CLEVELAND POLICE

Cyber Crime Newsletter

MAY 2023

CONTENTS

ACTION FRAUD

Holiday Fraud

Action Fraud, the national reporting centre for fraud and cybercrime, has published new data showing that in the last financial year, it received 6,457 reports of holiday fraud, amounting to over £15m lost.
Victims reported losing a total of £15,319,057, a 41 per cent increase on last year's results, which amounts to an average loss of £2,372 per victim. From May – August alone, more than £4.6m was lost.

With the summer months seeing the highest levels for holiday fraud reports, Action Fraud has launched a national awareness campaign today to urge the public to think twice before booking a holiday, so consumers don't get burnt before they are on the beach.

Pauline Smith, Head of Action Fraud, said:
"With summer only just around the corner, we enter a period where fraudsters ramp up efforts to catch out unsuspecting members of the public.
"Scammers prey on people wanting to find a good deal online – whether that's cheap flights, great hotels close to the beach at discounted rates or package holidays that undercut well-known travel operators and brands, people are more than willing to snap up a deal which sometimes comes at a heavy cost.
"When booking a holiday here or abroad, it's important to do your research before handing over any money and to double check any website. To avoid the wave of crime this summer we encourage people to stop, check and research before paying. If it sounds too good to be true – it most definitely is."

Anna Bowles, Head of Consumers and Enforcement at the UK Civil Aviation Authority, which runs the ATOL financial protection scheme, said:
"Before booking any trip abroad it is always worth doing some homework before you part with any money to make sure you limit your risk of being impacted by fraud. Make sure you research the company you're booking through - check reviews and ensure that your booking includes all the extras you're expecting, such as baggage allowance and transfers.
"We also recommend some simple measures to financially protect your well-earned holiday, including using the atol.org website to check your trip is financially protected by ATOL, consider paying by credit card and taking out travel insurance as soon as you book. This will add extra layers of protection against anything going wrong with your booking."

Data revealed that the top 10 hotspots of people being caught out by holiday fraud in the UK were as follows: London, West Midlands, Greater Manchester, Thames Valley, West Yorkshire, Hampshire, Essex, Sussex. Avon and Somerset and Kent.

Interestingly, People in their 20s and 40s who reported losses accounted for 44 per cent of all reports, further dispelling the myth that only older people are targeted by fraudsters.

Holiday fraud encompasses many different tactics employed by criminals to dupe unsuspecting members of the public. The most frequent frauds are clone comparison websites, airline websites and holiday websites.

At a quick glance it would appear you are on a trusted site, whereas in reality the URL has been changed. Here, victims assume they are on the genuine site and willingly hand over money at a great cost.

Fake confirmation emails or booking references are even sent, which has resulted in some cases of victims only realising they have fallen victim to fraud when they are at the airport to check in for their flight to be told that their booking does not exist.

An emerging trend is fraudsters using counterfeit Air Travel Organisers' Licensing (ATOL) protect numbers on their fake webpage. All credible and trusted companies are provided with a number that shows the company has passed the regulatory checks by ATOL, with this number being unique to the website. Recently, fake websites have used duplicate or fabricated numbers which have been edited onto an ATOL logo.

ATOL recommends double checking all numbers on websites and with travel operators before handing over any money. If you do pay, use a credit card as this can offer greater protection should you lose your money.

Top tips to avoid falling victim to holiday fraud.

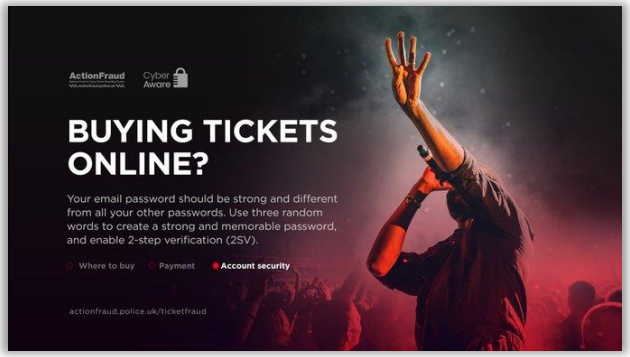
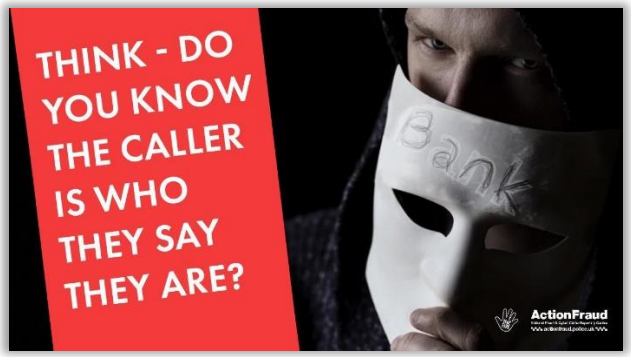
- **Do your own research**: Booking your trip via a company you haven't used before? Do some research to check they're legitimate. Read feedback from sources that you trust, such as consumer websites. You can find a company's official website by searching for them on Google or another trusted search engine.
- **Look for the logo**: Check whether the company is an ABTA Member. Look for the ABTA logo on the company's website. If you have any doubts, you can verify membership of ABTA online on their website. If you're booking a flight as part of a package holiday and want more information about ATOL protection, or would like to check whether a company is an ATOL holder, visit the ATOL or CAA website.
- **Pay safe**: Book your holiday with a credit card, if you have one. Most major credit card providers protect online purchases, and are obliged to refund you in certain circumstances. Using a **credit** card (rather than a **debit** card) also means that if your payment details are stolen, your main bank account won't be directly affected.
- **Secure your email:** If your email is hacked, it could allow a criminal to access information about your holiday booking. Use 3 randoms words to create a strong password for your email that's different to all your other passwords. If you're offered 2-step verification to protect your email and social media accounts, always use it.

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

If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040, or call Police Scotland on 101.

For more information visit https://www.actionfraud.police.uk/holidayfraud

---

AF Action Fraud Twitter @actionfrauduk	
Buying tickets online? If your email account gets hacked, you could lose your tickets too. Protect your important online accounts with passwords you don't use anywhere else. For more info, visit: Cyberaware.gov.uk #TicketFraud	
If you or someone you know receives an unexpected call by someone claiming to be from your bank or a police officer, verify who you are speaking to. Hang up, wait five minutes and call back on a number you know is genuine. #CourierFraud	
Looking to bag a bargain online? Follow this advice on how to shop safely and spot a scam website. https://www.ncsc.gov.uk/guidance/shopping-online-securely	
Help protect your friends and family who are online dating by raising awareness of the signs of romance fraud. It could help protect them and their money. #romancefraud	

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

GET SAFE ONLINE
Your Digital Footprint

Every time you use visit a website, send or receive a message or email, buy or book anything online, comment on a post, upload a photo or find directions on your phone, you're adding to your digital footprint. When you stream music, make a video call or use a smart speaker, that adds to your digital footprint too.
And when you post a photo of your children or friends, you're also adding to *their* digital footprint, even though they may not have agreed to it.

One of the commonplace consequences of having a digital footprint seeing an ad for something you've searched for online on your social media feed, or as a pop up. But there can be other, more serious outcomes too. Like when you don't make the shortlist for a job because a prospective employer has seen something you posted five years ago. When you're scammed because you've inadvertently shared some confidential details. Or when somebody sells on your personal information to a third party.

We could probably all benefit from thinking more about the trail we leave online. And how it could affect us and others now and into the future.

What happens when you have a digital footprint?
Your digital footprint is part of your online history and can potentially be seen by other people, or tracked and held in multiple databases, however careful you are with your privacy settings.

Here are just a few examples of what can happen:

- Prospective or current employers can look into your and family members' background.
- Applications for schools, colleges, universities, scholarships, clubs or even sports teams could be rejected.
- You, family members or friends could fall victim to fraud or identity theft … or both.
- Your children could be at risk of criminal activity threatening their online or physical safety.
- Records of your online activity could fall into the wrong hands, including organised crime groups.
- Tech companies such as browser and search engine providers can track and record what you've searched and viewed. This, in turn, could be shared with other parties including law enforcement agencies.
- You could be refused life, medical, property or vehicle insurance based on information you have shared online.
- Advertisers can track your movement from site to site to gauge your areas of interest.
- Companies can target you with specific marketing content on social media and other websites. You could also receive emails, letters or phone calls from these companies.

- Entertainment providers (such as music or films) could target you with unwanted recommendations for content based on what you download or stream.

Your top tips

- Think twice before sharing information about yourself, family members or friends that would be better kept private. That goes for social media, forms on websites and apps, responding to texts and messages and when taking part in surveys and quizzes.
- Think before you post. Even if your social media privacy settings are set up correctly, there's no guarantee that your posts or photos won't be shared beyond those who you want to see them.
- Be aware that every time you visit a website, your activity is visible to tech companies like website owners, browsers and search engines.
- Read terms and conditions and data privacy policies on websites and apps before providing any personal data or making transactions. What can the providers do with your data, and why would you agree to it? If you're not comfortable with the information being requested, don't provide it.
- Check geolocation settings on mobile devices, apps and cameras. If you don't want anybody to know your whereabouts – or where you've been – disable them.
- Never stop enjoying the many excellent benefits of using the internet, but always bear in mind the digital trail you may be leaving, who may be able to access it and how they may be able to use it.

For more information visit https://www.getsafeonline.org/digitalfootprint/

GET SAFE ONLINE
NEWS
Over £1.2 billion stolen through fraud in 2022, with nearly 80% of advanced push payment fraud cases starting online

UK Finance has released its Annual Fraud Report, detailing the amount of money reported by UK Finance members that was stolen by criminals through financial fraud in 2022.

- Over £1.2 billion was stolen by criminals through authorised and unauthorised fraud in 2022, equivalent to over £2,300 every minute.
- 78% of advanced push payment fraud (APP) cases start online and 18% start via telecommunications.
- The banking and finance industry prevented a further £1.2 billion of unauthorised fraud from getting into the hands of criminals.

Over £1.2 billion was stolen through fraud in 2022, a reduction of 8% on 2021. The number of fraud cases across the UK was down 4% to almost three million cases.

Unauthorised fraud

Within the total figure, unauthorised fraud losses across payment cards, remote banking and cheques reached £726.9 million in 2022, a decrease of less than 1% compared with 2021.

Remote purchase fraud, where a criminal uses stolen card details to buy something online, over the phone or through mail order, remains the biggest category of losses at £395.7 million – although this

figure was again down on the previous year. Fraud on lost and stolen cards increased by 30% to £100.2 million and card ID theft, where a criminal opens or takes over a card account in someone else's name, almost doubled to £51.7 million. Victims of unauthorised fraud cases such as these are legally protected against losses.

Authorised fraud
Authorised push payment (APP) fraud losses reached £485.2 million, down 17% compared with 2021. Within this, 57% of all reported cases related to purchase fraud, with case volumes breaking 100,000 for the first time. Investment fraud continued to be one of the largest proportions of APP losses (24%), although there was a 34% reduction compared with 2021. Overall, the amount of APP fraud losses reimbursed increased by 5% in 2022 compared with the previous year.

Fraud origination
The banking and finance industry spends billions of pounds each year fighting fraud and economic crime. However, the majority of fraud originates outside the banking sector and UK Finance has conducted analysis on over 59,000 APP fraud cases to show the sources of fraud.

The analysis showed that 78% of APP fraud cases originated online – these tend to include lower-value fraud such as purchase fraud and therefore account for 36% of losses. Social media platforms account for the greatest number of online fraud cases – around three quarters of online fraud starts on social media.

Meanwhile, 18% of fraud cases originate via telecommunications – these are usually higher value cases, such as impersonation fraud, and account for 44% of losses.

Given that so much fraud is initiated from criminal activity taking place through online platforms and telecommunications, UK Finance and its members have long called for far greater cross-sector action to tackle the problem at source.

David Postings, Chief Executive at UK Finance, said:
"Fraud has a devastating impact on victims and over £1.2 billion was stolen by criminals last year. The banking and finance sector is at the forefront of efforts to tackle this criminal activity. The sector spends billions on detection and prevention and also refunds people who have fallen victim, even if the fraud originated outside the banking system.
"Our data also makes clear just how much fraud emanates from online platforms and through telecommunications. The government's new fraud strategy rightly says we need to focus on stopping it at source and that these other sectors need to do far more to tackle the problem they are facilitating."

For more information visit https://www.getsafeonline.org/personal/news-item/over-1-2-billion-stolen-through-fraud-in-2022-with-nearly-80-of-advanced-push-payment-fraud-cases-starting-online/

GET SAFE ONLINE

World Password Day is ten years old!

It's time to review your password security!

It's ten years since Intel Security gave that name to every first Thursday in May.
Passwords are crucial in protecting our digital identities, allowing us to do everything from online shopping to social media, email to banking, dating to gaming and everything else we do online that we take for granted. And, of course, we also need passwords to use our computers and mobile devices at work. On this day every year, World Password Day quite simply promotes better password habits.

Get Safe Online has lots of free, expert, easy to follow advice on choosing and using passwords on its website. Simply visit www.getsafeonline.org and enter 'passwords' in the search box.

However, here are some top tips which should help you to ensure you are using passwords correctly to keep your information, identity and finances protected.

- Devise passwords that are long (at least 12 characters) and complex, with a combination of upper and lower-case letters, numerals and symbols.
- Don't use family members', pets' or sports club names in your password as someone could guess these from your social media or other online activity.
- You could use three completely random words interspersed with numerals and symbols.
- Never use the same password for more than one account or website. If you do – and a cybercriminal finds out your login details – they can access your other accounts.
- Turn on two-factor authentication (2FA/MFA) for your important accounts.
- Don't store passwords on your computer or phone. Use a reputable online password manager that features two-factor authentication.

Please share these tips far and wide on social media, using the hashtag **#WorldPasswordDay.**

Incidentally, it was not Intel Security but security researcher Mark Burnett who first encouraged people to have a 'password day' in his 200 book *Perfect Passwords,* which you can still buy from Amazon and other good retailers.

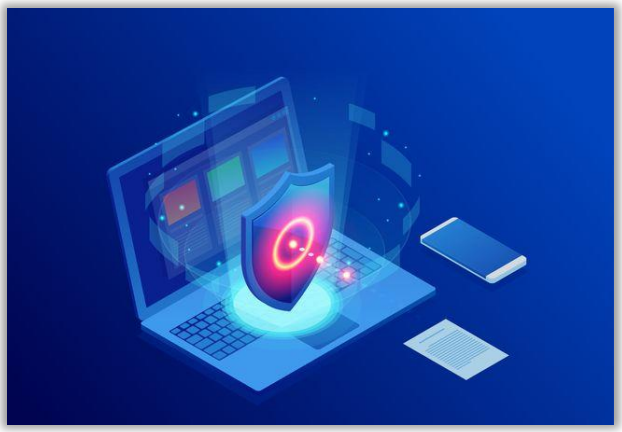
For more information visit https://www.getsafeonline.org/personal/news-item/world-password-day-2023/

Get Safe Online Twitter @getsafeonline

With the #CostofLiving still rising and having a massive effect on many people's lives, scammers are taking advantage by offering 'great deals' and 'freebies'. Seems too good to be true? Then it probably is! https://www.getsafeonline.org/personal/blog-item/frauds-you-may-encounter-during-the-cost-of-living-crisis/	
Fraudsters often use fake websites to scam their victims either for money, for personal information, or for both. Before you visit an unfamiliar website, why not check out whether it's likely to be legit or fraudulent on our fantastic, easy-to-use tool? https://www.getsafeonline.org/checkawebsite/	

NCSC – National Cyber Security Centre

Experts challenge myths around reporting cyber attacks to help break cycle of crime



Blog post from the NCSC and ICO aims to dispel common misconceptions that can discourage organisations from reporting a cyber-attack.

- A blog post from NCSC and ICO aims to dispel common misconceptions that can discourage organisations from reporting a cyber-attack.
- NCSC and ICO are concerned about incidents going unreported, which denies organisations the opportunity to learn from them and prevent future attacks.
- Advice on best practice offered to help organisations understand their responsibilities and the risk to their data and reputation.

Leading cyber security experts are pressing organisations to be more open about their experience of cyber-attacks, to encourage reporting and prevent future incidents.

In a new joint blog post, the National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO) identify six misconceptions that can discourage organisations from reporting attacks, particularly ransomware attacks, and is setting out to dispel them.

The misconceptions include the mistaken belief that reporting cyber-attacks to the authorities makes it more likely the incident will become public, and that paying a ransom automatically makes the incident go away.

With cyber-attacks continuing to cause significant disruption, the NCSC and ICO are concerned about incidents which go unreported because every 'hushed up' case that isn't shared or fully investigated makes other attacks more likely as no one can learn from them.

But being open with the authorities will give victims access to expert support and advice and will be taken into account favourably by the ICO when considering their regulatory response.

The six 'myths' which the NCSC and the ICO have identified as commonly held by organisations that have fallen victim to cyber incidents are:

1. If I cover up the attack, everything will be ok.
2. Reporting to the authorities makes it more likely your incident will go public.
3. Paying a ransom makes the incident go away.
4. I've got good offline backups; I won't need to pay a ransom.
5. If there is no evidence of data theft, you don't need to report to the ICO.
6. You'll only get a fine if your data is leaked.

Eleanor Fairford, NCSC Deputy Director for Incident Management, said:

“The NCSC supports victims of cyber incidents every day, but we are increasingly concerned about the organisations that decide not to come forward.

“Keeping a cyber-attack secret helps nobody except the perpetrators, so we strongly encourage victims to report incidents and seek support to help effectively deal with the fallout.

“By responding openly and sharing information, organisations can help mitigate the risk to their operations and reputation, as well as break the cycle of crime to prevent others from falling victim.”

Whilst the NCSC, as the national technical authority on cyber security, and the ICO, as the national data protection regulator, have different functions, both organisations work with victims of cyber incidents every day and have seen a wide range of incident responses.

Mihaela Jembei, ICO’s Director of Regulatory Cyber, said:
“It’s crucial that businesses are aware of their own responsibilities when it comes to cyber security. The fact remains that there is a regulatory requirement to report cyber incidents to the ICO, but transparency is more than simply complying with the law. Cyber-crime is a borderless and global threat and it’s through knowledge sharing that we can help organisations help themselves.

“It’s also really important that businesses do not lose sight of their basic cyber hygiene practices in a world where we are always hearing about new and exciting technologies and the risks they may pose.”

Victims that are proactive with reporting can benefit from expert NCSC advice and following this can positively impact the ICO’s response.

The blog post also addresses assumptions about data risk, highlighting that a lack of evidence that data has been stolen does not mean theft did not take place, while paying a ransom to criminals to restore services quickly can increase the likelihood of being retargeted and does not guarantee stolen information will not be leaked later.

The NCSC and ICO recommend that victims are open in the aftermath of an attack, reporting incidents via the government’s cyber reporting service and separately to the ICO to fulfil regulatory responsibilities. They also encourage sharing lessons learned with other organisations to help improve wider awareness and cyber resilience.

More guidance on how to effectively detect, respond to and resolve cyber incidents can be found on the NCSC website, including dedicated advice on handling ransomware attacks.

The NCSC is not a regulator; it provides support to victim organisations in confidence and does not share information about an incident with the ICO without an organisation’s consent. Victim **organisations should report breaches to the ICO.**

For more information visit https://www.ncsc.gov.uk/news/experts-challenge-myths-around-reporting-cyber-attacks-in-bid-to-help-break-cycle-of-crime

---

Top tips for staying secure online

Our top tips are:

Protect your email by using a strong and separate password

Cyber criminals can use your email to access many of your personal accounts, leaving you vulnerable to identity theft.

We're often told that the passwords to access our online accounts should be really strong, and not to use them anywhere else. This is especially true for the password for your **email account**. If you've used the same password across different accounts, cyber criminals only need one password to access **all** your accounts.

Always use a strong and separate password for your email; that is, a password that you don't use for any of your other accounts, either at home or at work.

If a criminal can access your email account, they could:

- access private information about you (including your banking details)
- post emails and messages pretending to be from you (and use this to trick other people)
- reset all your other account passwords (and get access to all your other online accounts)

Having a strong and separate password for your email means that if cyber criminals steal the password for one of your less-important accounts, they can't use it to access your email account. The NCSC encourages people to use password managers, which can create strong passwords for you (and remember them).

If you have re-used your email password across other accounts, **change your email password as soon as possible**. It should be strong and different to all your other accounts.

Ideally, you should use unique passwords for **all** your important online accounts (such as banking accounts, shopping/payment accounts and social media accounts), not just your email account. You should also provide additional protection by setting up 2-step verification (2SV) on your email account, which will prevent a criminal from accessing your email account even if they know your password

Install the latest software and app updates

Software and app updates contain vital security updates to help protect your devices 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.

Turn on 2-step verification (2SV)

Turning on 2SV is one of the most effective ways to protect your online accounts from cyber criminals. 2-step verification is recommended to help protect your online accounts.

You should protect your most important accounts (such as email, banking, social media and online shopping) by making sure you have **2-step verification** turned on for each of them.

2-step verification (2SV), which is also known as two-factor authentication (2FA) or multi-factor authentication (MFA), helps to keep cyber criminals out of your accounts, even if they know your passwords. The NCSC recommend you take time to set up 2-step verification on all your important accounts, even for ones that you've protected with strong passwords.

It's easier than you think for someone to steal your password.

Even if you've always looked after your passwords (and taken the time to create a strong one and avoided the worst passwords that millions of people still use), they can still be stolen through no fault of your own.

The most common way that passwords are stolen is when an organisation holding your details suffers a data breach. Criminals will use passwords stolen in the breach to try and access other accounts, a technique (known as 'credential stuffing') that works because many people use the same password for different accounts.

Criminals may also try and trick you into revealing your passwords by sending you links to scam websites asking you to log in, either by email, text message or direct messages/chat (a term known as 'phishing'). Even if your passwords are hard to *guess*, that doesn't make them any harder to *steal.* In other words, **even accounts protected with strong passwords will benefit from using 2-step verification.**

Password managers: how they help you secure passwords

Using a password manager can help you create and remember passwords.
We're often told that the passwords for our online accounts should be really strong, and to **not** use the same password anywhere else. Especially for those important accounts like email, banking, shopping and social media.

The trouble is, most of us have *lots* of online accounts, so creating *different* passwords for all of them (and remembering them) is hard.
This is where a password manager can help. A password manager (or a web browser) can store all your passwords **securely**, so you don't have to worry about remembering them. This allows you to use unique, strong passwords for all your important accounts (rather than using the same password for all of them, which you should *never* do).

Backing up your data

Safeguard your most important data, such as your photos and key documents, by backing them up to an external hard drive or a cloud-based storage system.

Most of us at some point have been unable to access important data, whether it's work documents, photos, videos, contact details or other personal information.
Making backups doesn't take very long and can usually be set up to take place automatically. So a little planning in advance to make backups could save you a lot of stress should the worst happen.

A backup is a copy of your important data that's stored in a separate safe location, usually on the internet (known as cloud storage), or on removable media (such as USB stick, SD card, or external hard drive). Once you've made a backup, if you lose access to your original data, you can restore a copy of it from the backup.

Most backup solutions allow you to choose what data is backed up, whether that's just documents and photos and videos, or the entire contents of your phone/computer (including the apps and programs you use).
As a rule of thumb, **you should back up anything that you value**. That is, anything that would inconvenience you - for whatever reason - if you could no longer access it.

Three random words

Use three random words to create a single password that's difficult to crack.
Combine three random words to create a password that's 'long enough and strong enough'.
Weak passwords can be cracked in seconds. The longer and more unusual your password is, the harder it is for a cyber-criminal to crack.

A good way to make your password difficult to crack is by combining three random words to create a single password (for example *applenemobiro*). Or you could use a password manager, which can create strong passwords for you (and remember them).

Avoid the most common passwords that criminals can easily guess (like '**password**'). You should also avoid creating passwords from significant dates (like your birthday, or a loved one's), or from your favourite sports team, or by using family and pet names. Most of these details can be found within your social media profile.

If you're thinking of changing certain characters in your password (so swapping the letter 'o' with a zero, for example), you should know that cyber criminals know these tricks as well. So your password *won't* be significantly stronger, but it *will* be harder for you to remember.

For details, please visit https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

---

NCSC Twitter @NCSC	
Protect your organisation from ransomware attacks with our guidance. Learn how to reduce the risk of an attack and what to do if your organisation is affected. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks	 ncsc.gov.uk Mitigating malware and ransomware attacks How to defend organisations against malware or ransomware attacks
Did you know you can forward scam SMS messages to us for free and we'll take care of them? Just forward the text to 7726	 ncsc.gov.uk Phishing: Spot and report scam emails, texts, we... How to recognise and report emails, texts, websites, adverts or phone calls that you think ar...

Childnet

Snapchat's New AI Chatbot and its Impact on Young People

Snapchat is an extremely popular social media platform used by young people to engage with each other through sharing stories, direct messages, and multimedia photo and video content.

Recently it has introduced a new Artificial Intelligence (AI) chatbot called "My AI" designed to help users with various tasks through their messaging section in the Snapchat app.

While this new feature can be helpful, there are some potential risks to young people who use this feature. In this article, we explore the latest AI chatbot on Snapchat and its potential impact on young people.

Are you looking for information about ChatGPT? Our partner Childnet has recently released guidance around supporting young people to use it safely and appropriately.

What is Snapchat?
Snapchat is a messaging app that allows users to share content, such as photos, texts and videos, i.e., 'Snaps'. Snaps only appear for a matter of seconds before disappearing from users' screens.

You can choose to send a 'Snap' directly to one other person, or you can post it on your 'Story' so that all your contacts can view it. Your contacts can view this for 24 hours before it disappears and can be found in your archives if you choose this setting.

What is "My AI" and how does it work?
My AI is a computer program designed to have conversations and dialogue with users like a person. As you input information, either by typing or speaking, it responds to you.

If you ask it a question, it searches available databases, gathers information, and formulates a response. As you engage with My AI, it grows in knowledge and becomes more specific to your interests and interactions. Parents and caregivers should be aware of the potential impact that My AI can have on young people who are using Snapchat.

Potential Impact on Young People's Mental Health
Snapchat's new My AI tool has the potential to affect young people's mental health. While it can provide helpful information and support, it may also contribute to feelings of isolation and loneliness.

As interactions with AI can feel like conversations with real people, young people may rely too heavily on the chatbot for emotional support or entertainment.

Since My AI uses its own knowledge and data, it may not always understand the subtle details in conversation or the slang used by young people. This could lead to the chatbot reinforcing negative self-talk and spreading harmful ideas.

It's important to keep in mind that chatbots, like My AI, cannot replace real conversations. Parents, carers, and professionals who interact with young people can help promote the right mindset when using My AI by reminding them that it may not be completely accurate.

Young people are encouraged to seek advice from a trusted adult if they encounter anything that makes them feel uneasy or concerned while using My AI.

Advertising within My AI
Snapchat is also testing sponsored links in My AI. This new feature will allow brands to advertise to Snapchat users through the My AI. Snap has also announced new ad products for Spotlight and Stories. While this may be seen as a new way for brands to reach their target audience, it may also lead to an increase in advertising on the platform.

Parents and carers should be aware of My AI ads' impact on young people, especially if some face challenging behaviour like compulsive buying or overspending. To help keep young people safe from potentially inappropriate content, Snapchat suggests parents use parental control options.

My AI Privacy Concerns
Snapchat has teamed up with OpenAI to incorporate the cutting-edge language model "GPT-3" into its platform. According to Snapchat My AI will use this technology to provide users with more accurate and helpful responses. However, some people have raised concerns about privacy for younger users.

Parents and carers are advised to remind young people to consider what personal details they share within the chat. To help address this issue, it may be a good idea to develop more resources in schools and other organisations to help young people navigate chatbot interactions and understand how to protect their personal information.

Guidelines to Help Young People Use My AI Responsibly
When it comes to helping young people use tools like Snapchat's My AI, there are a few guidelines parents and carers can follow:

1. Encourage open communication: It's important to have conversations with your child about their use of the chatbot. Encourage them to talk to you if they have any concerns or questions.
2. Set boundaries: Establish guidelines for when and how long your child can use the chatbot. This can help ensure that they don't become overly reliant on it for emotional support.
3. Monitor usage: Keep an eye on your child's use of the chatbot. If you notice any changes in their behaviour or mood, it may be a sign that they're struggling with something and need additional support.
4. Remind them of the limitations of chatbots: It's important to remind your child that chatbots, like Snapchat's My AI, cannot replace real conversations. Encourage them to seek out real human connections when they need emotional support.
5. Teach them about online safety: Remind your child to be careful about what personal details they share with the chatbot. Encourage them to only share information that they're comfortable with.

By following these guidelines, parents can help young people use chatbots like My AI in a safe and responsible way.

Conclusion
Snapchat's My AI tool offers many benefits, such as easy access to information and a virtual buddy that learns your preferences. However, parents and caretakers need to be aware of potential pitfalls to promote healthy use of My AI. As this field of technological advancement rapidly grows, we'll aim to keep our audience informed of changes.

For details, please visit - https://www.childnet.com/blog/snapchats-new-ai-chatbot-and-its-impact-on-young-people/

Childnet

Virtual reality – a guide for parents and carers

Ranging from high tech devices to cardboard phone holders, you may have seen Virtual Reality (VR) headsets on TV, at friends' houses, or even have one yourself.
Whatever experience you have with VR, this blog looks to cover the key things parents and carers need to know, as well as some considerations about keeping your children safe when using VR.

What is VR?
VR is a relatively new technology that allows users to fully immerse themselves in a virtual, computer-generated world. Users can use headsets to transport themselves to different settings, ranging from realistic cities or locations to spaceships or a favourite game or movie.

By using screens within headsets, users are fully surrounded by the virtual sights and sounds and can move and explore by physically moving in the real world.

VR headsets are becoming more widely available, and there is even new equipment out there that allows users to touch and feel things in VR too.

Why do young people like using VR?
VR headsets are an exciting new piece of technology that young people may be increasingly experiencing.

There are many reasons people, both younger and older, may enjoy using VR – not just for fun and leisure, but also for practical and educational reasons too.

From riding on a rollercoaster in space, to transporting back in time to explore Ancient Rome, VR gives a lot of opportunities to experience new things and find out information in an exciting way.

Many young people use VR headsets to play games. Interactive games within VR range across genres, age ratings and interactivity. Many VR games require users to use handsets and headsets to act out actions within a game, and to physically move in the real world in order for the character or avatar to move within the game.

Movement stretches beyond just walking in many VR experiences: for instance, handheld controllers can be linked with the headset to enable using your arms to play tennis, for instance.

What are the age restrictions around VR?
Many VR headsets have a minimum age restriction of 13 years old – this is due to a range of physical and legal restrictions around using this technology.

VR headsets need to take in and process information about us, like where we move and what we look at, for them to work. They also collect data on how long we look at things, ideas about our height and how much our pupils dilate when looking at different things.

It is illegal for companies to collect this data from under 13s in the UK without parental consent, which is why the minimum age to use most VR headset is 13 years old.

Considerations for using VR with young people
If you decide to get a VR headset for your family or are thinking about getting a headset with a lower age rating, there are some considerations you can take to help keep your family safe when using this technology.

Consideration	What this means	What you can do
The content young people might see or experience in VR	VR is designed to make things more realistic and immersive, so violent or gory visuals may be frightening.	Research and test any VR games or experiences before your children use them. Check the age ratings of the games they want to play or apps they want to use on sites such as PEGI or The Family Gaming Database. It is safest to stick to solo experiences (e.g., one player games) and avoid 'open' digital spaces where they might interact with people who may not be kind and considerate. You can also stream what they are seeing on to a TV screen. Search how to do this for the devices you have.
Risk of injury	As VR relies on a user moving in the offline world, users can get carried away and physically injure themselves or knock over things in the home. Although it may not be a problem for adults, VR headsets can be heavy for younger children and as using VR requires physical movement they may find it difficult or uncomfortable to use technology in this way.	Clear the area where you are using VR, including furniture and cables. Keep an eye on them too, as you can redirect them if they get too close to trip hazards!
Physical discomfort using the headset	The headsets used to interact within VR are often designed to be used by adults rather than young people, this can mean that the devices themselves can be heavy for younger users.	Talk to your child about how they feel when using the VR headset and set clear steps they can take if they feel uncomfortable. This could include taking off the headset, only going on for specific amounts of time, or talking to an adult.
VR sickness	Similar to 'car sickness' VR headsets can make some users feel queasy when using them. Some users find the movement makes them feel nauseous.	Warn your child that this could happen and to take the headset off if they start to feel unwell.
Contact from other users	Users of all ages can mix and there are not effective age	Some VR headsets allow you to create a virtual bubble around

	restrictions in place. Not all users are kind and considerate. When interacting with users in "open" spaces, they may say something inappropriate, or young people may overhear swearing and other unsuitable content.	your game character. There is often the option to 'teleport' to a safe space or another VR world if other users are an issue. It is possible to block and mute other users too.

Getting help and reporting in VR
Online safety in VR is improving, but platforms are also keen on creating new experiences and getting more users.

If you want to approach your child about online safety matters and VR, why not create a Family Agreement? It'll give you a chance to model positive uses of technology that you use yourself and support your child in learning about and using the safety features in the technology that they use.

The most important thing is to make sure your child knows to turn to you if something worries them online, and having a conversation about life online can help them remember this.

For details, please visit - https://www.childnet.com/blog/virtual-reality-a-guide-for-parents-and-carers/

Childnet @childnet	
You may want to take screenshots of entertaining moments from a video call. However, it's important to have consent from everyone in the video call before taking it or sharing it. More top tips on video calling https://www.childnet.com/help-and-advice/video-calls-11-18-year-olds/	
Worried about your child's safety while using #ChatGPT? Check out this guide for parents and carers: https://www.childnet.com/blog/what-do-i-need-to-know-about-chatgpt-a-guide-for-parents-and-carers/	

What are algorithms?
How to prevent echo chambers and keep children safe online

Algorithms are an important part of social media feeds, but they create echo chambers. These echo chambers lead to issues of online hate, misinformation and more.

What is an algorithm?
An algorithm is a set of instructions that a computer program follows to perform a specific task. There are different types of algorithms, but on social media, the list of instructions decides what content to show to users. Algorithms do this by learning from users' interaction with other content, such as through likes, comments and shares.

Social media uses algorithms to keep users engaged on their platform by providing relevant and interesting posts. This is similar to how websites collect cookies to show users advertisements relevant to them.

What is an echo chamber?
An echo chamber is a situation where people only see information that supports their current beliefs and opinions.

Social media echo chambers work by 'hiding' content that is irrelevant based on the algorithm. This is content that users swipe past, don't interact with or block on their feed.
However, the content users don't see may help create a balanced view of the world. So, not seeing this content may create confirmation bias where content users see confirms their beliefs with giving different points of view.

How do algorithms create echo chambers?
Algorithms create echo chambers through showing users content similar to that which they already engage with. If that content is hateful, the suggestions will also show hateful content. For example, many users who follow Andrew Tate find themselves surrounded by similar content that spreads misogyny and online hate against women and girls.

Computers and algorithms cannot assess the information they suggest. As such, an algorithm cannot make the choice to show users balanced views or facts. The echo chambers then instead show users that 'everyone' believes the same as them.

However, these users are only able to see content from those with similar views. Therefore, it is up to the individual to think critically about what they see and interact with.

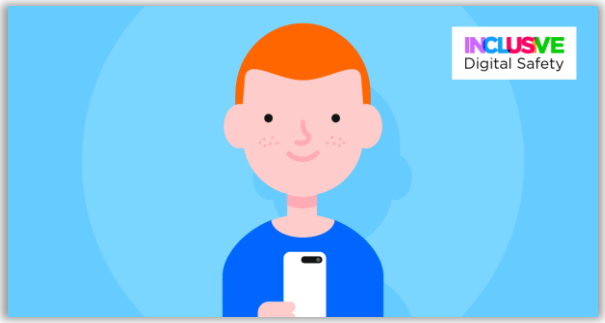
What are the risks of echo chambers for children and young people?
Online echo chambers may lead some users to becoming more extreme in their views because they don't experience opposing views. This can lead to exposure to harmful content, conspiracy theories and radicalisation.
Children are also at greater risk for believing misinformation or being manipulated online. They may not yet have the critical thinking or digital literacy skills needed to be a discerning consumer of content because of their stage of brain development. As such, they are more likely to believe extreme or controversial ideas.

Additionally, exposure to online hate like racism and misogyny or other harmful world views can take its toll on children's wellbeing and growth. Seeing content that is inappropriate, violent or hateful on a regular basis can lead to desensitisation. As a result, they might not be aware that the content they see is harmful and are therefore unable to know when it's right to take action.

Children and young people using social media may not yet understand how algorithms work. So, it's important to help them learn how to manage content suggestions to take action themselves.

How to prevent echo chambers on social media
While algorithms can offer tailored social media experiences unique to each user, it's important to recognise potential risks and solutions. Help children learn how to recognise when they're in an echo chamber, how to prevent it from happening and where to get help when needed.

For details, please visit - https://www.internetmatters.org/hub/news-blogs/what-are-algorithms-how-to-prevent-echo-chambers/

Internet Matters @IM_org	
While all children have some risk of experiencing #onlinesafety issues, there are some that children and young people in care are more likely to experience. Learn how to support them with our guides https://www.internetmatters.org/inclusive-digital-safety/advice-for-parents-and-carers/supporting-children-in-care/	
How do you manage in-game spending? With so many stories of children unknowingly spending hundreds or thousands on perks in their #videogames, it's important to talk to your child about these risks to prevent it from happening to them. https://www.internetmatters.org/resources/online-money-management-guide/in-game-spending-tips-to-support-young-people/	

TAKE FIVE

People under 35 are more at risk from impersonation scams

People under 35 are more likely than older age groups to have been targeted in an impersonation scam and be swayed to provide personal or financial information, according to a new survey by UK Finance's Take Five to Stop Fraud campaign.

An impersonation scam is where a criminal contacts you pretending to be a person or organisation you trust. These scams can be very sophisticated and often start with attempts to get you to disclose personal and financial information. They then use this information to impersonate someone you trust, making it seem more believable, but their ultimate aim is to try to steal your money.

71 per cent of 18 to 34-year-olds surveyed said they had been contacted by an impersonation scammer, with 73 per cent of those targeted saying they had subsequently been persuaded to either send money or share personal information.

Under 35's were more likely to be approached in a variety of ways (over the phone, email, text and WhatsApp). A recent and growing impersonation scam involves fraudsters sending WhatsApp messages that appear to be from a friend or family member with a seemingly genuine request for money, such as being stranded overseas or urgently needing to pay a debt or a bill.

Risk of misplaced confidence
Across all age groups, significantly more people rated themselves as being difficult to trick rather than easy to trick, but this level of confidence could put them at risk, as fewer than half said they will always take steps to check if the organisation or person can be trusted when asked for personal information out of the blue.

Katy Worobec, Managing Director of Economic Crime at UK Finance, said:
An alarming number of people fall for impersonation scams and whilst our findings show that younger people are the ones who are often targeted, it's important to remember that anyone can be caught out by these criminals and that you should always stay alert.

"Given the level of sophistication of some of these scams, we urge the public to be wary of unexpected requests for personal or financial information. Often these criminals will take their time to gather as much information about you as possible, so it's important that people follow the advice of the Take Five to Stop Fraud campaign – always be cautious of any messages or calls you receive out of the blue and avoid clicking on links in unsolicited emails or text messages.

Impressionist and former Britain's Got Talent contestant Francine Lewis from Blackpool knows only too well how convincing criminal scammers can be.
Francine and her family fell for a scam which cost them tens of thousands of pounds. Francine says:
I always thought that if I was targeted by a criminal I'd see straight through their scam, but these people are incredibly persuasive. They do their research on you and know what to say to pressure you into handing over information. I love using my impersonations to make people laugh but these scams are no laughing matter. Always stop and think before parting with your money or personal information. If someone is pressing you to act immediately, remember only criminals will try to rush or panic you.

Kathryn Harnett, Policy Manager at WhatsApp, commented:
WhatsApp protects our users' personal messages with end-to-end encryption, but we want to remind people of the other ways they can keep their accounts safe and remain vigilant to the threat of scammers.

We advise all users never to share their six-digit PIN code with others, not even friends or family, and recommend that all users set up two-step verification for added security. And, if you receive a suspicious message (even if you think you know who it's from), calling or requesting a voice note is the fastest and simplest way to check someone is who they say they are. A friend in need is a friend worth calling.

To help people stay safe, the Take Five to Stop Fraud campaign advice is to:

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 details, please visit - https://www.takefive-stopfraud.org.uk/news/people-under-35-are-more-at-risk-from-impersonation-scams/

Take Five @TakeFive

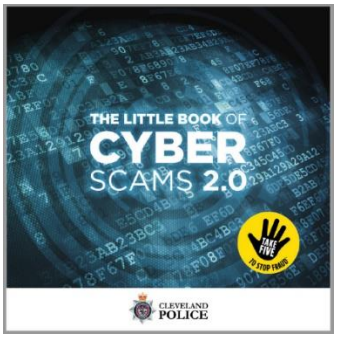
Criminals may purport to be from Take Five, using our official branding on websites, social media posts, literature or on the phone. Take Five doesn't provide endorsement or approval for any products/services and would never call anyone. For more info: https://www.takefive-stopfraud.org.uk/about/take-five/	
Criminals are hungry for your money and continue to take advantage of the Cost of Living Crisis. Always remember to #TakeFive and ask yourself, could it be fake? It's ok to reject, refuse or ignore any requests for personal or financial information.	

For further details visit https://www.takefive-stopfraud.org.uk/

Information in this newsletter has been collated from following online sources.
www.actionfraud.police.uk
www.getsafeonline.org
www.ncsc.gov.uk
www.childnet.com
www.internetmatters.org
www.takefive-stopfraud.org.uk

Should you become a victim of fraud or cybercrime please report to **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"