CLEVELAND POLICE

Cyber Crime Newsletter

MARCH 2023

CONTENTS

ACTION FRAUD

Warning issued to WhatsApp users over account takeover scam

Criminals are targeting WhatsApp users by posing as a friend and asking for a security code.
Action Fraud has received over 60 reports relating to a scam that steals access to a WhatsApp user's account.
The scam begins when a criminal gets access to another WhatsApp account which has you listed as a contact.
The criminal, posing as your friend or someone that's a member of a WhatsApp group you're in, will then send you seemingly normal messages to try and start a conversation with you.

However, around the same time you will receive a text message from WhatsApp with a six-digit code. This is because the criminal has been trying to login to WhatsApp using your mobile number.

The criminal will claim that they sent you their code by accident and ask you to help them by sending it to them. Once the criminal has this code, they can login to your WhatsApp account and lock you out.

The criminal will then use the same tactic with your WhatsApp contacts in an effort to steal more accounts and use them to perpetrate fraud.

What you need to do

- Set up two-step verification to give an extra layer of protection to your account: Tap Settings > Account >Two-step verification > Enable.
- THINK. CALL. If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.
- Never share your account's activation code (that's the 6-digit code you receive via SMS)
- You can report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions.

Every report matters.
If you have been a victim of fraud or cybercrime, report it to Action Fraud or **0300 123 2040.**

For more information visit https://www.actionfraud.police.uk and select 'news'

ACTION FRAUD

Spot the signs of Holiday Fraud

Whether you're planning a trip abroad or somewhere closer to home, make sure you do your research when booking online.
As demand for holidays soar, so does the number of scams, and criminals are always finding new ways to catch people out and make them part with their hard-earned cash.

When booking a holiday here or abroad, it's so important to do your research before handing over any money or personal details. Trust your instincts and remember, if a deal looks too good to be true, then it probably is.

Whilst many accommodation providers who make use of online booking platforms are legitimate, some criminals will use these platforms to defraud victims by advertising counterfeit accommodation.

Over 7% of victims reported falling victim to suspects impersonating legitimate travel companies, including clone comparison websites, airline websites and holiday accommodation websites.

In some cases, victims have searched for flight tickets online and have found a website they believe to be the company's genuine website. In other cases, victims reported responding to an approach or advertisement on social media or using what they believed to be legitimate flight comparison websites to search for flights.

In both instances, victims reported being contacted by someone purporting to be from the airline, or flight comparison website, to take them through the booking procedure and take payment.

The fraudster may completely end contact after receiving payment or provide the victim with fake booking information.

Sadly, some victims have only become aware that they have been the victim of fraud when they arrive at the airport and are unable to check-in.

Tops tip to avoid falling victim to holiday fraud

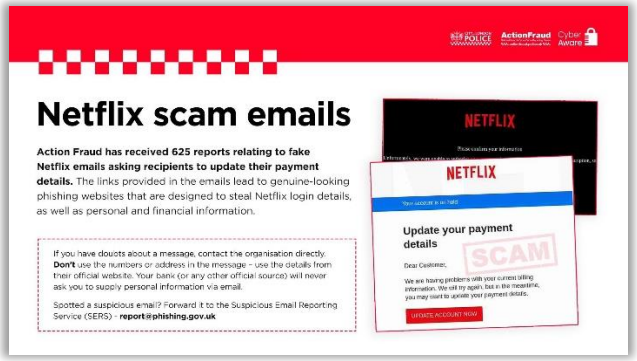
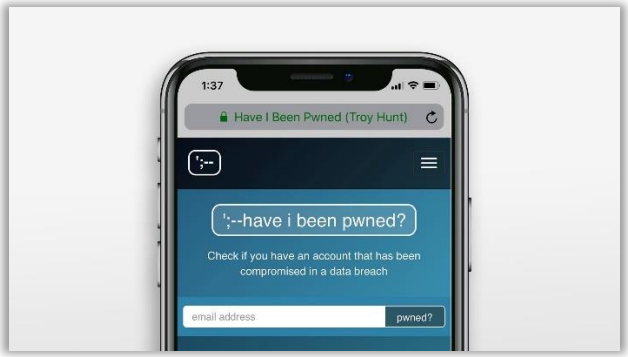
- **Stay safe online:** check the web address is legitimate and has not been altered by slight changes to a domain name – such as going from .co.uk to .org.
- **Do your research:** don't just rely on one review – do a thorough online search to ensure the company is credible. If a company is defrauding people, there is a good chance that consumers will post details of their experience, and warnings about the company.
- **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 CAA website.
- **Pay safe:** wherever possible, pay by credit card. You should avoid paying directly into a private individual's bank account.
- **Check the paperwork:** you should study receipts, invoices and terms and conditions, and be very wary of any companies that don't provide any at all. When booking through a Holiday Club or Timeshare, get the contract thoroughly vetted by a solicitor before signing up.

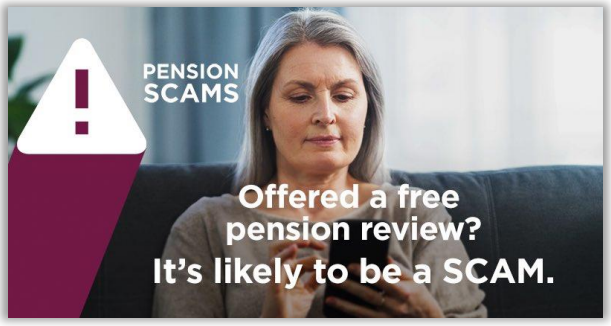
- **Use your instructs:** If a deal sounds too good to be true, it probably is.

For a full list of tips to avoid becoming a victim of fraud, please visit 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	
Watch out for these FAKE Netflix emails asking you to update your payment details. Report suspicious emails by forwarding them to: report@phishing.gov.uk Your reports have led to the removal of 214,000 scam websites as of Feb 2023 #CyberProtect	
Young people are being targeted by fraudsters abroad to use UK bank accounts to transfer criminal funds overseas. This is a crime with serious consequences. Learn more https://nationalcrimeagency.gov.uk/moneymuling #DontBeUsed	
Do you want to find out if one of your online accounts might have been compromised? Here's a quick and simple way to: https://haveibeenpwned.com/	

Releasing funds early, free pension reviews and time pressured offers are all signs of a pension scam. Find out how pension scams work, how to avoid them and what to do if you suspect a scam: https://www.fca.org.uk/consumers/pension-scams	

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
www.getsafeonline.org

GET SAFE ONLINE
Buying & Selling Vehicles Online

For people in the UK, the favourite way to buy and sell vehicles by far is online. This is whether via one of the dedicated vehicle advertising platforms, online marketplaces, social media marketplaces or dealer websites.
There have always been risks associated with buying or selling a pre-owned vehicle online, but right now fraudsters are exploiting situations like the cost-of-living crisis and limited availability of some models to attract their victims. These are in addition to the types of fraud and theft we've been witnessing for many years.

Here's some advice from our experts and partners in VSTAG*, provided to help you buy or sell your vehicle with safety and confidence.

Buying safely
Deposits
If a deposit is requested, don't pay more than you're willing to lose and confirm with the seller that they'll refund it if you don't buy. Requests for up-front transportation fees could spell a scam.

View the vehicle in person
Research the seller as well as their vehicle. Make sure it actually exists and see it in person. Most fraudulent 'sellers' will try to persuade you to transfer money up front, giving one excuse or another. Some also insist on communicating only via email rather than on the phone.

How's the price?
Does the price, condition, spec or mileage of the vehicle seem too good to be true? Research similar vehicles or perform a free valuation on AutoTrader. If the vehicle is below market value, think twice. Ask the seller questions, as there may be genuine underlying reasons if the vehicle is under-priced.

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

Vehicle history
This will tell you if the vehicle is recorded as stolen, written off, scrapped, or has outstanding finance. It's not worth the risk buying a vehicle that could be unroadworthy or worth a fraction of what you're paying for it. Check the service history and ask to see historic MOT certificates to check that the milometer hasn't been adjusted. Check that the VIN numbers on the vehicle and the V5C (logbook) match.

Know your rights
Check your statutory rights regarding quality and refunds before parting with any money.

Making payment
Never send money for a vehicle you haven't seen. Consider paying by credit card (if the seller offers the facility).

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

Paperwork
Have the V5C (logbook), service history and MOT certificate ready for potential buyers to review. They may ask to check details such as the address on the V5C and the mileage in the most recent MOT certificate. Never let anybody photograph or copy your documents in case the request is fraudulent.

Identity check
Always meet the buyer. Ask for their contact details including phone number and full home address, and proof of identity – a driving licence is ideal. A legitimate buyer should be happy to provide these.

Test drives
Ask buyers to bring their driving licence and proof of insurance if they want a test drive. Checking they have the right level of insurance to test drive should prevent you having to pay out for any damage. Always stay with the vehicle and keep hold of the keys. If you have a keyless ignition fob, keep hold of it at all times, even on a test drive. Many thefts take place by thieves who only need to be near the fob and not actually in possession … you can buy a special pouch to prevent this. Never jeopardise your personal safety and walk away if you feel uncomfortable at any time.

Taking payment
Never release the vehicle until you have confirmation of cleared funds. Cheques or banker's drafts can take days to clear. Don't take the buyer's word for it that they've transferred the money even if they show you an app … check with your bank instead.

#VehicleFraud

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

GET SAFE ONLINE
Check a website

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.

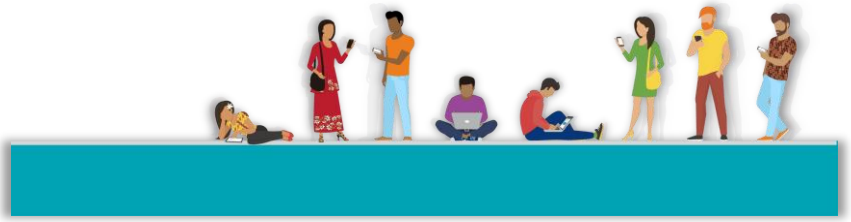
To check a website, visit https://www.getsafeonline.org/checkawebsite/
Simply type or paste the website address and click 'Check this site'.

Please note, this is for website addresses only e.g., www.getsafeonline.org, not for links or shortened links such as bit.ly or goo.gl. Also, it does not check email addresses.

Check a website is an easy-to-use online tool which helps you to determine whether a website is likely to be legitimate or a scam … before you visit it. Simply type in the address of the website you want to check, and your results will appear within seconds.

Provided in the UK by Get Safe Online in conjunction with Cifas, ScamAdviser and our other partners, it cleverly uses an algorithm to provide a trust score based on more than 40 data sources as well as thousands of reports of malicious websites from law enforcement agencies, regulators and consumer brands every week.

The tool was originally devised in 2012 and has been the subject of continuous improvement by the ScamAdviser technical team ever since.



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

GET SAFE ONLINE

Buying Online

It's easier than you might think to get scammed when buying online.

When you're buying online, how confident are you that you're dealing with a genuine seller and not a criminal? Or do you even think about it?

It can be tricky to tell the difference, because in many cases, online purchase fraud is committed NOT by opportunist scammers trying to make some extra money, but by highly skilled, professional organised crime groups with web designers, social media experts, call centres and accountants … just like legit companies.

Many people believe that purchase scams are easy to spot, with poor spelling or grammar, dodgy logos or unusual website or email addresses or phone numbers. However, this is now rarely the case, with scammers going to great lengths to earn your trust before cheating you out of your money. It's upsetting at the best of times, but even worse when money's tight. And because they have no conscience, nobody's immune to their crimes, including you!

Whether you're buying a car or a games console, trainers or a family pet, safeguard yourself and your money by following these top tips.

1. Pay by card – if buying online

If you're buying online, always pay by card. Fraudsters will almost always encourage you to pay by bank transfer as for them, it's money in the bank which you can't get back. Genuine sellers let you pay by card.

2. If you can, see the goods in person

Fraudsters take considerable time and effort to create profiles or sites to make you believe they're a genuine seller. So, to avoid a scam, always see the item in person before paying for it.

3. Look beyond the deal

Its natural to focus on the product and the price but take a moment to think about the advertisement. Does it seem genuine? Does anything not quite 'seem right' Is it easy to contact the seller to ask question?

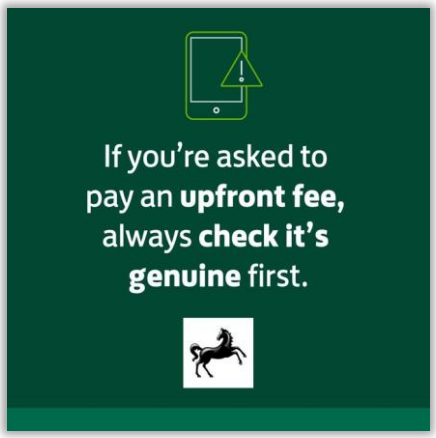
Now, do you think you could avoid an online purchase scam?

Take the Quiz – Visit https://www.getsafeonline.org/onlinebuying/

Get Safe Online Twitter @getsafeonline

Great advice on avoiding loan fee #fraud, from @LloydsBank

You don't have to pay a fee to get a loan. This is a trick fraudster use to steal your money. Call the company to check it's genuine. Use a number you trust, not one they give to you. Learn more about scams like this on Lloyds Bank Fraud Hub: https://www.lloydsbank.com/help-guidance/protecting-yourself-from-fraud.html

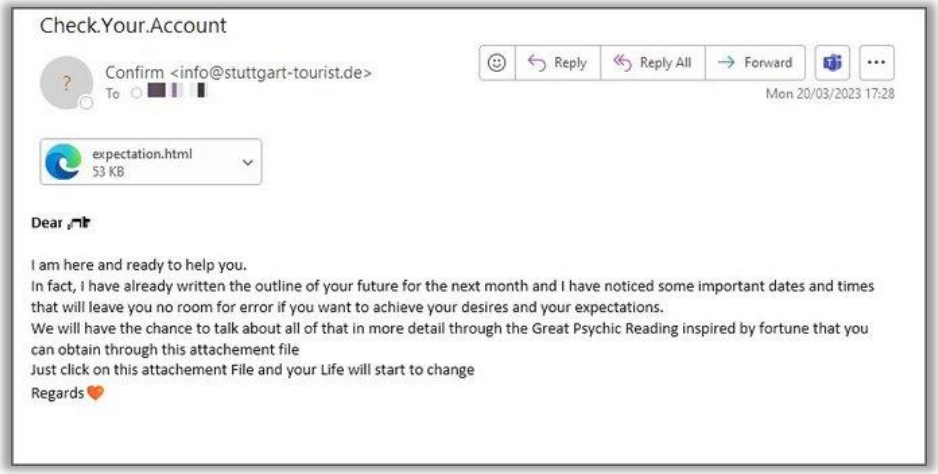


GetSafeOnline.org Retweeted

Fraud Advisory Panel @Fraud_Panel
Discover some simple precautions to help protect your sales here: https://lovebusiness-hatefraud.org.uk/understanding-staff-fraud/

Here is somebody offering your psychic reading, all you need to do is click on the attachment for your life to start to change. That's the only accurate bit ... you'd undoubtedly fall victim to some kind of scam, ID theft or malware attack!

Don't click on anything like this.



National Cyber Security Centre

NCSC – National Cyber Security Centre

NCSC launches flagship new services to help millions of small organisations stay safe online.

New online tools for small organisations to help find and fix any cyber security issues.

- NCSC urges organisations to utilise its Cyber Action Plan and check your Cyber Security services.
- Services unveiled during the NCSC's Cyber Aware campaign to raise awareness among small businesses, microbusinesses and sole traders.
- Small businesses remain a major target for cyber criminals with more than a third suffering a cyber incident according to most recent figures.

CYBER security experts have today (Tuesday) launched two flagship new services designed to help millions of UK small businesses stay secure online and protect their livelihoods.

The National Cyber Security Centre – a part of GCHQ – unveiled the services to coincide with the latest phase of its Cyber Aware campaign, which is aiming to raise awareness of cyber security among the country's small businesses, microbusinesses and organisations and sole traders.

With official statistics showing more than a third of small businesses suffered a cyber-attack last year, the NCSC urged them to make use of its Cyber Action Plan and Check Your Cyber Security tools.

The Cyber Action Plan can be completed online in under 5 minutes and results in tailored advice for businesses on how they can improve their cyber security.

Check your Cyber Security – which is accessible via the Action Plan – can be used by any small organisation including schools and charities and enables non-tech users to identify and fix cyber security issues within their businesses.

Small businesses are a common target for cyber criminals, with the Government's last Cyber Breaches Survey revealing that 38% of the UK's small businesses suffered a cyber incident over a 12-month period.
The range of attacks can vary widely, from business email compromise to denial of service and ransomware attacks.

Lindy Cameron, NCSC CEO said:
"Small businesses are the backbone of the UK, but we know that cyber criminals continue to view them as targets.
"That's why the NCSC has created the Cyber Action Plan and Check Your Cyber Security to help them boost their online defences in a matter of minutes.
"I strongly encourage all small businesses to use these tools today to keep the cyber criminals out and their operations on track."

Martin McTague, National Chair of the Federation of Small Businesses (FSB) said:
"A fifth of small businesses see cybercrime as the most impactful crime in terms of both cost and disruption to their operations.

“We’re glad to see our recommendations to raise small firms’ awareness on cybersecurity has been taken forward in NCSC’s Cyber Aware campaign.
“Equipping small firms with the right tools and tailor-made guidance could enable them to be more cyber resilient and in turn reduce costs in real life.”

The Cyber Action Plan and Check Your Cyber Security are among the services within the NCSC’s Active Cyber Defence programme, which help to protect the UK from millions of cyber-attacks each year.

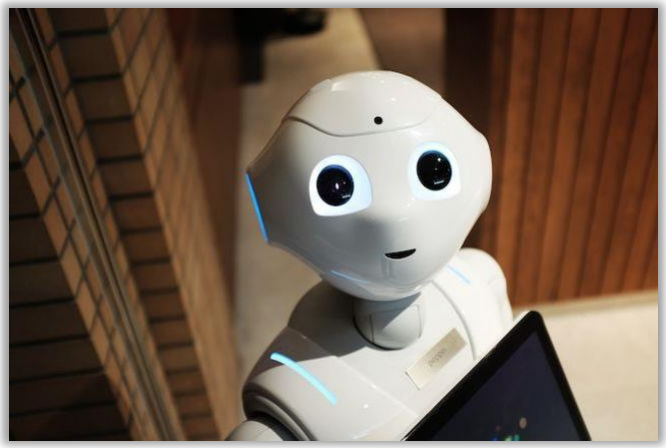
The NCSC continues to offer a wide range of guidance, products and services to small organisations, including its Small Business Guide.

For more information visit https://www.ncsc.gov.uk/news/ncsc-launches-new-services-help-small-organisations-online

---

NCSC – National Cyber Security Centre
BLOG POST

ChatGPT and large language models: what’s the risk?



Do loose prompts* sink ships? Exploring the cyber security issues of ChatGPT and LLMs.
Large language models (LLMs) and AI chatbots have captured the world's interest, ignited by the release of ChatGPT in late 2022 and the ease of querying it provides. It's now one of the fastest growing consumer applications ever, and its popularity is leading many competitors to develop their own services and models, or to rapidly deploy those that they’ve been developing internally.

As with any emerging technology, there's always concern around what this means for security. This blog considers some cyber security aspects of ChatGPT and LLMs more generally in the near term.

What is ChatGPT and what are LLMs?
ChatGPT is an artificial intelligence chatbot developed by OpenAI, a US tech startup. It's based on GPT-3, a language model released in 2020 that uses deep learning to produce human-like text, but the underlying LLM technology has been around much longer.

An LLM is where an algorithm has been trained on a large amount of text-based data, typically scraped from the open internet, and so covers web pages and - depending on the LLM - other sources such as scientific research, books or social media posts. This covers such a large volume of data that it’s not possible to filter all offensive or inaccurate content at ingest, and so 'controversial' content is likely to be included in its model.

The algorithms analyse the relationships between different words and turn that into a probability model. It is then possible to give the algorithm a 'prompt' (for example, by asking it a question), and it will provide an answer based on the relationships of the words in its model.

Typically, the data in its model is static after it has been trained, although it can be refined by 'fine-tuning' (which is training on additional data) and 'prompt augmentation' (which is providing context information about the question). An example of prompt augmentation might be:

Taking into account the below information, how would you describe...
and then copying potentially large amounts of text (or whole documents) into the prompt/question.

ChatGPT effectively allows users to ask an LLM questions, as you would when holding a conversation with a chatbot. Other recent examples of LLMs include the announcement of Google's Bard and Meta's LLaMa (for scientific papers).

LLMs are undoubtedly impressive for their ability to generate a huge range of convincing content in multiple human and computer languages. However, they're not magic, they're not artificial general intelligence, and contain some serious flaws, including:

- they can get things wrong and 'hallucinate' incorrect facts
- they can be biased, are often gullible (in responding to leading questions, for example)
- they require huge computer resources and vast data to train from scratch
- they can be coaxed into creating toxic content and are prone to 'injection attacks'

Will LLMs reveal my information?
A common concern is that an LLM might 'learn' from your prompts, and offer that information to others who query for related things. There is some cause for concern here, but not for the reason many consider. Currently, LLMs are trained, and then the resulting model is queried. An LLM does **not** (as of writing) automatically add information from queries to its model for others to query. That is, including information in a query will not result in that data being incorporated into the LLM.

However, the query **will** be visible to the organisation providing the LLM (so in the case of ChatGPT, to OpenAI). Those queries are stored and will almost certainly be used for developing the LLM service or model at some point. This could mean that the LLM provider (or its partners/contractors) are able to read queries, and may incorporate them in some way into future versions. As such, the **terms of use** and **privacy policy** need to be thoroughly understood before asking sensitive questions.

A question might be sensitive because of data included in the query, or because who is asking the question (and when). Examples of the latter might be if a CEO is discovered to have asked 'how best to lay off an employee?', or somebody asking revealing health or relationship questions. Also bear in mind aggregation of information across multiple queries using the same login.

Another risk, which increases as more organisations produce LLMs, is that queries stored online may be hacked, leaked, or more likely accidentally made publicly accessible. This could include potentially user-identifiable information. A further risk is that the operator of the LLM is later acquired by an organisation with a different approach to privacy than was true when data was entered by users.

As such, the NCSC recommends:
- not to include sensitive information in queries to public LLMs
- not to submit queries to public LLMs that would lead to issues were they made public.

How can I safely provide LLMs with sensitive information?
In the wake of the excitement around LLMs, many organisations may be wondering if they can use LLMs to automate certain business tasks, which may involve providing sensitive information either through fine-tuning or prompt augmentation. Whilst this approach is **not** recommended for public LLMs, 'private LLMs' might be offered by a **cloud provider** (for example), or can be entirely **self-hosted**:

- For **cloud provided LLMs**, the terms of use and privacy policy again become key (as they are for public LLMs), but are more likely to fit within the existing terms for the cloud service. Organisations need to understand how the data they use for fine-tuning or prompt augmentation is managed. Is it available to the vendor's researchers or partners? If so, in what form? Is data shared in isolation or

in aggregation with other organisations? Under what conditions can an employee at the provider view queries?
- **Self-hosted LLMs** are likely to be highly expensive. However, following a security assessment (which should include referring to the NCSC's principles for the security of machine learning), they may be appropriate for handling organisational data. In particular, organisations should refer to our guidance on securing your infrastructure and data supply chains.

Do LLMs make life easier for cyber criminals?

There have been some incredible demonstrations of how LLMs can help write malware. The concern is that an LLM might help someone with malicious intent (but insufficient skills) to create tools they would not otherwise be able to deploy. In their current state, LLMs suffer from *appearing* convincing (whether or not they are) and are suited to simple tasks rather than complex ones. This means LLMs are useful for 'helping experts save time', as the expert can validate the LLM's output.

For more complex tasks, it's currently easier for an expert to create the malware from scratch, rather than having to spend time correcting what the LLM has produced. However, an expert capable of creating highly capable malware is likely to be able to coax an LLM into writing capable malware. This trade-off between *'using LLMs to create malware from scratch'* and *'validating malware created by LLMs'* will change as LLMs improve.

LLMs can also be queried to advise on technical problems. There is a risk that criminals might use LLMs to help with cyber attacks beyond their current capabilities, in particular once an attacker has accessed a network. For example, if an attacker is struggling to escalate privileges or find data, they might ask an LLM, and receive an answer that's not unlike a search engine result, but with more context. Current LLMs provide *convincing-sounding* answers that may only be partially correct, particularly as the topic gets more niche. These answers might help criminals with attacks they couldn't otherwise execute, or they might suggest actions that hasten the detection of the criminal. Either way, the attacker's queries will likely be stored and retained by LLM operators.

As LLMs excel at replicating writing styles on demand, there is a risk of criminals using LLMs to write convincing phishing emails, including emails in multiple languages. This may aid attackers with high technical capabilities but who lack linguistic skills, by helping them to create convincing phishing emails (or conduct social engineering) in the native language of their targets.

To summarise, in the near term we might see:
- more convincing phishing emails as a result of LLMs
- attackers trying techniques they didn't have familiarity with previously.

There is also a low risk of a lesser-skilled attacker writing highly capable malware.

To wrap up

It's an exciting time for LLMs, and ChatGPT in particular has gripped the world's imagination. As with all technology developments, there will be people keen to use it and to investigate what it has to offer, and those who may never use it.

There are undoubtedly risks involved in the unfettered use of public LLMs, as we've outlined above. Individuals and organisations should take great care with the data they choose to submit in prompts. You should ensure that those who want to experiment with LLMs are able to, but in a way that doesn't place organisational data at risk.

The NCSC is aware of other emerging threats (and opportunities) in relation to cyber security and adoption of LLMs, and we will of course keep you informed of these in future blogposts.
David C - Tech Director for Platforms Research
Paul J - Tech Director for Data Science Research

For details, please visit https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk

---

Threat Reports

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

Threat Report 24th March 2023

Mandiant report that UNC3886 actor is targeting firewalls, IOT devices and VPNs.

The cyber security company Mandiant has published a blog detailing ongoing campaigns by a Chinese espionage threat actor it calls UNC3886. The actor takes advantage of technologies that don't support endpoint detection response, such as firewalls, IoT devices, hypervisors and VPN technologies.

The actor has exploited zero-day vulnerabilities and then deployed custom malware as an attack vector before traversing the target environment and gaining persistence.

The report that concludes that communication and collaboration across organisations is essential for both vendors and investigators to help mitigate the activity.

CISA establishes Ransomware Vulnerability Warning Pilot programme.

The Cybersecurity and Infrastructure Security Agency (CISA) has launched the Ransomware Vulnerability Warning Pilot (RVWP), which will alert critical infrastructure providers in the US of potential internet-accessible vulnerabilities linked to known threat actors and ransomware attacks.

CISA has reported they initiated the RVWP by alerting 93 organisations to the 'ProxyNotShell' vulnerability in certain instances of organisations using Microsoft Exchange.

The NCSC provides a range of advice, guidance and content aimed specifically at those with an interest in UK Critical National Infrastructure as part of the CNI Hub.

DNS data shows one in ten organisations have malware traffic on their networks.

An investigation by Akamai has shown that between 10% and 16% of organisations had Domain Name System (DNS) traffic originating on their network towards command-and-control (C2) servers associated with known botnets and various other malware threats.

The report also showed that over 9% of devices that generated C2 traffic, did so to domain names associated with known ransomware threats. Of these, REvil and LockBit were the most common ones.

The NCSC has produced guidance on the selection and deployment of protective DNS and there is also the Protective DNS for public sector organisations.

TrendMicro on the return of Emotet

A report by TrendMicro shows that Emotet activity resumed in March, using a botnet to deliver malicious documents via Zip file attachments to emails.

The documents use social engineering tactics to encourage the user to enable macros as Microsoft disabled macros by default in 2022. The botnet also uses binary padding to artificially inflate the file size in order to avoid triggering some security solutions.

The NCSC has guidance on implementing email security solutions and how to mitigate against malware attacks.

Threat Report 10th March 2023

New tool released to help with MITRE ATT&CK mapping.
CISA, along with key partners including MITRE, have released a free tool named Decider to help map threat actor behaviour to the MITRE ATT&CK framework.

The MITRE ATT&CK® framework is a global knowledge base of actor tactics, techniques and procedures that can be used to map activity. The NCSC uses MITRE ATT&CK references in its advisories.

Decider uses guided questions to help make mapping easier, and includes a search and filter function, as well as the capability to easily export results.

It comes with accompanying resources to help users to get started with Decider.

Tips to avoid Microsoft OneNote attachment spreading malware on your network
Bleeping Computer highlights threat actors' recent use of Microsoft OneNote file attachments to spread malware on Windows and offers advice on how to mitigate this on networks.

The use of OneNote files to spread malware follows Microsoft's decision to disable macros in Word and Excel documents in 2022 because of their widespread misuse. Rather than distributing via macros or vulnerabilities, in OneNote create templates appearing as protected documents, with an instruction message to double-click.

The article recommends blocking OneNote attachments by blocking .one file extensions at secure mail gateways or servers, but also provides other advice for when this isn't possible.

CISA ransomware advisory on the Royal variant
CISA and FBI in the US have published a new advisory on the ransomware variant known as Royal.

As the advisory reports, Royal is known to have impacted organisations in the US and internationally in critical national infrastructure (CNI) sectors.

It provides indicators of compromise and TTPs for detection of activity.
The NCSC also has guidance on mitigating malware and ransomware.

Cyber criminals use Eurovision as the latest phishing lure.
Cyber criminals are targeting hotels hosting people travelling to Liverpool for the Eurovision song contest event in May. The online travel agent booking.com has confirmed to the BBC they have seen evidence of "some accommodation partners being targeted by phishing emails."

Cyber criminals often take advantage of news and topical events to scam customers. There are some good ways you can prepare yourself and spot potential scams on the NCSC website, as well as guidance on what to do next if you are a victim of phishing.

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

NCSC Twitter @NCSC	
The new Emergency Alerts system will be tested on April 23. The system will warn people when their lives are in danger. An Emergency Alert is a loud, siren-like sound with a message on your mobile phone screen. To find out more, visit https://www.gov.uk/alerts	
NCSC Retweeted **Competition & Markets Authority** @CMAgov.uk This year, our online #RipOffTipOff campaign is urging shoppers like you, to call out and #report sneaky online sales tactics using our brand-new digital reporting form. Read more: https://www.gov.uk/government/news/shoppers-urged-to-call-out-online-rip-offs-as-cma-unveils-red-lines #OnlineShopping	

Childnet

TikTok to introduce 60-minute time limit for teens.

3 March 2023

Within a few weeks, all accounts belonging to a user under the age of 18 will automatically be set a daily 60-minute screen time notification.
They will be notified of this in the app and be required to type in their password to make an active choice to continue using TikTok. Users will however be able to disable this limit if they want to, unless Family Pairing settings have been put in place to stop this happening.

What is TikTok?
TikTok is one of the most popular social media apps among young people – we're always hearing about it in the schools we visit.

It is a social media platform where users can create videos, sharing these either publicly or privately. On TikTok you can like, comment, store and share content that appears on your homepage or discover page.

There is an in-app chat function and a "Live" feed where you can scroll through and comment on live content.
Head to the UK Safer Internet Centre to find out more information about TikTok and its online safety features.

What is TikTok's new online safety update for young people?
Last year, TikTok reinforced its digital wellbeing page to include screen time summaries and breaks.

They also started notifying users aged 13-17 when they spent 100 minutes on the app and invited them to consider switching off once this limit had been reached.

Yesterday, TikTok announced that they would be **changing this limit to 60 minutes**, so that young people will be notified of their consumption of the app 40% sooner.

The setting is designed to allow young users to have more control of how much time they spend on the app.

It will build awareness around screen time management: TikTok say they will also be prompting young users to set a limit for themselves if they decide to opt out of the 60-minute limit but still spend more than 100 minutes using the app in a day.

In addition, all users under the age of 18 will be sent a message to their inbox weekly, detailing a roundup of their screen time.

"This builds on a prompt we rolled out last year to encourage teens to enable screen time management; our tests found this approach helped increase the use of our screen time tools by 234%."
TikTok newsroom

Recognising the signs
We know that a common concern of parents and carers is that they wonder whether their child may be spending too much time in front of their screens.
If you are worried about the amount of time your child spends on their devices there's lots, you can do to help.
Have conversations and help your child to recognise how going online makes them feel and the importance of taking a break when they need to.

There are particular signs which can help your child to recognize if they have been spending too much time on their devices.
Some signs you may see include (but are not limited to):

- being distracted and struggling to focus
- feeling tired or sleepy
- feeling unusually emotional or upset

If your child uses TikTok, this new update could be a great starting point in having an open and honest conversation.

Another useful tip is to help remind them of the things they love to do offline; this will encourage a healthy mix of online and offline activities.
For further advice around screen time and healthy balance for your family, you can head to our Help and Advice page.

What is TikTok's new online safety update for families?

Last year, we wrote about how TikTok's Family Pairing was launched to help parents and carers support their child in browsing TikTok in a safer way .

Should you enable Family Pairing, your account will be linked to your child's and will provide more information about their time spent in the app.

TikTok have now updated the Family Pairing so that parents and carers can set a time limit which their child will not be able to override. Parents and carers can also use Family Pairing to disable notifications for their child.

If you are considering making a change to parental controls that will affect their privacy, try to explain your decision making and feelings to your child calmly so that they are more likely to listen and understand.

For details, please visit - https://www.childnet.com/blog/tiktok-to-introduce-60-minute-time-limit-for-teens-and-further-parental-controls/

TAKE FIVE

Take Five National Campaign

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

Fraud poses a major threat to the UK. It's a crime that the finance industry is committed to tackling, but it's also one that requires the combined efforts of every sector, both public and private, to overcome.

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

---

TAKE FIVE

NEWS

EYES DOWN – Remember to Take Five!
Fraud risk to over 65's is revealed as Scam Bingo game launches

Take Five to Stop Fraud campaign launches Scam Bingo game to help raise awareness as new research highlights the risk of fraud to over-65s

Key findings:

- The average loss for a fraud victim in the UK is £1,381.
- 20 per cent of over-65s have heard of all of the most prevalent types of authorised push payment (APP) fraud.
- 37 per cent of over 65s believe they have been approached with a purchase scam, and 25 per cent believe they have been approached with an investment fraud.

Research conducted for UK Finance's Take Five to Stop Fraud campaign shows that 87 per cent of over-65s say they are confident about spotting the signs of fraud, although only 20 per cent have heard of all the five most prevalent types of authorised push payment (APP) fraud. The survey showed that the average loss for a fraud victim in the UK is £1,381.

In response to this threat, Take Five has developed a free to play Scam Bingo game to help people learn about the most common types of fraud and scams. The game is available on the Take Five website and as part of the campaign, we have teamed up with Age UK to run bingo events at several local Age UKs across the country.

The new research shows that over half of over-65s (54 per cent) say that they always check whether a request for money or personal information is legitimate before responding to the request. However, criminals continue to target this age group.

For example, 37 per cent of over-65s believe they have been approached with a purchase scam, when a criminal convinces someone to buy goods or services that don't exist. Similarly, 25 per cent believe they have been approached with an investment scam and 32 per cent with an advanced fee scam, when a criminal convinces a person to pay an upfront fee in order to receive a prize, service, high-value goods or a loan which never materialises.

Over a third (35 per cent) of over-65s think they are most likely to be approached by a criminal via an email, and over a fifth (23 per cent) say it is most likely to be via a phone call.
In contrast, just seven per cent say it is most likely a fraudster would contact them via a text message despite this being a common way for fraudsters to get in touch with potential victims.

Katy Worobec, Managing Director of Economic Crime at UK Finance said:
"While our research shows over-65s say they are confident about spotting fraud and scams, it is crucial to understand the changing tactics criminals use to convince people they are legitimate.
"That is why we've created Scam Bingo to empower people to challenge all unexpected requests for their information – it's a fun way to connect and learn how to protect ourselves from fraud and scams. It is important to remember the advice of the Take Five to Stop Fraud campaign and to stop and think when faced with requests for payment or personal and financial information."

Sally Dervan, CEO of Age UK Manchester said:
"The Scams Prevention work that Age UK Manchester has been involved in over recent months has given us the opportunity to raise awareness of scams with older people and their carers across the city. Being the

victim of a scam not only causes people to lose out financially, falling victim to a scam can have a long lasting effect on an individual's confidence and wellbeing. The Scam Bingo event is a great opportunity to deliver information in a friendly and entertaining way that will give older people knowledge of current scams, and enable them to better protect themselves against this growing area of risk."

Sue Holderness (73), best known for her role as Marlene Boyce in Only Fools and Horses, knows only too well how convincing criminal scammers can be. Sue lost money when criminals hijacked her computer and pretended to be tech people who were helping her regain access. Sue who is supporting the Take Five campaign says:
"Criminals are so sophisticated with the tricks they use to panic you into sharing personal details, which under normal circumstances you never would disclose to a stranger! Your bank or any other legitimate organisation won't try to rush you into making decisions, so if you're feeling pressured by someone, taking a moment to stop and think before parting with your money or information could keep you safe. Don't feel embarrassed if you think you might have fallen for a scam, fraudsters can be incredibly convincing, but do protect yourself by contacting your bank immediately and reporting it to Action Fraud."

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money. To help people stay safe, the Take Five to Stop Fraud campaign advice is to:

- **STOP**: Taking a moment to stop and think before parting with your money or information could keep you safe.
- **CHALLENGE**: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **PROTECT**: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

The five most common types of APP scam are:

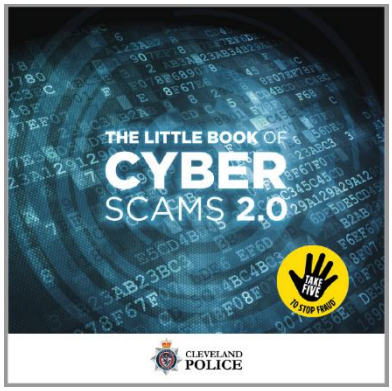
- **Purchase scam** – a type of fraud in which a criminal convinces you to buy a product/service that does not exist.
- **Investment scam**– a type of fraud in which a criminal convinces you to invest money in a fake or fictitious investment opportunity.
- **Romance scam** – a type of fraud in which a criminal creates a fake online identity to gain the trust and affection of someone, usually through a dating website or social media platform, with the goal of tricking them out of money.
- **Advance Fee scam**– a type of fraud in which a criminal convinces you to pay an upfront fee in order to receive a prize, service, high-value goods or loan which never materialises.
- **Impersonation scam** – a type of fraud in which a criminal impersonates a person, organisation or the police in order to trick you into handing over money or personal information.

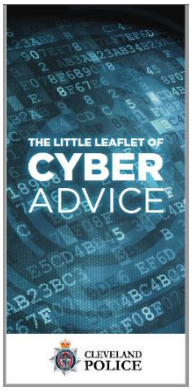
For further details visit https://www.takefive-stopfraud.org.uk/

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.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"