CLEVELAND POLICE

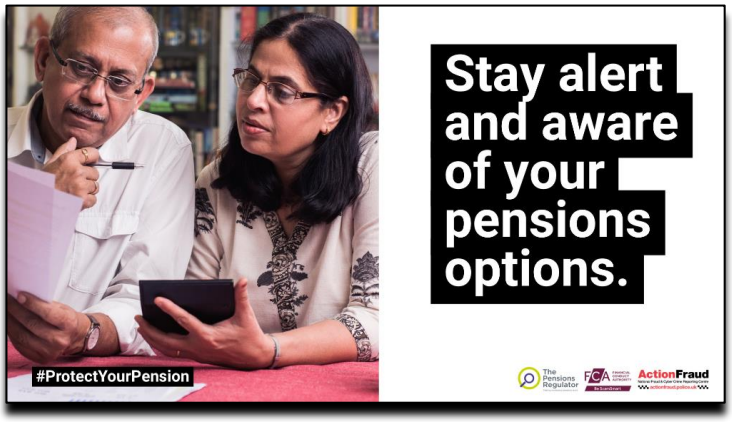
Cyber Crime Newsletter

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

WARNING from Action Fraud to #ProtectYourPension as £1.8 million lost to pension fraud so far this year.

ALERT 202-03-2021



Action Fraud is warning savers to remain vigilant and protect their pensions, as figures from the national reporting centre for fraud and cyber crime reveal £1.8 million has already been lost to pension fraud this year.

Data from Action Fraud shows a steady fall in pension scam reports from 1,788 in 2014 to 358 in 2020 – a reduction of almost 80 per cent.

However, there has been an increase in reporting so far this year, with 107 reports of pension fraud received in the first three months of 2021. This is an increase of almost 45 per cent when compared to the same period in 2020.

Action Fraud have launched a national awareness campaign (Tuesday 20 April 2021) to remind the public about the importance of doing your research before making changes to your pension arrangements.

Pauline Smith, Head of Action Fraud, said:

“Criminals are malicious and unapologetic when it comes to committing pension fraud. They are motivated by their own financial gain and lack any kind of empathy for their victims, who can often lose their whole life savings to these scams.

“We know pension fraud can have a devastating impact, both financially and emotionally, but any one of us can fall victim to a fraud and it’s nothing to feel ashamed or embarrassed about. It’s incredibly important that instances of pension fraud, and attempted scams, are reported to Action Fraud. Every report helps police get that bit closer to the people committing these awful crimes. Reporting to Action Fraud also allows our specialist victim-support advocates to provide people with important protection advice and signpost them to local support services.”

Pension scams often include free pension reviews, “too good to be true” investment opportunities, or offers to help release money from your pension even though you’re under 55.

Sadly, the true scale of pension fraud is likely to be much higher than what is being reported, as victims often don’t realise they have been scammed until many years later.

Nicola Parish, The Pensions Regulator’s Executive Director of Frontline Regulation, said:
“Pension scams are devastating with victims potentially losing life-changing sums.
“Savers must be cautious about making decisions about money that may have taken a lifetime to build, as it can be snatched away in an instant.
“Being ScamSmart and learning the signs of a scam can help prevent savers becoming a victim in the first place. Before making decisions about their pension savers should visit The Pensions Advisory Service website for impartial guidance or get financial advice from a FCA-authorised financial adviser.
“Savers should be able to be confident their pensions are secure. We want the pensions industry to help build that confidence by signing up our Pledge to Combat Pension Scams. By making the pledge, industry can show its intent to protect savers.”

Mark Steward, Director of Enforcement and Market Oversight at the Financial Conduct Authority (FCA), said:
“Scammers target people from all walks of life. It doesn’t matter the size of your pension pot, scammers destroy retirement dreams so it’s vital that consumers know how to protect themselves from scammers.
“The best way to protect yourself is to know who you’re dealing with. Always check the FCA Register to make sure that anyone offering you pension advice or any other financial service is authorised by the FCA to perform the service they are providing for you, and that the details they are providing are the same as those on the Register.
“Unexpected and unsolicited offers, free pension reviews, promises of high returns which sound too good to be true and pressure to make a decision quickly are all warning signs of scam. Use the tools on our ScamSmart website to protect yourself and your retirement.”

Some simple steps to protect yourself from pension scams

- Reject unexpected pension opportunities, such as free pension reviews or investment opportunities involving your pension, whether made via email, social media, text, or over the phone.
- Research who you’re dealing with before changing your pension arrangements – check the FCA Register, or call the FCA on 0800 111 6768 to see if the firm is authorised by the FCA.
- Don’t be rushed or pressured into making any decision about your pension – consider getting impartial information and advice from a financial advisor authorised by the FCA to help you make the best decision for your own personal circumstances.
- Be suspicious if you are contacted out of the blue about an investment opportunity - seek advice from trusted friends, family members or an independent professional advice service before making a significant financial decision, especially when it involves your pension pot. Even genuine investment schemes can be high risk.
- Be ScamSmart and visit the ScamSmart websiteto learn how to protect yourself from pensions scams.

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

You can also report an unauthorised firm or a scam to the FCA by using their reporting form or by calling 0800 111 6768.

Cold calls about your pension are illegal. You can report nuisance calls and messages to the Information Commissioner's Office using their online reporting tool or by calling 0303 123 1113.

If you've agreed to transfer your pension and now suspect a scam, contact your pension provider straight away. They may be able to stop a transfer that hasn't taken place yet. If you are unsure of what to do contact the Pensions Advisory Service for help.

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

---

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

Watch out for scams related to census 2021

ALERT 06-04-2021

Every household is required by law to complete the census and even though Census Day – 21 March 2021 – has been and gone, it is not too late to complete a questionnaire. If you don't complete it, you may be fined.
Official census-branded reminder letters are being sent by post to households who have not yet completed their census. A census field officer may also knock on the door of a home to provide help and encouragement to those who have not yet filled in their census questionnaire online and direct them to any support services they might need.

To help keep you safe from census-related scams, read our handy Q&A below.

I haven't filled in my census yet – will i receive a reminder about doing so?
The ONS will send census branded reminder letters by post to households who have not yet completed their census. If someone receives a reminder letter they should complete their census as soon as possible. If they have already submitted their census form they can ignore any reminder letter.
A census field officer may also knock on the door of your home. The role of field officers is to give help and encouragement to those who have not yet filled in their census questionnaire online, or on paper, and direct them to any support services they might need to complete it.

They will not enter the household, and will carry ID to show they are genuinely working on the census.
Field officers will never ask for payment or bank details.

I missed Census Day – will I be fined for a late submission?
People still have time to complete their census and should do so as soon as possible to avoid getting a fine. Any letters, phone calls, texts, or emails, attempting to take payment for a late or incorrect submission now are not genuine.
For a fine to be imposed your case must go to court for non-completion of the census. Any fines issued for those refusing to complete their census, will be done via the courts.
You will never be issued with a fine by text message, phone call or email.

I've received an email/text that says I need to pay a fine because I haven't filled in my census, is this legitimate?
For a fine to be imposed your case must go to court for non-completion of the census. You will never be issued with a fine by text message, phone call, email, or on social media. You will not be fined for a mistake on your census.
The ONS have a Cyber Intelligence Team who are taking down fake sites related to the Census. If you find a site that looks suspicious or receive text messages with links to sites asking for money related to the census, do not engage with them. Report them to the Census 2021 Contact Centre by ringing 0800 141 2021 in England and 0800 169 2021 in Wales

Do census field officers get in touch before they visit? Do I need to book an appointment?
Households who have not completed their census will receive a reminder letter in the post. Field officers do not get in touch with you before they visit and you do not need to make an appointment for them to attend your home. However, you can book an appointment with the public contact centre to complete your Census over the telephone if you do not want to complete it online.

What happens when the field officers visit your home?
The role of field officers is to give help and encouragement to those who have not yet filled in their census questionnaire online, or on paper, and direct them to any support services they might need to complete it.
The only personal information a field officer requires is your name. If you need a new online code to fill out the census, you will be asked to provide your phone number.
Field officers will never ask to see personal documents like passports, pay slips or birth certificates. Field officers will never ask for payment or your bank details. They will never ask for your national insurance number.

Field officers do not need to enter your home.

How do I know a field officer is legitimate?
Census field officers carry ID to show they are genuinely working on the census and will be wearing Census branded high Vis. They do not need to enter your home and they cannot issue fines.

Will census field officers ask for my personal information?
The only personal information a field officer requires is your name. If you need a new online code to fill out the census, you will be asked to provide your phone number.
Field officers will never ask to see personal documents like passports, pay slips or birth certificates. Field officers will never ask for payment or your bank details. They will never ask for your national insurance number.
Field officers do not need to enter your home.

Can census field officers fine me on the doorstep?
Census field officers will never ask for a payment on the doorstep. The role of field officers is to give help and encouragement to those who have not yet filled in their census questionnaire online, or on paper, and direct them to any support services they might need to complete it. You are required to complete the census by law. If you refuse, you can be interviewed under caution. This may be followed by a court summons, a fine of up to £1,000 and a criminal record.

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

---

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

Pension schemes urged to step up reporting to stop scammers

ALERT 26-03-2021

The pensions industry is being called on to raise the alarm over suspected scams following a concerning long-term drop in reporting.
Data from the national fraud and cybercrime reporting centre, Action Fraud, shows a steady fall in pension scam reports from 1,788 in 2014 to 358 in 2020 – an almost 80% reduction.

In January, The Pensions Regulator (TPR) warned the Work and Pensions Committee investment fraud, where the source of funds may derive from pension assets, could be on the increase. However, a lack of data may be hiding the true picture of the pension scams landscape.

While there has been a slight rise in reporting so far in 2021, TPR is calling on industry to be on high alert for criminal or suspicious activity and to sign up to its Pledge campaign to help combat pension scams.

So far, more than 200 organisations have signed up to the Pledge campaign, which is designed in part to encourage better reporting. The campaign follows changes the regulator has made to protect savers in light of COVID-19 including the introduction of new scams training for all trustees, (as a new module of the Trustee toolkit), and a 'warning letter' for all those looking to transfer out of a defined benefit pension.

Action Fraud figures show pension scam losses can range from under £1,000 up to £500,000. But the true scale of the amount lost to pension scams, and the number of victims, is likely to

be much higher as victims often don't realise they have been tricked until many years later. Once the money is gone, it is often gone for good.

And with the COVID-19 pandemic impacting many peoples' finances – despite the unprecedented government support – there are fears scammers will use this to their advantage to steal hard-earned cash from savers.

Nicola Parish, The Pensions Regulator's Executive Director of Frontline Regulation, said: "To fight the scourge of pension scams and keep up with scammers' ever-changing tactics, we need a clear understanding of the size of the problem and good-quality intelligence.

"While we've seen no evidence of a significant increase in pension scams during COVID-19, we believe many across the industry, including trustees, pension providers and administrators, are not reporting suspected scams at a time when the pandemic could leave savers more vulnerable.

"It's vital the pensions industry reports suspected scams via Action Fraud, or by calling 101 in Scotland, which is why we made reporting one of the six principles in our Pledge to Combat Pension Scams campaign.
"We are working with Action Fraud and industry to ensure the reporting process is clear, understood and effective."

Pauline Smith, Head of Action Fraud, said: "It's vital that instances of pension fraud and attempted scams are reported to Action Fraud. Every report helps police get that bit closer to the people committing these awful crimes. Information provided in reports to Action Fraud also allows for quick-time disruption activity to take place, such as the removal of fraudulent websites and the blocking of telephone numbers being used to commit fraud, which helps prevent more people falling victim."
Margaret Snowdon, Chair of the Pensions Scams Industry Group (PSIG), said: "There are lots of reasons for under-reporting. Schemes may not report because they think it is a hassle, they are not certain something is a scam, or they are concerned the report won't be dealt with, but reports to Action Fraud are fundamental if scammers are going to be caught out by law enforcement.

"If we have better information on the scale of pension scams and the methods used, we are more likely to get the resources and attention we need to combat scams more effectively. The pensions industry must step up and improve reporting or it will make defeating scammers all the more difficult.

"The Pledge to Combat Pension Scams rightly requires schemes to commit to reporting suspected scams."

Pension scams are devastating. Scammers often approach people about a pensions or investment opportunity out of the blue with genuine sounding investments. They use sophisticated techniques to win trust before stealing people's hard-earned retirement cash and can leave victims facing retirement with limited income and little or no opportunity to build back their savings.

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

NEWSROOM

Action Fraud warning as demand for tickets increases ahead of lockdown easing

ALERT 25-03-2021

Following the announcement of the easing of lockdown restrictions over the coming months, several festivals and concerts have been announced, with demand expected to be incredibly high. Some festivals have already sold out.

As a result of the high demand for tickets, the National Fraud Intelligence Bureau (NFIB) are warning buyers to take extra care when buying tickets online. We are urging people to be wary of fraudsters selling fake or non-existent tickets to events. NFIB have already started seeing reports of non-existent tickets being advertised for sale online, some at inflated prices.

In February 2021, Action Fraud received 216 reports of ticket fraud. This is an 62% increase on the previous month and the highest number of reports received since March 2020 when lockdown restrictions were first implemented. Victims reported losing £272,300 in February 2021 – an average loss of just over £1,260 per victim.

It is anticipated that increased demand for tickets following lockdown restrictions will lead to greater numbers of victims and higher losses as a result.

Spot the signs of ticket fraud and protect yourself:

- Only buy tickets from the venue's box office, official promoter or agent, or a well-known and reputable ticket site.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal offer greater protection against fraud.
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets. If it sounds too good to be true, it probably is.
- Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information: star.org.uk/buy safe

Every report matters. If you have been a victim of fraud or cyber crime report it to us online or by calling 0300 123 2040.

Keep up to date with Action Fraud news, please visit: www.actionfraud.police.uk and select 'Newsroom' followed by 'News'. Alternatively you can follow Action Fraud Twitter account at https://twitter.com/actionfrauduk

---

To many of us, the last year has seemed the longest of our lives … a time of enforced adaptation to new lifestyles and working practices combined with reduced or no contact with loved ones and concerns about health and wellbeing.

If these circumstances have affected us, as adults, so deeply, the effect on most of our children has, understandably, been more profound. A year represents a large proportion of their young lives. Like us, the impacts of the respective lockdowns have been social, emotional and in many cases, physical. But unlike most adults, it has also heavily affected their learning and development.

In terms of being online, your child's internet usage has almost certainly increased during the pandemic, whether it's doing what they like, or what they need to do. For many parents, balancing their child's online safety with everything else that's going on can be very challenging.

To help, our online safety experts have put together some expert tips. And please look out for further campaigns this summer focusing on your child's online safety.

SWITCHED ON
To your children's online world

Top tips for a switched-on parent

- **Talk regularly with your child** about the good and not-so-good aspects of the internet. Get them to show you what they're doing and try it out for yourself. Get to understand new online technologies and trends. Discuss potential issues like stranger danger, accessing inappropriate content, bullying, oversharing personal information and spending too much time on their devices.
- **Discuss and agree boundaries and rules** from a young age, including time limits and appropriate online usage. Empower your child, but remember that they don't have the maturity or experience to always make the right decisions.
- Apply **parental control software and apps** on computers, mobile devices and games consoles, privacy features on social networking sites, safety options on search engines and safe location settings on devices and apps. Turn on ISP family filters.
- Explain and encourage **safe searching, websites and apps**. Check what your child is watching on streaming sites like YouTube and TikTok, as well as what they're sharing.
- Social networking, picture/video sharing, gaming and other sites and apps have **lower age limits** for a reason. Download apps only from recognised sources like App Store and Google Play. Add your own email address when setting up accounts and apps for your child.
- **Keep yourself up to date** with new game and social media trends, especially those with negative publicity because they may be violent, encourage gambling or leave the way open for messaging anybody, and hence potential grooming.

- **Ensure your child's video call safety** by updating to the platform's latest version, following its safety advice and making sure call invitations and responses can't be seen by anybody outside their group of friends, or their teacher/school.
- **If your child is into online gaming**, make them aware of things like chatting to strangers, in-game purchases (including using your credit card) and spending too much time online.
- **Fake news and misinformation** are rife on the internet. Advise your child that they shouldn't believe everything they read or see, and to avoid spreading random or sensational content.
- Warn about **oversharing confidential information or personal details** in posts, profiles, messages and chats. Consider what you share yourself.
- If your household is using technology for home schooling, try to **familiarise yourself with how it works** and make sure your child is following the platform's safety advice.
- Unfortunately, criminals have exploited increased online use for recruiting children into **illegal activities** such as cybercrime and drug muling. Keep tabs on your child's online activities and get to know the signs of something not being right.

#kidsonline2021

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

Cleveland Police Cyber Crime Team in collaboration with Get Safe Online

Get Safe Online
Free expert advice

It is more important than ever to understand the online world your child has access to and how to keep them safe.
To help with this, we are holding two interactive events, a 90 minute webinar with plenty of time to ask questions.

The online webinars are aimed at parents/carers and explore some of the key factors to be aware of regarding the online space and exploitation.

The aim of this event is to give you an overview of what young people may experience online & explore the harms that they may face on a daily basis.
The webinar will raise your understanding of how the online space can be exploited and will discuss examples of how online platforms are used to achieve this. It will better equip you to engage and support children and young people in their online world.

Learning outcomes:
If you apply what you have learned you will be able to:

- Recognise online risks and identify effective ways to support young people to interact safely with the online space.
- Demonstrate an understanding of what could make a young person vulnerable to online harms.
- Identify some key signs that your child may be struggling with in their online space.
- Know how to report any concerns.
- Understand the support/resources available.

There are two events are available for you to attend.

The first session is aimed at parents of primary school age, the later one for secondary school parents however you are welcome to attend either or even both.

Thursday April 29th 2021 10.00 - 11.30am: https://www.eventbrite.co.uk/e/staying-safe-online-an-insight-into-your-childs-online-world-tickets-145458312729?aff=erelpanelorg or Click here

Thursday April 29th 2021 1.30pm - 2.30pm: https://www.eventbrite.co.uk/e/staying-safe-online-an-insight-into-your-childs-online-world-tickets-145485114895?aff=erelpanelorg or Click here

Once you register with Eventbrite, full joining instructions will be sent out closer to the time.
If you have any problems please contact us on cyber.protect@cleveland.pnn.police.uk

---

Let's keep kids safe online

NEWS

Getting to know what your child is doing online

21-04-2021

Find out the different things your child likes to spend time on online. The online world is full of lots of great resources and you should try to make sure your child is making the most of them all!

Understanding what your child likes to do online is a good first step in helping them manage how they spend time on their favourite device. There's no set amount of time your child should or shouldn't spend online and it's important to do what's right for your family. Remember not every online activity is the same and children can still experience risks even when online for a short time.

It's best to start any conversation about keeping safe online with the positives. So why not start by exploring what your child likes to do and which are their favourite apps and games. Making sure your child is doing a range of different activities online will help them develop new skills and good online habits as they get older.

We know children like to use apps and games to watch, create, connect, play and learn so we've put together some questions to help you talk about each of these different types of apps. This will help give you an overview of how they like to spend their time online and get to know some of the apps, sites and games they use a little better.

Family activity
Talk to your child about what they like to do online and why. Try to fit every app, site or game you discuss under at least one of the five categories (some may go under more than one). Aim to have at least one activity for each category.

As well as fun time, try to ensure your child is using the internet in other ways, such as for learning, exercise and developing new skills.

Get to know what your child is doing online
Once you've decided what categories the apps, sites and games your child uses fit under, talk through the questions and information under each category below

Connect – messaging and content sharing

Many of us use the internet to connect with friends and family. This might be through traditional messaging apps like **WhatsApp** or through content sharing apps like **Snapchat** or **TikTok**.

- Which apps do you use to chat with your friends outside of school?
- Have you tried any new chat apps or are your friends using any new chat apps? When are your friends mainly online chatting?

Create – the content they're creating online

The internet is a great space for kids to create and develop new skills. For example, **Roblox** has entire sections dedicated to teaching kids how to code. It's important to talk to your child about the content they're creating online and who they're sharing it with.

- What apps do you use to create things online (videos, pictures etc.)? Who do you share these with?
- Can you show me what app you used to create that or something you've made before?

Learn – school work, hobbies, crafts and more

Recently kids have used online tools as a way of learning more than ever before and not just for school work. There are lots of resources for learning new hobbies or crafts too. The internet is full of amazing opportunities for us to learn but it's not always easy to separate fact from fiction. Read our article to help support your children with **fake news, misinformation and disinformation**.

- What apps or sites have you used to learn new things?
- How did it teach you – video's, pictures, live chat etc.?
- Did you share what you learnt with anyone? Can you show me?

Play – all the different types of gaming

It's important to not forget that being online is a great way for kids to have fun! There are endless activities online, like gaming that can help kids relax and escape from everyday life.

- What are your favourite games to play on?
- How long do your favourite games last?
- Can you speak to other people while playing?
- Who do you like playing games with? What time of day do they like to play?

Watch – any activity that involves streaming content online

Watch will cover any activity that involves streaming content online, such as using **Netflix** to watch their favourite programme or spending time on **TikTok** watching videos on the 'For You' page. It might also cover more educational activities like watching documentaries or videos on sites like **BBC Bitesize**, or the **Oak National Academy** whose videos are free to stream if you're on O2.

- What are your favourite things to watch online? And why?
- What was the last video you watched online? What was it about?
- How long do these videos usually last?

You could also ask your child which influencers and YouTubers they follow and why. Use this as an opportunity to explore their content together to see whether it's appropriate.

Top tips

Ask them to give you a demo of their favourite app, site or game

If your child mentions a specific app or game use this opportunity to ask them to give you a demo of it. This will give you a chance to ask them questions about how and why they use it.

Get to know the safety settings on their favourite apps, sites and games

Once you've had the demo use this as an opportunity to talk about privacy setting and safety tools. You could use our Net Aware reviews to help you set up important safety settings

Create or review a Family Agreement
Once you've talked through what they like to do online use our Family Agreement to create some online rules together. Make sure to use the insight you've gathered from the activity above to discuss when they go on certain apps.

For full details, please visit www.net-aware.org.uk and select 'News and advice'

Let's keep kids safe online
NEWS

Gaming apps with adult themes you should know about

07-04-2021

Games have always been used by young people as a way to relax, get creative and compete against friends. However, not all games available online are targeted at under 18s, but their graphics and game play might feel like they are which can make them more appealing to children. Recently we've come across a few cartoon games containing adult themes that we think you should know about. Here's our advice.

Cunch-line Chronicles
What you should know
Official age rating – 17+ 89

Cunch-line chronicles is a mobile game which is a similar style to Mario Kart, where you run through obstacles collecting various items while being chased by a Police Officer.

The game contains adult themes that aren't suitable for children, including references to drugs and criminal activity. 'Cunch' is a slang word used for 'Country lines' which is the term used to describe transporting drugs from urban areas to more remote locations.
The game also has in-app purchases that players are encouraged to buy to help them progress further in the game. We also came across lots of ads for games that promote gambling which are not be suitable for under 18s.
We wouldn't recommend this game for anyone under the age of 18.

ProjectMakeover
What you should know
Official age rating – 4+

Project Makeover is a puzzle game where you're set different tasks to makeover a client's physical appearance and home. To complete the makeover, you must play a candy-crush style game and win gems to gain access to beauty tools, clothes and interior choices.

The game has in-app purchases where players can buy access to new features and tools to help them complete the makeover quicker.
The game also promotes specific beauty ideals and the idea that there is a correlation between what you look like and being happy. Some of the tasks included paying to remove the client's glasses and getting rid of body hair. While research is still ongoing about the effect apps like this can have on young people, it could cause them to have self-esteem issues and imply that they need to conform to certain beauty standards in order to be accepted.

Because of the themes in this you should explore this game yourself before you let your child use it. We don't recommend it for anyone under the age of 13.

Hello Neighbour
What you should know
Official age rating – 12 +

Hello Neighbour is horror game where you break into a neighbour's house to investigate their suspicious behaviour. You must perform various tasks and gain access to the basement without being caught. It is rated 12+.

The game contains horror and violent themes include strangulation and imprisonment, which younger children might find scary. We wouldn't recommend this game for under 16s.

Gacha Life
What you should know
Official age rating – 9+

Gacha Life is a role-play game where you can create and dress anime style characters. You can also join scenes and chat with other players and play games as your character.

The game is rated 9+ on the Apple App and Google Play store. You should be aware that is has an in-app chat features and in-game purchases available. Make sure to talk to your child about what they're sharing on the app and who they're talking to. Remind them that conversation should only be about the game and they shouldn't share any personal information.
Be aware, there are some sexual themes in the game, with some of the characters displaying outfits and poses that might not be appropriate for young people.

Top tips to help you manage what games your child plays online

1. Download and explore the game before you let your child play it. This way you can see if it features any adult themes that you don't want them to see.

2. Speak to other parents and carers about the games their kids are using and ask if they have concerns.

3. Check out our **Net Aware reviews** to find age-appropriate games.

4. Get clued up on how games are rated by reading our advice on **Age and Content ratings**. Many official ratings only cover the actual content of the game and not whether it poses a contact risk so it's important to check the game out before you let your child play on it.

5. Have regular conversations with your child about the different games they're playing. You could try hosting a family games night where you compete against each other to win a prize. Take it in turns to choose the game, get to know the different features and set some rules around when they can play.

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. Sign up

For full details, please visit www.net-aware.org.uk and select 'News and advice'

National Cyber Security Centre
NEWS

Advice on Pulse Connect Secure RCE Vulnerability

Advice for UK organisations using Pulse Connect Secure (PCS) VPN appliances.
Published 20-04-2021

FireEye has published a blog today saying that APT actors are actively exploiting vulnerabilities in Pulse Connect VPN appliances.

The NCSC is aware of an unauthenticated remote code execution vulnerability affecting Pulse Connect Secure (PCS) version 9.0R3 and higher (CVE-2021-22893). Pulse Secure says it recently discovered that a limited number of customers have experienced evidence of exploit behaviour on their Pulse Connect Secure (PCS) appliances.

Pulse Secure has published a workaround that should be implemented immediately. However, Pulse have said that the workaround does not work for PCS versions 9.0R1 - 9.0R4.1 or 9.1R1-9.1R2. Therefore, an upgrade of PCS will need to be undertaken before implementing the workaround. The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities.

The workaround is a temporary measure until Pulse Connect Secure server version 9.1R.11.4 has been released. Read the Pulse Secure advisory for more information.

The NCSC strongly advises UK customers using Pulse Connect Secure VPN devices to regularly run the integrity tool checker provided by the vendor. This tool checks the integrity of the complete file system and finds any additional/modified file(s). This will help identify possible activity resulting from the exploitation of Pulse Secure Connect vulnerabilities.

The US Department of Homeland Security's (DHS) Cybersecurity Infrastructure Security Agency (CISA) has published an Emergency Directive on this issue.

Reporting a compromise
Affected UK organisations should report any suspected compromises to the NCSC via the website.

For details, please visit - https://www.ncsc.gov.uk and select **News**

Weekly Threat Report 16th April 2021

DNS vulnerabilities could impact millions of devices worldwide

Cyber security researchers have uncovered a series of new DNS vulnerabilities which could impact more than 100 million internet connected devices worldwide.

California based software company, Forescout, partnered with JSOF Research, disclosed nine vulnerabilities – collectively known as NAME:WRECK – affecting four popular TCP/IP stacks (FreeBSD, Nucleus NET, IPnet, and NetX).

These vulnerabilities enable either remote code execution or denial of service, with sectors including government, healthcare, manufacturing, and retail at risk.

In the UK alone it is estimated that around 36,000 devices could be affected. Forescout and JSOF have recommended a series of mitigations, which can be found here.

The NCSC has published guidance for the management of public domain names, which has been written for administrators of public and private sector organisations of all sizes.

Information on the NCSC's Protective DNS (PDNS), including eligibility criteria, can be found here.

NCSC recommends organisations install critical Microsoft Exchange updates

The NCSC has issued an alert this week encouraging organisations to install new security updates released for Microsoft Exchange Server as soon as practicable.

As part of its scheduled update cycle, Microsoft released more than 100 security patches, some of which address critical severity vulnerabilities in versions of Microsoft Exchange Server.

While the NCSC has no information to suggest these vulnerabilities are being actively exploited, the alert recommends that organisations as a first step should install the latest updates immediately. This follows reporting last month of vulnerabilities in Exchange servers being targeted for attackers.

The affected versions of Microsoft Exchange Server are:

- Exchange Server 2013
- Exchange Server 2016
- Exchange Server 2019

Exchange servers were in the news following exploitation of vulnerabilities last month. The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. More information about installing the updates for Microsoft Exchange Server can be found on the company's Exchange Team blog.

UK and US call out Russia for SolarWinds compromise

The UK and US have revealed for the first time that Russia's Foreign Intelligence Service (SVR) was behind a series of cyber intrusions, including the SolarWinds compromise.

The National Cyber Security Centre (NCSC), a part of GCHQ, assesses that it is highly likely the SVR was responsible for gaining unauthorised access to SolarWinds Orion software and subsequent targeting.

The NCSC has previously published guidance for organisations on this compromise:

- Dealing with the SolarWinds Orion compromise
- Identifying suspicious credential usage

You can read the Foreign Secretary's statement on this action in full on GOV.UK.

Weekly Threat Report 12th April 2021

Spoof job offer for LinkedIn users

Cyber security researchers, Esentire, have warned of a harmful spear-phishing campaign that targets individuals with malicious zip files using the job position listed on the target's LinkedIn profile as a lure.

If the fake job offer were to be opened, this would trigger an installation of the backdoor Trojan known as more eggs and, once installed, would allow the malicious software to download harmful plugins and provide access to the victim's computer.

The NCSC has guidance on how to spot the most obvious signs of a scam but if you believe you have been the victim of a successful phishing attack you should report it to Action Fraud as soon as possible.

Facebook user data leaked online

The information of 553 million Facebook users has been posted online including Facebook IDs, gender, location and date of birth.

Researchers have said that the data covers 533 million people across 106 countries, with 11 million of those being in the UK.
Facebook have issued a statement in response.

Despite this not being a new breach, users can find out whether their phone numbers or email have been breached by using the Have I Been Pwned online tool.

The NCSC has published useful advice on how to protect yourself from the impact of data breaches and using social media safely.

Fresh warning over risks to unpatched Fortinet VPN devices

The NCSC has issued a new warning about critical vulnerabilities in unpatched Fortinet VPN devices.

We have previously warned how Advanced Persistent Threat (APT) groups and cyber criminals are actively exploiting the CVE-2018-13379 vulnerability.

APT actors have continued to scan for this and two other Fortinet vulnerabilities; CVE-2020-12812 and CVE-2019-5591. Evidence of this has been disclosed by the FBI and CISA in a new joint report.

We urge all organisations to ensure that the latest security updates are installed on Fortinet VPN devices for all vulnerabilities.

More information can be found in the NCSC's full Fortinet VPN vulnerability alert.

Weekly Threat Report 2nd April 2021

Education continues to face ransomware threat

The UK education sector continues to face an increased threat from ransomware attacks with a notable rise since students returned to the classroom.

Ransomware is a type of malware which can make data or systems unusable until the victim makes a payment. This can obviously have a huge impact in an education environment.

The Harris Federation, who run a number of primary and secondary schools in the London area, issued a statement confirming they had been victims of a ransomware attack. They have been working with the NCSC and the NCA since the incident.

Last week we re-issued an alert to the education establishments with updated advice and guidance following the trend of attacks against the sector. The original alert was published in September 2020 and schools, colleges and universities are urged to read and use the advice where possible.

The NCSC has also published a number of resources for schools to help them improve their cyber security.

CEOs identify cyber security as an ongoing concern

A recent report from PwC cites the increase in cyber attacks and spread of misinformation online as top issues globally for CEOs.

Many companies had their digital transformation underway, but the coronavirus pandemic has accelerated their move to operating online. Although the majority in the report give cyber security as a primary concern, many are not planning on additional investment in their online security and data privacy.

The NCSC has created the Board Toolkit to encourage essential discussions about cyber security to take place between the Board and their technical experts.

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

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.

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

---

Upcoming Events

Upcoming Event - eventbrite

The North East Regional Cyber Crime Unit in partnership with Cleveland Police; Durham Constabulary and Northumbria Police cyber crime event

About this Event
The North East Regional Cyber Crime Unit (NERCCU) in partnership with Cleveland Police; Durham Constabulary and Northumbria Police present Cyber Essentials: A Cyber Basic Review 2021.

Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats. This event will explain what Cyber Essentials will and will not defend against, the five technical controls made easy for everyone to understand and what to expect if you do decide to go for certification.

Even if you decide not to go for certification; cyber essentials is still a good standard for all businesses to work towards.

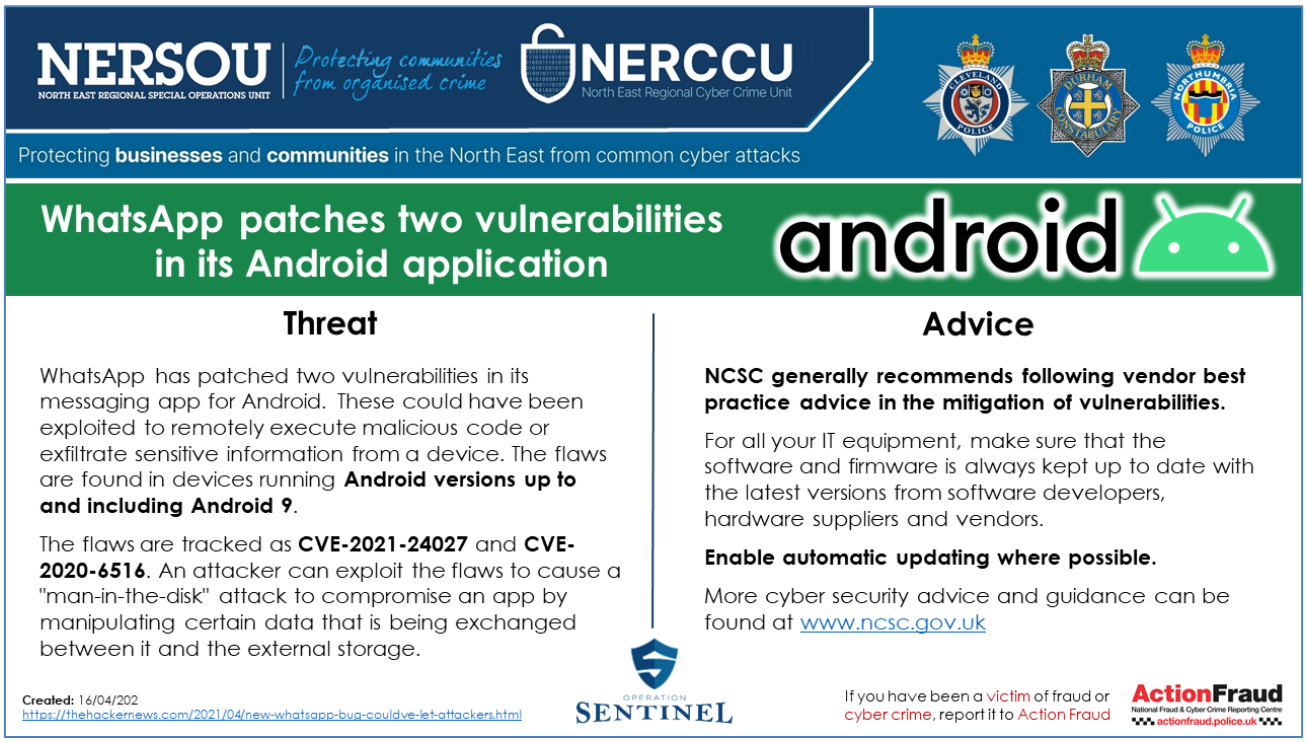
Register your place quickly as spaces are limited. Click here or visit eventbrite.co.uk and search for nerccu

A link to the event will be emailed 1hr before they begin.

Next event will take place on Wednesday 28th April 2021 14:00 – 15:30 BST
Alternative dates will become available – please continue to check via the eventbrite page

---

Notifications



NERSOU | Protecting communities from organised crime
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT

NERCCU
North East Regional Cyber Crime Unit

Protecting **businesses** and **communities** in the North East from common cyber attacks

Zero click vulnerability in Apple's macOS Mail

macOS

Threat

A zero-click security vulnerability, tracked as CVE-2020-9922, has been found in Apple's macOS Mail, which could allow a threat actor to add or modify arbitrary files inside the Mail sandbox environment.

This could result in sensitive information disclosure, and modification of Mail configuration. This could provide access to the victim's mail and allow a threat actor to take over other accounts via password resets, or even to propagate to contacts in a worm-like manner.

Advice

The NCSC generally recommends following vendor best practice advice in the mitigation of vulnerabilities.

For all your IT equipment (so tablets, smartphones, laptops and PCs), make sure that the software and firmware is always kept up to date with the latest versions from software developers, hardware suppliers and vendors.
Enable automatic updating where possible.

More cyber security advice and guidance can be found at www.ncsc.gov.uk

Created: 07/04/2021
Source: https://mikko-kenttala.medium.com/zero-click-vulnerability-in-apples-macos-mail-59e0c14b106c

OPERATION SENTINEL

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

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

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

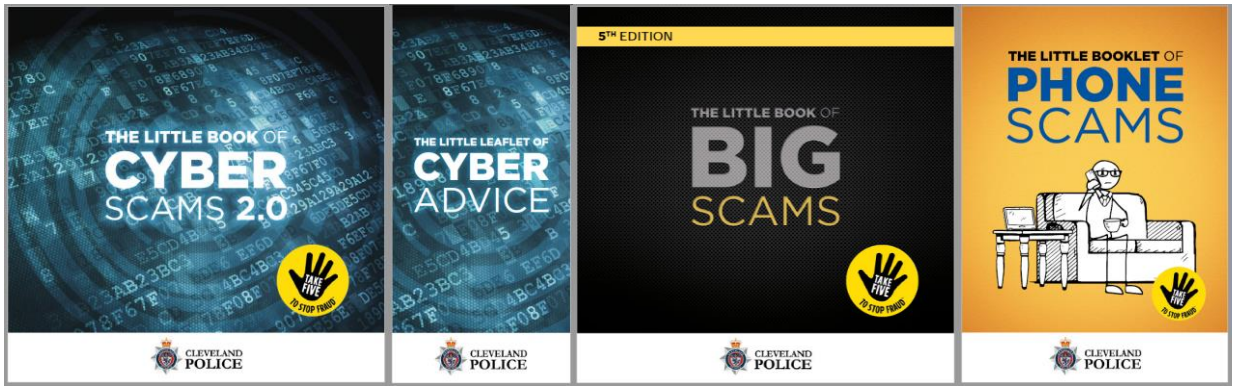
1. Never disclose security details, such as your PIN or full banking password
2. Don't assume an email, text of phone call is authentic
3. Don't be rushed – a genuine organisation won't mind waiting
4. Listen to your instincts – you know if something doesn't feel right
5. Stay in control – don't panic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

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.net-aware.org.uk/
www.ncsc.gov.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/	

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"