CLEVELAND POLICE

Cyber Crime Newsletter

MARCH 2024

CONTENTS

GOV.UK

Stop! Think Fraud

Giving you the knowledge and tools you need to stay ahead of scams.

Fraudsters are not fussy. They will pick on anyone.
Nobody is immune from fraud. The criminals behind it target people online and, in their homes, often emotionally manipulating their victims before they steal money or personal data.

But there is something we can do. By staying vigilant and always taking a moment to stop, think and check whenever we are approached. We can help to protect ourselves and each other from fraud.

Did you know?
In just one year, 1 in 17 adults were victims of fraud.
Source: Crime Survey for England and Wales, year ending September 2023.
That is nearly 3 million of us.

Are you at risk?
Fraud accounts for almost 40% of all crime.

1 in 5 businesses were also a victim of fraud over a 3-year period.
Source: Economic Crime Survey 2020

Think you are immune from fraud?
Fraudster can use highly manipulative methods to get us when our defences are down. Nobody is immune from fraud. We can all be more alert to the risks, and we can all do more to protect ourselves.

How to spot fraud

Would you know if someone was trying to defraud you? We might like to think we could spot a scam a mile off – but fraudsters are ruthless, and their methods are getting more sophisticated.

Even though there are many types of fraud, with new ones appearing all the time, there are some **psychological tactics fraudsters commonly use**. These tactics have the sole aim of making people act before they have time to stop, think and check if it is genuine.

One of our best weapons against fraud is knowledge. Once you know the tactics fraudsters commonly use and the signs to look out for, you have more chance of avoiding them.

Recognise the tactics
Learn about the psychological tactic's fraudsters use to get you to act without taking the time to stop, think and check.

Stay alert to fraud
The more you know, the better prepared you will be to spot a fraud attempt if it happens to you or someone you know.

Where to look out for fraud
Fraud can take place anywhere. Online, on social media, by email, by phone, on your doorstep and elsewhere. If you know where scammers might show up, you will be more likely to spot suspicious activity whenever and wherever it happens.

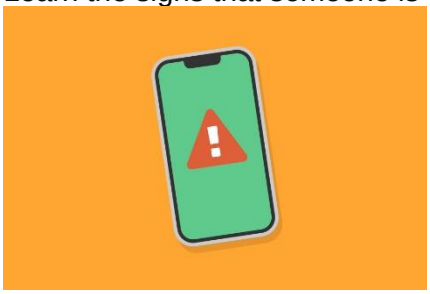
How to spot a phishing email
Learn the signs of a fake email designed to steal your money or personal information.

Visit:
https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-to-spot-a-phishing-email/

How to spot a fake text message
Learn the signs of a fake text message designed to steal your data or money.

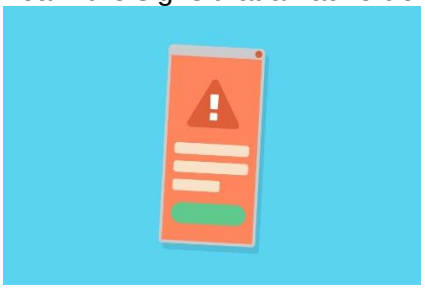
Visit:
https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-to-spot-a-fake-text-message/

How to spot phone fraud
Learn the signs that someone is trying to defraud you over the phone.



Visit:
https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-to-spot-phone-fraud/

How to spot a fake online advert
Learn the signs that an advert on a website, search engine or social media platform is not genuine.



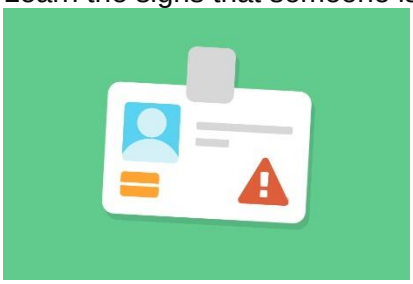
Visit:
https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-to-spot-a-fake-online-advert/

How to spot a fake website
Learn the signs of a bogus website created to take payment for goods that do not exist or infect your device with a virus.

Visit:
https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-to-spot-a-fake-online-advert/

How to spot doorstep fraud

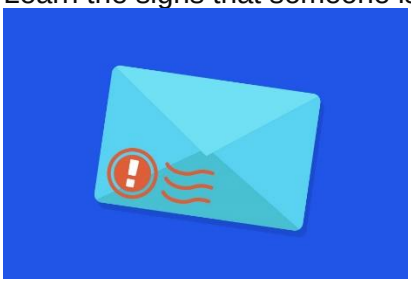
Learn the signs that someone is trying to defraud you in person.



Visit:
https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-to-spot-doorstep-fraud/

How to spot postal fraud

Learn the signs that someone is trying to defraud you through the post.



Visit:
https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-to-spot-postal-fraud/

Campaign partners.

The National Campaign Against Fraud is brought to you by UK Government in partnership with City of London Police, National Cyber Security Centre and National Crime Agency.

Action Fraud
https://www.actionfraud.police.uk/

The National Cyber Security Centre (NCSC)
https://www.ncsc.gov.uk/

National Crime Agency
https://www.nationalcrimeagency.gov.uk/

For more information visit https://stopthinkfraud.campaign.gov.uk/

ACTION FRAUD

Action Fraud issues a new warning to stay safe online after £1.3 million lost from hacked email and social media account scams last year.

More than 22,500 people had their social media accounts hacked last year, new data shows.
Data from Action Fraud, the National Fraud and Cybercrime Reporting Service, shows that 22,530 people reported that their online accounts had been hacked in 2023, with victims losing a total of £1.3 million.

Pauline Smith, Head of Action Fraud, said:
"Anyone with a social media or email account can be a target for fraudsters or cyberattacks. It is important to take action to secure your accounts, as fraud becomes even harder to detect with technology on a global scale.
"Protect your information by ensuring your email and social media passwords are secure and different from all your other passwords. You can also set up 2-step verification for a layer of extra security. Remember, prevent the potential for fraud and hacking, never share your password or any 2-step verification code with anyone."
In the reports made to Action Fraud, there were various methods of hacking reported, including:

On-platform chain hacking
This is when a fraudster gains control of an account and begins to impersonate the legitimate owner. The goal is to convince people to reveal authentication codes that are sent to them via text. Many victims of this type of hacking believe it is a friend messaging them; however, the shared code was associated with their own account and the impersonator can now use it to access their account. Usually when an account is taken over, fraudsters monetise control of the account via the promotion of various fraudulent schemes, while impersonating the original account owner.

Leaked passwords and phishing
The other predominant method of hacking reported is leaked information used from data breaches, such as leaked passwords, or account details gained via phishing scams. This becomes prevalent as people often use the same password for multiple accounts, so a leaked password from one website can leave many of their online accounts vulnerable to hacking.

What can you do to avoid being a victim?

- **Use a strong and different password for your email and social media accounts.** Your email and social media passwords should be strong and different from all your other passwords. Combining three 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.
- **Turn on 2-Step Verification (2SV) for your email and social media accounts**. 2-Step Verification (2SV) gives you twice the protection so even if cyber criminals have your password, they cannot access your email or social media account. 2SV works by asking for more information to prove your identity. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password. You will not be asked for this every time you check your email or social media.

If you live in England, Wales and Northern Ireland and have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040. In Scotland, victims of fraud and cybercrime should report to Police Scotland on 101.

Suspicious emails should also be sent to SERS at report@phishing.gov.uk.

Find out how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk

For more information visit https://www.actionfraud.police.uk/news/action-fraud-issues-a-new-warning-to-stay-safe-online-after-1-3-million-lost-from-hacked-email-and-social-media-account-scams-last-year

---

ACTION FRAUD

Do not lose out before flying out: Action Fraud urge holiday makers to watch out for fraudsters online

Sun seekers looking to book their summer getaway are being warned to look out for fraudulent deals, as new data released today shows victims lost a staggering £12.3 million to holiday fraud last year.

Action Fraud, the national fraud and cybercrime reporting service, has launched a holiday fraud campaign ahead of the summer months, urging holiday goers to play it safe online and do their research before booking their trip.

Last year, 6,640 reports of holiday fraud were made to Action Fraud and data shows July and August saw highest number of reports made, at 804 and 781, respectively.

Holiday makers lost a combined total of £ 12.3 million, meaning there was an average loss of £1,851 per victim.

Pauline Smith, Head of Action Fraud, said:

"As people think ahead to book their holidays, understandably everyone is increasingly on the lookout for the best deals. With the cost-of-living crisis squeezing our finances, it is easy to forget to stay vigilant against fraudsters offering cheaper deals and great prices that are too good to be true.

"We want to avoid people losing their hard-earned money and help raise awareness of the signs of holiday fraud. Before booking any trips or signing up to any deals, do your research and check for ABTA and ATOL logos before clicking the confirmation button. Remember: stay alert online and be wise to fraudsters."

Mark Tanzer, ABTA Chief Executive, said:

"Fraudsters are using increasingly sophisticated methods to target consumers, with a particular focus on destinations and times of year when demand is high and availability limited, as they know people will be looking for good deals. Victims will often only find out they have been defrauded just before they are due to travel, or even in a resort, when it can be difficult to find a legitimate replacement leading to yet more cost and potential disappointment.

"One of the simplest ways to protect yourself when booking is to look for a company that is a member of ABTA when booking your holiday."

Anna Bowles, Head of Consumers and Enforcement at the UK Civil Aviation Authority, which runs the ATOL financial protection scheme, said:
"Our research shows almost three in five of us are planning to go overseas this summer and expect to spend thousands of pounds on these trips. Before booking your trip abroad make sure you are doing everything you can to thwart fraudsters.
"Some protective measures include visiting the atol.org website to check your package trip is financially protected by ATOL, pay by credit card if you can, and take out travel insurance as soon as you book."
Holiday makers are encouraged to take precautions and do their research online to ensure holidays are booked safely, without a hitch. Remember, do not get caught out and lose out.

Top tips to help prevent falling victim to holiday fraud:

- **Do your research:** before committing and booking your dream holiday, make sure that you do a thorough online search to ensure the company is credible.

- **Pay safely:** use a credit card when shopping online if you have one. Most major credit card providers protect online purchases.

- **Look for the logo:** make sure they are a licensed company and check that they are properly accredited. Look for an ATOL (Air Travel Organiser's Licence) or a membership of ABTA, The Travel Association.

- **Stay safe online:** use three random words to create a strong password for your email that is different to all your other passwords. If a 2-step verification option is available, always set it.
    - **Beware of suspicious messages:** be cautious of unexpected emails or messages offering unrealistic holiday deals. If you receive a suspicious email, report it by forwarding it to report@phishing.gov.uk
    - **Protect personal information:** only fill in the mandatory details on a website when making a purchase. If possible, do not create an account for the online store when making your payment.

- **Book with confidence:** be sceptical of unrealistic holiday deals. If it sounds too good to be true, it probably is. Exercise caution and research before making purchases.

For further tips from ATOL and ABTA, 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. If you live in Scotland, call Police Scotland on 101.

For more information visit https://www.actionfraud.police.uk/news/dont-lose-out-before-flying-out-action-fraud-urge-holiday-makers-to-watch-out-for-fraudsters-online

---

ACTION FRAUD

Fraudsters impersonate NCA officers in 'child pornography' scam emails.

NEWS 05.01.2024

Action Fraud have received 180 reports regarding fake emails claiming to be from the NCA.
Since the beginning of December 2023, Action Fraud and the Suspicious Email Reporting System (SERS) have received over 180 reports concerning the impersonation of National Crime Agency (NCA) agents.

The victims describe receiving an email purporting to be from the NCA. The email states that the NCA has evidence that the recipient has accessed and viewed "child pornography" or other "illegal pornographic content".

The emails demand that the recipient make contact within a specified deadline. If they do not, the email claims that a warrant will be issued for their arrest and that the recipient's details will be added to the sex offenders register, quoting legislation to make the threat sound legitimate.

It is assessed that the intention of the email is to prompt the victim into initiating communication with the suspects so that personal information can be disclosed to be used for blackmail or to commit fraud. Unlike other emails which impersonate law enforcement, there is no up-front demand for money however, where victims have engaged with the suspects, they have demanded money at a later stage.

The use of such threatening language creates a significant and emotional impact upon the recipient. The time pressure that is applied encourages victims to panic and act without thinking, unknowingly exposing themselves to compromise and blackmail.

What you need to do

- **The NCA will not send unsolicited correspondence requesting money or bank details**. If you have doubts about the authenticity of a message received from the NCA, please call 0370 496 7622.
- Remember, your bank (or any other official source) will not ask you to supply personal information over email.
- If you think an email is suspicious, you can report it by forwarding the email to: report@phishing.gov.uk.

Every report counts.

- If you have been a victim of fraud or cybercrime, report it to us at online or by calling 0300 123 2040.

For more information visit https://www.actionfraud.police.uk/news/fake-nca-emails

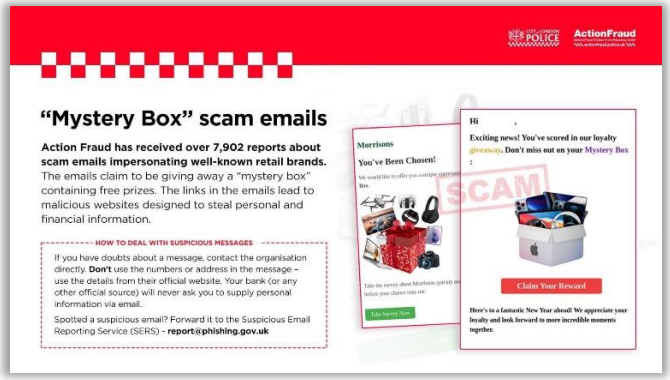
Action Fraud Facebook

EMAIL SCAM!
Watch out for these fake emails claiming you have won a “mystery Box” of free prizes. The only “reward” they lead to are phishing websites designed to steal your personal information.

Forward suspicious emails to:
report@phishing.gov.uk

Your reports have led to the removal of 306,000 websites.

#CyberProtect



Criminals will try to lure you in with adverts or via social media offering easy money quickly.

Stop and think. It could protect you and your money.

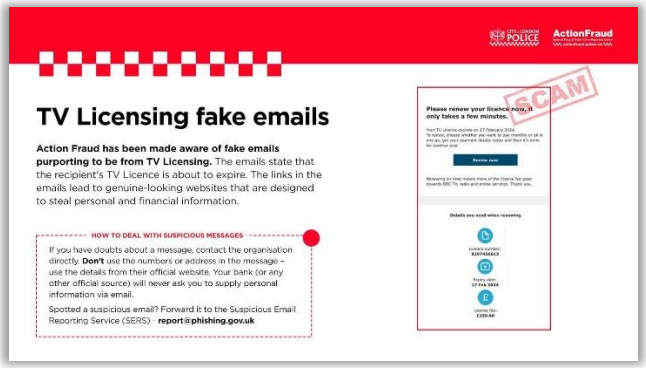
Read more
https://www.actionfraud.police.uk/investmentfraud

Watch out for the latest @tvlicensing scam.

The sender’s email address has been spoofed to appear genuine. You can verify its authenticity by checking the senders address is donotreply@tvlicensing.co.uk

Remember, @tvlicensing will always include the name and/or part of your postcode In their emails.

Check out the @tvlicensing advice
https://www.tvlicensing.co.uk/faqs/FAQ288#email



Beware of bank transfer requests, never pay directly into a private individual’s bank account. Whenever possible, pay by credit card if you have one. Most major credit card providers protect online purchases.

Stay safe while making payments online.

Find out more tips
https://www.actionfraud.police.uk/holidayfraud

#StopHolidayFraud

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 child and online gambling

In common with many online activities, there are both positive and negative aspects to gaming. But the commonly held traditional view that children's gaming is largely a negative thing, is becoming rapidly overturned as more people appreciate its many positive aspects.

Depending on the games in question, these include:

- Supporting development of a wide range of cognitive and motor skills
- Developing qualities such as strategic thinking, rationalising, problem solving and persistence
- Encouraging creativity
- Teaching teamwork, in the case of many Massive Multiplayer Online Role-Playing Games (MMORPGs or MMOs)
- Teaching competitiveness, again in the case of multiplayer games
- Socialising with friends, especially when doing so in person is challenging owing to various restrictions.
- Learning the value of money and spending it wisely.

All of these are qualities are vital not only in gaming, but also in equipping our young people for life ahead of them.
Also, as an industry, game development often leads the way in technology, with innovations in functionality and features finding their way into not only other consumer products, but defence, communications and many other sectors. Gaming equips children to understand and embrace this evolution and its benefits.

Working with your child
Check out these findings from an Ofcom survey of internet usage in 2023[1], based on children's responses:

- Around 9 in 10 children aged 3-17 played games online.
- **25%** of children aged **8-17** played games online with people they do not know, and 22% chatted to people they don't know when gaming.

It is especially important that you understand and support your child's interest in online gaming. Like many parents, you may have little or no interest in it yourself, but there are things you can do to both encourage them to find the best games as well as helping them avoid the negative aspects mentioned above. Who knows, you may even find a favourite game for yourself.

- [1] *Children and parents: media use and attitudes report 2023, Ofcom*

What are the risks?

- Risks to children who play games online arise largely from the vast number of people both in the UK and abroad who are also playing, the minimal restrictions involved and the fact that they are not playing face-to-face.
- Stranger danger can pose a risk to the safety of the child, or a risk of financial or identity theft to you, if your child overshares personal family information online. Cybercriminals also use gaming platforms and forums to recruit young people for illicit activities such as malware coding and money muling, and some radicalisation begins on gaming platforms.
- Playing games with an inappropriate age rating, potentially exposing them to violent, sexual or other unsuitable content.
- Playing games which either reference gambling, or involve gambling to, for example, predict results or win money.
- Running up bills (for example, on in-game properties/in-app purchases), perhaps on your credit card.
- Spending excessive time gaming, to the exclusion of social contact, exercise and schoolwork, and potential health risks.

Keep your child's online gaming safe.

- **Work with your child** to find the best games for their age, interests and personality.
- **Join your child** in online gaming from time to time and randomly. This will give you an idea of the games they are playing and who they connect with.
- **Have open and honest conversations** with your child about their online gaming and the risks involved including stranger danger, bullying and oversharing. Tell them that not everybody they meet on gaming platforms and forums is who they claim to be.
- **Set and monitor limits** for the amount of daily or weekly time your children spend online gaming.
- You could pre-load spending money on to their game, but **when it's gone, it's gone.**
- Check PEGI (Pan European Game Information) **age ratings of games** to ensure your children are not accessing inappropriate content.
- **Do not give your child access to your payment card details** as extras can be very costly.
- Impress upon your child that **they can come to you or another responsible adult** with any concerns. Depending on their age, you could also discuss **how to report issues** to the gaming platform and/or the police.

There's much more information about researching the online games your child does and could play – including content, features, benefits, negatives and age ratings – on the Family Gaming Database at www.familygamingdatabase.com

You could also pick up a copy of Taming Gaming, a book by gaming expert Andy Robertson who has been helping families get more from video games for 15 years.

View our free Webinars.
Our inspiring webinars feature gaming experts giving easy-to-follow advice on children's gaming.
Watch webinars - https://www.getsafeonline.org/gaming4good-webinars/

#gaming4good

For more information visit: https://www.getsafeonline.org/gaming4good/

GET SAFE ONLINE
Buying Tickets

Watching you favourite band, team or stand-up comic from the comfort of your armchair is great, but it's nothing like being there live, on the day.

Tickets to big entertainment and sporting events sell out very quickly, which is very disappointing when you've really been looking forward to the big day. This can make it very tempting to buy them from sources other than official websites. However, one in ten people in the UK have been victims of a ticketing scam online, paying for tickets that do not exist, being refused entry to an event or revealing their payment card details to an identity thief or fraudster.

The risks

- Fraud resulting from making payments over unsecured web pages.
- Bogus ticketing sites – fake websites and email offers for tickets that do not exist.
- Bogus posts on fan forums – buying tickets that do not exist.
- Not receiving tickets, having transferred money directly into a fraudster's bank account.
- Receiving tickets which do not match the seller's description.

Safe ticket buying

- Buy tickets only from the venue box office, promoter, official agent or reputable ticket exchange sites.
- Remember that paying by credit card offers greater protection than with other methods in terms of fraud, guarantees and non-delivery.
- Double check all details of your ticket purchase before confirming payment.
- Do not reply to unsolicited emails from sellers you do not recognise.
- Before entering payment card details on a website, ensure that the link is secure, in two ways:
    - There should be a padlock symbol in the browser window frame, which appears when you attempt to log in or register. Be sure that the padlock is not on the page itself … this will probably indicate a fraudulent site.
    - The web address should begin with 'https://.' The 's' stands for 'secure'.
- The above indicate only that the link between you and the website owner is secure, and not that the site itself is authentic. You need to do this by carefully checking the address for subtle misspellings, additional words and characters and other irregularities.
- Some websites will redirect you to a third-party payment service (such as WorldPay). Ensure that these sites are secure before you make your payment.
- Safeguard and remember the password you have chosen for the extra verification services used on some websites, such as Verified by Visa.
- If you choose to buy tickets from an individual (for example on eBay), never transfer the money directly into their bank account but use a secure payment site such as PayPal, where money is transferred between two electronic accounts.
- Check sellers' privacy policy and returns policy.
- Always log out of sites into which you have logged in or registered details. Simply closing your browser is not enough to ensure privacy.
- Keep receipts.
- Check credit card and bank statements carefully after ticket purchase to ensure that the correct amount has been debited, and that no fraud has taken place as a result of the transaction.
- Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.

More information

If you think you have been a victim of fraud: Report it to Action Fraud, the UK's national fraud reporting centre by calling 0300 123 20 40 or by visiting www.actionfraud.police.uk. If you are in Scotland, contact Police Scotland on 101.

If you've experienced cybercrime, you can contact the charity Victim Support for free and confidential support and information.

For more information visit: https://www.getsafeonline.org/personal/articles/buying-tickets/

Get Safe Online Facebook	
Do proper research into package holidays, accommodation, flights, cruises, pilgrimages or any other kind of break to check it really exists and is being advertised legitimately. Don't fall victim to fraud. #holiday www.getsafeonline.org/holiday	

Did you meet someone new online on #ValentinesDay? Good luck with your new relationship but do take some time to read our top safety tips, including on how to avoid romance fraud. #datesafe www.getsafeonline.org/datesafe	
Looking to book an @Airbnb? Always communicate and pay on the Airbnb platform to ensure you are fully protected and use the Airbnb app or go directly www.airbnb.co.uk before you search a stay. #holiday www.getsafeonline.org/holiday	

NCSC – National Cyber Security Centre

AI and cyber security: what you need to know

This image was generated using Copilot, Microsoft's 'AI-powered digital assistant.

Understanding the risks – and benefits – of using AI tools.

Ignited by the release of ChatGPT in late 2022, artificial intelligence (AI) has captured the world's interest and has the potential to bring many benefits to society. However, for the opportunities of AI to be fully realised, it must be developed in a safe and responsible way, especially when the pace of development is high, and the potential risks are still unknown.

As with any emerging technology, there is always concern around what this means for security. **This guidance is designed to help managers, board members and senior executives (with a non-technical background) to understand some of the risks - and benefits - of using AI tools**.

Managers don't need to be technical experts, but they should know enough about the potential risks from AI to be able to discuss issues with key staff.

What is artificial intelligence?

Artificial intelligence (AI) can be described as *'Any computer system that can perform tasks usually requiring human intelligence. This could include visual perception, text generation, speech recognition or translation between languages.'*

One of the most notable recent AI developments has come in the field of **generative AI**. This involves AI tools that can produce several types of content, including text, images and video (and combinations of more than one type in the case of 'multimodal' tools). Most generative AI tools are geared towards specific tasks or domains. For example, ChatGPT effectively allows users to 'ask a question' as you would when holding a conversation with a chatbot, whereas tools such as DALL-E can create digital images from natural language descriptions.

It appears likely that future models will be capable of producing content for a broader range of situations, and both Open AI and Google report success across a range of benchmarks for their respective GPT-4 and Gemini models. Despite this broader applicability, there remains no consensus on whether artificial general intelligence – the dystopian vision of the future where an autonomous system surpasses human capabilities – will ever become a reality.

How does AI work?

Most AI tools are built using **machine learning** (ML) techniques, which is when computer systems find patterns in data (or automatically solve problems) without having to be explicitly programmed by a human. ML enables a system to 'learn' for itself about how to derive information from data, with minimal supervision from a human developer.

For example, **large language models** (LLMs) are a type of generative AI which can generate different styles of text that mimic content created by a human. To enable this, an LLM is 'trained' on a large amount of text-based data, typically scraped from the internet. Depending on the LLM, this potentially includes web pages and other open-source content such as scientific research, books, and social media posts. The process of training the LLM covers such a large volume of data that it is not possible to filter all of this content, and so 'controversial' (or simply incorrect) material is likely to be included in its model.

Why the widespread interest in AI?

Since the release of ChatGPT in December 2022, we've seen products and services built with AI integrations for both internal and customer use. Organisations across all sectors report they are building integrations with LLMs into their services or businesses. This has heightened interest in other applications of AI across a wide audience.

The NCSC want **everyone** to benefit from the full potential of AI. However, for the opportunities of AI to be fully realised, it must be developed, deployed and operated in a secure and responsible way. Cyber security is a necessary precondition for the safety, resilience, privacy, fairness, efficacy and reliability of AI systems.

However, AI systems are subject to novel security vulnerabilities (described briefly below) that need to be considered *alongside* standard cyber security threats. When the pace of development is high – as is the case with AI – security can often be a secondary consideration. Security must be a core requirement, not just in the *development* phase of an AI system, but *throughout its lifecycle*.

It is therefore crucial for those responsible for the design and use of AI systems – including senior managers – to keep abreast of new developments. For this reason, the NCSC has published AI guidelines designed to help data scientists, developers, decision-makers and risk owners build AI products that function as intended, are available when needed, and work without revealing sensitive data to unauthorised parties.

What are the cyber security risks in using AI?
Generative AI (and LLMs in particular) is undoubtedly impressive in its ability to generate a vast range of convincing content in different situations. However, the content produced by these tools is only as good as the data they are trained on, and the technology contains some serious flaws, including:

- it can get things wrong and present incorrect statements as facts (a flaw known as 'AI hallucination')
- it can be biased and is often gullible when responding to leading questions.
- it can be coaxed into creating toxic content and is prone to 'prompt injection attacks.'
- it can be corrupted by manipulating the data used to train the model (a technique known as 'data poisoning')

Prompt injection attacks are one of the most widely reported weaknesses in LLMs. This is when an attacker creates an input designed to make the model behave in an unintended way. This could involve causing it to generate offensive content, or reveal confidential information, or trigger unintended consequences in a system that accepts unchecked input.

Data poisoning attacks occur when an attacker tampers with the data that an AI model is trained on to produce undesirable outcomes (both in terms of security and bias). As LLMs in particular are increasingly used to pass data to third-party applications and services, the risks from these attacks will grow, as we describe in the NCSC blog 'Thinking about the security of AI systems'.

How can leaders help ensure that AI is developed securely?
The Guidelines for Secure AI System Development, published by the NCSC and developed with the US's Cybersecurity and Infrastructure Security Agency (CISA) and agencies from 17 other countries, advise on the design, development, deployment and operation of AI systems. The guidelines help organisations deliver *secure outcomes*, rather than providing a static list of steps for developers to apply. By thinking about the overall security of systems containing AI components, stakeholders at all levels of an organisation can prepare to respond to system failure, and appropriately limit the impact on users and systems that rely on them.

Crucially, keeping AI systems secure is as much about *organisational* culture, process, and communication as it is about *technical* measures. Security should be integrated into all AI projects and workflows in your organisation from inception. This is known as a 'secure by design' approach, and it requires strong leadership that ensures security is a *business* priority, and not just a technical consideration.

Leaders need to understand the consequences to the organisation if the integrity, availability or confidentiality of an AI-system were to be compromised. There may be operational and reputational consequences, and your organisation should have an appropriate response plan in place. As a manager you should also be particularly aware of AI-specific concerns around data security. You should understand whether your organisation is legally compliant and adhering to established best practice when handling data related to these systems.

It's also important to note that the burden of using AI safely should **not** fall on the individual users of the AI products; customers typically won't have the expertise to fully understand or address AI-related risks. **That is, developers of AI models and systems should take responsibility for the security outcomes of their customers**.

In addition to the AI Guidelines, the NCSC's Principles for the security of machine learning (published in 2022) provide context and structure to help organisations make educated decisions about where and how it is appropriate to use ML, and the risks this may entail. Some of the principles are particularly relevant to those in senior decision making and executive or board level roles. These are highlighted in the quick reference table on the front page of the principles.

Questions to ask about the security of your organisation's AI systems.
Managers, board members and senior executives can use the following questions in discussions with technical and security staff, to help you understand how your organization is dealing with the AI/ML threat.

- Do you understand where accountability and responsibility for AI/ML security sit in your organisation?
- Does everyone involved in ML deployment, including board members and/or senior executives, know enough about AI systems to consider the risks and benefits of using them?
- Does security factor into decisions about whether to use ML products?
- How do the risks of using ML products integrate into your existing governance processes?
- What are your organisation's critical assets in terms of ML and how are they protected?
- What is the worst case (operationally or reputationally) if an ML tool your organisation uses fails?
- How would you respond to a serious security incident involving an ML tool?
- Do you understand your data, model and ML software supply chains and can you ask suppliers the right questions on their own security?
- Do you understand where your organisation may have skills or knowledge gaps related to ML security? Is a plan in place to address this?

Further reading
If you'd like to know more about AI, the NCSC has produced a series of relevant publications, please see link below.

For more information visit https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know

---

NCSC – National Cyber Security Centre Guidance

Responding to a cyber incident – a guide for CEOs

Who is this guidance for?
This guidance helps CEOs in public and private sector organisations manage a cyber incident. It sets out aspects to consider at the start of an incident and throughout it.

Why do I need this guidance?
If your organisation is victim of a significant cyber-attack, the immediate aftermath will be challenging. You may find there is a lot of information in some areas, and none in others. There will be difficult risk-based decisions to make to protect your operations. Your aim will be to limit the impact on your business, clients and staff in the weeks and months which follow.

Put in place proportionate and effective governance.
A cyber security incident is not just a cyber security problem. It is also a business continuity and communications issue and can be a financial and legal one too.

It may be helpful to appoint a separate SRO (Senior Responsible Officer) or to use a broader governance command structure, such as the bronze, silver and gold model to assign overall responsibility for the incident.

To help your team make effective decisions, you should make sure structures are in place to:

- take account of the **full** impact across the **whole** organisation
- make it easy for those managing the response to regularly come together.
- inform and empower senior decision-makers by explaining how technical issues impact them.
- allow a robust response to all the demands of an incident (internal and external communications, working with regulators and insurers, providing updates to the board)

Bring in resources for advice and support.

Surrounding your teams with reliable external experts who can take an objective view can significantly improve the quality of decision making and help you manage the legal, technical, operational and communications considerations that a serious incident brings. The role of these experts is to provide advice, not to make key decisions.

The NCSC advises using a cyber incident response (CIR) company to help you manage and recover from the incident. The NCSC assures a number of CIR companies.
If your organisation has cyber insurance in place, you should let your insurer know, as they may have in-house or preferred CIR companies, as well as other services to help you during a cyber incident.

Consider the impact of a data breach.

Once a cyber security incident is resolved, there are often still outstanding questions about the risk to data, whether the data is your own, or customer and staff data that you hold. **It is critical that you communicate any risks to data to the data owners, and that you consider the regulatory requirements you may have to report breaches**.

The ICO (Information Commissioner's Office) has guidance on personal data breaches which sets out clearly how to respond to a suspected breach. The ICO is clear that you must report a notifiable breach to them 'without undue delay' and not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Think about your public messaging.

Effective and transparent communications in a crisis won't just reassure your employees, but could also help protect your organisation's reputation externally. Any communications should be factual and clear, and you should be careful not to misrepresent or downplay the incident in a way that creates future difficulties or relationship issues.

You might need to give a different level of detail to different groups – key decision-makers and stakeholders in your organisation, wider staff, your partner organisations or communications to the public. Make sure you know in advance who needs to be brought in to your communications planning.

In a ransomware attack, consider the risks of making a payment.

If your organisation is the victim of a ransomware attack, you may find the actor sets tight timescales for payment. You should read the NCSC guidance pages on ransomware and payments.

The NCSC and UK law enforcement don't encourage, endorse or condone the payment of ransom demands – but you should be aware that there are risks around making payments to criminals, and that if you do pay, there is no guarantee that you will get access to your data or networks. Research shows that it's also more likely that you will be targeted in future.

Consider team resilience and welfare.

During a crisis, staff at all levels of your organisation will probably experience stress and uncertainty, which can be extremely detrimental. You should put their welfare and morale at the top of your response plan.
The NCSC has guidance on staff welfare during an incident.

Incidents often start with an intense period of activity, but many also have a ‘long tail’ with the impact lasting for months. The team will need to make important decisions throughout, but particularly when you are working out how to rebuild and prevent future incidents. It is important to make sure that staff aren’t exhausted.

Staff with incident experience are valuable to an organisation, and putting in place good wellbeing practices may also have the benefit of helping to retain staff in the long term.

Review the lessons learned.
Following the incident, make sure there is a debrief with those who helped manage it. You should consider both the things that went well and what you would do differently. This also helps with staff welfare.

You should conduct a review with a genuine intention to learn from the experience and to understand what factors led to the incident in the first place. This should be systemic in nature, rather than trying to pin down a single root cause. Your aim here should be to prevent and improve for the future, not to apportion blame.

There will be many factors in play, and it is important to understand how they relate to each other to improve your organisational resilience.
Conducting a general cyber security review should also be a priority to help understand and manage any vulnerabilities in your systems that may lead to further attacks.

The NCSC Cyber Security Toolkit for Boards helps embed cyber resilience and risk management through the whole organisation, including its people, systems, processes and technologies and is a good starting point.

Report it.
And finally, you should report significant incidents to the NCSC and UK law enforcement who can provide support. This also enhances understanding of the threat landscape, helping to prevent further incidents and improve security for everyone.

Report your cyber incident using the UK government signposting tool which lets you know which organisations to notify, based on the circumstances of the incident.

Downloads

Responding to a cyber incident - a guide for CEOs
This guidance helps CEOs in public and private sector organisations manage a cyber incident. It sets out things to consider at the start of https://www.ncsc.gov.uk/files/Responding-to-a-cyber-incident-a-guide-for-ceos.pdf

For details, please visit https://www.ncsc.gov.uk/guidance/ceos-responding-cyber-incidents

---

FCA Financial Conduct Authority

Crypto: The basics

If you are thinking about buying crypto you need to know the basics and understand the risks before jumping in. And remember, if you decide to invest in crypto then you should be prepared to lose all the money you have invested.

What is crypto?
Crypto has grown rapidly in the last few years, accompanied by a surge in speculative trading – which means people trading just because they have heard it may rise in value, rather than seeing evidence to support a potential rise.

Crypto can be thought of as 'digital representations of value or rights' that are secured by encryption and typically use some type of 'distributed ledger technology' (DLT). DLT allows data to be recorded and stored across a network of participants. This keeps the data secure and means there is no one single central data storage point or one central authority that grants participants permission to access and participate in the network.

Where does crypto come from?
There are many types of crypto and the market continues to evolve rapidly.
The way some cryptos are created and operated makes them quite different from what some people would class as 'tangible' assets (meaning things that you can physically see and touch) like gold or cash. So called 'unbacked' crypto have no tangible assets that sit behind them. Their price can increase or decrease depending on whether other people are willing to buy them. If people stop buying, the price could fall dramatically.

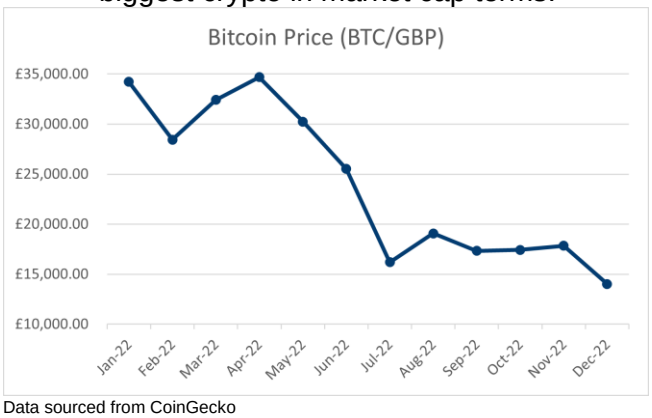
Whereas central banks – like the Bank of England – issue and oversee the money we use daily, cryptos are developed and run by groups, individuals or companies. Publicly available information about some of these groups/individuals can be vague, and as crypto activity is not regulated yet in the UK, there is no safety net if things go wrong.

The underlying technology behind crypto, in particular DLT, and certain cryptos might have a positive impact on the future on financial services. It may lower costs, increase efficiency, enable faster settlements and help better monitor transactions. There could be benefits for consumers and businesses when a subset of crypto assets – stablecoins – are used for payments. This is especially the case for cross-border (remittance) payments, where stablecoins may lower the costs and speed up settlement for business and consumers.

Some investors see appeal in crypto, either because they want digital finance decentralised and/or they see the assets as investments that may grow in value. However, the volatility of crypto can lead to people questioning its value.

Crypto you (might have heard of)
As of early 2023, there were over 20,000 cryptos, many of which are no longer traded, and will never grow a significant market capitalisation (cap), a term used to measure the size of a certain crypto and its popularity, because they do not have a unique selling point. Of the 20,000+, there is probably a few you have heard of:

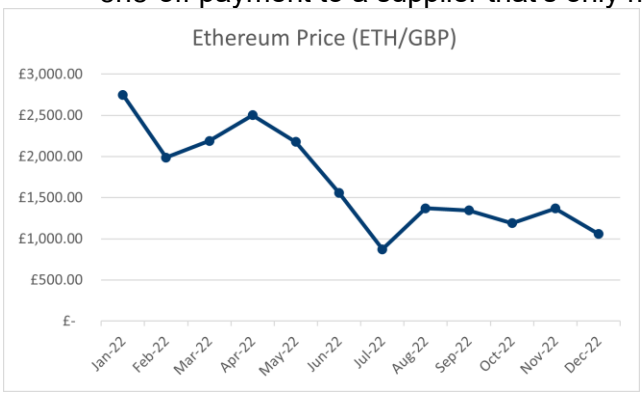
- Bitcoin: Bitcoin (sometimes abbreviated to 'BTC') was created in 2009 following a whitepaper publication a year earlier. That makes Bitcoin the longest-running crypto, and it is also by far the biggest crypto in market cap terms.



Data sourced from CoinGecko

The peak trading price of Bitcoin was in November 2021 when its value reached £51,032.02. At the end of December 2022, this had fallen by 73.12%, and value was £13,724.88. If you invested £300 at its peak, this would be worth £80.64 in December 2022.

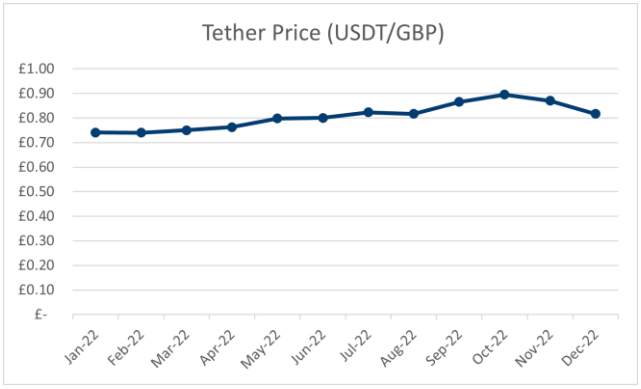
- **Ethereum ('ETH'):** The Ethereum blockchain differs to Bitcoin's as it enables functions to be pre-programmed through so-called 'smart contracts', a kind of computer-code that runs on the "Ethereum Virtual Machine" that automatically activates when pre-agreed conditions are met. In practice, which means you could set up a regular payment to be made on your mate's birthday, or a one-off payment to a supplier that's only made once you confirm you've received the goods.



Data sourced from CoinGecko

The peak trading price of Ethereum was in November 2021 when its value reached £3,610.11. By December 2022, the value had fallen to £992.02. If you invested £300 at its peak, this would be worth £82.41 in December 2022.

- **Tether:** Tether (USDT) is a form of crypto called a 'stablecoin', meaning that its value is linked to stable assets like the US Dollar or gold. Theoretically this makes the price less volatile than cryptos like BTC and ETH. However, the extent to which stablecoins have reserves of 'stable assets' to keep their values linked, varies in practice. Tether was fined $41 million by US regulators in October 2021 for making untrue and misleading statements about the extent to which it was linked to the dollar.

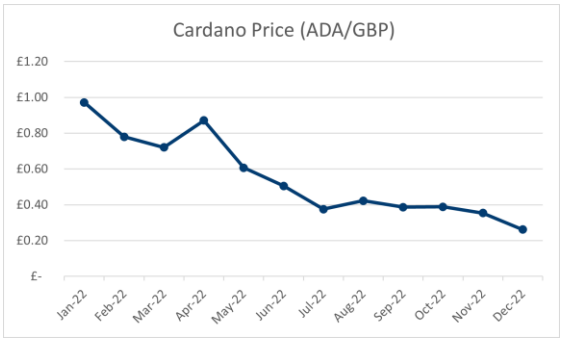


Data sourced from CoinGecko

The peak trading price of Tether was in July 2018 when its value reached £1.01. In December 2022, this had fallen by 17.82% and value was £0.83. If you invested £300 at its peak, this would be worth £246.54 in December 2022.

Some other so called 'stablecoins' also have no assets backing them and have been known to lose their value completely after delinking from the assets they were meant to match in value. An example of this is the 'stablecoin' crypto project TerraUSD (UST). In 2022, the value fell quickly which led to panic, as the coin's value collapsed and detached from the US Dollar.

- **Cardano:** 'ADA' has rapidly gained popularity since release in 2017. Cardano aims to combine the appeal of Ethereum's 'smart contracts' with energy-saving validation methods.



Data sourced from Coin Gecko

The peak trading price of Cardano was in September 2021 when its value reached £2.23. At the end of 2022, this had fallen by 91.03% and the value was £0.20. If you invested £300 at its peak, this would now be worth just £26.91 in December 2022.

Using crypto?

Currently, using crypto as a means of payment is extremely limited – certain IT and travel companies accept them, for example, but you probably won't be doing your weekly shop or paying your 5-a-side football subs with crypto. The reason for this is that crypto assets tend to be very volatile, so it is hard to pinpoint their value from one day to the next, which makes them unreliable as a payment method. However, we see potential benefits in using certain types of crypto assets, specifically those that are linked to fiat currency, which are less volatile and more stable, as they could provide faster, cheaper and more efficient payments, e.g., cross border or micro payments. Some investors take the view that cryptos could one day be accepted in everyday transactions and see potential beneficial applications of DLT in the payment space.

Investing in crypto comes with all kinds of risks, some of which you might not even have thought of. For example, even getting your money out of crypto and back into your bank account as cash is risky and tax may be payable on any gains that you have made. In 2022, crypto lender, Celsius, filed for bankruptcy and owed its users $4.7 billion, meaning many investors could not get their money out and did not get anything back.

Investing in crypto?

Many people are treating crypto as an investment. While not all crypto assets are the same, they are all high risk and speculative as an investment.
If you decide to invest in crypto then you should be prepared to lose all your money, for any one of a variety of reasons, including sudden market moves, the failure of a firm, poor segregation of client funds or cyberattacks.

It is important to remember that crypto is largely unregulated in the UK, so it is highly unlikely you will be covered by the Financial Services Compensation Scheme, so you should not expect any kind of compensation to cover any form of crypto-related losses.
The marketing of crypto is regulated, and you can help protect yourself by recognising regulated crypto marketing.

Whenever you invest in crypto you should see prominent warnings about the risk of losing your money, and you should not be offered any free gifts to join or refer a friend bonuses.

If you do not see these warnings and are offered an incentive to invest it means the company offering your investment is not following our rules, and could be illegal, or even a scam.
Even with these rules, crypto remains high risk with no protections if something goes wrong.

Scammers are active around crypto markets.
Following the surge in people's interest in crypto over the last few years, scammers have been increasingly active in targeting potential investors. Remember - if something sounds too good to be true then it probably is. Find out how to protect yourself and others from investment scams on our ScamSmart site.

For details, please visit https://www.fca.org.uk/investsmart/crypto-basics

---

Help and Advice
Digital Wellbeing for 11–18-year-olds

Going online and using technology can impact our emotions and mental health.
Digital wellbeing is about recognising the way going online makes us feel and knowing how to manage this.

Questions you may have.

Is going online good for me?
It can be! There are loads of positives to going online and using technology, like being able to stay in touch with friends and family or learning about what is going on in the world. Unfortunately, there are also negatives – sometimes the time we spend online can leave us feeling stressed, anxious, upset or alone. It is important to recognise how time online makes you feel whether it is good or bad.

Why does going online sometimes make me feel bad?
As amazing as the internet is, unfortunately there is always the possibility that you might see something that you did not want to. A particular type of content might be triggering for you and make you feel anxious or upset. Perhaps the way other people are behaving online is upsetting or unkind. Sometimes even seemingly harmless content can affect the way we feel – for example if you find yourself comparing your own life to the images and videos shared by others. However it happens, our emotional responses to things we see and hear are part of what makes us human. If something online upsets you, it is important to remember that it's not your fault, but there are steps you can take to prevent it from happening again.

How can I make my experience online more positive?
The first step is to try to identify the things you see or hear that make your online experience a negative one. Once you have identified what is upsetting you, consider: can I or should I cut this out of my online experience completely? For example, you could unfollow or block an account that shares things you do not want to see.
You may decide that it is important you still engage with the content to some extent e.g. breaking news stories. In this case, can you control how it appears to you or limit the number of times you come across it? This could be achieved by turning off notifications, so the content does not 'pop-up' when you're not expecting it.

Finally, use the positive to outweigh the negative – follow accounts that make you smile or balance your time reading up on news with videos of cute puppies!

What is self-care?
Self-care is about actively taking steps to protect your own wellbeing. This could be:

- limiting the negative impact of the things you see online by unfollowing or blocking particular types of content,
- seeking out more positive experiences online,

- balancing your time online with offline activities that help you recharge, get some space and feel better.

Self-care is different for everyone but lots of young people have told us they enjoy going outside and getting some exercise, spending time with friends and family, taking a long bath, listening to music, reading, baking or other similar hobbies.

What tools exist to help me manage my digital wellbeing?
Many social media services now provide specific tools designed to support with digital wellbeing. Most of these tools focus on monitoring and managing the amount of time you spend on a device and using a particular service. For example, by allowing you to set a time limit, after which an app is temporarily locked. Other tools include the notification settings on your device and reporting or blocking tools.
Turning off push notifications can have a real impact on what content you see throughout the day, whilst being able to report upsetting content online means the safety team can investigate and prevent similar content being posted in the future.

I need help! Where can I go?
Sometimes the things we see or hear online can feel overwhelming and it is okay to reach out for help. Having a strong support network of friends, family and other adults you know to support you, is really important. However, you may prefer to speak with someone you do not know, in which case the helpline services provided by Childline and The Mix are available 24 hours a day. Their friendly, fully trained, supportive advisors are happy to talk about anything you want to get off your chest, big or small.

Top Tips
1. Be conscious of how going online makes you feel and whether different activities have a positive or negative impact on your emotions.
2. Make use of wellbeing tools to manage your time online and manage notifications to make your experiences more positive.
3. Make your feed a place of positivity and follow accounts that make you feel good. You can see other posts by visiting profiles and pages directly, instead of them popping up in your feed.
4. Practise self-care and make time for yourself. Try out different offline activities and find one that leaves you feeling recharged – whatever works for you!
5. Sometimes being online can be overwhelming, but having people who want to support you is invaluable. Reach out if you need to – getting help is a sign of strength, not weakness.

For details, please visit - https://www.childnet.com/help-and-advice/digital-wellbeing-for-11-18-year-olds/

Childnet International Facebook

What do I need to know about Palworld? A guide for parents and carers

This blog covers the important questions you may have about this new game including age restrictions, gameplay and more!

https://bit.ly/3HFvYNr

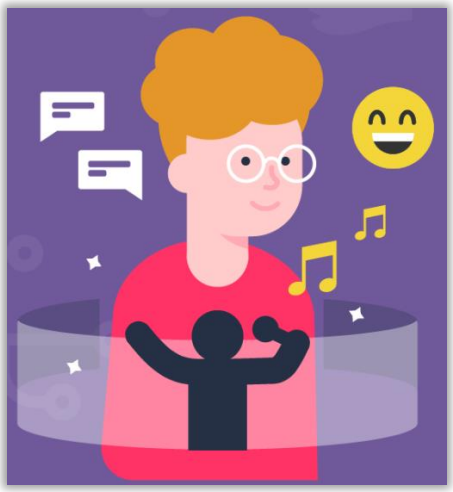
https://www.childnet.com/blog/what-do-i-need-to-know-about-palworld-a-guide-for-parents-and-carers/

Working with kids between the ages 4-11? Here is a great framework on being safe online. Check out the guide here: https://www.childnet.com/young-people/4-11-year-olds/get-smart/	

Internet matters.org

Tech & Kids

Virtual events and entertainment in the Metaverse



The metaverse is more than just gaming. Explore how children are using it for other forms of entertainment.

What do virtual events look like in the metaverse?

Gen Z and Gen Alpha like to immerse themselves in digital worlds like Roblox, Fortnite and Minecraft. They tend to prefer these environments to traditional film and television, says lecturer Justin Trevor Winters. Many children and young people also dedicate hours to these spaces every day. “This trend underscores the metaverse’s role as a vibrant digital playground, offering a wide array of entertainment beyond gaming that nurtures creativity, learning and social connections.”

Socialisation and personal identity

“After an exhausting basketball practice,” says Justin, “my nephew eagerly rushes home, not to rest, but to dive into Fortnite. While he loves the gameplay, it is the connection with his friends he cares most about, especially on school nights when in-person gatherings are off the table.”

This digital arena becomes their meeting ground, a place where conversations flow freely. Children in these spaces can talk about the day’s stresses, budding relationships, homework dilemmas, upcoming birthday plans and more. But their interaction does not stop at conversation.

In this virtual space, children can express themselves through the artful selection of ‘skins’ for their avatars. In this way, they craft digital personas that reflect their individuality and sense of style.

“The metaverse, for my nephew and his friends, transcends being merely a game,” Justin adds. “It’s a social hub, a dynamic space where the lines between gaming, socialising and self-expression blur into a cohesive, immersive experience.”

Concerts in the metaverse

A popular type of virtual event in the metaverse is concerts. Instead of watching a livestream on a screen, your child can join the digital crowd and dance along to their favourite artists. Platforms like Roblox and

Fortnite have hosted concerts by stars like Twenty One Pilots, Lil Nas X and Ariana Grande. These virtual events often attract massive audiences.

In 2023, Epic Games also launched Fortnite Festival. The video game shares similarities to Rock Band and Guitar Hero. However, it is accessible via the Fortnite launcher. Additionally, Fortnite Festival features collaborations with celebrities like Lady Gaga and The Weeknd.
Fortnite Festival and virtual concerts can provide music experiences to large crowds. They also often include interactive elements like games and challenges to engage users further. Therefore, kids can experience a concert's energy and excitement from the comfort of home.

Gaming tournaments
Online video games are more than just a place for children to play. According to our Parent Generation Game report, 40% of parents agree that gaming helps children's social development. Additionally, 62% of children view multiplayer games like Fortnite and Roblox as good for their health and wellbeing.
Virtual gaming events offer children new and exciting ways to game and socialise.

Cinema and other virtual events
The metaverse opens the possibilities to other types of virtual events for children across the world. For example, film directors are now experimenting with different types of augmented and virtual reality technologies. The overall goal is to make movie-going experiences more immersive.
"Many movies," says futurist Bernard Marr, "are also shooting behind-the-scenes footage that is available to watch in VR." This can allow users to explore sets and explore the movie-making process.
Cinema screenings with other people, celebrity interviews and virtual conventions can create a more accessible entertainment industry. These types of events are still under development, but it is likely we will see more in the near future.

How virtual events can benefit children.
Virtual events and entertainment in metaverse can offer several benefits for children and young people.

Accessibility
In the metaverse, children can connect with others all over the world. Our research shows that vulnerable children benefit more than non-vulnerable children in the metaverse.
For instance, 42% of vulnerable children cited making friends as a benefit to using the metaverse, compared with 27% of non-vulnerable children. Vulnerable children also say the metaverse helps them have new experiences (40%) and stay in contact with people they know (37%).
The accessibility of the metaverse also means that any child can engage in virtual events and experiences. And while VR headsets can negatively impact some users, the metaverse does not exist solely in virtual reality. For example, both Roblox and Rec Room are metaverse-based games which users can access in the traditional way or through virtual reality headsets.
Virtual events therefore offer both an accessible and customisable experience for all users.

Immersive experiences
Beyond accessibility, a major benefit of virtual events and entertainment in the metaverse lies in the immersive experiences. Unlike traditional forms of entertainment, the metaverse lets children go beyond the screen to become active participants in their entertainment.
Children can experience concerts and film as if they are the stars. These experiences can also encourage and expand children's learning, interacting with history instead of reading about it. This level of immersion deepens understanding and connection, sparking a sense of wonder.

Socialisation
When it comes to gaming, children say they play to 'hang out with friends' (24%) or 'with family' (12%). In the metaverse, around 1 in 3 children and parents say a top benefit of the metaverse is 'staying in contact with people they know'. Additionally, 30% of children cite 'making new friends' as another benefit.
The wide reach of the metaverse also means that children can connect with others like them from all over the world. As such, they can develop their world view and understanding of others. The immersive nature of these interactions might allow children to feel deeper connections.

Potential risks of metaverse events

"Although there are many benefits," says Justin Winters, "the metaverse does come with risks." Like any digital space where children interact with others, there is risk of exposure to harms. Cyberbullying, hate, inappropriate content and scams are all as prevalent in the metaverse as elsewhere.

Virtual events also tend to lend themselves to additional risk. Some might recall stories around zoombombing during Covid-19 lockdowns. This was where uninvited guests would join a Zoom call and sometimes share disturbing or illegal content.

Without safety measures in place, similar issues could happen during other virtual events in the metaverse.

4 tips to support children in the metaverse.

Put safety first.

Communicate about safety.

Platforms like Roblox, Fortnite and Minecraft all have parental controls options to support children's safety. See our step-by-step guides. Before your child engages in metaverse entertainment, it is important to first set them up for safe experiences.

However, parental controls are only a part of online safety. Regular conversations about their experiences online and in the metaverse are even more important. Just like you would ask them about their day at school, make sure you ask them about their virtual experiences.

Regular conversations make it a lot easier for children to tell you when something goes wrong or when they need help.

Create a family agreement.

Set clear boundaries and limits.

With any technology, it is important to set boundaries to limit time spent in the metaverse. Create a family agreement for all devices, or a specific agreement for attending events in the metaverse.

Boundaries might include:

- asking permission/telling you about an event they wish to attend virtually.
- limits against content not suitable for their age or development.
- restrictions for where they can attend events (such as in a living room rather than a bedroom).
- time limits for when or how long they can use consoles or VR headsets (or spend on one particular platform).

Whatever boundaries you set, make sure you involve your child in the choices. Come to a compromise and sign the agreement as a family.

Experience it together.

Explore and participate with your child.

As with any type of technology, the best way to understand it is to explore it. Ask your child to show you around their favourite platform and attend an event together. This should not interfere with their regular time with friends; instead, set a separate time to explore together.

This can help you:

- understand the environments they engage with.
- set boundaries together.
- answer any questions they might have.
- discover educational or creative experiences you can enjoy as a family.

Additionally, our research regularly shows that parent confidence is key to keeping their child safe online.

Choose the right experiences.

Prioritise quality experiences.

Consider the impacts of the concerts and virtual events your child wants to join. Some might not be appropriate for their age or development.

- Research and choose activities that supports your child's interests.
- Find virtual experiences that offer educational or social value.
- Look for experiences with age-appropriate content from reputable developers.
- Encourage children to try a range of different experiences.

For details, please visit - https://www.internetmatters.org/tech-and-kids-digital-futures/virtual-events-entertainment-in-the-metaverse/#virtual-events-metaverse

Internet Matters Facebook

Did you know that we have over 100 #parentalcontrols guides to keep kids safe?

From broadband and mobile controls to consoles, smartphones, streaming services and apps, our step-by-step guides show you how to set up safe.

https://www.internetmatters.org/parental-controls/

#parents #onlinesafety

Any child is at risk of exploitation online, whether that's through County Lines, via scams, through sextortion or in any other form.

This National Child Exploitation Awareness Day, see what you can do to protect children from online sexual harm with advice from NWG Network.

https://www.internetmatters.org/hub/news-blogs/how-to-protect-children-from-online-sexual-harm/

#CEADay24

Have you heard of #Y99?

If your teen was a keen user of the now-shut #Omegle, they may have come across Y99 chat rooms when searching for alternatives.

But there are some concerns you need to know about https://www.internetmatters.org/hub/news-blogs/what-is-y99-chat/

#parents #chatrooms #onlinesafety

Friends Against Scams Facebook

WhatsApp messaging scams are on the rise. Would you recognise one? See an example and read the advice from Police Service of Northern Ireland https://www.psni.police.uk/safety-and-support/keeping-safe/protecting-yourself/scams-and-fraud/whatsapp-family-impersonation #ScamAware	
As the financial year-end nears, the risk of phishing and tax scams increases. Sign up for Early Warning, the National Cyber Security Centre has a free service that provides advanced alerts to keep you one step ahead of cyber security threats. Set up Early Warning with the National Cyber Security Centre now. https://www.ncsc.gov.uk/ #ScamAware	

NCA

National Crime Agency

One In five children found to engage in illegal activity online.

The National Crime Agency is calling on parents and teachers to help young people understand the implications of their behaviour online, raising concerns about the rise in cybercrime.

The ask comes after a recent survey of children aged 10-16 showed that 20% engage in behaviours that violate the Computer Misuse Act, which criminalises unauthorised access to computer systems and data. The figure is higher for those who game, standing at 25%.

The consequences of committing Computer Misuse Act offences are serious. In addition to being arrested and potentially given a criminal record, those caught can have their phone or computer taken away from them, risk expulsion from school, and face limits on their internet use, career opportunities and international travel.

Many offenders participating in low level cybercrime are unaware that their actions are criminal, but can progress to participate in more complex, serious offending after a brief period of time.
Examples of low-level offending include downloading software to get access to someone else's device, trying to access a protected server or buying something using the saved card details on someone else's account. Gamers who make in-game purchases without the permission of the account holder or engage in DDoS-ing are breaking the law, despite often doing so unwittingly.

Parents and teachers of those aged 10-16 are encouraged to help their children understand the severity of these offences and develop their skills in positive ways.
Skills in coding, gaming, cyber security or anything digital related are in high demand, both in the UK and abroad, and those with talent have many lucrative and legal options open to them.

For those looking for guidance, the Agency's dedicated website, Cyber Choices, provides resources on the Computer Misuse Act, as well as information on online training, further education and future careers.

NCA Deputy Director Paul Foster, Head of the National Cyber Crime Unit, said:
"Many young people are getting involved in cybercrime without realising that they are breaking the law.
"Our message to these teenagers is simple – do not play games with your future.
"Whether you engage in this behaviour knowingly or without realising, you are committing an offence – and could face serious consequences for your actions.
"We would encourage any concerned parents and teachers to speak to young people with an interest in tech, help them understand the dangers, and highlight the many rewarding and varied careers available to them.
"Our Cyber Choices team are here to help children, teachers and parents with advice and guidance."

The NCA's campaign tackling the issue will run for the next 3 weeks and includes video content on Snapchat and YouTube that will reach over three million young people.

For more information visit https://www.nationalcrimeagency.gov.uk/news/one-in-five-children-found-to-engage-in-illegal-activity-online

---

Cleveland Police
Cybercrime Team

Cyber Choices is a national programme coordinated by the National Crime Agency and delivered by Cyber Choice teams within Regional organised crime units and local police force cyber teams.

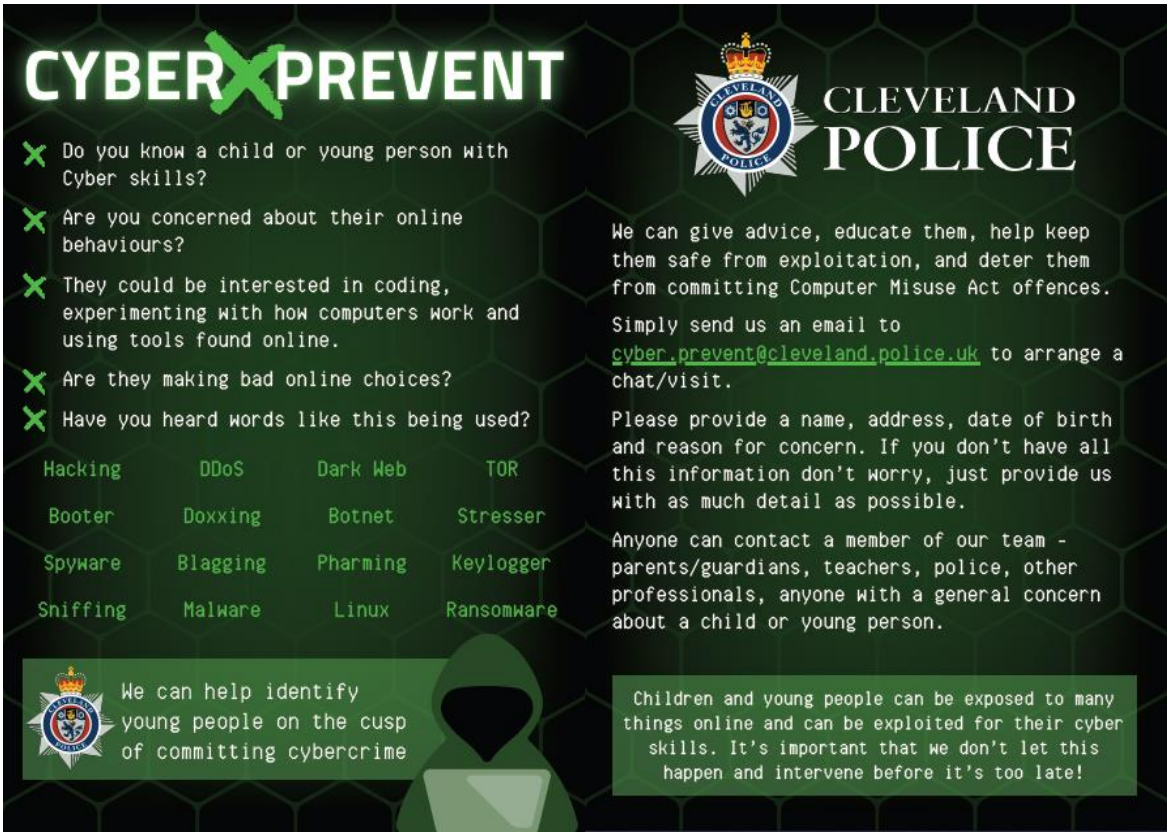
The Cleveland Police cybercrime team are here to help you safeguard children and young people from Cyber dependant crime and to help people make informed choices and to use their cyber skills in a legal way.

What we do

- Educate – Raise awareness of the Computer Misuse Act 1990 and explain the difference between legal and illegal cyber activity, by giving examples of what is and is not an offence.
- Deter and/or divert individuals away from cybercrime – Engaging with those that are on the cusp of committing cybercrime, or those that have committed low level cybercrime and those that are at risk of being exploited for their cyber skills.
- Encourage individuals to make informed choices about their use of technology.
- Promote legal cyber opportunities by providing resources where they can progress their skills in a positive way and to encourage a career in the cyber industry.

If you live or work in the Cleveland area and would like to arrange a free Cyber Choices session/presentation, please contact us at cyber.prevent@cleveland.police.uk

If you are concerned about a young person/child, we are here to help. We can collaborate with them before it gets too late.



TAKE FIVE

National Campaign

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

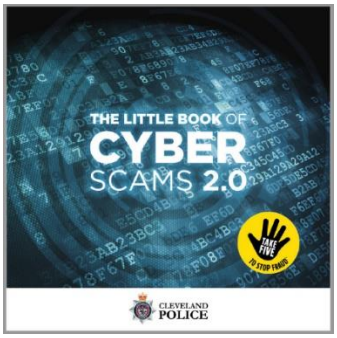
For details, please visit - https://www.takefive-stopfraud.org.uk/

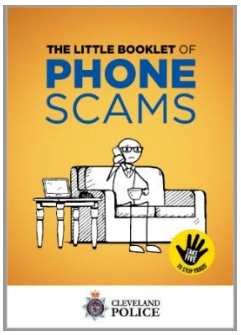
Information in this newsletter has been collated from following online sources.

www.gov.uk
www.actionfraud.police.uk
www.getsafeonline.org
www.ncsc.gov.uk
www.fca.org.uk
www.childnet.com
www.internetmatters.org
www.friendsagainstscams.org.uk
www.nationalcrimeagency.gove.uk
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"