CLEVELAND POLICE

Cyber Crime Newsletter

OCTOBER 2022

CONTENTS

Fraud is a crime that can happen to anyone. There are many types of fraud including complex scams that are carried out over long periods of time, for example, dating scams, mortgage fraud and investment scams.

Often when someone is a victim of a fraud they are uncertain if a crime has been committed, or whether or not to report what has happened to them. Many frauds go unreported by victims because of personal embarrassment. It is likely that if a fraud has been committed against you someone else may have suffered a similar crime. The more individuals report, the more likely it is that fraudsters will be arrested, charged and convicted.

What is Action Fraud?

Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cybercrime in England, Wales and Northern Ireland.

They provide a central point of contact for information about fraud and financially motivated internet crime. Their aim is to stop people from being scammed, ripped off or conned, which is occurring every day.
The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB) who are responsible for assessment of the reports and to ensure that fraud reports reach the right place. The City of London Police is the national policing lead for economic crime.

People who report to Action Fraud represent a wide cross-section of the UK. They vary in age from young adults to the elderly. As frauds can be committed online, face to face, over the telephone or via the post, most people will have experienced fraud or know someone who has been a victim.

Reporting fraud and cyber crime

You can report fraud or cybercrime using an online reporting service any time of the day or night; the service enables people to both report a fraud and find help and support. This can be found on their website - https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime.
They also provide help and advice over the phone through the Action Fraud contact centre. You can talk to the fraud and cybercrime specialists by calling **0300 123 2040.**

When you make a report you will receive a police crime reference number. Reports taken are passed to the National Fraud Intelligence Bureau for assessment. This assessment of fraud and cybercrime reports from across the UK, helps to build a clear picture of where and how fraud and cybercrime is being committed.
Experienced Reviewers will assess the data contained in the crime reports to determine whether there is enough information to send to a police force. It is important to be aware that police forces cannot be compelled to accept crime reports sent to them by NFIB for investigation, they will review the report themselves and decide on their course of action.
Action Fraud does not investigate the cases and cannot advise you on the progress of a case.

The NFIB receives all the Action Fraud reports. Millions of reports of fraud and cybercrime are used by the NFIB to identify serial offenders, organised crime groups and find emerging crime types.

What the NFIB do with Action Fraud reports

- The reports are assessed and analysed by NFIB experts
- Data matching allows reports from different parts of the country to be linked through analysis, identifying the criminals behind the frauds.
- Reports are sent to local police forces/law enforcement agencies for investigation
- Bank accounts, websites and phone numbers which are used by fraudsters can be taken down by the NFIB

- Not every report results in an investigation, but every report helps build a clear picture. This contributes to making the UK a more hostile place for fraudsters to operate in and helps to keep other potential victims safe.

Fraud is a serious crime.
Sometimes people choose not to report fraud because they are embarrassed that they fell for a scam, con, swindle, or any other word used to describe the crime.

Remember that **fraud is a crime** and that fraudsters will constantly reinvent themselves to find new ways of tricking people. Anyone could be a victim.

Some people also think that fraud is a victimless crime, or that it's not as serious as other crimes. This is not true. Fraudsters are often part of serious organised criminal gangs, who use the money to fund other crimes such as human trafficking, illegal firearms trade and terrorism.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

ACTION FRAUD NEWS

Hacked social media accounts used to post indecent images of children

ALERT/ 07-10-2022

Social media accounts are being hacked and flooded with indecent images of children, potentially causing distress and reputational damage to the account holder. Since January 2022, 325 people have reported falling victim to this type of hack.
Analysis of crime reports by the National Fraud Intelligence Bureau indicates that criminals may be targeting social media accounts registered with email addresses that use custom domain names which have expired. Some victims also reported receiving suspicious emails from social media platforms asking them to "verify their account", with the links in the emails leading to genuine-looking websites that were designed to steal login details.

What you need to do

- If you come across indecent images of children online, report it to the police by calling 101 or visiting your local police station. You should take with you the device you were using when you came across the images.
- Do not, **under any circumstances**, screenshot, save or share the image. You will not be required to share the images with the police when making a report.
- Use 2-step verification (2SV) to protect your social media accounts. 2SV can keep people from gaining access to your accounts, even if they know your password.

- Ensure your social media accounts use a strong and different password to your other accounts. Combining 3 random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.
- Victims of account hacking should not pay any ransoms, whether it is monetary or in the form of a 'testimony' video.
- If your social media account has been hacked, you should report it to Action Fraud by visiting actionfraud.police.uk, or by calling **0300 123 2040.**

For details please visit: www.actionfraud.police.uk and select 'Newsroom' and 'News'

AF Action Fraud Twitter @actionfrauduk	
Reusing the same password means criminals only need to steal one of your passwords in order to get into many of your accounts Check out these top tips on how to secure your accounts properly: ncsc.gov.uk/cyberaware/home #TurnOn2SV	
Victims of email and social media account hacking reported being extorted by criminals who had stolen their personal photos and videos. Find out how to secure your accounts with 2-step verification (2SV): ncsc.gov.uk/cyberware/home #TurnOn2SV	
Has your email or social media account ever been hacked? Enabling 2-step verification (2SV) can keep hackers out of your account, even if they know your password Find out more here: ncsc.gov.uk/cyberaware/home #TurnOn2SV	

If you think you've been a victim of fraud, report it to Action Fraud online at https://www.actionfraud.police.uk or by calling 0300 123 2040

TWITTER ACCOUNTS

City of London Police Fraud @CityPoliceFraud

Fraudsters are evolving the way they work and are targeting victims on social media to encourage them to put their money in bogus investments.

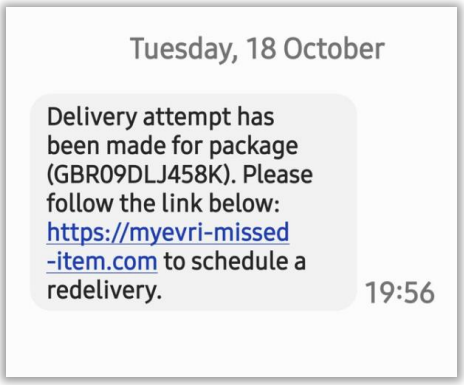
Find out more - @CityPoliceFraud
https://www.cityoflondon.police.uk/news/city-of-london/news/2022/october/warning-on-get-rich-quick-schemes-as-investment-fraud-soars-among-young-professionals-on-social-media

#investmentfraud #scamaware

SCAMWhere? @ScamWhere

Please be aware of this Evri redelivery scam text message.
This attempt has used a tracking number to add a sense of legitimacy to the message.
You can forward suspicious text messages to 7726

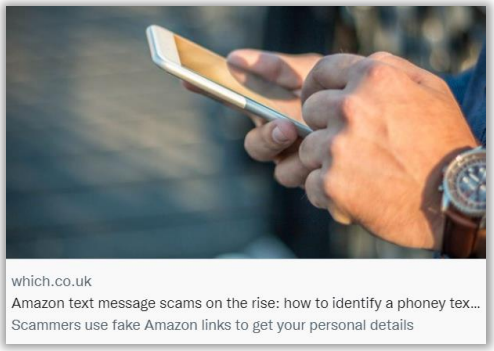
#Scamaware



SCAMWhere? Recently shared an example of one of these Amazon scams that was received only a few days ago.

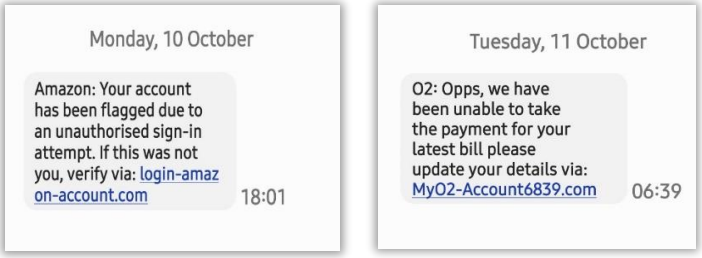
Please be aware if you receive one of these text messages out of the blue and forward suspicious txt messages to 7726

https://www.which.co.uk/news/article/amazon-text-message-scams-on-the-rise-how-to-identify-a-phoney-text-axMsy2Q2lKDn



SCAMWhere? Please be aware of these phishing scam text messages, purporting to be from both Amazon and O2.

You can forward suspicious text messages to 7726



Get Safe Online

In a business, cybersecurity is everybody's business

Whatever size or type of business you own, manage or work in, it's a target for cybercriminals, desperate to steal your money, customer data, intellectual property or other vital assets. The consequences can include financial losses, reputational damage, regulatory penalties, litigation or even business failure. And inevitably, a substantial amount of recovery work and trauma.

We recommend investing in the best security you can afford, which may mean physical measures as well as data security on computers, networks and storage. But even the most robust systems can be compromised by the behaviours of colleagues, employees and, maybe, yourself. In fact, 95% of cybersecurity issues can be traced to human error, and insider threats – either intentional or accidental – account for 43% of all breaches *(source: World Economic Forum Global Risks Report 2022).* Not only this, but the chance of cyberattacks succeeding has increased with more home and hybrid working.

What can go wrong?
Prevalent types of cybercrime affecting businesses right now include:

- Payment diversion fraud, where businesses are tricked into changing regular or one-off payments into fraudulent bank accounts. Also known as invoice fraud.
- CEO fraud, where an employee receives an email, text or phone call from someone impersonating a senior manager, instructing them to make an urgent one-off payment.
- Other types of impersonation or 'social engineering', where an employee is tricked into providing bank login details or other confidential information that could result in theft of money or data.
- Ransomware, where your computers or systems are infected by malware and files locked, accompanied by a ransom demand.

Make online security part of *your* business culture.
Start safeguarding your business *now* by following these top tips:

- Ensure all employees receive regular, up-to-date training on protecting the business and themselves from online threats.
- Introduce acceptable usage policies including what websites may and may not be visited and what employees post or publish online about the business.
- Have a robust password policy that includes choosing, using and protecting passwords carefully, having a different one for every account, use of password managers and two-factor authentication

(2FA). When creating secure passwords, you could start by using three random words and adding capital letters, numbers and symbols.

- Ensure that computers and mobile devices are physically protected from theft and loss as they generally contain – and provide access to – confidential business information. All devices should be protected with a password or passcode.
- Ensure that reputable internet security software and apps are loaded to all devices, kept updated and switched on.
- Ensure all data that the business needs to retain is backed up so that it is secure and accessible.
- Have and enforce a BYOD policy to govern employees' use of their own devices for business purposes.
- Always download updates to software, apps and operating systems when prompted, as they frequently contain vital security fixes. Better still, set them to update automatically.
- Never reveal too much personal or financial information in response to emails, phone calls or letters. Check that such requests are genuine, as senders or callers may not be who they seem and can spoof sender addresses and caller numbers.
- email attachments and links in emails, texts and posts should be treated with caution – and not clicked on – if the source is not 100% known and trustworthy. If in doubt, call the organisation on the phone number you know to be correct, to check the request is genuine.
- If you or an employee receives instructions to change payee details for supplier payments or subscriptions. Again, call the organisation to check.
- If your business falls victim to a ransomware attack, do not pay the ransom but seek professional assistance.
- Carefully control access to your data – both by employees/contractors and externally. Protect your customers and employees from breaches, and your business from contravening the Data Protection Act.

You should also consider gaining certification to the government's Cyber Essentials scheme. If you want to do business with the government or are in a government supply chain, you may be obliged to do this anyway.

For expert, practical, free advice on the above topics and much more, visit www.getsafeonline.org/business

Find comprehensive, easy-to-follow advice about online safety at www.getsafeonline.org

---

Get Safe Online

Frauds you may encounter during the cost-of-living crisis

You can be sure that whenever there's a crisis, it will be accompanied by fraudsters preying on our emotions, needs and fears. From a humanitarian crisis in Asia, the Russian invasion of Ukraine or a fatal fire in the UK, you can be sure that the fake appeals for charity donations and invitations to enter your personal details in return for graphic images, will follow.

The dire cost-of-living situation currently facing the UK does, indeed, represent a crisis. However, rather than one which we view remotely via our TV screens and newsfeeds, it's one that is affecting millions of us right here in this country. Which makes it even easier than usual for fraudsters to successfully exploit those emotions, needs and fears. Not dissimilar, in a way, has been the raft of COVID-19 related scams doing the rounds over the last two and a half years, with fake offers of anything from PPE to recovery loans, vaccinations to tax rebates and COVID passports to free shopping deliveries. To say nothing of the rash of fake texts and emails from 'parcel delivery firms' attributable to the quantum leap in online shopping spawned by the pandemic.

Now, with inflation running at a forty year high of 10.1% driving up the cost of consumer goods, income falling by 3% in value between April and June and the threat of a bleak winter of spiralling energy bills, motive, rationalisation and opportunity (known as the 'Fraud Triangle') exist in ample measure.

Many readers will remember (and compare the current crisis with) the 17% base rate in the late 1970s, when rising wages and oil prices fuelled a surge in inflation, or if not, maybe the slightly lower interest rate and accompanying mortgage payments in the early 1990s. However, the opportunities for fraudsters to further exploit people's hardship were relatively limited, given that it was only in 1991 that Tim Berners-Lee revealed his invention of the World Wide Web to the public, 1992 that the first text message was sent and 1997 that the first social networking site was launched.

That's all changed.

The above mentioned – together with the promise of various relief payments for UK households over the coming months – have conspired to create the perfect storm for fraudsters to do their worst.

Types of scams
Here are some of the scams that you're likely to hear about – or may even be affected by – as people's purse strings are tightened and increasing financial pressures. The list is by no means exhaustive as fraudsters are highly adept at keeping abreast of unfortunate situations with very convincing and persuasive messages.

- Texts purporting to be from 'Gov.org' or the 'DWP' inviting applications or claims for cost-of-living payments. In fact, payments are made automatically so there's no need to make such a claim.
- Bogus emails, texts or calls claiming to be from the local council requesting bank or card details so that the £150 council tax rebate can be paid. Again, this is not necessary to receive the payment.
- Fake messages about energy payments relief purporting to be from Ofgem, the energy regulator. Payments are actually being overseen not by Ofgem, but the Treasury.
- Emails, texts or calls claiming to be sent by energy suppliers offering switching deals, cheaper tariffs, discounts on prepayment meters or rebates.
- WhatsApp scams where you receive a message from someone on a number you don't recognise claiming to be a family member or friend, informing you they have changed their phone number. A short while later, they request money to solve 'a problem which needs payment' (made more believable by the cost-of-living crisis), also known as the 'Friend in Need' or 'Mum and Dad' scam.
- Advertisements, emails, texts or social media posts offering either non-existent loans or those with incredibly high interest rates, to help you through a period of financial hardship.
- An invitation to join 'get rich quick' schemes or jobs, with seemingly (so probably) impossible returns. These range from supposed high return pension and other investment schemes to being paid for the use of your bank account – the latter almost certainly resulting in money muling, a criminal offence in its own right.
- A general increase in 'traditional' scams offering great deals on tickets, holidays, vehicles, consumer goods, fashion and other things you purchase online. What you buy is either non-existent or not as advertised.

Protect yourself
- Do your research: never send money to anyone you don't know personally, or buy anything you're not entirely sure of.

- Look out for spelling and grammatical errors in emails and texts, not being addressed by your name and poor layouts.
- Never reveal personal or financial data including usernames, passwords, PINs, or ID numbers.
- Don't open email attachments or click on links in communications from unknown sources.
- Make sure your antivirus software is up to date and run a scan before opening anything you're suspicious of. Always update software, apps and operating systems when prompted, or set them to update automatically.
- Think before you click: if something seems too good to be true, it probably is.
- **To check whether a website is likely to be legitimate or fraudulent, enter its address at** getsafeonline.org/checkawebsite

---

Get Safe Online

It's Charity Fraud Awareness Week 2022

Get Safe Online is proud to support this year's Charity Fraud Awareness Week which runs from 17th October until Friday 21st October.

Now in its seventh year, Charity Fraud Awareness Week is an award-winning campaign, run by a partnership of charities, regulators, representatives, umbrella bodies and other not-for-profit stakeholders, across the world. Its aim is to bring together the third sector to share knowledge, expertise, and good practice in fraud prevention, at a time when many in the sector continue to remain susceptible to fraud and cybercrime.

Tony Neate, Chief Executive, Get Safe Online, said: *"The thousands of charities across the UK are doing a fantastic job in supporting deserving causes which would otherwise suffer. They rely on the hard work and dedication of not only paid professionals, but an army of volunteers and, of course, donations in the form of fundraising and legacies, amongst others. Right now, finances are even more stretched because of the cost-of-living crisis and seemingly more potential recipients for donations, such as the war in Ukraine.*

"Unfortunately, charities are far from immune from fraud, and that's why we're again getting involved in this year's Charity Fraud Awareness Week, organised jointly by the Charity Commission and the Fraud Advisory Panel. We encourage all third-sector organisations to sign up too, particularly at a time when, more than ever before, charities need to be aware of the risks from fraud and take appropriate steps to ensure their money, people and data are kept safe."

For more information about Charity Fraud Awareness Week visit: preventcharityfraud.org.uk and/or join the conversation at: #StopCharityFraud

For details please visit: www.getsafeonline.org

Get Safe Online Twitter @GetSafeOnline

Will you start buying #Christmas #presents online this weekend? Before you do, check that the website is legit with our fantastic #CheckAWebsite tool, from @GetSafeOnline & @CifcasUK and make sure you don't fund Christmas for a fraudster https://www.getsafeonline.org/checkawebsite/	
Android security warning: These crooks phone you and trick you into downloading malware @ZDET & @dannyjpamer https://www.zdnet.com/article/android-security-warning-these-crooks-phone-you-and-trick-you-into-downloading-malware/	
#FIFAWorldCup kicks off in less than 6 weeks! Still trying to get tickets and accommodation in #Qatar? Read our expert advice on buying tickets safely before you spend or commit any money https://www.getsafeonline.org/personal/articles/buying-tickets/	
Retweet Amanda Todd: Dutchman sentenced for fatal cyber-stalking **bbc.co.uk** Amanda Todd: Dutchman sentenced for fatal cyber-stalking. He showed no remorse in court as he learned his fate for tormenting the girl whose ordeal shocked Canada. https://www.bbc.co.uk/news/world-us-canada-63218797	

STOP SCAMS UK
STOP, HANG UP, CALL 159

At the end of September 2021, we launched 159, a memorable short-code phone service that connects the vast majority of UK banking customers safely and securely with their bank when they receive an unexpected or suspicious call about a financial matter.

This breaks the scam 'journey' at the critical moment when you are at most risk of being manipulated into making a payment. So, even if scammers can make contact with you, that link will be broken by your call to 159, before any information is shared, any payment is made, and any harm is done.

How it works: 'Stop, Hang Up, CALL 159'
If you think someone is trying to trick you into handing over money or personal details…
…Stop, hang up and call 159 to speak directly to your bank.

Last year criminal gangs stole over £583m by pretending to be your bank or another service provider.

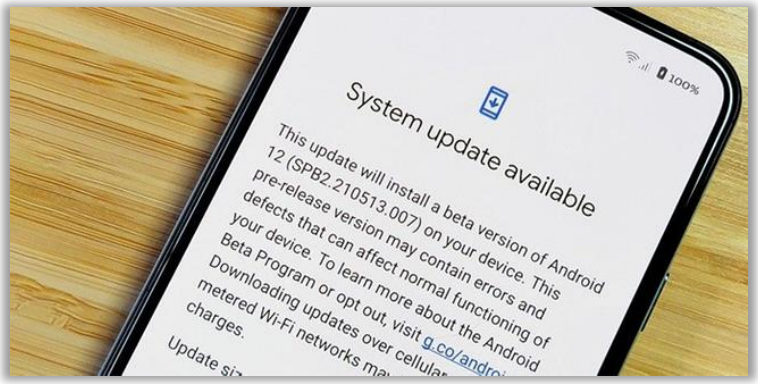
159 is the memorable, secure number that connects you directly to your bank if you think you might be being scammed.

159 works in the same way as 101 for the police or 111 for the NHS. It's the number you can trust to get you through to your bank, every time.
Since 2014 UK Telecommunications Operators have significantly reduced the 'call clearing delay time' to under two seconds, meaning calling 159 will always be a route back to safety.

159 will **never** call you. **Only a fraudster** will object to you calling 159.
For details please visit: https://stopscamsuk.org.uk/159

Cyber Aware
Install the latest software and app updates

Applying security updates promptly will help protect your devices and accounts from cyber criminals.



You should apply updates to your apps and your device's software as soon as they are available. Updates include protection from viruses and other kinds of malware, and will often include improvements and new features.

If you receive a prompt to update your device (or apps), don't ignore it. Applying these updates is one of the most important (and quickest) things you can do to keep yourself safe online.

You should also turn on 'automatic updates' in your device's settings, if available. This will mean you do not have to remember to apply updates.

Note that:

- Updating your device may take some time and requires a reliable internet connection, so it's best to do it at home where you can access your Wi-Fi (and keep your device plugged in)
- Older devices will eventually stop receiving updates

Keeping your phones, tablets and computers up to date

For detailed instructions about how to keep these devices up to date, refer to the support area within the manufacturers' official websites. If you're advised to back up your data, you can refer to the NCSC's guidance on how to do this.

To get you started, we've included links to popular devices.

- Update your iPhone, iPad or iPod touch
- Update your Mac computer
- Update your Windows 10 or Windows 11 laptop/PC
- Update your Android device (Samsung, Google Pixel, Huawei phones and tablets etc.)

Updating devices automatically

- Update Android apps automatically
- Turn automatic updates on/off on Apple devices (middle of page)

Keeping 'smart' devices up to date

For instructions about how to keep smart devices up to date (such as smart speakers, fitness trackers and security cameras), refer to the support area within the manufacturer's official website, and look for information about updating your device.

To get you started, we've included links to popular smart devices.

- Amazon devices (Fire Tablets, Kindle E-readers, Alexa Devices, Fire TV)
- Apple Watch
- Fitbit devices
- Garmin devices
- Google Nest or Home speakers
- Ring doorbells

When your device no longer receives updates

Manufacturers eventually stop providing updates for older devices. If you continue to use a device that's no longer supported:

- **It won't receive updates that contain new features and performance improvements**
- **It won't receive the security updates from the manufacturer (and without these your phone is less secure)**

You don't need to buy the latest (or most expensive) model to stay safe, but if possible, **avoid** buying and using devices that are no longer supported. You can check online to find if a specific model still receives updates from the manufacturer. Here are the details for iPhone, Chrome, and Pixel/Nexus devices.

- Supported iPhone models
- Chrome OS (e.g. Chromebooks)
- Pixel devices

If you have another type Android device (such as those manufactured by Samsung or Huawei), you'll have to check with the manufacturer.

For details please visit: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

National Crime Agency

Twitter @NCA_UK

A money mule is someone who lets someone else use their bank account to send money, keeping a little bit for themselves. It's a crime. #DontBeUsed	
Want quick and easy cash? What about a criminal record? Transferring money for someone else and keeping some of the cash for yourself is a crime. Don't be a money mule. Learn more - https://nationalcrimeagency.gov.uk/moneymuling #DontBeUSed	
Impersonation fraud often starts with a call, email or message that appears to be from a trusted organisation or a friend or family member. Only criminals will try to rush or panic you. Think you've fallen for a scam? Contact your bank immediately and report to @actionfrauduk	 

NCSC – National Cyber Security Centre

NEWS

NCSC issues fresh guidance following recent rise in supply chain cyber attacks

Guidance to help organisations assess the cyber security of their suppliers.

- New cyber security guidance issued in response to growing trend in supply chain attacks
- GCHQ's National Cyber Security Centre advises organisations to work with suppliers to identify weaknesses and boost resilience
- Businesses urged to take action as just over 1 in 10 review the risks posed by immediate suppliers

CYBER security experts have issued a fresh warning over the threat of supply chain attacks following a rise in the number of incidents.

The National Cyber Security Centre (NCSC) – a part of GCHQ – has today (Wednesday) published new guidance to help organisations effectively assess and gain confidence in the cyber security of their supply chains.

It follows a significant increase in cyber attacks resulting from vulnerabilities within supply chains in recent years, including some high-profile incidents such as the SolarWinds attack.
The new guidance is designed to help medium and larger organisations effectively assess the cyber risks of working with suppliers and gain assurance that mitigations are in place.
Supply chain attacks can cause far-reaching and costly disruption, yet the latest government data shows just over one in ten businesses review the risks posed by their immediate suppliers (13%), and the proportion for the wider supply chain is just 7%.

Ian McCormack, NCSC Deputy Director for Government Cyber Resilience, said:
"Supply chain attacks are a major cyber threat facing organisations and incidents can have a profound, long-lasting impact on businesses and customers.
"With incidents on the rise, it is vital organisations work with their suppliers to identify supply chain risks and ensure appropriate security measures are in place.
"Our new guidance will help organisations put this into practice so they can assess their supply chain's security and gain confidence that they are working with suppliers securely."

Cyber minister Julia Lopez, said:
"UK organisations of all sizes are increasingly reliant on a range of IT services to run their business, so it's vital these technologies are secure.
"I urge businesses to follow this expert guidance from our world-leading National Cyber Security Centre. It will help firms protect themselves and their customers from damaging cyber attacks by strengthening cyber security right across their supply chains."

The guidance has been published in conjunction with the Cross Market Operational Resilience Group (CMORG) which supports the improvement of the operational resilience of the financial sector, though the advice is for organisations in any sector.

It aims to help cyber security professionals, risk managers and procurement specialists put into practice the NCSC's 12 supply chain security principles and follows the government's response to a call for views last year which highlighted the need for further advice.

It describes typical supplier relationships and potential weaknesses that might expose their supply chain to attacks, defines the expected outcomes and sets out key steps that can help organisations assess their supply chain's security.

In addition to guidance focused on improving supply chain cyber resilience, the NCSC has published a range of advice to help organisations improve their own cyber security.

This includes the 10 Steps to Cyber Security guidance, aimed at larger organisations, and the Small Business Guide for smaller organisations.

For details, please visit - https://www.ncsc.gov.uk/news/ncsc-issues-fresh-guidance-following-recent-rise-in-supply-chain-cyber-attacks

---

NCSC – National Cyber Security Centre
NEWS
Leading women in tech urge schoolgirls to take on the UK's flagship cyber security contest

Registration opens for the CyberFirst Girls competition 2023

- Registration is now open for the 2023 Girls Competition: the prestigious national cyber contest led by GCHQ's National Cyber Security Centre
- Schools and teachers can enrol teams now to inspire more girls to consider a future in technology and cyber security
- This year some of the UK's leading voices in tech have come together to encourage students to sign up to the CyberFirst Girls Competition

Some of the country's leading women in the tech industry today urged schoolgirls to put their skills to the test in the UK's flagship cyber security competition.

The call came on the day registration opened for the CyberFirst Girls Competition 2023, where they will be able to try their hand at cracking codes, decrypting messages and solving coding puzzles.

The annual competition is run by the National Cyber Security Centre (NCSC) – a part of GCHQ – and aims to introduce girls aged 12 and 13 to cyber security, with the ultimate goal of increasing diversity in the industry.

With women making up just 16% of the UK's cyber security workforce, a number of female leaders in tech urged the next generation to enter the competition and see where it leads them.

Dr Anne-Marie Imafidon, CEO of Stemettes, said:
"The gender gap in technology is holding all of us back. In cyber, this gap is important to fill as we need to keep folks safe and secure as technology becomes more important - entering this competition is a brilliant way to ensure you can help us all!"

Charlene Hunter MBE, CEO and Founder of Coding Black Females, said:
“The CyberFirst Girls Competition has already impacted so many girls, and I'm excited to see the 16% increase to a much higher number with opportunities like this.
“Competitions like this are vitally important to ensure that girls and young women are exposed to technology from an early age.
“I've had the privilege of having parents in tech and involvement in the industry has been a large part of my upbringing, this enabled me to see fewer barriers when I started my career as a software engineer and so much of that has had an impact on the creation and development of Coding Black Females.”

Anna Brailsford, CEO of Code First Girls, said:
“There are so many exciting career opportunities in the tech industry, but sadly far too many girls and women still think the industry isn’t for them. They couldn’t be more wrong.

“Tech businesses and organisations are increasingly recognising the importance of diverse workforces because it makes their tech products and systems much stronger - so there has never been a better time to get involved.
“I’d encourage any girl to take part in the CyberFirst Girls Competition, and you don’t need to be a fan of science and maths. You might just find a new skill and a new passion, and become part of the next generation of tech talent!”
The competition welcomes everyone from beginners to experts, so entrants don’t need to have any previous knowledge to sign up. The same goes for teachers, who don’t need to have technology experience to put together teams of students.

Chris Ensor, NCSC Deputy Director for Cyber Growth, said:
“It’s great to have the support of fantastic role models to help inspire the next generation.
“The Girls Competition is a great introduction to the world of cyber that’s both fun and challenging and a great chance for the girls to pit their wits against local rivals.
“Thousands of girls have already enjoyed what the competition has to offer, and I would urge even more schools to come forward this year, including those that have never entered before.”

In their teams the girls tackle fun and challenging puzzles, covering topics from cryptography to AI to logic, in a bid to see off rivals and develop cyber skills. The highest scoring teams will go through to one of 13 finals held across the UK as part of a country-wide celebration of the next generation of cyber talent.

Special individual and team prizes are also up for grabs and considered eligibility rules aim to rally more schools to register – even if they have little cyber experience.

The qualifying round opens at noon on Monday 21st November and runs until Wednesday 30th November. The top teams will then compete at finals held simultaneously on Saturday 4th February in 13 locations, with one held in each of Scotland, Wales and Northern Ireland and in English regions.

Girls in Year 8 in England and Wales, S2 in Scotland, and Year 9 in Northern Ireland are encouraged to enter the contest in teams of up to four. A teacher at their school or a school guardian must act as their mentor and register them via the NCSC website.

Independent schools are also required to provide details of two non-selective state schools that they have encouraged to register, to help the contest reach more girls from more diverse backgrounds. Following the

introduction of this initiative last year, state schools that had never entered the contest before made up more than 25% of the total number taking part in the 2022 competition: an increase on the 2021 competition.

Since 2017, more than 43,000 girls have taken part in the CyberFirst Girls Competition, with many then going on to take part in other CyberFirst activities. This includes our CyberFirst courses starting at Trailblazers (ages 12-13) and going all the way through to our advanced course for pre-university aged students.

The NCSC also runs CyberFirst Bursary and Degree Apprenticeship programmes helping young people to kick start their careers in the industry and support the next generation of cyber talent.

For details please visit: https://www.ncsc.gov.uk/news/schoolgirls-urged-to-take-on-the-uks-flagship-cyber-security-contest

---

Threat Reports

The NCSC's threat report is drawn from recent open source reporting

Threat Report 14th October 2022

New NCSC guidance to support organisations to assess the supply chain risk

The NCSC has published new guidance 'How to assess and gain confidence in your supply chain cyber security' aimed at medium to large organisations. Supply chain attacks can result in devastating, expensive and long-term ramifications for affected organisations and their customers, and the guidance aims to help mitigate this.

US publishes advisory on top CVEs exploited by Chinese state

US agencies CISA, FBI and NSA have published a new advisory about Chinese state actors continuing to use open source tools and to exploit vulnerabilities to gain access to critical infrastructure networks of interest to them. It lists the 20 most exploited vulnerabilities since 2020, which includes many familiar and much publicised ones, such as Log4j.

Legal notices issued following Huawei consultation

By the end of 2027, Huawei technology must be removed from the UK's 5G public networks.

Following a consultation, legal documents have been issued to 35 UK telecoms network operators and has been based on guidance from the National Cyber Security Centre.

In 2020, the NCSC published guidance relating to Huawei as well as a collection of content around 5G and the future of UK telecoms:

- Summary of the NCSC analysis of May 2020 US sanction
- A different future for UK telecoms – blog post
- Huawei advice – what you need to know
- What is 5G – an explainer

Launch of DCMS 2023 cyber security survey of UK organisations

The Department for Culture Media and Sport (DCMS) has now started the research for its latest survey of UK businesses, academia and charities to understand the cyber security issues they face.

Organisations are selected randomly and the survey is a chance to contribute to research and work that will inform UK government cyber security policy and how the government works with organisations to keep UK businesses safe online. Participation is voluntary and conducted over phone interviews by Ipsos on behalf of DCMS

Threat activity attributed to Iranian IRGC in joint international advisory

On 14 September, the NCSC and international partners issued an advisory which attributes previously reported Iranian state activity to the Iranian state Islamic Revolutionary Guard Corps.
The activity is targeting vulnerabilities, including Log4J, on critical national infrastructure (CNI) networks.

US advisory on cyber threats to ICS and OT systems

The US agencies CISA and NSA have published an advisory relating to the threats against Industrial Control Systems and operational technology (OT), called 'Control System Defense: Know the Opponent'.
It recognises the specific threats and challenges these systems face and includes mitigations for organisations to protect networks.
The NCSC also has cyber security guidance on operational technologies.

Attackers' use of domain shadowing technique

A report by Palo Alto (Unit 42) researchers indicates that the technique of domain shadowing, a form of DNS hijacking, may be more widespread than previously thought.

Here an attacker compromises the DNS of a legitimate domain – without modifying the DNS entry – to host their own subdomain, and create malicious pages on the attacker's own server.

These malicious pages are valuable to an attacker, who can use them to make phishing sites, command and control (C2) servers look more legitimate to evade detection and presenting a real threat

The research shows 12,000 cases in web scanning between April-June 2022, with VirusTotal marking only 200 as malicious.

The NCSC has guidance for organisations on actions to help defend against phishing attacks, as well as other protective measures, through 10 Steps to Cyber Security.

For details, please visit - https://www.ncsc.gov.uk and select 'News, blogs, events' then select 'Threat reports'

NCSC UK Twitter - @NCSC

Whether it's your email, a social media account, or your online bank, losing access to a digital account can be stressful. Check out #NCSC's guidance on recovering and protecting your accounts. https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account	

Keeping kids safe: Phishing and ransomware

October is Cyber Security Month. This year, we're exploring phishing and ransomware.
As young people engage with the online space, they may fall victim to phishing and ransomware. To help prevent such harm, Georgie Price from ESET provides guidance for parents and carers.

Though there are many new cyber security threats to be aware of today, we mustn't ignore two of the most widespread: phishing and ransomware.

Psychological manipulation is a key characteristic of social engineering attacks like these, so it's important to know how to identify them. With less experience in the digital world, children are more vulnerable to these cyber attacks. Let's break down these scams to help you protect against them.

What is phishing?

Phishing is an attack where cyber criminals act as trusted senders to 'fish' for information. They may send fraudulent emails, texts or social media messages to do this. Because attackers can reach millions of people both directly and instantly, this technique is very popular.

How it works

Typically, hackers prey on their subject's goodwill, influencing them to perform specific actions like sharing sensitive information. Essentially, they design messages to create a sense of urgency and demand immediate action. As such, their targets have less time to consider their response.

Phishing attempts might also install malware and obstruct systems.

Receive an unexpected and urgent request? Think twice before you click.

Learn about cyber security

What is ransomware?

Ransomware is a type of malicious software (malware). Once installed, it encrypts files or blocks access to a system – effectively holding it hostage – until a sum of money is paid.

How it works

Usually, ransomware spreads through email attachments or through downloading infected files. The hacker may then threaten to share the target's personal data or permanently block access unless the ransom is paid. However, it's important to remember there is no guarantee of its return.

Inevitably, ransomware can be devastating. Therefore, it is important to be aware of the risks and take necessary precautions. Always back up your important files and don't open attachments or links from unknown sources.

Ransomware can be extremely difficult to remove. The best thing to do is seek professional help rather than pay the ransom.

How phishing and ransomware attacks target children

It's no secret that cyber criminals target the vulnerable using various techniques. Malicious links often exploit a child's curiosity and naivety; the phishing and ransomware attacks begin with a simple click.

Children are not always conscious of the risks associated with downloading files from unknown sources. Additionally, hackers recognise that parents share devices with their children at an increasing rate. This dynamic creates ample opportunity to also target professionals through their kids.

Social media versus social engineering

Today, young people increasingly turn to social media for entertainment. Cyber criminals monitor these trends closely. With the internet at their fingertips, they are inevitably more at risk of online harms such as phishing and ransomware or other scams associated with social media.

TikTok, for instance, is the most downloaded app and has over 1.2 billion daily users. It continues to break records and expand its audience, presenting a field day for scammers.

Like TikTok, Instagram and Snapchat's minimum age is also thirteen – which many argue is too young. Unfortunately, many children under this minimum age also have access to these platforms.

We recommend you make use of any platform's built-in security features and encourage open dialogue about the use of these apps. Set parent controls with broadband and mobile providers to help as well.

Protect children from phishing and ransomware

Phishing and ransomware are serious threats that can affect anyone. Therefore, knowing what they are and how to avoid them is essential to keeping children and young people protected. Here are some tips to help:

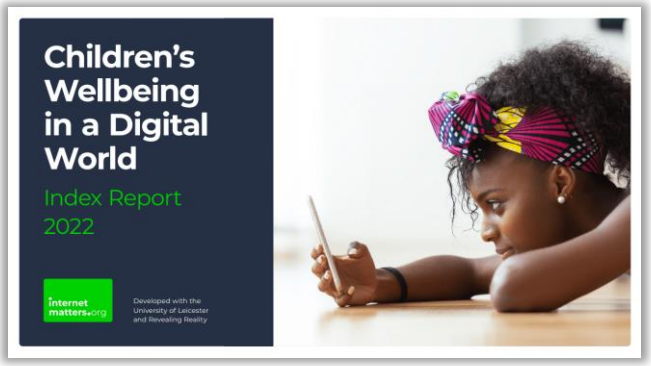
- Teach your child not to open unknown attachments or links in suspicious emails
- If they get an unexpected message requiring urgent action, ask them to think twice before clicking. They should always ask you if they are unsure
- Look out for grammatical and spelling errors and generic or impersonal greetings that aren't normal to how someone communicates with you
- Keep their social media accounts set to private and explore other social media settings that can keep them safe
- Back up your family's data on their devices
- Install reliable security software and keep operating systems updated
- Use multi-factor authentication to protect your accounts

To learn more about keeping kids safe online, visit Digital Matters. The free online interactive learning platform helps support teachers and parents navigating their children through key online safety and media literacy skills.

For further information, visit https://www.internetmatters.org/hub/expert-opinion/phishing-and-ransomware/

Internet matters.org

The impact of technology on children's digital wellbeing



In our Children's Wellbeing in a Digital World Index Report 2022, we assessed the impact of digital technology on the wellbeing of children and young people.
Our research revealed interesting aspects of digital participation in the modern UK home.

Children's Wellbeing in a Digital World 2022 Index Report

We learned that as children get older and spend more time with digital technology, they experience more of the positives as well as the negatives. The report also demonstrated the potential wellbeing outcomes of excessive social media usage and gaming.
Additionally, and fundamentally, it reinforced the point that vulnerable children experience greater impact from participation in the digital space.

Ahead of the launch of the 2023 Index, we conducted additional research with parents of children aged 4-16 and children (aged 9-16). We looked at subjects that impact children's digital lives, including a focus on wellbeing. Here we examine how this further builds the picture of children's wellbeing in a digital world.

Key findings in our additional research

- Parents who feel confident in online safety are more likely to believe digital technology impacts children's wellbeing in a positive way
- Parents are more likely than their children to perceive negative impacts on their children's emotions
- Vulnerable children have more upsetting experiences online compared to non-vulnerable children

Parental confidence in online safety

When asked about the overall impact of digital technology on their children's wellbeing, parents were mostly supportive. When speaking directly to parents, we see growth in that positivity over time.

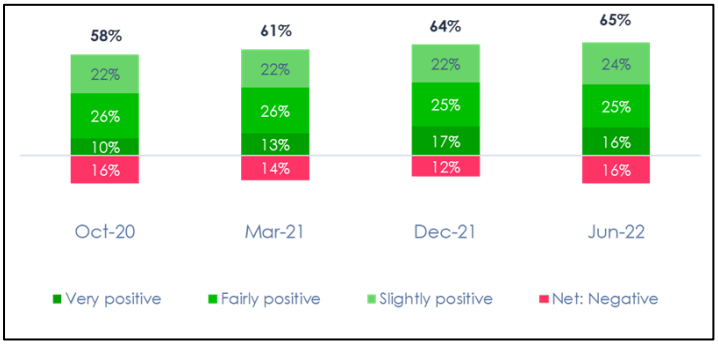


Table 1. Taking all things into consideration, do you think [child's name]'s experience and use of technology and the internet has positive or negative impact on their overall wellbeing? c. N-2,000 parents per wave.

Differences in positivity levels between parents
Parents of younger children (4-8 years old) were less positive about digital technology (59% net positivity) than parents of older children (62%, 15-16 years old). This suggests the benefits of being online increase as children get older.

Fathers (67%) were significantly more positive than **mothers** (54%) about the impact of digital technology usage amongst their children. This may link to dads feeling more confident in knowing how to keep their children safe online. For instance, 80% of fathers felt confident about how to do this vs. 74% of mothers.

When we look at those 'confident' mums and dads, both were significantly more positive towards internet usage overall. The gap between them was also smaller – 84% of dads feel positive about the internet's impact on their children's wellbeing vs. 81% of mums.

Conclusion
We can conclude that with increased understanding and confidence, parents acknowledge and appreciate the benefits of digital technology for their children more so than parents lacking that confidence.

Helping parents learn how to keep their children safe online may support parents in understanding the aspects of the digital world, which enhance wellbeing. As such, the potential for children accessing these elements also increases.

Parents see greater emotional impacts than children
We asked parents to reflect on what being online does to children's wellbeing, asking children the same for themselves. There was an interesting split in the interpretation about being online. As expected, parents were more likely to show concern about their children's usage of the internet compared to children themselves.

The starkest difference was around 'feeling sad' – a complex emotion that around a third of parents (31%) link to their children's online use. However, less than one in five children (18%) share this view.

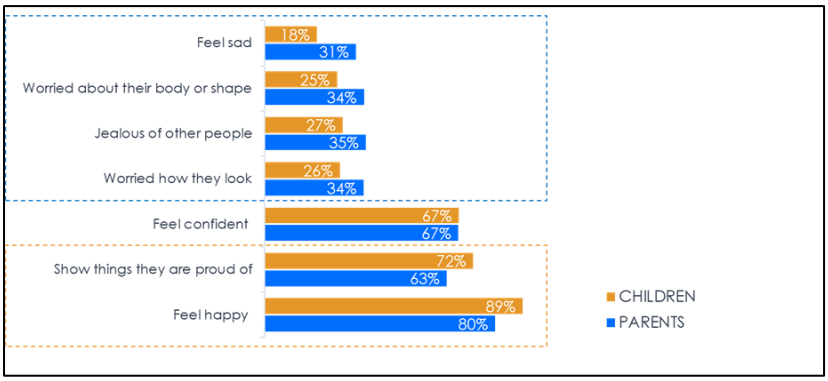


Table 2 Thinking about how being online and access to digital technologies impacts your child/children's/your own wellbeing, when your child/children goes online, does it do any of these things? Taken from June-22 wave; Parents N-2,001 ('Yes, definitely', 'Yes, mostly' excluding 'a mix' responses to make comparable with Children responses), Children N-1,000 ('Yes, definitely', 'Yes, mostly')

Positive versus negative impacts
The positive impact of the internet comes through more than negative impacts for both parents and children. 'Feeling happy' was the most selected option for both parents (80%) and children (89%). Also, 'showing things they are proud of' was widely agreed with (63% parents, 72% children).

Parents with greater confidence in online safety have greater positive responses to the internet as well. For example, 84% of confident parents acknowledge the internet makes their children 'feel happy' compared to 72% of parents who lack confidence.
This is also true of the more negative traits. For example, 38% of confident parents say the internet makes their children 'feel sad'. However, just 18% of unconfident parents say the same.

Parents of boys versus parents of girls

Additionally, parents of boys were more likely to identify the positive impact of the internet when compared to parents of girls. This includes feelings of feeling happy, proud and confident. Also, parents of older teen boys (15-16) were significantly more positive that the internet made their sons more confident (48% vs. 42% overall).

'Definitely / Mostly'	Total - all parents	Boy, 11 and under	Boy, 12-14	Boy, 15-16	Girl, 11 and under	Girl, 12-14	Girl, 15-16
Makes your child/children feel happy	57 %	59%	59%	60%	54%	54%	57%
Let's your child/children show people things they are proud of	44 %	48%	47%	45%	41%	44%	42%
Makes your child/children feel confident	42 %	46%	46%	**48%**	39%	39%	43%
Makes your child/children feel worried about their body shape or size	27 %	30%	**35%**	29%	23%	**34%**	28%
Makes your child/children jealous of other people	27 %	30%	**37%**	30%	**23%**	32%	25%
Makes your child/children feel worried about how they look	27 %	30%	**35%**	31%	23%	**33%**	25%
Makes your child/children feel sad	25 %	28%	**35%**	26%	**21%**	**31%**	21%

Table 3. Thinking about how being online and access to digital technologies impacts your child/children's wellbeing, when your child/children goes online, does it do any of these things? Taken from June-22 wave; Total – all parents N-2,000. Boy, 11 and under N-771, Boy, 12-14 N-340, Boy, 15-16 N-308, Girl, 11 and under N-627, Girl, 12-14 N-297, Girl, 15-16 N-286. Bold indicates significant difference against the Total score.

However, parents of boys were also more negative about the internet's impact, counteracting this positivity. Parents of 12–14 year old boys in particular scored higher across all the negative issues (i.e., body shape, jealousy, worried about looks and feeling sad).

This correlates with the lower levels of confidence in staying safe online for this group. Just 35% of 12-14 year old boys feel 'very' or 'totally' confident in staying safe online, compared to 39% for girls aged 12-14 and 48% for 15-16 year old boys.

Parents of girls aged 12-14 had similar concerns to parents of boys of the same age. Parents of younger girls (<11) were generally less critical about the role of the internet on their children. For instance, they scored lower on the negative impacts of jealousy (23%, 27% total) and feeling sad (21% vs. 25%).

Children's responses

Children were asked the same set of questions about the impact of the internet on their wellbeing, but the difference between genders was less obvious. The only significant differences between genders were seen in 'makes you feel confident' (71% amongst boys, 64% for girls) and in 'makes you feel worried about how you look' – this time lower for boys (22%) compared to girls (31%).

Similarly, when split by age, the only significant differences were in impacts more associated with older teens. These included 'worried about how you look' (24% for under 13s and 31% for 14–16-year-olds) and in 'worried about body shape or size' (22% for under 13s, 30% for 14-16).

Vulnerable children more significantly impacted

When looking at digital wellbeing of children more broadly, we can see a familiar pattern of those children with a vulnerability. Generally, they experience more of the negative aspects of being online. This results in some of the starkest differences seen between segments in the dataset.

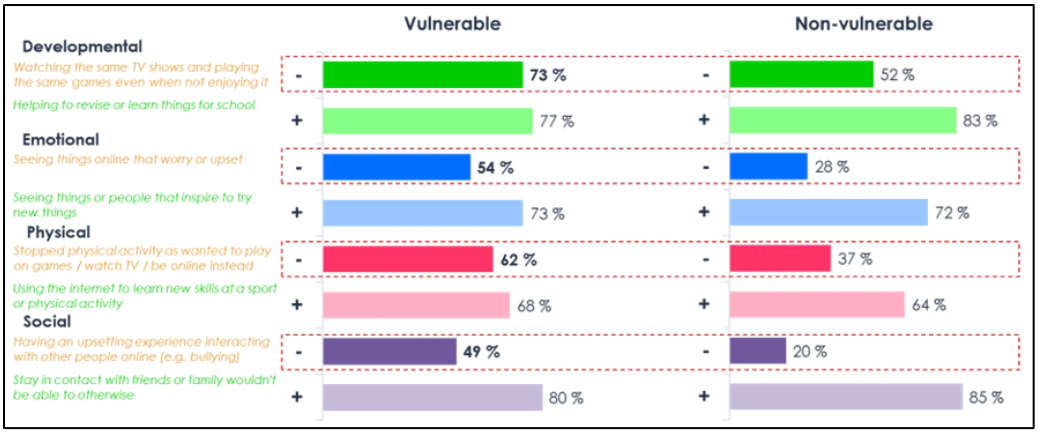


Table 4. Digital Wellbeing index measures asked in June-22 children's tracker. Bold figures show the significantly higher score compared to the total. Vulnerable N-202, Non-vulnerable N-805. Full descriptions for each dimension in the Appendix.

Impacts across developmental, emotional, physical and social wellbeing

When assessing the **social** aspect of children's wellbeing, we used the statement 'having upsetting experiences interacting with other people online (e.g., bullying)'.

We can see that nearly half of children (49%) with a vulnerability experienced this ('all the time', 'quite a lot'). This is compared to just one in five of children without any vulnerabilities. Similarly large differences were seen between vulnerable and non-vulnerable in 'unenjoyable repetitive digital behaviours' (73% to 52%; Developmental) and 'seeing upsetting things online' (54% to 28%; Emotional).

However, the positive scores across the digital wellbeing areas were not significantly lower for those classed as vulnerable. In fact, in some cases the score was higher. For example, 83% of vulnerable children agreed with '[the internet] helps me to revise or learn things for school' in **developmental** compared to 77% of non-vulnerable children. Again, this shows that this group of children had similar levels of positive experiences as their non-vulnerable peers.

Varying results in vulnerable children of different ages

When we looked at parent scores of vulnerable and non-vulnerable children, the results were even more noteworthy. Parents of vulnerable children scored significantly higher for all measures — both positive and negative ones — compared to parents of non-vulnerable children.

When looking at the breakdown of the ages of the vulnerable children, we can see interesting differences.

	Parents of vulnerable children		
	Aged 4-10	Aged 11-13	Aged 14-16
Developmental			
Watching the same TV shows and playing the same games even when not enjoying it	78 %	79 %	80 %
Helping to revise or learn things for school	58 %	55 %	63 %
Emotional			
Seeing things online that worry or upset	60 %	59 %	58 %
Seeing things or people that inspire to try new things	73 %	70 %	75 %
Physical			
Stopped physical activity as wanted to play on games / watch TV / be online instead	69 %	70 %	73 %
Using the internet to learn new skills at a sport or physical activity	59 %	53 %	58 %
Social			
Having an upsetting experience interacting with other people online (e.g. bullying)	43 %	34 %	39 %
Stay in contact with friends or family wouldn't be able to otherwise	59 %	58 %	64 %

Table 5. Digital Wellbeing index measures asked in June-22 parent's tracker. Bold figures show the significantly higher scores against the total. Parents of vulnerable children N-797; 4-10 n-394, 11-13 n-208, 14-16 n-195.

Generally, parents of vulnerable children aged 11-13 have the lowest scores amongst the age ranges. Although still significantly higher than non-vulnerable children, parents of this age group saw less of the positives and negatives of the internet for the children compared to parents of older and younger vulnerable children.

The other age groups have more varied responses. Some measures being more age specific than others may explain this. 'Stopped physical activity as wanted to play on games / watch TV' may be higher for those aged 14-16 (73%) compared to under 10s (69%) because media and internet consumption levels differ significantly between these age groups.

However, being bullied online may be a greater concern for parents of younger children (43%) compared to older children (39%) where maturity levels and greater support networks exist.

Conclusion
Vulnerable children and their parents recognise that their status puts them at greater risk of some of the negative aspects of being online. Due to the varied responses by parents of vulnerable children, tailored age-specific guidance is needed for this group. This will ensure that vulnerable children get the best out of digital and have the correct support in place when bad experiences occur.

Inclusive Digital Safety hub

VISIT HUB

Children's Wellbeing in a Digital World 2023
We will continue to measure and track the important factors that help us better understand the impact of digital on children's wellbeing. Our second annual report on Children's Wellbeing in a Digital World will be released in January 2023.

Appendix
Methodologies from research sources

- Parent tracker: N-2,000 UK parents of children aged 4-16 years old
- Children tracker – N-1,000 9–16-year-olds representative of the UK
- Both surveys are conducted twice per year

For further information, visit https://www.internetmatters.org/hub/research/impact-technology-on-childrens-digital-wellbeing/

Internet matters.org

Internet Matters Twitter - @IM_org

Win a trip to Sky Up Academy Studios for your #KS2 class with Digital Matters. Simply register with the platform and then enter at the link below https://www.internetmatters.org/digital-matters/win-with-digital-matters/	
Do you know what #doxxing is? Learn how it might affect your child and what you can do to keep them safe https://www.internetmatters.org/hub/news-blogs/what-is-doxxing-and-how-can-you-keep-your-child-safe/	

Childnet

Childnet

Blog - Upcoming updates for users of WhatsApp – a guide

Did you know that there are over two billion users signed up to WhatsApp? If you and your family are among them then this blog can tell you more about the recently announced privacy updates.

What is WhatsApp?
Launched in 2009, WhatsApp is a free messaging app which allows you to send texts, images, and videos to each other, as well as having conversations over both video and voice call.

WhatsApp requires a minimum age of 16, and users only need a phone number to sign up for an account.

"View Once" messages on WhatsApp
Recently, WhatsApp introduced the ability to send "View Once" photos and videos.

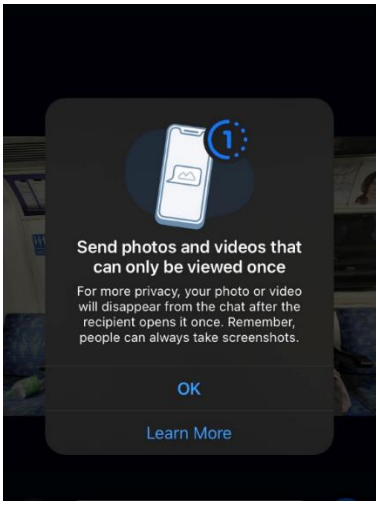
When you receive a View Once image the photo will not be stored on their device and will disappear once the user has viewed it.

To send a View Once message, click on the icon in the text box after selecting an image or video to send as normal, and it will provide you with the option for recipients to View Once.

WhatsApp messages are end-to-end encrypted – this means that nobody except you and the person you are messaging can see the content of your chat.

In the next couple of months, WhatsApp will be rolling out a “Screenshot Blocking” feature which will enable you to block others from taking screenshots of a View Once message.

Although settings such as View Once do give you some control over what they are sharing and who can see it, it is important to remember to think carefully before you share online.



The message prompted when opting to send a View Once message

Who can see when I’m online on WhatsApp?
When using WhatsApp, you may have noticed timestamps of the last time a contact was “seen online”, referring to the last time they clicked on the app.

WhatsApp have announced that, later this month, you will be able to control which of your contacts can and can’t see the last time they were online.

Leaving a group without sending a notification
The final update that WhatsApp have announced means that you can leave group chats silently.

Rolling out this month, you will be able to exit a group chat without notifying everybody in that chat. A notification will still be sent to the admin of this group that you have left but this will not be viable more widely.

This could ease the pressure for users who do not wish to be in a group chat but do not want others to see that they have left it.

For further information, visit https://www.childnet.com/blog/upcoming-updates-for-users-of-whatsapp-a-guide/

TAKE FIVE

TAKE FIVE TO STOP FRAUD™

Take Five National Campaign

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	CHALLENGE	PROTECT
Taking a moment to stop and think before parting with your money or information could keep you safe	Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.	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 or 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;

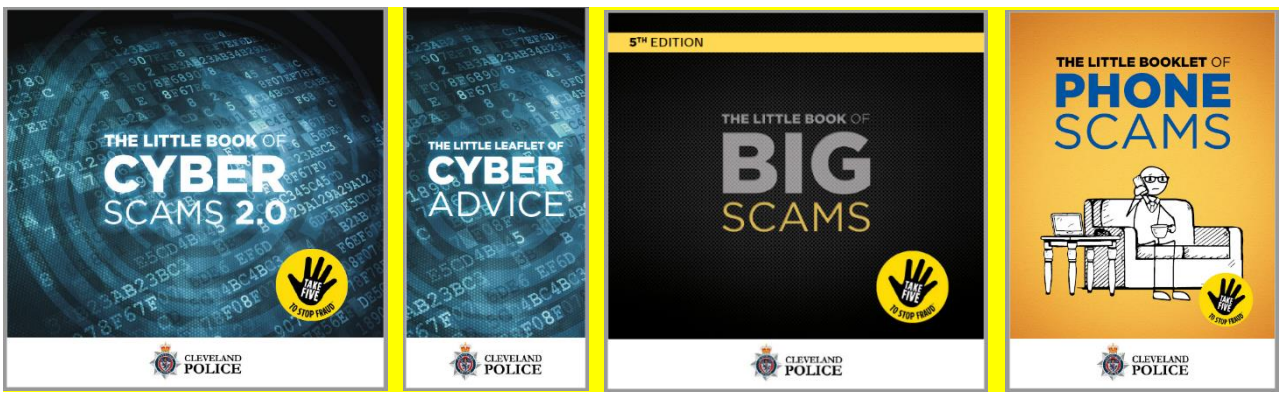
www.actionfraud.police.uk
www.getsafeonline.org
www. stopscamsuk.org.uk
www.ncsc.gov.uk/cyberaware
www.nationalcrimeagency.gov.uk
www.ncsc.gov.uk
www.internetmatters.org
www.childnet.com
www.takefive-stopfraud.org.uk

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.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"