CLEVELAND POLICE

Cyber Crime Newsletter

September 2021

Contents

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

Warning from Action Fraud as criminals continue to target the elderly

ALERT 20-09-2021

Action Fraud is warning the public to protect their loved ones as criminals cheat older and vulnerable victims out of cash and high items through courier fraud.

Data from Action Fraud, the national reporting centre for fraud and cyber crime, reveals that £10,325,133 has been lost by victims to courier fraud since the start of this year – an increase of almost two thirds (63 per cent) compared to the same period last year.

What is courier fraud?

Courier fraud is when victims receive a phone call from a criminal who is pretending to be a police officer or bank official. Typically, victims are told to withdraw a sum of money and someone is sent to their home address to collect it.

Criminals may also convince the victim to transfer money to a 'secure' bank account, hand over their bank cards or give the criminals high value items, such as jewellery, watches and gold (coins or bullion).

Temporary Detective Chief Inspector Craig Mullish, from the City of London Police, said:

"This is a dreadful crime in which fraudsters specifically target older and vulnerable people, by exploiting their trust. Courier fraud can have devastating consequences on victims, both financially and emotionally, which is why we're asking the public to remain vigilant and follow some simple steps to help protect themselves and their loved ones.

"Remember, just because someone claims to know a few basic details about you, such as your name and your address, it does not mean they are genuine."

Since the start of this year, Action Fraud has received 2,060 reports of courier fraud, with an average loss per victim of just over £5,000.

Almost two thirds (64 per cent) of victims were aged 70 to 89 years old, and over three quarters (84 per cent) of victims were aged 60 to 99 years old.

One common tactic used is where victims are contacted by a suspect who attempts to persuade them to purchase gold as part of a 'police investigation' that is later collected by a courier on behalf of the criminals.

In some cases, the suspects have invited themselves into the victim's home and collected other valuables, saying that the victim's possessions are no longer safe and they, 'as the police', can safeguard them.

Back to Top

Another common tactic used is called “open phone” where the victim is persuaded to stay on the phone to the criminal whilst they go to withdraw money or go to a jewellers. This stops the victim interacting with anyone else, or having the chance to think about what is really happening.

How to protect yourself and your loved ones:

- Your bank or the police will never call you to ask you to verify your personal details or PIN by phone, or offer to pick up your bank card by courier. Hang up immediately if you receive a call like this.
- If you need to contact your bank to check the call was legitimate, wait five minutes as fraudsters may stay on the line after you hang up. Alternatively, use a different line altogether to contact your bank and ensure you call them back on a number listed on the bank’s website, or on the back of your debit or credit card.
- Your debit or credit card is yours: don’t let a stranger take it from you. You should only ever have to hand it over at your bank. If it’s cancelled or expired, you should destroy it yourself.

Tell-tale signs of attempted courier fraud:

- Someone claiming to be from your bank or local police force calls you to tell you about fraudulent activity, but is asking you for personal information, or even your PIN, to verify who you are.
- They are suggesting that you call them back, so you can be sure they are genuine, but when you try to return the call, there’s no dial tone.
- They say they are trying to offer you peace of mind by having somebody pick up the card for you, to save you the trouble of having to go to your bank or local police station.

Action Fraud also advises that the public follow the advice of the Take Five to Stop Fraud campaign to keep themselves safe from fraud.

- **Stop:** taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** could it be fake? It’s okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** 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.

For full details, please visit: www.actionfraud.police.uk and select ‘Newsroom’ followed by ‘News’

Beware of NHS COVID pass fraud

ALERT 17-09-2021

Back to Top

Criminals are using the NHS COVID Pass as a way to target the public by convincing them to hand over money, financial details and personal information
They are sending imitation text messages, emails and making phone calls pretending to be from the NHS, and offering fake vaccine certificates for sale online and through social media.

If you are contacted about your NHS COVID Pass:

1. Be alert to links and attachments in unexpected text messages or emails
2. Do not respond to requests for money, passwords or financial details
3. Challenge: Could it be fake?
4. Use the official NHS COVID Pass website (see below)

The NHS COVID Pass is available to demonstrate your COVID-19 status either in a digital or paper format via the NHS App, the NHS website or by calling 119.

For information on how to get your **free** NHS COVID Pass, visit www.nhs.uk/nhscovidpass.

What to do if you suspect you have been a victim of an NHS COVID Pass scam
If you receive a call and suspect it to be fraudulent, hang up. If you are suspicious about an email, forward it to report@phishing.gov.uk. If you are suspicious about a text message, forward it to the number 7726, which is free-of-charge.

If you believe you are the victim of a fraud, please report this to Action Fraud as soon as possible by visiting actionfraud.police.uk or calling 0300 123 2040.

If you have any information relating to NHS COVID Pass or vaccine certificate fraud you can stay 100% anonymous by contacting Crimestoppers online at covidfraudhotline.org or phone on 0800 587 5030.

For details please visit: https://www.actionfraud.police.uk/news

---

HMRC warns students of scams

ALERT 09-09-2021

HMRC is warning university students to be wary of potential scams, especially if they have a part-time job and are new to interacting with the department.
University students taking part-time jobs are at increased risk of falling victim to scams, HM Revenue and Customs (HMRC) is warning.

Higher numbers of students going to university this year means more young people may choose to take on part-time work. Being new to interacting with HMRC and unfamiliar with genuine contact from the department could make them vulnerable to scams.

In the past year almost one million people reported scams to HMRC.

Back to Top

Nearly half of all tax scams offer fake tax refunds, which HMRC does not offer by SMS or email. The criminals involved are usually trying to steal money or personal information to sell on to others. HMRC is a familiar brand, which scammers abuse to add credibility to their scams.

Links or files in emails or texts can also download dangerous software onto a computer or phone. This can then gather personal data or lock the recipient's machine until they pay a ransom.

Between April and May this year, 18 to 24-year olds reported more than 5,000 phone scams to HMRC.

Mike Fell, Head of Cyber Security Operations at HMRC, said:
"Most students won't have paid tax before, and so could easily be duped by scam texts, emails or calls either offering a 'refund' or demanding unpaid tax.
"Students, who will have had little or no interaction with the tax system might be tricked into clicking on links in such emails or texts.
"Our advice is to be wary if you are contacted out of the blue by someone asking for money or personal information. We see high numbers of fraudsters contacting people claiming to be from HMRC. If in doubt, our advice is – do not reply directly to anything suspicious, but contact HMRC through GOV.UK straight away and search GOV.UK for 'HMRC scams'."

In the last year (September 2020 to August 2021) HMRC has:

- responded to 998,485 referrals of suspicious contact from the public. Nearly 440,730 of these offered bogus tax rebates
- worked with the telecoms industry and Ofcom to remove 2,020 phone numbers being used to commit HMRC-related phone scams
- responded to 413,527 reports of phone scams in total, an increase of 92% on the previous year. In April last year we received reports of only 425 phone scams. In August 2021 this had risen to 3,269
- reported 12,705 malicious web pages for takedown
- detected 463 COVID-19-related financial scams since March 2020, most by text message
- asked Internet Service Providers to take down 443 COVID-19-related scam web pages.

By June this year, more than 680,000 students had applied to university, and over 900,000 held part time jobs during the 2020 to 2021 academic year.

Further information

More information on how to recognise genuine HMRC contact and how to avoid and report scams.

Forward suspicious emails claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599. Report scam phone calls via GOV.UK.

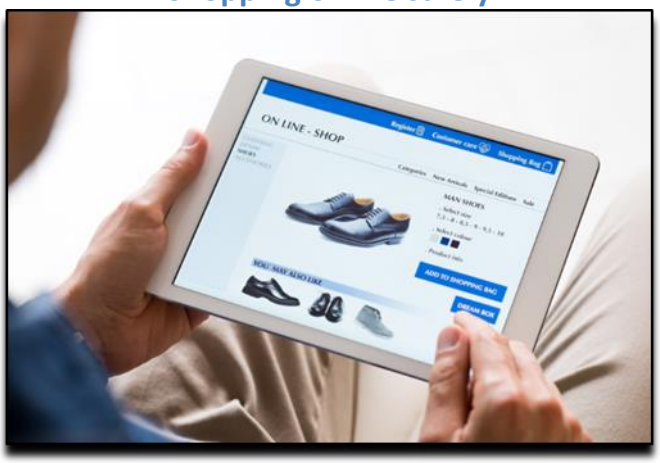
Data about student university applications.

Data on part-time student employment.

For more information and guidance please visit: https://www.actionfraud.police.uk/news

Back to Top

Shopping online safely



Top tips to shop online securely.

Figures reveal reports of online shopping fraud have surged by 30% over the pandemic as many of us continue to shop online in light of current restrictions. Action Fraud is warning the public to take extra care when shopping online.

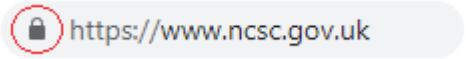
Choose carefully where you shop

It's worth doing some research on online retailers to check they're legitimate. Read feedback from people or organisations that you trust, such as consumer websites.
Some of the emails or texts you receive about amazing offers may contain links to fake websites. If you're unsure, don't use the link, and either:

- type a website address that you trust directly into the address bar
- search for it, and follow the search results

Use a credit card for online payments

Use a credit card when shopping online, if you have one. Most major credit card providers protect online purchases, and are obliged to refund you in certain circumstances. Using a **credit** card (rather than a **debit** card) also means that if your payment details are stolen, your main bank account won't be directly affected.
Debit card payments and purchases are **not** covered by section 75 of the Consumer Credit Act. But you might be able to make a claim for a refund under a voluntary scheme called 'chargeback'.
You should also consider using an online payment platform, such as PayPal, Apple Pay or Google Pay. Using these platforms to authorise your payments means the retailer doesn't even see your payment details. They also provide their own dispute resolution should anything go wrong. However, they may not provide the same protection as a card provider, so check their terms and conditions before your sign up.
When it's time to pay for your items, check there's a 'closed padlock' icon in the browser's address bar. It will look like this:



The padlock icon doesn't guarantee that the retailer itself is legitimate/reputable (and that their website is secure). It means that the *connection* is secure.
If the padlock icon is **not** there, or the browser says **not secure**, then **don't** use the site. Don't enter any personal or payment details, or create an account.

Only provide enough details to complete your purchase

You should only fill in the **mandatory** details on a website when making a purchase. These are usually marked with an asterisk (*), and will typically include your delivery address and

Back to Top

payment details. You shouldn't have to provide security details (such as your mother's maiden name, or the name of your first pet) to complete your purchase.
If possible, **don't** create an account for the online store when making your payment. You can usually complete your purchase without having to create an account, or by using an online payment platform (such as PayPal). If you think you'll become a regular customer with the store, then you may want to create an account with them.
The store may also ask you if they can save your payment details for a quicker check-out next time you shop with them. Unless you're going to use the site regularly, **don't** allow this.

Keep your accounts secure

If you're using the same password for your online accounts (or using passwords that could be easily guessed), then you're at risk. Hackers could steal your password from one account, and use it to access your other accounts. For this reason, you should make sure that your **really important accounts** (such as your email account, social media accounts, banking accounts, shopping accounts and payment accounts like PayPal) are protected by strong passwords **that you don't use anywhere else**.
The trouble is that most of us have lots of online accounts, so creating strong passwords for all of them (and remembering them) is hard. This NCSC infographic explains how you can create strong passwords and store them safely (so you don't need to remember them).
You can further protect your important accounts from being hacked by turning on two-factor authentication (2FA). It's also referred to as 'two-step verification' or 'multi-factor authentication'. Turning on 2FA stops hackers from accessing your accounts, even if they know your password. It does this by asking you to confirm that it's really you in a second way - usually by asking you to enter a code that's sent to your phone.

Watch out for suspicious emails, calls and text messages

You'll probably receive many messages from online stores, as a result of 'opting in' to receiving communications from them. Lurking amongst these genuine messages, there may well be fake ones (containing links designed to steal your money and personal details) that can be very difficult to spot.
Of course, not all messages are bad, but if something doesn't feel right, follow the NCSC guidance on dealing with suspicious emails, phone calls and text messages:

- If you have received an **email** which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at **report@phishing.gov.uk**.
- If you've received a suspicious **text message**, forward it to **7726**. It won't cost you anything, and allows your provider to investigate the text and take action (if found to be a scam).
- If you come across an **advert** online that you think might be a scam, report it via the Advertising Standards Authority (ASA) website. This allows ASA to provide online service providers with the details they need to (if appropriate) remove these from websites.

If things go wrong

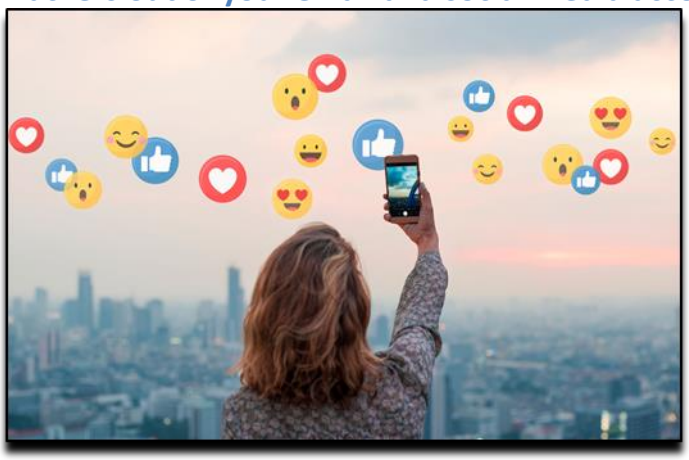
If you think your credit or debit card has been used by someone else, let your bank know straight away so they can block anyone using it. Always contact your bank using the official website or phone number. Don't use the links or contact details in the message you have been sent or given over the phone.
Back to Top
If you think you have responded to a suspicious email or text message, or visited a scam website, don't panic. Read the NCSC's guidance on dealing with scam emails, phone calls and text messages.
If you've lost money, tell your bank and report it as a crime to Action Fraud (for England, Wales and Northern Ireland) or Police Scotland (for Scotland). By doing this, you'll be helping to prevent others becoming victims of cyber crime.

If you don't receive the item (or it doesn't match the description given), Citizens Advice has some useful information about getting your money back if you paid by credit card, debit card or PayPal.

For full details, please visit: https://www.actionfraud.police.uk/shoponlinesafely

---

Keep hackers out of your email and social media accounts



If a hacker got into your email or social media account, what would they find? Health and banking information? Names and contact details for your friends and family? Private photos and messages? For most people, it's at least one of those.

Your email and social media accounts contain a wealth of personal information about you, which makes them a lucrative target for cyber criminals. Between February 2020 and February 2021, Action Fraud received 15,214 reports about email and social media account hacking. The majority of reports (88%) were made by individuals, with 12% of reports being made by businesses.

Analysis of the crime reports revealed that Facebook, Instagram and Snapchat were the most affected social media accounts, with phishing messages being the most common tactic used by cyber criminals to lure unsuspecting victims. The motivation behind the hacks are varied and can range from financial gain, to revenge or personal amusement. Some victims are extorted for money, whilst others have their accounts used to send malicious links to their contacts. One victim who had multiple email and social media accounts hacked paid over £2,000 to regain access to them. Another victim reported that her hacked Facebook account was used to trick her friends into sending money into a PayPal account they thought belonged to her.

Superintendent Sanjay Andersen, Head of the City of London Police's National Fraud Intelligence Bureau, said:
"Criminals hack people's email and social media accounts to access a wealth of valuable personal information about the individual, which they can use to commit fraud. This includes passwords for other accounts like online banking. Criminals also use compromised accounts to imitate the victim online and trick their family and friends into sending money.

"One of the most important things that you can do to improve the security of your online accounts is having two-factor authentication enabled. Not only will it prevent hackers accessing your accounts even if they have your password, but it will also keep your valuable information out of the hands of criminals."

Back to Top

How to keep hackers out of your email and social media accounts

1: Secure your email accounts
If a hacker gets into your email, they could:

- reset your other account passwords
- access private information such as contacts, messages or photos.

Your email password should be strong and different to all your other passwords. This will make it harder to crack or guess. Using 3 random words is a good way to create a strong, unique password that you will remember. Enable Two-factor authentication (2FA) in your email account settings, it will help to stop hackers from getting into your account, even if they have your password.

How to change your email password:

- Gmail (opens in a new tab)
- Yahoo! Mail (opens in a new tab)
- Outlook (opens in a new tab)
- BT (opens in a new tab)
- AOL Mail (opens in a new tab)

2: Enable two-factor authentication (2FA)
If a hacker gets into your social media account, they could:

- access private information such as contacts, messages or photos.
- send messages containing malicious links to your followers.
- trick friends or followers into sending them money by pretending to be you.
- extort you for money in exchange for restoring access to your account.

Use three random words to create a strong, unique password for your social media accounts. Enable Two-factor authentication (2FA) in your account settings, it helps to stop hackers from getting into your accounts, even if they have your password.

How to turn on two-factor authentication (2FA)

For email accounts:

- Gmail (opens in a new tab)
- Yahoo (opens in a new tab)
- Outlook (opens in a new tab)
- AOL (opens in a new tab)

For social media accounts:

- Instagram (opens in a new tab)
- Facebook (opens in a new tab)
- Twitter (opens in a new tab)
- LinkedIn (opens in a new tab)

Watch out for suspicious messages
Be cautious of social media messages that ask for your login details or authentication codes, even if the message appears to be from someone you know.

What to do if one of your online accounts has been hacked
If your email or social media account has been hacked, it's important that you act fast. Here's some useful information on the steps you can take to try and recover the account.

Report it
If one of your online accounts has been hacked, report it to Action Fraud by visiting www.actionfraud.police.uk, or calling 0300 123 2040.

Back to Top

Buying or selling a vehicle online can be risky.

Whether you're buying or selling your car, van, truck, motorcycle or other vehicle online, read Get Safe Online expert safety tips before you look or list.

There have always been risks associated with buying or selling a vehicle online. But recent increases in used car prices, limited availability of some models and restrictions to travel and accompanied test drives have created additional risks, giving fraudsters new excuses to deceive both buyers and sellers.

Now that things are returning to normal, it's easier for you to exercise more care when buying or selling your vehicle. Please take time to read these expert tips before you go online to buy or sell.

How can you tell what ads, vehicles, buyers and sellers are genuine?

Safe buying

Paying a deposit

If a deposit is requested or agreed, don't pay more than you are willing to lose and confirm with the seller that they will refund the deposit if you don't purchase the vehicle. Be wary of requests for up-front transportation fees, it could be a scam.

Always view the vehicle before paying the full amount

Research the seller as well as their vehicle. Try to ascertain that the vehicle actually exists. Most fraudulent sellers will try to persuade you to transfer money before you've even had sight of the vehicle, citing any one of a number of excuses. Often, they will insist on communicating only via email rather than on the phone.

Check that the price of the vehicle is in line with the market value

If the price, condition, specification or mileage of the vehicle seems too good to be true, that could indeed be the case. Research other similar vehicles or perform a free valuation on AutoTrader. If the vehicle is below market value, think twice. Ask the seller questions about its valuation, there may be genuine underlying reasons if the vehicle is under-priced.

Take the vehicle for a test drive

Thoroughly inspect any vehicle you are looking to purchase, and take it for a test drive. This should always be done from the seller's premises or their home; never let the person meet you by the roadside or any other random location. Also, consider an inspection by the AA, RAC o other reputable organisation offering the service.

Back to Top

Carry out a vehicle history check and inspection

This will tell you if the vehicle is recorded as stolen, written off, scrapped, or has outstanding finance. It's not worth the risk buying a vehicle that could be unroadworthy or worth a fraction of what you're paying for it. Check the service history and ask to see historic MOT certificates to

check that the milometer hasn't been adjusted. Make sure you know your statutory rights regarding quality and refunds, before parting with any money.

Making payment
Never send money for a vehicle you haven't seen. Don't carry large amounts of cash. Consider paying by bank transfer or credit card (if the seller offers the facility).

Safe Selling
Be prepared
Have all the relevant paperwork together, such as the V5C, service history and MOT certificate, for a potential buyer to review. Buyers may wish to check details such as the address on the V5C and the mileage in the most recent MOT certificate. Never let the buyer photograph your documents, in case the request is fraudulent.

Beware of scammers
Always meet the buyer. Request their contact details, such as their phone number and full home address, and proof of identity – a driving licence is ideal. This should give you further reassurances, and a legitimate buyer should be happy to provide this information.

Test drive advice
Make sure you ask the buyer to bring their driving licence and proof of insurance if they want to test drive the vehicle. Check their level of insurance to test drive, this should prevent you having to pay out for damages.

Never allow a buyer to test drive the vehicle alone
Never leave a potential buyer alone with the vehicle, nor give them the keys. If you have a keyless ignition fob, keep hold of it at all times, even on a test drive. Be aware that this type of vehicle is becoming increasingly stolen by thieves who only need to be near the fob and not actually in possession, you can buy a special pouch to protect this occurring. Never jeopardise your personal safety and if you feel uncomfortable at any time, walk away.

Stay on home ground
Always arrange to meet a buyer at your home; never meet at the roadside or at their premises.

Taking payment
Never release the vehicle until you have confirmation of cleared funds. If you accept a cheque or banker's draft for payment, be aware it can take days for funds to clear.
#autofraud

For full details, please visit: https://www.getsafeonline.org/autofraud/

NATIONAL TRADING STANDARDS

Protecting Consumers Safeguarding Businesses

News

Doorstep crime to rise as office return gathers pace

16-09-2021

Twin threats to vulnerable as criminals resume doorstep tactics whilst scaling up mass marketing scams; reports jump 76% during pandemic.

Back to Top

The current flow of people back to workplaces is leaving the elderly and vulnerable at renew risk from doorstep crime, according to new intelligence published by National Trading Standards (NTS). The annual NTS Consumer Harm Report reveals how criminals have adapted to the pandemic, sparking fears of a return to 'business as usual' on the doorstep as citizens have fewer opportunities to keep an eye on vulnerable neighbours.

Whilst doorstep criminals have continued to operate during the pandemic, data shows that lockdowns may have 'held them in check' as opportunities to pressurise people on their doorsteps – typically older people or those living alone – were restricted by more communities staying at home, more opportunities for neighbours to meet and informal befriending schemes set up to provide support. Doorstep crime complaints dropped significantly during the first lockdown* and overall the year 2020-21 saw a 3% decrease in reported incidents compared with 2019-20**.

But whilst doorstep crime and other pressurising tactics were curtailed in the height of lockdowns, criminals don't just stop operating – they adapt***. The new report shows starkly how criminals reacted to the restrictions, revealing a huge rise in mass marketing scams, with intelligence reports in this area increasing by 76% on the previous year†. Whilst mass marketing scams include postal mailings such as fake competitions and lotteries, the rise has been driven by criminals moving online and adapting their scams, such as by preying on people's fears about Covid-19 to sell fake medication to prevent or treat the virus. So-called 'Impersonation scams', where people receive texts, emails or calls that appear to be from trusted organisations such as NHS, HMRC or parcel delivery firms have also increased.

After the first lockdown doorstep crime reports did bounce back – with complaints to Citizens Advice more than doubling between the first and second quarters of 2020-21* – though the fact that 'working from home' largely continued is believed to have held numbers steady. NTS is concerned that seasoned criminals may not only revert to aggressive doorstep tactics as even more people head back to workplaces, but will continue to use lucrative skills learned during lockdowns to exploit the vulnerable in other ways.

Lord Toby Harris, Chair, National Trading Standards, said:
"Lockdown restrictions and a focus on protecting the vulnerable during the pandemic created a tougher environment for doorstep criminals. Whilst it's great that normality is returning for many, we must not forget those who will still be at home and who may be at risk from doorstep criminals looking to return to their aggressive ways.
"We're calling on communities to continue to look out for one another and to keep in contact with family and friends who may be at risk. If you see anything suspicious, report it to the Citizens Advice Consumer Service on 0808 223 1133.
"Equally challenging is the threat from criminals who have diversified into scams that don't involve face-to-face contact – they will certainly be maintaining and ramping up these other areas of criminality. As ever, our teams are working around the clock to stay ahead of the trends and stop the scammers in their tracks."

John Hayward-Cripps, CEO of Neighbourhood Watch Network, said:
"During lockdown, many of us felt more connected to our neighbours and a greater sense of belonging to our communities. As more of us now leave our homes for extended periods, the elderly and vulnerable may be feeling concerned that we could lose the valuable sense of community built up during the pandemic. It is important we continue to take moments out of our day to watch out and care for those in our communities, especially our elderly and vulnerable neighbours."

John Herriman, Chief Executive of the Chartered Trading Standards Institute, said:
"The changing national measures in response to the COVID-19 pandemic led to fraudsters demonstrating how quickly they can adapt their fraud campaigns to the situation at hand. During lockdown, we witnessed fraudsters pretending to be COVID-19 secure marshals to gain access to homes. It never ceases to amaze and appal me in equal measure the depths that some will go to rob people and especially during a time of unprecedented challenges.

Back to Top

"Today, consumer vulnerability is far more profound than many imagine and has devastating impact across all age groups and ethnicities. We need a new national conversation about consumer vulnerability and consumer protection, and CTSI will kick-start that conversation at this year's CTSI Symposium in Birmingham at the end of September."

Current and emerging threats related to doorstep crime:

- **Use of telephone calls, emails, leaflets and websites** to make initial contact with victims. Deceptive marketing may make them appear local.
- **Use of fake 'approved trader' websites**, which list supposed 'official' approved businesses when in fact the approval scheme is non-existent and most traders listed appear to be connected to known doorstep crime offenders.
- **Repeat victimisation** of the most vulnerable.
- **Links with organised crime** including money laundering and modern slavery.

Other emerging threats identified in relation to mass marketing and other scams:

- **Mass marketing scams** including mail scams for fake lotteries, competitions, clairvoyancy services etc., digital and telephone scams.
- **Impersonation scams**, where scammers pretend to be from trusted organisations to defraud consumers.
- **Clone websites** which mirror seemingly legitimate businesses.
- **Investment scams** promising high returns.
- **Fair Trading issues** associated with the ongoing pandemic, such as businesses not adhering to legislation and restrictions, and price-gouging, where businesses heavily inflate prices for everyday goods and services to exploit increased demand.
- **The UK's departure from the European Union** is a major policy change that will continue to provide opportunities for scammers to target SMEs.
- **The government's response to climate change** will continue to be exploited, for example criminals posing as part of official 'green' home improvement schemes.

If you or someone you know has been a targeted by a scam you should report it to **Action Fraud** online at www.actionfraud.police.uk/ or by calling **0300 123 2040**.

For advice and information on how to check if something might be a scam, visit: www.citizensadvice.org.uk/consumer/scams/check-if-something-might-be-a-scam/.

People can also protect their neighbours by joining Friends Against Scams, which provides free online training to empower people to take a stand against scams.

For full details, please visit: https://www.nationaltradingstandards.uk and select 'News'

Net Aware | O2 | NSPCC
Let's keep kids safe online

NEWS

A parent's guide to location settings

14-09-2021

On many of our app reviews we recommend switching off location settings for your child. This is because having them turned on could show your child's location, or frequently visited places to lots of people – either to all their contacts on a private profile, or to any user on a public profile

Back to Top

But are there times that you might want to allow an app to have access to location settings?

Many apps and games give users the option to share their location. You should sit down with your child and review the location settings on their favourite app or game and talk to them about what they're sharing online. Remind them, and explain why, they shouldn't share location on posts, or public forums and chats, videos or with people they don't know.

What apps allow you to share your location:

- Instagram
- Facebook
- Pokemon Go
- Snapchat
- and many more.

What are the risks of location sharing?

- If shared publicly, their location could be seen by someone they don't know.
- People could find out where they go to school or live.
- Allow accurate picture of movements / routine to be built up.

All of these things increase risk to children, of cyberbullying, stalking or unwanted contact (from friends or others) or becoming a target.

Is it ever ok to share your location?
Set some rules together around how and if they will use location sharing. If your child needs to walk home they might like to think that you can check where they are and welcome that you can track them on a private, secure app till they get home. You could also share your location with your child so that they can follow your journey – such as if you are out for a walk or run.

If your child is going out alone or travelling back from somewhere, encouraging them to share their location with you or other family members can be a good way to help keep them safe. However, if your family decides to use an app like this you should always speak to your child first and make sure they understand why it's necessary. Remember to check the age recommendation for any app too.

Here are some apps that you could discuss with your child to see if you want to use them.

Hollie Guard App

This app has lots of different features, from letting a contact know the journey you are planning and when you have reached your destination, to an emergency alarm and accident alerts. This could be very useful for older kids wanting more independence. Make sure to explore the app together and discuss how it works and what to do if they are unsure about any situation.

WalkSafe App

The WalkSafe app has local crime data available to allow users to plan a safer route home. You can plan arrival times and Check-Ins to be shared with chosen contacts with alerts if you don't arrive or check in at the arranged time. This app might be useful to check areas where you are spending time or walking through, but it might mean some people feel more anxious about what is happening around them.

WhatsApp

WhatsApp allows users to either share their current location, or share their live location with a contact. You could use this if your child was walking home and you both wanted some reassurance. This feature is end-to-end encrypted, which means no one can see your live location except the people you shared with.

There are other apps that are primarily for managing the use of a child's device, such as wha content or apps they can access, or who they can call and message, that also have location tracking included. If you decide to use one of these, be honest with your child and discuss wny you feel that you need to use the features of the app. We wouldn't recommend using these apps without talking about it with your child – open conversation is a better option.

Back to Top

It is a good idea to regularly review settings on your child's phone to see which apps have access to location and to check if those apps share any info publicly. And while you are talking

with your child about location settings, remind them to be careful not to share their location in content they are sharing. Ask them to think about if they show street names, school badges etc. in pictures or videos they are posting.
You might find going back over the **tips to setting up your child's device** helpful.

Stay up to date
Get emails on the latest social networks, apps and games your kids are using, so you're always up to date.
To signup please visit - https://www.net-aware.org.uk/newsletter

For full details, please visit: https://www.net-aware.org.uk/news/a-parents-guide-to-location-settings/

Net Aware
Apps, games and social media sites

We've reviewed the most popular apps, games and social media sites your kids are using

PlayerUnknown's Battleground (PUBG) Mobile			
Like Fortnite, PUBG Mobile is a battle royale shooter and fighting game. Teams of up to 4 players battle to be the last one standing. It contains more gore than Fortnite and there might be some inappropriate content in the chat.			
Official age rating	13+	**Net Aware age recommendation**	16+
Kids use this to : Play and Connect			
Net Aware Safety ratings		**Overall safety rating :** Poor	
Safety features As the game is rated 16+ there are no parental controls available. You can switch off the chat function but this has to be done on each individual game.	**Privacy & location** Because the game requires people to play in teams, there are limited privacy settings available. However, you can set the visibility of your profile to private so other people can't add you. Only your nickname will appear to other players and it's up to the user how much information they share in the chat box.	**Reporting & blocking** The reporting and blocking tools are very limited and you can only block or report users you're friends with. This means your child could see something inappropriate on a public chat box, but would only be able to report it, if they added the user as a friend. To report users you aren't friends with you need to contact Customer Support.	**Content** The game features violence and weapons that some children might find upsetting. There might also be a risk your child could come across inappropriate language via the chat function.
02 Guru top tip On PUBG blocking users Show your child how to report and block other players in a chat by clicking on their name. Remind them they can talk to you if anything on PUGB upsets them			

Back to Top

Visit the Net Aware website and review the app, game or social media site that your child is using – visit https://www.net-aware.org.uk/networks/

Top tips for staying safe

Explore it together

Sitting down with your child and exploring their favourite app or game is a great way for you to learn more about what they like to do online.
You can ask them why they like to use an app or play certain games, as well as who they're talking to and what sorts of things they're sharing.
You can also read our **Net Aware reviews** for tips on how to keep kids safe on popular apps, sites and games.

Talk to your child about what they're sharing

Help your child think about what they share online and who sees it. Compare it to what they would be happy to share offline.
Use examples that are easy for them to understand: "You shouldn't give your number to somebody you don't know on the street. Is somebody online you don't know any different?"
Listen to their answers. And be positive and encouraging.
Remind them that they shouldn't share private things, such as:

- personal information, like names, emails, phone numbers, location and school names
- other people's personal information
- links to join private group chats
- photos of themselves
- photos of their body, such as sexual photos or videos.

Let your child know they can talk to you

Explain that you understand the internet is a great place to play, create, learn and connect. But remind them they can talk to you if anything upsets or worries them.
Reassure them that you won't overreact – you're just looking out for them.
It's important to remind your child that they can talk you, another adult they trust, like a teacher, or **Childline** about anything they see online.

Check the age rating of the game

Always check the age ratings of games. You can usually find this on the official site or wherever you downloaded the app.
Most games should have a PEGI rating which represents the recommended minimum age a player should be based on the content and themes of the game. But PEGI ratings don't consider communication features, such as chat. You can find more info on the **official PEGI site**.

Remember that age ratings are a general guide and don't cover everything. It's important to check the game out for yourself before letting your child play it. And you know your child better than anyone, so think about whether it's suitable for them as an individual.

Show them how to report or block other users

Your child might come across upsetting or negative things while playing. If this happens, they might want to report or block them.
There's a report button within the game that you can use if somebody is being inappropriate or abusive. You can also report and block other players in a chat by clicking on their name.
And remember to let your child know that they can always talk to you about worrying things they see online.

Back to Top

Talking to your child

Having open, regular conversations with your child will help you to really understand and explore the online world together. Our tips and advice can help you start these conversations.
Talk about staying safe online

Cyber Choices: Helping you choose the right and legal path

The Cyber Choices programme was created to help people make informed choices and to use their cyber skills in a legal way.
This is a national programme co-ordinated by the National Crime Agency and delivered by Cyber Choices teams within Regional Organised Crime Units and Local Police Force Cyber Teams.

The aims of the programme are to:

- Educate on the Computer Misuse Act 1990 and the possible consequences should they break the law.
- Encourage individuals to make informed choices about their use of technology
- Deter and/or divert individuals from cyber crime
- Promote legal and positive cyber opportunities

What you need to know
So what is cyber crime?
Cyber offences are committed when someone is using a computer or other digital technology. There are two main types of cyber offences - There's 'Illegal hacking' also known as cyber-dependent crime, where someone gains access to another person's computer network or device without permission. The other type is where technology has been used to enhance another crime, like fraud. This is also known as cyber-enabled crime.

Examples of illegal hacking/cyber-dependent crime include:

- Adam watches a friend entering their username and password. Adam remembers their login details and without their permission, later logs in and reads all their messages.

- Raj's Teacher leaves their tablet on their desk. Without their permission, Raj accesses their online shopping account and buys items with the attached credit card.

- Sarah is playing an online game with a friend who scores higher than her. Sarah uses a 'Booter' tool knowing it will knock them offline, so she can win the game.

- Kim hacks a phone company. This hack stops some people phoning the Police when they are in danger. They didn't mean for this to happen but they were reckless.

- Robin downloads software so they can bypass login credentials and hack into a friend's laptop, however they've not had a chance to use it yet.

Back to Top

Are you a parent, guardian, carer or teacher? Click here to find out more, or visit
https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices#Parent

Unfortunately the digital world can be tempting for young people for the wrong reasons. Many are getting involved in cyber crime without realising that they are breaking the law. This can have serious consequences for someone's broader future and not just their career. Cyber

crime is taken very seriously by law enforcement. So make sure you're aware of the debuffs to your future that can come with committing cyber crime, and boost your skills so you can level up, in a legal way.

Consequences
Make no mistake, cyber crime is a serious criminal offence. Law Enforcement will make every effort to arrest and prosecute offenders.
Anyone (including young people) who commits cyber crime could face:
- A visit and warning from police or NCA officers
- A Cease and Desist visit from police or NCA officers
- Computers being seized and being prevented from accessing the internet
- A penalty or fine
- Being arrested
- Up to life in prison for the most serious offences

You really don't want a permanent criminal record, which could seriously affect your education and future career prospects. You also wouldn't want anything that might hinder any potential overseas travel you have in mind.

So if you want to level up your knowledge of cyber crime, make sure you're fully aware of the Computer Misuse Act.

To view the Cyber Choices Level up Campaign Video please visit -
https://www.youtube.com/watch?v=j9TExA67XNY

Resources
Using cyber skills positively
With great tech knowledge, comes great responsibility, and great opportunities too. People with impressive cyber skills are in high demand. Not just in the UK but also abroad, which means that young people may have an opportunity to travel to new places whilst learning new cyber skills. Plus you get to the chance to play with all the latest tech whilst making a name for yourself in the digital space. So if you're interested in tech, don't miss your chance to level up. The Cyber Choices programme was created to help people make informed choices and to use their cyber skills in a legal way. If you're looking for more information specific to you, then download one of these helpful leaflets.

- pdf Under 12 years old (1.57 MB)
- pdf 12 to 17 years old (4.25 MB)
- pdf Over 18 years old (1.44 MB)
- pdf Introduction to the Computer Misuse Act 1990 (426 KB)
- pdf Developmental Resources (338 KB)

Resources
People with impressive cyber skills are in high demand. Not just in the UK but also abroad, which means that young people may have an opportunity to travel to new places whilst learning new cyber skills. The Cyber Choices Network was created to help people make informed choices and to use their cyber skills in a legal way. If you're looking for more information specific to you, then download one of these helpful leaflets:
pdf Parents/Guardians/Carers Leaflet (1.87 MB)
pdf Teachers Leaflet (1.96 MB)
pdf The Law and Consequences of Breaking It Leaflet (426 KB)
pdf Development Resources Leaflet (338 KB)

Back to Top

For further information please visit the NCA website https://nationalcrimeagency.gov.uk/ and search **Cyber Choices**
Alternatively click this link

If you're worried about someone, speak to them about legal ways for using technology and the internet, the consequences of cyber crime and show them positive ways to use their skills with resources above.
For further information, advice or assistance, please contact the Cyber Choices team at cyberchoices@nca.gov.uk

---

National Cyber Security Centre

NEWS

Email innovation simplifies takedown of cyber scams

Scam emails can be sent directly to SERS via a new button organisations can add to their Microsoft Office 365 accounts.

- One single click will flag scam emails to the National Cyber Security Centre
- Latest innovation in campaign that has received 6.5 million reports from the public and removed over 50,000 online scams
- Cloned login pages, spoofs of enterprise software and tricks to download malware bring cyber crime to the workplace.

CYBER experts have made it easier than ever for UK employees to join the fight back against email scams targeting their organisation.

In its latest bid to protect the UK from phishing scams, the National Cyber Security Centre (NCSC), a part of GCHQ, has today published guidance for IT administrators on a new reporting tool that can be added to their organisation's Microsoft Office 365 accounts.

By clicking the new button, employees will report potential scams directly to the NCSC's Suspicious Email Reporting Service (SERS) as well as their organisation's IT team. The automated NCSC service will process emails and take down previously unseen malicious content where found.

Since its launch in April 2020, the Suspicious Email Reporting Service has received over 6,500,000 reports from the public – resulting in the removal of more than 97,000 scam URLs. This July, it took just four hours on average to remove malicious URLs in phishing emails reported to the SERS.

NCSC Technical Director Dr Ian Levy said:
"Opportunistic scams during the pandemic have demonstrated how cyber criminals constantly find new ways to target us.
"The good news is that you can help protect your workplace by forwarding suspected scam emails to the Suspicious Email Reporting Service from your work email account at the click of a button.
"This simple technical innovation could enable millions more people to join our mission to stop scam emails from ever reaching UK inboxes."

Federation of Small Businesses National Chair Mike Cherry said:
"Innovations like this are crucial to calling time on business crime. Small achievable steps wi¨ go a long way to protect thousands of small firms from cyber attacks. Every year, there are almost four million cases of cyber attacks against small businesses in the UK, and more than 50 per cent of these come from phishing.
"We'd encourage as many small firms as possible to look further into this NCSC tool and see how they can implement it to protect employees as well as businesses from harm. And anyone

Back to Top

can take part, any small business, employee or self-employed person can forward attempted scam emails to **report@phishing.gov.uk**."
"These systems not only help prevent disruption to small firms today but will become increasingly important to help safeguard small businesses for the future."

Organisational filtering systems block most phishing attacks before they reach staff inboxes, but cyber criminals are innovative and some scam emails can bypass defences in place.

Typical phishing URLs identified by NCSC experts that target organisations in particular include;

- **Malware**: Employees will be tricked into downloading malware onto their work computer. They could unwittingly download malware from a scam URL emailed to them that appears to be operated by IT support.
- **Clone login pages**: Employees can unwittingly enter personal details into fake, but legitimate appearing, login page URLs sent via email.
- **Enterprise software spoofs**: Emails containing fake alerts from popular pieces of workplace software, such as Microsoft Teams, direct targeted employees to a legitimate appearing URL which harvest personal details.

The NCSC is taking unprecedented action to remove malicious scams from the internet as part of its Active Cyber Defence programme.

Working in partnership with the City of London Police, the NCSC is committed to protecting organisations from cyber crime, which cost over £5 million in the last 13 months.

Temporary Commander, Clinton Blackburn, of the City of London Police, said:
"Sadly, criminals will use every opportunity they can to trick people into handing over their personal and financial details. Phishing messages provide criminals with a gateway to obtain this information, which they will then use to commit fraud.
"This new reporting tool means that employees can protect their workplace by reporting phishing emails at the click of a button — which provides the police with more information about who is behind these crimes — preventing more people from falling victim."

Where organisations cannot install the button, employees are still be encouraged to forward or attach scam emails to send to **report@phishing.gov.uk**.

People can visit the Cyber Aware website to learn about the critical steps to take to stay secure online and fill out a Cyber Action Plan tool to generate some tailored cyber security advice.

For details, please visit: https://www.ncsc.gov.uk/news/email-innovation-simplifies-takedown-of-cyber-scams

---

Weekly Threat Reports

Back to Top

Weekly Threat Report 24th September 2021

Data of 106 million visitors to Thailand breached

A British cyber security researcher at Comparitech has discovered an unsecure database containing the personal information of millions of visitors to Thailand, including his own.

Inside the 200GB digital index were records dating back ten years containing the personal details of more than 106 million international travellers. As per the Comparitech report, anyone who has travelled to Thailand in the last decade may have been exposed to the incident.

The data breach has been reported to Thai authorities, who secured the database within 24 hours and stated the exposed data was not accessed by any unauthorised parties.

The NCSC has produced guidance which explains what data breaches are, how they can affect you and actions to take following a breach.

US issues alert on Conti ransomware activity

Earlier this week the US Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued an alert on the increased use of Conti ransomware.

The agencies revealed they had seen more than 400 attacks on US and international organisations, with actors gaining initial access to networks via spear phishing emails, fake software downloads and malicious Microsoft Word documents that contain malware.

While Conti is considered a ransomware-as-a-service (RaaS) model, it is noted that this model operates differently to others. It is reported that developers pay the deployers of the ransomware a wage, rather than a percentage of the proceeds from ransom payments. CISA, the FBI, and the National Security Agency (NSA) have outlined recommended mitigation measures, including the implementation of multi-factor authentication (MFA).

Ransomware is a serious cyber threat and it is vital that organisations familiarise themselves with advice and guidance on how to defend their networks.

The NCSC's Exercise in a Box helps organisations check their resilience against cyber attacks and practise their response in a safe environment.

We also encourage organisations to sign up to the NCSC's Early Warning service, which is designed to inform of potential attacks on your network.

VMware Security Advisory

The NCSC is aware of a number of vulnerabilities affecting VMware vCenter Server and VMware Cloud Foundation. The vulnerabilities include a file upload vulnerability that could lead to remote code execution (CVE-2021-22005).

Back to Top

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In this case, the most important aspect is to install the latest version as soon practicable.

More information regarding this advisory can be found on the VMware website.

Weekly Threat Report 17th September 2021

Financial services firms wounded by ransomware but show resilience compared to other sectors.

Ransomware is a serious and growing threat for a wide range of professional sectors. Financial services are no exception.

New research by Sophos has revealed that 34% of financial services firms were hit by ransomware in the last year – with attacks costing an average of $2.1 million.

51% of firms who fell victim said criminals successfully encrypted their data; 62% of these managed to restore this data by using backups.

Despite the large number of firms hit, financial services experienced a below average number of ransomware attacks. The survey shows 44% of retail firms and education firms were affected in the last year, business and professional services closely followed with 42% falling victim.

The survey also revealed that financial services have a below average tendency to pay ransoms. Only 25% of firms hit by ransomware paid out a ransom in the last year. The global average was 32%.

The NCSC has produced guidance for system owners on Mitigating malware and ransomware attacks guidance. Following the guidance will help organisations better defend against ransomware.

The NCSC's Cyber Security Toolkit for Boards can help business leaders to understand and mitigate the impact of ransomware and other malware on their organisations. There is a helpful blog post spotlighting the questions boards should be asking their technical experts to assure themselves that cyber security best practices are being implemented within their organisation.

Microsoft Security Updates

Microsoft released the September 2021 Security Update addressing a number of vulnerabilities, including a remote code execution vulnerability in MSHTML (CVE-2021-40444).

In addition, the Open Management Infrastructure software was updated to address a number of security issues.

Separately, Microsoft Exchange administrators should ensure they have updated to the latest available Cumulative Update (CU) and Security Update (SU). This will protect the server and server data from known vulnerabilities including ProxyLogon, ProxyOracle and ProxyShell.

Back to Top

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. The most important aspect is to keep technology updated – ideally automatically.

Weekly Threat Report 10th September 2021

Details of French visa applicants exposed

The details of more than 8,000 people who applied for French visas have been compromised following a cyber attack.

The attack struck a section of the France-Visas website which attracts around 1.5 million applications per month. The French Ministry of Foreign Affairs and Ministry of Interior announced in a statement that the attack had "been quickly neutralized" but personal details such as names, dates of birth, nationalities and passport numbers had been leaked.
They also stressed that no 'sensitive' data had been compromised in line with GDPR's definitions.
Data breaches can be concerning for those affected. The NCSC has published data breach guidance for individuals and families which sets out steps you can take to protect yourselves.

Phishing is a serious threat facing those who have had their data leaked in breaches such as this. If you're concerned about scam messages then we have produced advice on how to deal with suspicious messages you may receive.

Ransomeware group REvil resurfaces, according to reports

The REvil ransomware group appear to have resurfaced as several associated sites and their Happy Blog have come back online, according to reports.

The group appeared to go 'offline' in July following a ransomware attack upon Kaseya products which impacted organisations worldwide, including Coop supermarkets in Sweden and a number of schools in New Zealand. The group claimed responsibility for the attack which prompted global condemnation.

You can read more details about the attack in our Threat Report written back in July.

Ransomware is a common attack and a type of malware which can make data or systems unusable until the victim makes a payment. Paying a ransom of course does not guarantee the criminals will halt the attack.

The NCSC has produced guidance designed to help organisations defend themselves against malware and ransomware attacks.

Russian organisation reports successful defence against the largest known DDoS attack

The tech company Yandex has reported that they repelled the largest known Denial of Service (DDoS) attack in the history of the internet.

Back to Top

The DDos attack was said to have reached a record level on September 5 after initially starting in August.

Yandex reported that they repelled nearly 22 million requests per second at the height of the campaign.

You can read [NCSC guidance to help organisations understand and mitigate Denial of Service attacks here](#).

For details, please visit - https://www.ncsc.gov.uk and select Keep up to date then select Weekly threat reports

North East Cyber Protect Network

Cleveland Police Cyber Crime Unit are part of the North East Cyber Protect Network. We work with the North East Regional Special Operations Unit (NERSOU) and North East Regional Cyber Crime Unit (NERCCU) alongside neighbouring police forces, Durham Constabulary and Northumbria Police. Together we work to protect businesses and communities in the North East from common cyber attacks.

Did you know that the **Cleveland Police Cyber Crime Unit** can help your business learn more about protecting yourselves from cyber crime and the associated risks.

Below is a list of the services we offer, all free, and can be delivered online or face to face (restrictions allowing). For more information please contact;
cyber.protect@cleveland.pnn.police.uk

Cyber Basic Review –
Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation. If you are looking at Cyber Essentials or Cyber Essentials plus we can help you get certified.
Staff Awareness Training - We can talk about a whole range of topics, depending on your requirements and needs – current threats, how to spot phishing emails, why password security is important, staying safe at home, social engineering, device security and much more. We even offer a live hack demo to show how criminals can exploit vulnerabilities in out of date systems and software.

Vulnerability Assessment – Criminals use software to scan your network to look for weaknesses in your hardware or software, we are able to also do this to make you aware of where you are vulnerable to allow you to secure any weaknesses.

Cyber Exercising – Bespoke cyber incident exercise to test your responses in the event of an incident – the exercise tests your people and processes to help you ensure that everyone knows what they need to do should the worst happen.
Decisions & Disruptions – this is a game played with Lego that puts teams in charge of a company's security budget over a number of rounds. This is an interactive game that shows the consequences – good or bad from your decisions.
Police Cyber Alarm - Police Cyber Alarm (PCA) is a free to use tool aimed at helping businesses and organisations monitoring and understanding malicious cyber activity. PCA acts as a 'CCTV camera' by monitoring the traffic seen by your business' connection to the internet. It will detect and report on suspicious activity, enabling your business to minimise your vulnerabilities.

Back to Top

You can contact a member of our team on the following email address
cyber.protect@cleveland.pnn.police.uk

If you want to contact any of our colleagues in the North East Cyber Protect Network or just simply ask them a question, you can get in touch at nerccuprotect@durham.pnn.police.uk

---

EVENTS

Cybersecurity Awareness Month – October 2021

Previously known as National Cybersecurity Awareness Month and originated from the United States, specifically the department of homeland security and the National Cyber Security Alliance. Cybersecurity Awareness month is now recognised by many countries around the globe, the goal is to raise awareness of cybersecurity among people and businesses.

To help raise awareness and provide the most up to date cyber security advice, **Cleveland police** have a number of cyber security blogs on relevant and engaging topics. Keep an eye on our social media channels in October. The **Cyber Crime Team** will be giving advice on subjects including passwords, Two-Factor authentication (2fa), malware, patching and digital hygiene. Check out our Facebook and Twitter (@ClevelandPolice) pages.

TAKE FIVE

Take Five is a national campaign offering straight-forward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations.

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 and think. It could protect you and your money.

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

CHALLENGE
Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT
Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud

STOP AND THINK

1. Never disclose security details, such as your PIN or full banking password
2. Don't assume an email, text of phone call is authentic
3. Don't be rushed – a genuine organisation won't mind waiting
4. Listen to your instincts – you know if something doesn't feel right
5. Stay in control – don't panic and make a decision you'll regret

Back to Top

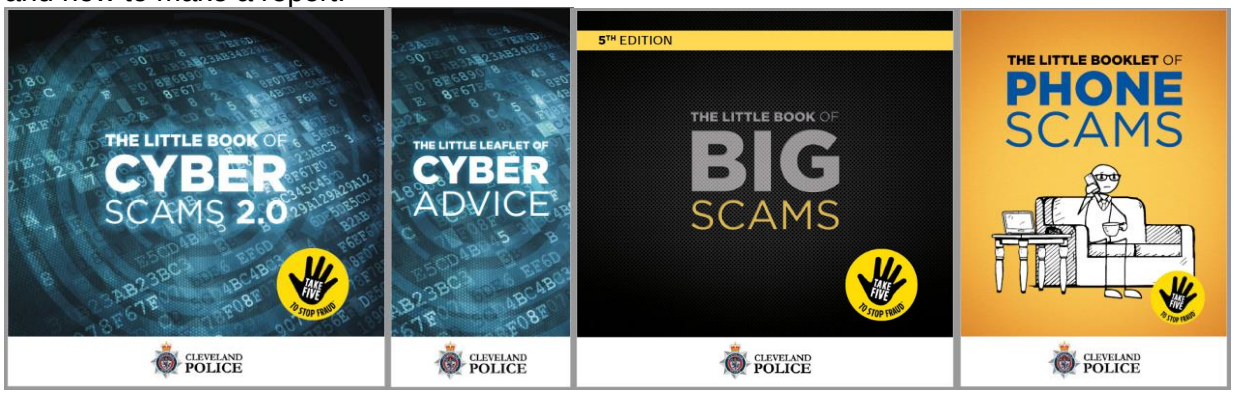
For further details visit www.takefive-stopfraud.org.uk

Information in this newsletter has been collated from following online sources;
www.actionfraud.police.uk
www.getsafeonline.org

www.nationaltradingstandards.uk
www.net-aware.org.uk/
www.nationalcrimeagency.gov.uk
www.ncsc.gov.uk
www.nerccu.police.uk
www.takefive-stopfraud.org.uk

Should you become a victim of online crime please contact your local force on **101.** You can also report via **Action Fraud** using their online fraud reporting tool at **www.actionfraud.police.uk.**
Alternatively you can report to **Action Fraud** and get advice by calling **0300 1230 2040.**
Cleveland Police are dedicated to working with you to reduce vulnerability to fraud, and to protect you from harm. We are pleased to offer you the **Little Book Series**.

The booklets will help you to identify frauds and give you advice on how to best protect yourself and how to make a report.



If you would like a copy please email the Cyber Crime Team email address below and we will send you a PDF copy via email or through the post.
Alternatively you can access the booklets by visiting the Cleveland Police website via the following links/ QR Codes

Booklet Title	Website Link	QR Code
The Little Book of Cyber Scams and **The Little Leaflet of Cyber Advice**	https://www.cleveland.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/	
The Little Book of Big Scams	https://www.cleveland.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/prevent-personal-fraud/	
The Little Book of Phone Scams	https://www.cleveland.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/internet-email-mobile-fraud/	

Back to Top

If you would like to be added to the mailing list to receive this monthly newsletter or if you have any queries and would like further details on any of the above please contact:

Cyber Crime Unit
Cleveland Police
cyber.crime@cleveland.pnn.police.uk

Middlesbrough Police Office **|** Bridge Street West **|** Middlesbrough **|** TS2 1AB
Website | Facebook **|** Twitter **|** Instagram | LinkedIn

CLEVELAND POLICE

Public Service | Transparency | Impartiality | Integrity

"Delivering outstanding policing for our communities"