If someone calls asking you to do this, ring off immediately.

■Don't rely on the caller display on your phone to confirm a caller is genuine – fraudsters can manipulate this

■Always check the call is properly disconnected before calling the bank or police to report it – wait 5 minutes or use a different phone

Malware

OTHER emails and texts trick you into downloading malicious software (malware) that helps fraudsters get hold of your details and your money.

The messages look like they're from legitimate organisations and give a plausible story to try to trick you into clicking a link, downloading something or opening an attachment.

Security tips

■Protect your computer and mobile devices with the most up-to-date security software such as our free Kaspersky Internet Security software

■Keep your important files backed up off your network

■Be wary of opening attachments or links in emails or texts you're not expecting or are unsure about

■Never share any security information in response to an email or text or on a site accessed via a link in an email or text

Romance scams

DATING or romance fraud is when you think you've met your perfect partner online, but they aren't who they say they are. Once they've gained your trust, they ask for money for a variety of emotive reasons.

You register with an internet-based dating agency or join an online dating chat room. You receive a contact from someone who shows an interest in you. They may be from overseas, or they might tell you they are in the same country as you.

Gradually, you develop a long-distance relationship through emails, instant messaging, texting and phone calls. As the relationship develops, exchanges become more intimate.

The person you have fallen for will probably send you their photograph and give you a pet name. They may also ask you for naked photos of yourself and/or ask you to perform sexual acts in front of a webcam, particularly if you are female.

The person you've developed a relationship with is not who they say they are. In fact, you have probably been in contact with several members of a criminal gang.

Once the fraudsters are confident that you have enough sympathy and desire for them, they will tell you about a problem they are experiencing and ask you to send money.

If you send money, the fraudsters will keep coming back for more money money. If you send pictures of a sexual nature, the fraudsters will threaten to send them to your family, friends and work colleague. If you've recorded any sexual acts in front of a webcam, the fraudsters will also use these to threaten you.

Phishing

PHISHING is where fraudsters send you emails or texts, often appearing to be from your bank, asking you to reply with your security information or click on a link, where they can then access your details. These emails often look like a genuine company, but they are fakes.

Text messages may ask you to call a number claiming to be the bank's fraud department, but the number is often a premium rate number and connects you to a fraudster.

Fraudsters may also send a text warning that you'll soon receive a call from the bank's fraud department. However, it's actually the fraudster that calls and tries to get your security information.

To make the texts seem authentic, fraudsters use special software that changes the sender ID on a message, so that you see the name of your bank as the sender. This can mean the text shows within an existing text message thread from your bank.

Pension scams

PENSION scams typically involve promises of pension investment opportunities or unsolicited offers to help you release cash from your pension early.

With over 55s getting greater access to their retirement savings since April 2015, there are more opportunities for investment scammers to convince people to invest their pension pots in unregulated or bogus schemes.

Anything claiming you can cash in your pension before you're 55 is also likely to be a scam. and early pension release may cost you most of the money in your pension fund.

Ignore offers of a 'free pension review' and calls out of the blue to discuss your pension.

■Never be rushed into agreeing to a pension transfer or investment decision, and always speak to a financial adviser who is registered with the Financial Conduct Authority.

Online shopping scams

SCAMMERS will advertise goods/services that don't exist or are not theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive.

Before buying online, do some research into the seller to check they're genuine and avoid those with poor ratings.

■Insist on seeing high-value items, like cars on online auction sites, before paying and always use secure payment methods, such as PayPal or credit card.

■Use a computer, laptop or mobile device protected with up-to-date security software

■Know who you're buying from before giving your card details online or over the phone Register for Verified by Visa and/or MasterCard Secure Code

■ Enter your card details on secure sites – check the web address begins with 'https' and that there's an unbroken padlock symbol in the browser address bar

■Avoid entering your card details on shared or public computers

■Always log out after shopping and save the confirmation email as a record of your purchase

Travelling abroad

■NOTE your bank's 24-hour emergency number if you're calling from outside the UK

■If your cards are registered with a card protection agency, take their number too

■Take another card or alternative payment method with you so that you're not reliant on one card

■Check the information on the sales voucher before you sign or enter your PIN

■Keep a copy of your sales receipts and check your statement carefully .

WARNING OVER WATER SAFETY THIS SUMMER

SCHOOLS will soon be breaking up for the summer holidays and as Covid restrictions ease that means many pupils will be heading for coastal location and inland water beaty spots.

That also means they will be faced with many dangers and unless they are alert an aware they could be putting their lives at risk.

Few people would think they might become a water incident statistic. But the fact is in the UK in 2019 more people died from accidental drowning than cyclists did on the road...a truly startling statistic.

The National Fire Chiefs Council's (NFCC) Be Water Aware campaign, which took place in May, offers help and advice that should be taken on board anytime of the year.

County Fire and Rescue Services took part in events to encourage people not to be complacent when spending time in and around water. The aim is to encourage people to be safe by being aware of the risks.

Following simple advice will help to reduce the 223 accidental drownings reported in 2019 and the many more injuries, which can be lifechanging, following avoidable water related incidents.

The advice includes:

■ Never swim alone in case you need help

■ Don't drink alcohol when undertaking water related activities, it impairs judgement and your ability to swim

■ Avoid walking routes near water if you have been drinking alcohol

■ Don't dive or jump straight into open water, this can cause potentially fatal cold water shock even on the warmest day

■ Actively supervise children in and around water - drowning can happen fast and silently

■ If you find yourself unexpectedly in the water, don't panic, extend your arms and legs out and float on your back until the effect of cold water shock pass

■ Never enter the water to try and rescue someone, call 999 and ask for the Fire Service if inland and the Coastguard if you are at the coast.

A member of the Fire Service Water Safety service: "Most people don't think of the fire service when it comes to water rescues, but it's an important part of our work which is why we want people to enjoy spending time in and around water safely.

"Firefighters and Community Safety Officers have been out around the country at locations we've identified as being high risk for water incidents.

"If you see our crews, please do come over and say hello and find out more about how you can keep yourself and family safe around water.